Summer-15

1. Define 'packet' in concern with computer communication. (Definition – 2 Marks)

Answer:

Packet: A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network.

2. What is PPP? Describe in brief. (Meaning- 1Mark, Description- 1 Mark)

Answer:

PPP:

- PPP is Point-to-Point Protocol.
- It is a data link protocol commonly used in establishing a direct communication between two networking nodes.
- It can also provide authentication, transmission encryption & compression.

3. Describe connection oriented and connectionless services.
(Connection oriented services 2 marks and connectionless services 2 marks).

Answer:

Connection-oriented:

- communication includes the steps of setting up a call from one computer to another, transmitting/receiving data, and then releasing the call, just like a voice phone call.
- However, the network connecting the computers is a packet switched network, unlike the phone system's circuit switched network.
- Connection-oriented communication is done in one of two ways over a packet switched network: with and without virtual circuits.
- Connection oriented service is more reliable than connectionless service.
- We can send the message in connection oriented service if there is an error at the receivers end.
- Example of connection oriented is **TCP (Transmission Control Protocol)** protocol.

Connectionless:

- Communication is just packet switching where no call establishment and release occur.
- A message is broken into packets, and each packet is transferred separately.
- Moreover, the packets can travel different route to the destination since there is no connection.
- Connectionless service is typically provided by the **UDP (User Datagram Protocol).**
- The packets transferred using UDP are also called **datagrams**.

Difference between connection oriented and connectionless services:

1. In connection oriented service **authentication** is needed while connectionless service does not need any authentication.
2. Connection oriented protocol makes a connection and checks (confirms delivery of message) whether message is received or not and sends again if an error occurs connectionless service protocol does not guarantees a delivery.
3. Connection oriented service is more **reliable** than connectionless service.
4. Connection oriented service interface is **stream based** and connectionless is **message based.**

4. Compare UDP and TCP (four points) (Any 4 points, 1 mark each)
Answer:

TCP	**UDP**
1. TCP is connection oriented protocol	1. UDP is connection less protocol
2. It provides reliable delivery of messages	2. It provides unreliable delivery of messages
3. It assigns datagram size dynamically for efficiency.	3. Every datagram segment is of the same size.
4. TCP has flow control	4. UDP has no flow control
5. Overhead is low	5. Overhead is very low.
6. Transmission speed is high	6. Transmission speed is very high

5. Describe different IP address classes. (Any 4 classes with explanation 1 mark each)

Answer:

The Internet community originally defined five *address classes* to accommodate networks of varying sizes. Microsoft TCP/IP supports class A, B, and C addresses assigned to hosts. The class of address defines which bits are used for the network ID and which bits are used for the host ID. It also defines the possible number of networks and the number of hosts per network.

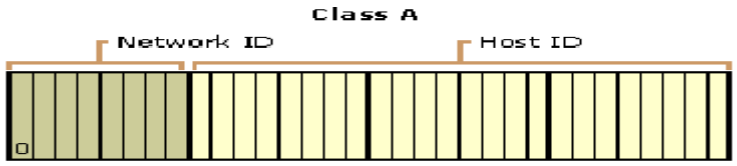
Class	Range for first byte
A	0-127
B	128-191
C	192-223
D	224-239
E	240-255

1) Class A:

- *Class A* addresses are assigned to networks with a very large number of hosts.
- The high order bit in a class A address is always set to zero.

- The next seven bits complete the network ID. The remaining 24 bits (the last three octets) represent the host ID.
- This allows for 126 networks and 16,777,214 hosts per network.

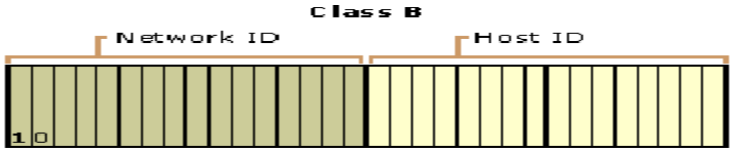
Figure illustrates the structure of class A addresses.



2) Class B:

- *Class B* addresses are assigned to medium-sized to large-sized networks.
- The two high order bits in a class B address are always set to binary 1 0.
- The next 14 bits complete the network ID. The remaining 16 bits represent the host ID.
- This allows for 16,384 networks and 65,534 hosts per network.

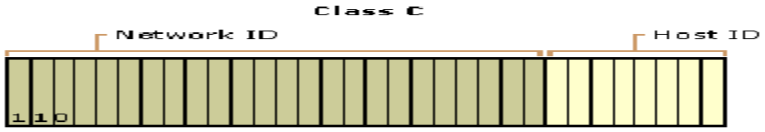
Figure illustrates the structure of class B addresses.



3) Class C

- *Class C* addresses are used for small networks.
- The three high-order bits in a class C address are always set to binary 1 1 0.
- The next 21 bits complete the network ID.
- The remaining 8 bits (last octet) represent the host ID. This allows for 2,097,152 networks and 254 hosts per network.

Figure illustrates the structure of class C addresses.



4) Class D

- *Class D* addresses are reserved for IP multicast addresses.
- The four high-order bits in a class D address are always set to binary 1 1 1 0.
- The remaining bits are for the address that interested hosts recognize.
- Microsoft supports class D addresses for applications to multicast data to multicast-capable hosts on an internetwork.

5) Class E

Class E is an experimental address that is reserved for future use. The high-order bits in a class E address are set to 1111.

6. **Compare IPv4 and IPv6.**

IPv4	**IPv6**
1. Source and destination addresses are 32 bits (4 bytes) in length.	1. Source and destination addresses are 128 bits(16 bytes)in length.
2. Uses broadcast addresses to send traffic to all nodes on a subnet.	2. There are no IPv6 broadcast addresses. Instead, multicast scoped addresses are used.
3. Fragmentation is supported at Originating hosts and intermediate routers.	3. Fragmentation is not supported at routers. It is only supported at the
4.IP header include a checksum.	4. IP header does not include a checksum.
5.IPheader includes options.	5. All optional data is moved toIPv6 extension headers.
6.IPsec support is optional	6.IPsec support is required in a full IPv6 implementation.
7. No identification of payload for QoS Handling by routers is present within the IPv4 header.	7. Payload identification for QoS handling By routers is included in theIPv6 header using the Flow Label field.
8. Address must be configured either manually or through DHCP.	8. Addresses can be automatically assigned using stateless address auto configuration, assigned using DHCPv6, or manually configured.
9. *IP* address represented in decimal number system	*9. IP* address is represented in hexadecimal number system
10. "*.*" used as seperator	10. '*:* ' used as separator .
11. Uses host address (A) resource records in the domain name system to map host names to IPv4 addresses.	11. Uses host address (AAAA) resource records in the domain name system to map host names to IPv6 addresses.

7. **List any four IP functions. (Each function 1 mark)**

Answer:

1. **Addressing:** In order to perform the job of delivering datagrams, IP must know where to deliver them to. For this reason, IP includes a mechanism for host addressing. Furthermore, since IP operates over internetworks, its system is designed to allow unique addressing of devices across arbitrarily large networks. It also contains a structure to facilitate the routing of datagrams to distant networks if that is required.

2. **Data Encapsulation and Formatting/Packaging:** IP accepts data from the transport layer protocols UDP and TCP. It then encapsulates this data into an IP datagram using a special format prior to transmission.

3. **Fragmentation and Reassembly:** IP datagrams are passed down to the data link layer for transmission on the local network. However, the maximum frame size of each physical/data-link network using IP may be different. For this reason, IP includes the ability to *fragment* IP datagrams into pieces so they can each be carried on the local network. The receiving device uses the reassembly function to recreate the whole IP datagram again.

4. **Routing / Indirect Delivery:** When an IP datagram must be sent to a destination on the same local network, this can be done easily using the network's underlying LAN/WLAN/WAN protocol using what is sometimes called *direct delivery*. However, in many (if not most cases) the final destination is on a distant network not directly attached to the source. In this situation the datagram must be delivered *indirectly*. This is accomplished by routing the datagram through intermediate devices.

8. Differentiate SLIP and PPP.(any four points) (Any 4 each 1Mark)
Answer:

SLIP	**PPP**
Serial Line Internet Protocol does not establish or maintain connection between the client and ISP server.	In PPP, LCP (Line Control Protocol) is responsible for establishing, maintaining and termination connection between two end points.
Communication starts once the connection between two modems are established.	Communication begins only after authentication and the types of traffic is sent by the client.
Type of traffic cannot be selected in SLIP.	Type of traffic can be selected by NCP(Network Control Protocol)
No protocol for termination.	IPCP(IP Control Protocol) terminates a network layer connection between the user and ISP.
No addressing mechanism provided.	Additional services for addressing mechanism is provided
Doesn't allow error control	Allows error control
No provision for data compression	Provides Data compression.

9. **Site addresses 201.70.64.0. The company needs six subnets. Design subnets. Write addresses of all subnets.** (Identify the class and bits : 1M; Each subnet address : ½ M.)

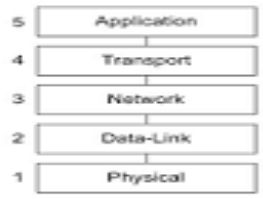
Answer:

Site Address: 201.70.64.0
No. of Subnets : 6
Class : Class C
Default subnet mask : 255.255.255.0

To design 6 subnets :
No. of bits used in the host id:
2n -2 ≥ 6 ; where n = number of bits
If n= 3;
23 – 2 ≥ 6.
Therefore**, n= 3.**
Given IP: 201.70.64.0
Network ID : 201.70.64
Subnet 1:
The bit combination is **001**.
Taking last octet in binary :**0 0 1** 0 0 0 0 0 = 32 (10)
Hence the subnet address is, 201.70.64. **32**
Subnet 2:
The bit combination is **01 0**.
Taking last octet in binary :**0 0 1** 0 0 0 0 0 = 64(10)
Hence the subnet address is, 201.70.64. **64**
Subnet 3:
The bit combination is **011**.
Taking last octet in binary :**0 1 1** 0 0 0 0 0 = 96(10)
Hence the subnet address is, 201.70.64. **96**
Subnet 4:
The bit combination is **100**.
Taking last octet in binary :**1 0 0** 0 0 0 0 0 = 128(10)
Hence the subnet address is, 201.70.64. **128**
Subnet 5:
The bit combination is **101**.
Taking last octet in binary :**1 0 1** 0 0 0 0 0 = 160(10)
Hence the subnet address is, 201.70.64. **160**
Subnet 6:
The bit combination is **110**.
Taking last octet in binary :**1 1 0** 0 0 0 0 0 = 192 (10)
Hence the subnet address is, 201.70.64. **192**

10. **Describe TCP/IP model with suitable diagram. Describe the function of each layer. (Diagram 2M; Explanation 6M)**

Answer:



TCP/IP Model

1. **Application Layer:**
   - The application layer is concerned with providing network services to applications.
   - There are many application network processes and protocols that work at this layer, including Hyper Text Transfer Protocol (HTTP), Simple Mail Transport Protocol (SMTP) and File Transfer Protocol (FTP).
2. **Transport Layer**
   - This layer is concerned with the transmission of the data. The two main protocols that operate at this layer are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
   - TCP is regarded as being the reliable transmission protocol and it guarantees that the proper data transfer will take place. UDP is not as complex as TCP and as such is not designed to be reliable or guarantee data delivery.
3. **Network Layer or Internet layer:**
   - This layer is concerned with the format of datagrams as defined in the internet protocol (IP) and also about the mechanism of forwarding datagrams from the source computer to the final destination via one or more routers.
   - The other protocol in this layer include Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP) and Internet Control Message Protocol (ICMP).
4. **Data Link layer**:
   - This is similar to the other network models which deal with Media Access and Control (MAC) and also with the frame formats.
5. **Physical Layer*:***
   This deals with hardware level, connections as in other network model.
   [Note: TCP/IP four or Five layer May be considered]

Winter-14

1. **Define protocol. Give the name of any two protocols.**
   (Definition -1 mark, any two examples- 1 mark)

Answer: Define protocol: There are certain rules that must be followed to ensure proper communication & a set of such rules is known as protocol. Example: UDP, TCP/IP, SMTP, HTTP, SSL, FTP etc.

2. **List different classes of IP Address.**
   (½ mark for each class, Any four classes)

Answer: Different classes of IP address. Class A , Class B, Class C, Class D, Class E

3. Explain the services provided by transport layer in TCP/IP model. (Any four functions 1 mark each)

Answer: Responsibility of process to process delivery of message Ensure that whole message arrives in order.

1. Service point addressing: -several programs run at a time on computer. Delivery is not only from one computer to another but also from specific process on computer to specific process on another computer. For this transport layer uses port addresses. Transport layer delivers entire message to the correct process on the computer.
2. Segmentation and reassemble: -Each segment of a message contains a sequence number which is used to reassemble the message correctly upon arriving at destination and to identify and replace packets that are lost in transmission.
3. Connection control:-Logical connection is created between source and destination for the duration of complete message transfer.
4. Flow control:-Flow control is performed end to end**.**
5. Error control:-Error control is performed process to process. It ensures that entire message arrives at receivers transport layer without error (damage or loss or duplication). Error correction is done by retransmission.

4. Explain following protocols:
I. PPP II. SLIP (2 marks for PPP explanation,2 marks for SLIP explanation)
Answer:

(i) PPP:-

- PPP means point to point protocol.
- It is a much more developed protocol than SLIP (which is why it is replacing it).
- It transfers additional data, better suited to data transmission over the Internet (the addition of data in a frame is mainly due to the increase in bandwidth).
- PPP is a collection of three protocols:
    - A datagram encapsulation protocol LCP i.e. Link control Protocol, enabling testing and communication configuration.
    - A collection of NCPs i.e. Network Control Protocols allowing integration control of PPP within the protocols of the upper layers.
    - Data encapsulated in a PPP frame is called a packet.
    - These packets are generally datagrams, but can also be different. So one field of the frame is reserved for the type of protocol to which the packet belongs.

The PPP frame looks like:

Data to be Transmitted	Padding Data

The padding data is used to adapt the length of the frame for certain protocols.

(ii) SLIP:-

- SLIP means Serial Line Internet Protocol.
- SLIP is the result of the integration of modern protocols prior to suite of TCP/IP protocols.
- It is a simple internet link protocol conducting neither address nor error control.
- Data transmission with SLIP is very simple.
- This protocol sends a frame composed only of data to be sent followed by an end of transmission character (the END character, the ASCII code of which is 192).

A SLIP frame looks like:

Data to be Transmitted	END

5. Compare IPv4 and IPv6. (Any four points) (any 4 points,1 mark each)

Answer:

IPv4	IPv6
1. Source and destination addresses are 32 bits (4 bytes) in length.	1. Source and destination addresses are 128 bits(16 bytes) in length.
2. Uses broadcast addresses to send traffic to all nodes on a subnet.	2. There are no IPv6 broadcast addresses. Instead, multicast scoped addresses are used.
3. Fragmentation is supported at originating hosts and intermediate routers.	3. Fragmentation is not supported at routers. It is only supported at the originating host.
4. IP header include a checksum.	4. .IP header does not include a checksum.
5. IP header includes options.	5. All optional data is moved to IPv6 extension headers.
6. IPsec support is optional	6. IPsec support is required in a full IPv6 implementation.
7. No identification of payload for QoS handling by routers is present within the IPv4 header.	7. Payload identification for QoS handling by routers is included in the IPv6 header using the Flow Label field.
8. Address must be configured either manually or through DHCP.	8. Addresses can be automatically assigned using stateless address auto configuration, assigned using DHCPv6, or manually configured.
9. Uses host address(A) resource records in the domain name system to map host names to IPv4 addresses.	9. Uses host address (AAAA) resource records in the domain name system to map host names to IPv6 addresses

6. **Explain sub-netting and super-netting with example.** (Sub-netting 2 marks, super-netting 2 marks)

Answer:
Sub-netting:

Subnet mask is a net mask with the only real difference being that breaking a larger network into smaller parts and each smaller section will use different sets of address numbers. The subnet mask is 32 bit value that usually express in dotted decimal notation used by IP address. This is the combination of net-ID and host-ID.

Example: Consider the subnet mask as 255.255.0.0.

convert the 255.255.0.0 subnet mask to binary.

255.255.0.0 = 11111111 11111111 00000000 00000000 (in binary)

add 1s right after the last 1 on the right (in the middle of the mask, between the 1s and 0s) I add five 1s to make it look like this:

11111111 11111111 11111000 00000000

Using the subnet's formula, this would give us 25 = 32 networks

Super-netting:

To create a supernetwork, the procedure is to be reversed. The networks are combined by creating space for a larger number of hosts. To accomplish this, we start with the default subnet mask of 255.255.255.0 and use some of the bits reserved for the Netid to identify the Hostid. The following exampleshows we would create a new supernetwork by combining four separate subnetworks.

Example:

If a packet arrives at the router with the destination address 192.168.64.48, the supernet mask 255.255.252.0 is applied to the destination address.

11000000.10101000.01000000.00110000 (destination IP address)
AND
11111111.11111111.11111100.00000000 (supernet mask)
Returns
11000000.10101000.01000000.00000000

7. **Explain connectionless and connection oriented protocol. Give the example for each type. (Explanation 1 mark each, any one example 1 mark for each type)**

Answer: Connection less protocol: These protocols do not establish a connection between devices. It is manually achieved by transmitting information in one direction, from source to destination without checking to see if the destination is still there or if it is prepared to receive the information.

Connection-oriented protocol: It means that when devices communication they perform hand sharing to set up on end to end connection. Usually one device begins by sending a request to open a connection, and the other responds.

Connectionless protocols:

1) IP
2) ICMP
3) UDP

1. IP: IP is internet Protocol. It is unreliable protocol because it does not provide any error control and flow control. Packets in IP are called "Datagram"
2. ICMP: It is internet control message protocol. It reports error and sends control messages. Error reporting messages include – destination unreachable, source quench , time exceed, parameter problem, redirection etc. Query message includes –echo request and reply, time stamp request and reply, router solicitation and advertisement. etc
3.UDP: UDP is user datagram protocol. It is connectionless protocol because data is sent without establishing a connection between sender and receiver before sending the data. UDP is unreliable because data is delivered without acknowledgement. UDP does not perform Auto retransmission. UDP does not use flow control. UDP has high transmission speed.

Connection oriented protocol:

1) **TCP**
2) **SLIP**
3) **PPP**
4) **SMTP**

1) TCP: TCP is transmission control protocol. It is connection oriented protocol because connection must be establish prior to transmission of data. TCP is reliable protocol because data is delivered with acknowledgement. TCP perform Auto Retransmission if the data is lost. TCP use flow control. TCP has low speed of transmission.
2. SLIP: SLIP is serial line internet protocol SLIP does not perform error detection and correction. SLIP does not provide any authentication. SLIP is not approved internet standard. SLIP supports only Internet protocol (IP) SLIP supports static IP address assignment
3. PPP: PPP is point to point protocol. PPP perform error detection PPP provides authentication and security. PPP is approved internet standard. PPP supports IP and other protocols. PPP supports Dynamic IP address assignment

4. **SMTP:** SMTP is simple mail transfer protocol. It is connection oriented text based protocol in which sender communicates with receiver using a command and supplying data over reliable TCP connection. SMTP is standard application layer protocol for delivery of email over TCP/IP network. SMTP establish a TCP connection between Sender And port number 25 of receiver.

8. Give the name of protocols used by different layers of TCP/IP. Discuss the function of ARP and RARP. (4 marks for protocols, 2 marks of ARP, 2 marks of RARP)

Answer: TCP/IP Model contains following layer.

1) Host-to-Network Layer - It defines characteristics of transmission media. It also concern with delivery of data when two systems are attached to same network SLIP PPP

2) Internet Layer – This layer permits host to inject packets into network and packet travels independently to destination. This layer defines packet format and protocol called IP (internet Protocol) ARP RARP IP

3) Transport Layer - It has TCP and UDP. TCP (transmission control protocol) –it is Reliable & connection oriented protocol. UDP (User Datagram Protocol)- it is Unreliable & connectionless protocol.

4) Application Layer - It includes virtual Terminal (TELNET), file transfer Protocol (FTP), simple Mail Transfer Protocol (SMTP) and other protocols like HTTP, WWW, DNS.

ARP:(Address resolution protocol)

Networking H/W demands that a datagram contain the physical address of the intended recipient. For this problem Address Resolution protocol (ARP) was developed. ARP takes the IP address of a host as input & gives its corresponding physical address as the output. As it doesn't know who must be having address it sends the broadcast message to all the computer on the network. The computer whose IP address matches the broadcast IP address sends a reply and along with it, its physical address to the broadcasting computer. All other computers ignore the broadcast message as IP address is different. Now, when it is responding whose IP address gets match is aware of the sender. So it doesn‟t require sending broadcast message. As it knows sender hardware as well as IP address that is the reason it unicast the reply so that sender only receive it.

RARP: (Reverse Address Resolution protocol)

ARP is used for solving the problem of finding out which Ethernet address corresponding to a given IP address. But sometimes we have to solve a reverse problem. That means we have to obtain the IP address corresponding to the given Ethernet address. Such a problem can occur when booting a diskless workstation. The problem of obtaining the IP address when an Ethernet address is given, can be solved by using RARP (Reverse Address Resolution protocol) The newly booted workstation is allowed to broadcast its Ethernet address. The RARP server looks at this request. Then it looks up the Ethernet address in its configuration files and sends back the corresponding IP address. Using RARP is actually better than embedding an IP address in the memory image because it allows the same image to be used on all machines. If the IP address were buried inside the image, each workstation would need its own image. The disadvantage of RARP is that it uses a destination address of all ls (limited broadcasting) to reach the RARP server. But such broadcasts are not forwarded by routers, so a RARP server is needed on each network.

Summer-14

- **Define Protocol with reference to computer network. What is the function of IP?** *(Definition of protocol - 1 Mark, Function of IP - 1 Mark)*

Ans: Protocol: - Protocol is set of rules and conventions. Sender and receiver in data communication must agree on common set of rules before they can communicate with each other. Protocol defines. a) Syntax (what is to be communicated) b) Semantics (how is it to be communicated c) Timing (When it should be communicated)

Function of IP:

a. Addressing
b. Routing
c. Data encapsulation
d. Fragmentation & reassembly

2. What is meant by subnet? How to use subnet masking to create two subnets? *(Explanation of subnet -2 Marks, Subnet masking explanation with any suitable example - 2 Marks).*

Ans:

A **subnet** is a logical grouping of connected network devices. Nodes on a subnet tend to be located in close physical proximity to each other on a LAN. Network designers employ subnets as a way to partition networks into logical segments for greater ease of administration. When subnets are properly implemented, both the performance and security of networks can be improved.

In Internet Protocol (IP) networking, devices on a subnet share contiguous ranges of IP address numbers. A mask (known as the *subnet mask* or network mask) defines the boundaries of an IP subnet. The correspondence between subnet masks and IP address ranges follows defined mathematical formulas. IT professionals use *subnet calculators* to map between masks and addresses. Subnet masking for 2 subnet: To calculate the number of subnets or nodes, use the formula (2n-2) where n = number of bits in either field, and 2n represents 2 raised to the nth power. Multiplying the number of subnets by the number of nodes available per subnet gives you the total number of nodes available for your class and subnet mask. Also, note that although subnet masks with non-contiguous mask bits are allowed, they are not recommended.

Example:

10001100.10110011.11011100.11001000 140.179.220.200 IP Address
11111111.11111111.**11**000000.00000000 255.255.**192**.000 Subnet Mask

---

10001100.10110011.11000000.00000000 140.179.192.000 Subnet Address

Hence

Subnet number	Address
1	140.179.64.0
2	140.179.128.0

3. Describe the importance/role of presentation layer in OSI model.

(Any 4 importance/functions of presentation layer – 1 Mark each)

Ans: Role of presentation layer in OSI model the presentation layer makes it sure that the information is delivered in such a form that the receiving system will understand and use it. The form and syntax (language) of the two communicating systems can be different e.g. one system is using the ASCII code for file transfer and the other one user IBM's EBCDIC.

Under such condition the presentation layer provider the "translation" from ASCII to EBCDIC and vice versa.

The presentation layer performs the following function:

1. It translates data between the formats the network requires and the format the computer expects.
2. It does the protocol conversion
3. For security and privacy purpose it carries out encryption at the transmitter and decryption at the receiver.
4. It carries out data compression to reduce the bandwidth of the data to be transmitted.
5. Unlike the session layer, which provides many different functions, the presentation layer has only one function.
6. It basically functions as a pass through device. It receiver primitives from the application layer and issues duplicate primitives to the session layer below it using the Presentation Service Access point (PSAP) and Session Service Access point (SSAP)

4. Explain the working of "File Transfer Protocol" with a neat diagram.

(Working - 3 Marks, Diagram 1 Mark)

Ans: FTP is a stranded mechanism provided by the Internet for copying a file from one host to the other.

1) Some of the problem in transferring files from one system to the other are as follows: Two systems may use different file name conventions. Two systems may represent text data in different types. The directory structure of the two systems may be different.
2) FTP provides a simple solution to all these problems.
3) The basic model of FTP is shown
4) FTP established two connections between the client and server. One is for data transfer and the other is for the control information.
5) The fact that FTP separates control and data makes it very efficient.
6) The control connection uses simple rules of communication. Only one line of command or a line of response is transferred at a time.
7. But the data connection uses more complex rules due to the variety of data types being transferred.
8. FTP uses port 21 for the control connection and port 20 for the data connection.
9. As shown in the figure client has three components namely: i. User interface ii. Control process and iii. Data transfer process.

10. The Server has two components: the control process and data transfer process.
11. The control connection is maintained during the entire interactive FTP session. The data connection is first opened, file is transferred and data connection is closed. This is closed. This is done for transferring each file.

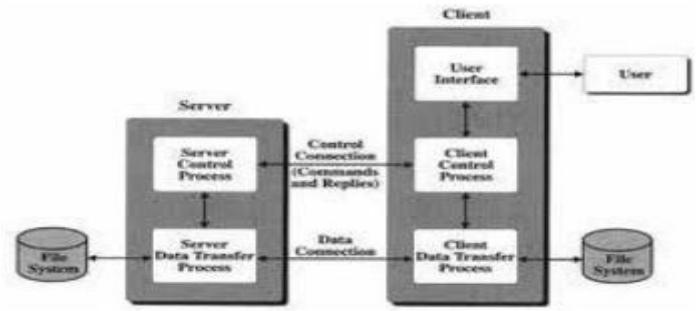


Fig. Basic Model Of FTP

Control connection: This connection is created in the same way as the other application programs described earlier. Control connection remains alive during the entire process. The IP uses minimize delay type services because this is an interactive connection between a user and server.

Data Connection: Data connection uses the port 20 at the site. This connection is opened when data to be transferred is ready and it is closed when transfer of data is over. The service types used by IP is maximize throughput.

12. **Describe TCP used in computer communication.**
(Any 4 Services/ Relevant explanation – 1 Mark each)

Ans: Following are some of the services offered by TCP to the process at the application layer:

1. Stream delivery service
2. Sending and receiving buffers
3. Bytes and segments
4. Full duplex service
5. Connection oriented service
6. Reliable service.
7. Process to process communication

1. Stream delivery service: TCP is a stream oriented protocol. It allows the sending process to deliver data as a stream of bytes and the receiving process to obtain as a stream of bytes. TCP creates a working environment in such a way that the sending and receiving processes seem to be connected by an imaginary "tube" This is called as stream delivery service.

2. Sending and receiving buffers: The sending and receiving process may not produce and receive data at the same speed. Hence TCP needs buffers for storage. There are two types of buffers used in each direction:

1) Sending buffer
2) Receiving buffer.

A buffer can be implemented by using a circular array of 1 byte locations as shown.

The movement of data in one direction on the sending side the buffer has three types of locations:

- Empty Locations
- Location containing the bytes which have been sent but not acknowledgement. These bytes are kept in the buffer till an acknowledgement is received.
- The locations containing the bytes to be sent by the sending TCP.

3. Bytes and segments: Buffering is used to handle the difference between the speed of data transmission and data consumption. But only buffering is not enough. We need one more step before sending the data. The IP layer, as a service provider for TCP, need to send data in the form of packets and as a stream of bytes. At the transport layer, TCP groups a number of bytes together into a packet called a segment. A header is added to each segment for the purpose of exercising control. The segments are encapsulated in an IP datagram and then transmitted. The entire operation is transparent to the receiving process. The segments may be receiver out of order, lost or corrupted when it reaches the receiving end.

4. Full duplex service: TCP offers full duplex service where the data can flow in both the direction simultaneously. Each TCP will then have a sending buffer and receiving buffer. The TCP segments are sent both the directions.

5. Connection oriented service: TCP is a connection oriented protocol. When process –I wants to communicate (send and receive) with another process (process-2), the sequence of operations is as follows: TCP of process -1 informs TCP of process -2 and gets its approval. TCP of process -1 and TCP of process -2 exchange data in both the directions. After completing the data exchange, when buffers on both sides are empty, the two TCPs destroy their buffers.

1. The type of connection in TCP is not physical, it is virtual. The TCP segment is encapsulated in an IP datagram and can be sent out of order.
2. These segments can get lost or corrupted and have to be resent.
3. Each segment may take a different path to reach the destination.

6. Reliable services: TCP is a reliable transport protocol. It uses an acknowledgment mechanism for checking the safe and sound arrival of data.

7. Process to process communication: The TCP user port numbers a transport layer addresses.. Note that if an application can use both UDP and TCP, the same port number is assigned to this application.

13. Computer IPv4 and IPv6 (four points).
(Any four points -1 Mark each)
Ans:

14. Describe meaning and function of:

i) MAC address

ii) IP address

(MAC address explanation- 1 Mark, Example- 1 Mark)

Ans:

i) MAC Address:

- The MAC address is a unique value associated with a network adapter.
- MAC addresses are also known as **hardware** addresses or **physical** addresses.
- They uniquely identify an adapter on a LAN. MAC addresses are 12-digit hexadecimal numbers (48 bits in length).
- By convention, MAC addresses are usually written in one of the following two formats:
- MM:MM:MM:SS:SS:SS The first half of a MAC address contains the ID number of the adapter manufacturer.
- These IDs are regulated by an Internet standards body (see sidebar).
- The second half of a MAC address represents the serial number assigned to the adapter by the manufacturer. Example, 00:A0:C9:14:C8:29

ii) IP Address: *(IP address Explanation -1 Mark, Example – 1 Mark)*

- An **Internet Protocol address** (**IP address**) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.
- An IP address serves two principal functions: host or network interface identification and location addressing.
- Its role has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there."

1. The IP address consists of two parts namely a network identifier and a host identifier.
2. All the computers on a particular subnet will have the same network identifier but different host identifiers
3. The internet Assigned Number Authority (IANA) assigns network identifiers to avoid any duplication of addresses.
4. An IPv4 address consists of two parts. The first part of the address, called the network number, identifies a network on the internet; the remainder, called the host ID, identifies an individual host on that network.

Classful Addressing: The IPv4 addresses are classified into 5 types as follows:

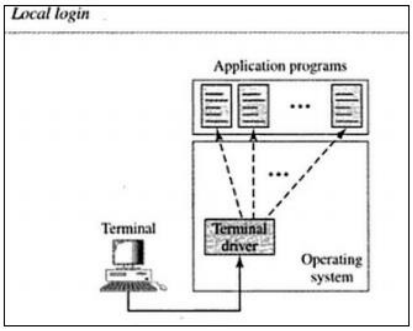
1. Class A
2. Class B
3. Class C
4. Class D
5. Class E

9. Explain the working of "TELNET"

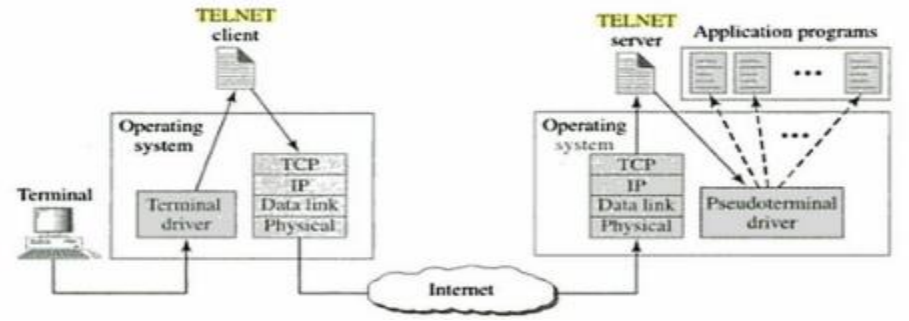
(Explanation - 4 Marks)

Ans: TELNET TELNET is abbreviation for Terminal Network. It is standard TCP/IP protocol for virtual terminal services proposed by ISO. TELNET enables establishment of connection to a remote system in such a way that a local terminal appears to be terminal at remote system. TELNET is general purpose client server application program.

Local Login When user log in to local time sharing system it is called local login. The keystrokes accepted by terminal driver. Terminal driver passes the character to the operating system. Operating system, in tern interprets the combination of character and invoke the desired application or utility.



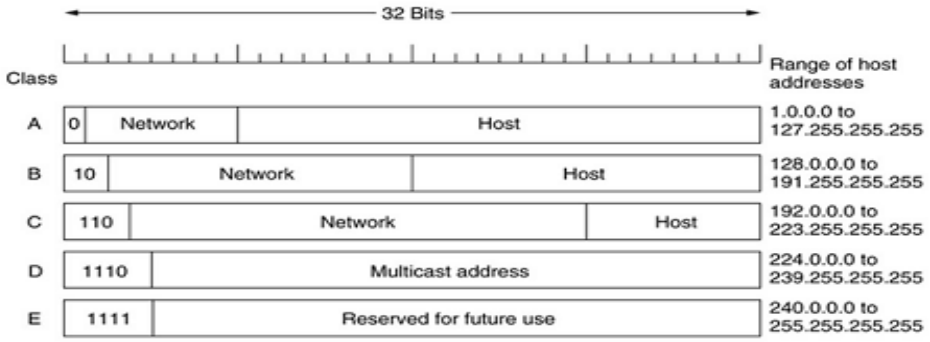
Remote login When user wants to access the application or utility located at the remote machine ,he or she performs remote login. Here the telnet client and server program come into use. The user sends the keystrokes to local operating system. local operating system accept is, but do not interpret them. The characters are send to TELNET client. TELNET client transform the character to a universal character set called Network Virtual Terminal Character and deliver them to the local TCP/IP stack.



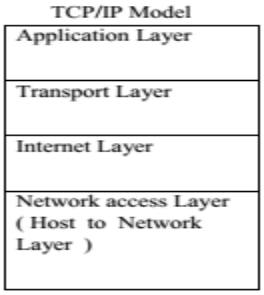
As shown in above figure the command/text in NVT form travel through internet, and arrive at TCP/IP stack of remote Machine. Here the characters are delivered to the operating system and Passed to the TELNET server. Which changes the characters to the understandable characters by the remote computer. However characters could not directly pass to the operating system because remote operating system is not designed to receive characters from TELNET server. The solution is to add piece of software called Pseudo- terminal driver, which pretends that characters are coming from terminal. The operating system passes the characters to appropriate application program.

11. Which different classes are used for IP addressing? Describe each in brief.
(Listing of classes - 1 Mark, Explanation - 3 Marks).

Ans: IP Address is classified into 5 types as Class A Class B Class C Class D Class E



12. **Describe TCP/IP with neat sketch. Compare TCP/IP and OSI reference model.**
(TCP/IP model digram-2 Marks, explanation 2 Marks, Comparison of TCP/IP with OSI model any 4 points - 4 Marks)



TCP/IP Model contains following layer.
1) Network Access Layer It defines characteristics of transmission media. It also concern with delivery of data when two systems are attached to same network.
2) Internet Layer – This layer permits host to inject packets into network and packet travels independently to destination. This layer defines packet format and protocol called IP (internet Protocol)
3) Transport Layer - It has TCP and UDP TCP (transmission control protocol) –it is Reliable & connection oriented protocol. UDP (User Datagram Protocol)- it is Unreliable & connectionless protocol.
4) Application Layer - It includes virtual Terminal (TELNET), file transfer Protocol (FTP), simple Mail Transfer Protocol (SMTP) and other protocols like HTTP, WWW, DNS.

13. Describe any two connectionless and connection oriented protocols.
(Any 2 Connectionless protocol- 4 Marks, Any 2 connection oriented protocols - 4 Marks)
Ans: Connectionless protocols:
1) IP
2) ICMP
3) UDP

IP:

- IP is internet Protocol.
- It is unreliable protocol because it does not provide any error control and flow control.
- Packets in IP are called “Datagram”.
- Datagram is variable length packet with two parts –header and data

ICMP:

- It is internet control message protocol.
- It reports error and sends control messages.
- **Error reporting messages** include – destination unreachable, source quench , time exceed, parameter problem , redirection etc.
- **Query message includes** –echo request and reply, time stamp request and reply, router solicitation and advertisement. etc

UDP:

- UDP is user datagram protocol.
- It is connectionless protocol because data is sent without establishing a connection between sender and receiver before sending the data.
- UDP is unreliable because data is delivered without acknowledgement.
- UDP does not perform Auto retransmission. UDP does not use flow control.
- UDP has high transmission speed.

Connection oriented protocol:

1) TCP
2) SLIP
3) PPP
4) SMTP

TCP:

- TCP is transmission control protocol.
- It is connection oriented protocol because connection must be establish prior to transmission of data.
- TCP is reliable protocol because data is delivered with acknowledgement.
- TCP perform Auto Retransmission if the data is lost. TCP use flow control.
- TCP has low speed of transmission.

SLIP:

- SLIP is serial line internet protocol SLIP does not perform error detection and correction.
- SLIP does not provide any authentication.
- SLIP is not approved internet standard.
- SLIP supports only Internet protocol (IP).
- SLIP supports static IP address assignment

PPP:

- PPP is point to point protocol.
- PPP perform error detection PPP provides authentication and security.
- PPP is approved internet standard.
- PPP supports IP and other protocols.
- PPP supports Dynamic IP address assignment

SMTP:

- SMTP is simple mail transfer protocol.
- It is connection oriented text based protocol in which sender communicates with receiver using a command and supplying data over reliable TCP connection.
- SMTP is standard application layer protocol for delivery of email over TCP/IP network.
- SMTP establish a TCP connection between Sender And port number 25 of receiver.

Winter-15

1. **Define connection oriented protocol.**
   (Definition -2 Marks)

Ans: Connection-oriented protocol service is sometimes called a "reliable" network service, because it guarantees that data will arrive in the proper sequence. Connection-oriented describes a means of transmitting data in which the devices at the end points use a preliminary protocol to establish an end-to-end connection before any data is sent.
Example: Transmission Control Protocol (TCP) is a connection-oriented protocol.

2. **List two DHCP protocols**
   (Listing any Two Protocols -1 Mark each)

Ans: 1. ARP 2. RARP 3. IP 4. BOOTP

3. Explain the SLIP protocol. *(Explanation - 4 Marks)*
Ans:
SLIP:
1. Serial Line Protocol is an encapsulation of the Internet Protocol designed to work over serial ports and modem connections.
2. This protocol defines a sequence of bytes that frame IP packets on a serial line.
3. SLIP is commonly used for point-to-point serial connections running TCP/IP
4. It is designed to transmit signals over a serial connection and has very low overhead.
5. SLIP is serial line internet protocol
6. SLIP does not perform error detection and correction.
7. SLIP does not provide any authentication.
8. SLIP is not approved internet standard.
9. SLIP supports static IP address assignment.

4. Explain RARP and BOOTP.
(Explanation - 2 Marks For Each Protocol)

Ans:
RARP:

The **Reverse Address Resolution Protocol** (**RARP**) is an obsolete computer networking protocol used by a client computer to request its Internet Protocol (IPv4) address from a computer network, when all it has available is its Link Layer or hardware address, such as a MAC address.

The client broadcasts the request, and does not need prior knowledge of the network topology or the identities of servers capable of fulfilling its request. RARP is described in Internet Engineering Task Force (IETF) publication RFC 903.

RARP requires one or more server hosts to maintain a database of mappings of Link Layer addresses to their respective protocol addresses. Media Access Control (MAC) addresses needed to be individually configured on the servers by an administrator. RARP was limited to serving only IP addresses. Reverse ARP differs from the Inverse Address Resolution Protocol (InARP) described in RFC 2390, which is designed to obtain the IP address associated with a local Frame Relay data link connection identifier. InARP is not used in Ethernet.

BOOTP:

The Bootstrap Protocol (BOOTP) is a computer networking protocol used in Internet Protocol networks to automatically assign an IP address to network devices from a configuration server. The BOOTP was originally defined in RFC 951. When a computer that is connected to a network is powered up and boots its operating system, the system software broadcasts BOOTP messages onto the network to request an IP address assignment. A BOOTP configuration server assigns an IP address based on the request from a pool of addresses configured by an administrator. BOOTP is implemented using the User Datagram Protocol (UDP) as transport protocol, port number 67 is used by the server to receive client requests and port number 68 is used by the client to receive server responses. BOOTP operates only on IPv4networks.

5. What is MAC addresss? How it is located? *(MAC address - 2 Marks, Locating of MAC - 2 Mark)*

Ans:

MAC (Media access control address) MAC address is a unique id associated with the network adapter (NIC) and it uniquely identifies an adapter on a LAN or internet. Media Access Control (MAC) address is a binary number used to uniquely identify computer network adapters. These numbers (sometimes called "hardware addresses" Or "physical addresses") are embedded into the network hardware during the manufacturing process, or stored in firmware, and designed to not be modified. MAC addresses are 12-digit (6 bytes or 48 bits) hexadecimal numbers. By convention, they are usually written in one of the following three formats:

a. MM:MM:MM:SS:SS:SS

b. MM-MM-MM-SS-SS-SS

c. MMM.MMM.SSS.SSS

The leftmost 6 digits (24 bits) called a "prefix" is associated with the adapter manufacturer.

Locating a MAC Address in Windows XP, Vista, NT 2000, 2003,7, 8, 10.

1) Click the Start button, select Run.
2) Type CMD and click OK.
3) In Command prompt, Type ipconfig/all and press Enter. ...
4) MAC address (Physical Address) will be displayed in the Ethernet Adapter Local Area Connection section.

6. What are the different IP address classes? Explain any one in brief.
(Enlisting IP classes -1 Mark & Any one class Explanation - 3Marks)

Ans: Already Given.

7. Compare ARP and RARP *(Any four points - 4 Marks)*

Ans:

ARP	RARP
ARP converts an Internet Protocol address to its physical network address (MAC).	RARP converts Ethernet MAC address to IP address.
ARP broadcast an IP address in an effort to discover its equivalent hardware address.	RARP broadcast the System's hardware address.
Local host maintain the ARP Table.	A RARP server maintain the RARP table.
RFC 826 describes ARP	RFC 903 describes RARP

8. Describe the term subnet masking.
(Subnet masking Explanation -2 Marks & Example - 2 Marks)

Ans:

- An IP address has two components, the network address and the host address. A subnet mask separates the IP address into the network and host addresses.
- In Internet Protocol (IP) networking, devices on a subnet share contiguous ranges of IP address numbers.
- A mask (known as the *subnet mask* or network mask) defines the boundaries of an IP subnet.
- The correspondence between subnet masks and IP address ranges follows defined mathematical formulas. IT professionals use *subnet calculators* to map between masks and addresses.

- A Subnet mask is a 32-bit number that masks an IP address, and divides the IP address into network address and host address.
- Subnet Mask is made by setting network bits to all "1"s and setting host bits to all "0"s. Within a given network, two host addresses are reserved for special purpose, and cannot be assigned to hosts.
- The "0" address is assigned a network address and "255" is assigned to a broadcast address, and they cannot be assigned to hosts. Subnet masking for 2 subnet: To calculate the number of subnets or nodes, use the formula (2n-2) where n = number of bits in either field, and 2n represents 2 raised to the nth power. Multiplying the number of subnets by the number of nodes available per subnet gives you the total number of nodes available for your class and subnet mask. Also, note that although subnet masks with non-contiguous mask bits are allowed, they are not recommended.

Example:
10001100.10110011.11011100.11001000 140.179.220.200 IP Address
11111111.11111111.**110**00000.00000000 255.255.**192**.000 Subnet Mask
---
10001100.10110011.11000000.00000000 140.179.192.000 Subnet Address Hence

Subnet number	Address
1	140.179.64.0
2	140.179.128.0

9. Which of the following TCP/IP transport layers is faster? Justify your answer:
i. TCP
ii. IP
iii. UDP ***(Explanation of TCP - 2Marks, IP - 1Mark, UDP - 1Mark)***

Ans:

- **TCP**
  - TCP is transmission control protocol.
  - It is connection oriented protocol because connection must be establish prior to transmission of data.
  - TCP is reliable protocol because data is delivered with acknowledgement.
  - TCP perform Auto Retransmission if the data is lost.
  - TCP use flow control.
  - TCP has low speed of transmission.
  - Features of TCP are: connection oriented, point to point communication, support duplex mode.
- **IP:**
  - IP is internet Protocol.
  - It is unreliable protocol because it does not provide any error control and flow control.
  - Packets in IP are called “Datagram”

- Datagram is variable length packet with two parts –header and data.
- Features of IP are encapsulation, addressing, routing, fragmentation, protocol identification.

UDP:

- UDP is user datagram protocol.
- It is connectionless protocol because data is sent without establishing a connection between sender and receiver before sending the data.
- UDP is unreliable because data is delivered without acknowledgement.
- UDP does not perform Auto retransmission.
- UDP does not use flow control.
- UDP has high transmission speed.

10 Explain the term SMTP. ***(Explanation - 4 Marks)***

Ans :

- It is Simple Mail transfer Protocol.
- It is connection oriented text based protocol in which sender communicates with receiver using a command and supplying data over reliable TCP connection.
- SMTP is standard application layer protocol for delivery of email over TCP/IP network.
- SMTP establish a TCP connection between Sender And port number 25 of receiver.
- It is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server.

11. Compare IPv4 and IPv6. ***(Any 4 Points - 1Mark each)***

Ans: Already Answered.

12. **Compare UDP with TCP protocols with respect to:**

(i) Complexity
(ii) Connection
(iii) Reliability
(iv) Function
(v) Which layer they exist
(vi) Flow controlling
(vii) Overhead
(viii) Which is powerful

(Each Parameter - 1Mark each)
Ans:

	UDP	TCP
Complexity	**UDP is less complex**	**TCP is more complex**
Connection	**UDP is connection less protocol**	**TCP is connection oriented protocol**
Reliability	**It provides unreliable delivery of messages**	**It provides reliable delivery of messages**
Function	**By using this protocol one program can send a load of packets to another and that would be the end of the relationship.**	**As a message makes its way across the internet from one computer to another. This is connection based.**
layer they exist	**Transport layer**	**Transport layer**
Flow controlling	**UDP has no flow control**	**TCP has flow control**
Overhead	**Overhead is very low**	**Overhead is low**
Which is powerful	**UDP is less powerful**	**TCP is more powerful.**

OSI reference model	TCP/IP network model
1)It has 7 layers	**1)It has 4 layers**
2)Transport layer guarantees delivery of packets	**2)Transport layer does not guarantees delivery of packets**
3)Horizontal approach	**3)Vertical approach**
4)Separate presentation layer	**4)No session layer, characteristics are provided by transport layer**
5)Separate session layer	**5)No presentation layer, characteristics are provided by application layer**
6)Network layer provides both connectionless and connection oriented services	**6)Network layer provides only connection less services**
7)It defines the services, interfaces and protocols very clearly and makes a clear distinction between them	**7)It does not clearly distinguishes between service interface and protocols**
8)The protocol are better hidden and can be easily replaced as the technology changes	**8)It is not easy to replace the protocols**
9)OSI truly is a general model	**9)TCP/IP cannot be used for any other application**
10)It has a problem of protocol filtering into a model	**10) The model does not fit any protocol stack.**