14IT505

Hall Ticket Number:

III/IV B.Tech (Regular\Supplementary) DEGREE EXAMINATION

November, 2019 — **Information Technology**

Fifth Semester — **Data Communication & Computer Networks**

Time: Three Hours — **Maximum:** 60 Marks

Answer Question No.1 compulsorily. (1X12 = 12 Marks)

Answer ONE question from each unit. (4X12=48 Marks)

1. Answer all questions (1X12=12 Marks)
   - a) Define data communication.
   - b) What is topology?
   - c) Define burst errors.
   - d) What is optimality principle?
   - e) Define load shedding.
   - f) What is jitter?
   - g) Define socket.
   - h) Define multiplexing.
   - i) Differentiate TCP and UDP.
   - j) What is the purpose of DNS?
   - k) List out application layer protocols.
   - l) What are the advantages of MIME protocol?

UNIT I

2. a) Explain five components of a data communication model with a diagram. 6M
   b) Describe TCP/IP protocol architecture. 6M

(OR)

3. a) List out and explain various types of topologies. 6M
   b) Differentiate Asynchronous and synchronous transmission 6M

UNIT II

4. a) How virtual circuit subnet is different from datagram subnet? Explain. 6M
   b) Briefly explain flooding routing algorithm 6M

(OR)

5. a) How to avoid congestion in datagram subnet? Explain. 6M
   b) Write a short note on IP classes. 6M

UNIT III

6. a) List out various Berkeley socket primitives for TCP 6M
   b) Derive the steps for Remote Procedure Call (RPC) with neat diagram 6M

(OR)

7. a) Briefly explain TCP segment header format with a neat diagram 6M
   b) Narrate TCP connection establishment 6M

UNIT IV

8. a) Explain Domain resource records. 6M
   b) What are the roles of the user agent? Explain all. 6M

(OR)

9. a) Narrate architecture of a Web with a neat diagram. 6M
   b) List out the built-in HTTP request methods. 6M

1. Answer the questions 1*12=12M

(a) Define data communication.
Ans: **Data communication** refers to the exchange of databetween a source and a receiver via transmission media.

(b) What is topology?
Ans: The way how computers are connected to form a network.

(c) Define burst errors.
Ans: Two or more bits are changed during the transmission are called burst errors.

(d) What is optimality principle?
Ans: The optimality principle states that if router J is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same route.

(e) Define load shedding.
Ans: when too much traffic in channel, which we cannot control it leads stop the services this situation load shedding.

(f) What is jitter?
Ans: **jitter** refers to the delay variation in the packets' arrival

(g) Define socket.
Ans: A **socket** is one endpoint of a two-way communication link between two programs running on the **network.**

(h) Define multiplexing.
Ans: **multiplexing** is a method by which multiple analog or digital signals are combined into one signal over a shared medium.

(i) Differentiate TCP and UDP.
Ans: 1) TCP is connection oriented. UDP is connection less.
2) TCP is reliable. UDP is un-reliable.

(j) What is the purpose of DNS?
Ans: The main **function** of **DNS** is to translate domain names into IP Addresses.

(k) List out application layer protocols.

(l) Ans: TELNET, FTP, NFS and SMTP

(m)What are the advantages of MIMEprotocol?
Ans: **MIME** provided support for varying content types and multi-part messages.

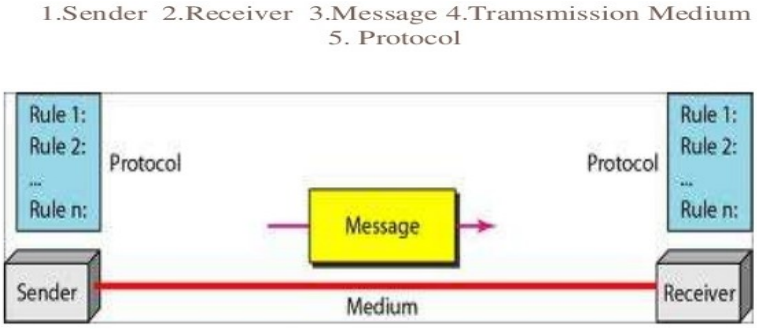
UNIT- I

2. (a) Explain five components of a data communication model with a diagram. (6M)

Ans: Diagram---3M Explanation----3M

Following are the five components of a data communication network.

1. Data
2. Sender
3. Receiver
4. Transmission Medium
5. Protocol



1. Data:

Communication of data means a message or data will be transmitted from one device and will be received in the destination or target device. Thus the first component in a data communication network is data or message to that needs to be delivered and received. Data or message can be of various forms such as text, audio, video, image or combinations of these forms etc.

2. Sender:

A data must has to be sent to a destination from a source. This source is called thesender. The device that sends the data to the destination or target is the Sender. It can be a computer, cell phone, video camera and so on.

3. Receiver:

The destination of a transmitted data is the receiver which will receive the data. The device that receives the data that was sent by the Sender is the Receiver. A receiver can again be a computer, cell phone, video camera and so on.

4. Transmission medium:

In data communication network, the transmission medium is the physical path for the data to travel to its destination after being sent by the Sender. Receiver receives the data at one end of this path and the sender sent from another end of the path. Transmission medium could be like twisted-pair cable, coaxial cable, fiber-optic cable etc.

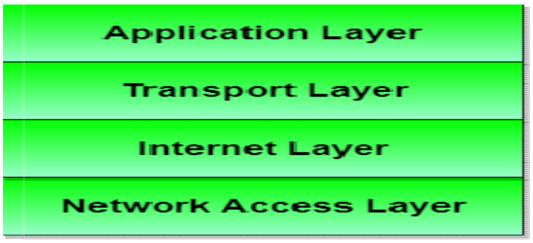
5. Protocol:

A protocol is nothing but a set of rules that applies on the full data communication procedure. This is like an agreement between the two devices to successfully communicate with each other. For example, how the data will be sent, how the data will be traveling, how to ensure that full data has received, how to handle errors in transmission etc. Both devices follow the same set of rules or protocol so that they understand each other.

(b) Describe TCP/IP protocol architecture. (6M)

Diagram---2M Explanation ---4M

Ans:TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. **Protocols** are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the internet. They also offer simple naming and addressing schemes. The following diagram depicting various layers in TCP/IP model.



Following are some of the features of TCP/IP model.

- Support for a flexible architecture. Adding more machines to a network was easy.

- The network was robust, and connections remained intact until the source and destination machines were functioning.

Layer 1: Host-to-network Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.

Layer 3: Transport Layer

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. **TELNET** is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
2. **FTP**(File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. **SMTP**(Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. **DNS**(Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.

(OR

3. (a) List out and explain various types of topologies. (6M)

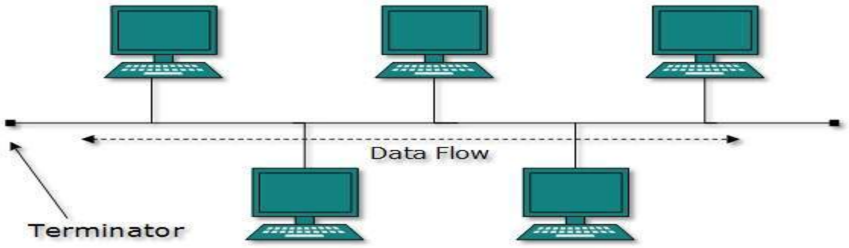
Types---2M Diagram---2M Explanation—2M

Ans:A Network Topology is the arrangement with which computer systems or network devices are connected to each other.

1. Bus 2. Ring 3. Mesh 4.Star 5. Hybrid.

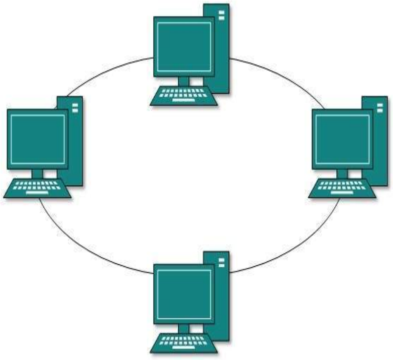
1. **BUS**: Bus topology, all devices share single communication line or cable.Bus topology may have problem while multiple hosts sending data at the same time. Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue. It is one of the simple

forms of networking where a failure of a device does not affect the other devices. But failure of the shared communication line can make all other devices stop functioning.



Both ends of the shared channel have line terminator. The data is sent in only one direction and as soon as it reaches the extreme end, the terminator removes the data from the line.

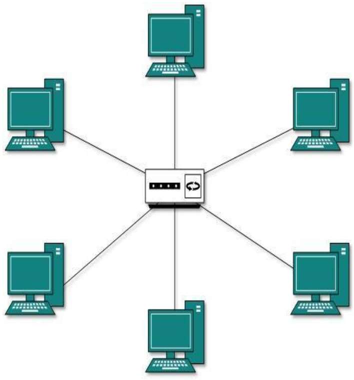
2. **Ring:** In ring topology, each host machine connects to exactly two other machines, creating a circular network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts. To connect one more host in the existing structure, the administrator may need only one more extra cable.



Failure of any host results in failure of the whole ring.Thus, every connection in the ring is a point of failure. There are methods which employ one more backup ring.

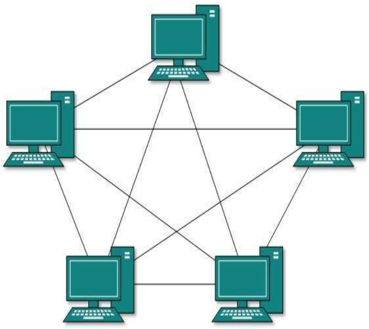
3. **Star :**All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection. That is, there exists a point to point connection between hosts and hub. The hub device can be any of the following:

- Layer-1 device such as hub or repeater
- Layer-2 device such as switch or bridge
- Layer-3 device such as router or gateway



As in Bus topology, hub acts as single point of failure. If hub fails, connectivity of all hosts to all other hosts fails. Every communication between hosts, takes place through only the hub.Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.

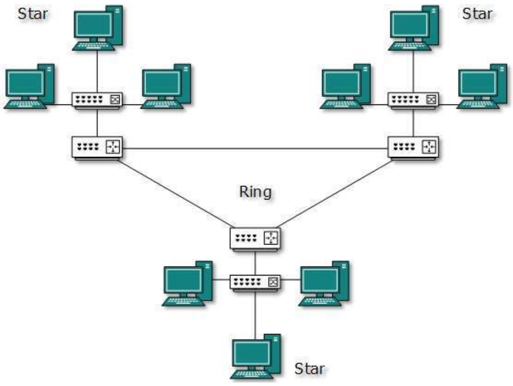
4. **Mesh :**In this type of topology, a host is connected to one or multiple hosts.This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only.



Hosts in Mesh topology also work as relay for other hosts which do not have direct point-to-point links. Mesh technology comes into two types:

- **Full Mesh**: All hosts have a point-to-point connection to every other host in the network. Thus for every new host n(n-1)/2 connections are required. It provides the most reliable network structure among all network topologies.
- **Partially Mesh**: Not all hosts have point-to-point connection to every other host. Hosts connect to each other in some arbitrarily fashion. This topology exists where we need to provide reliability to some hosts out of all.

5. **Hybrid :**A network structure whose design contains more than one topology is said to be hybrid topology. Hybrid topology inherits merits and demerits of all the incorporating topologies.



The above picture represents an arbitrarily hybrid topology. The combining topologies may contain attributes of Star, Ring, Bus, and Daisy-chain topologies. Most WANs are connected by means of Dual-Ring topology and networks connected to them are mostly Star topology networks. Internet is the best example of largest Hybrid topology

(b) Differentiate Asynchronous and synchronous transmission. (6M)

Ans: **4-Points ---6M**

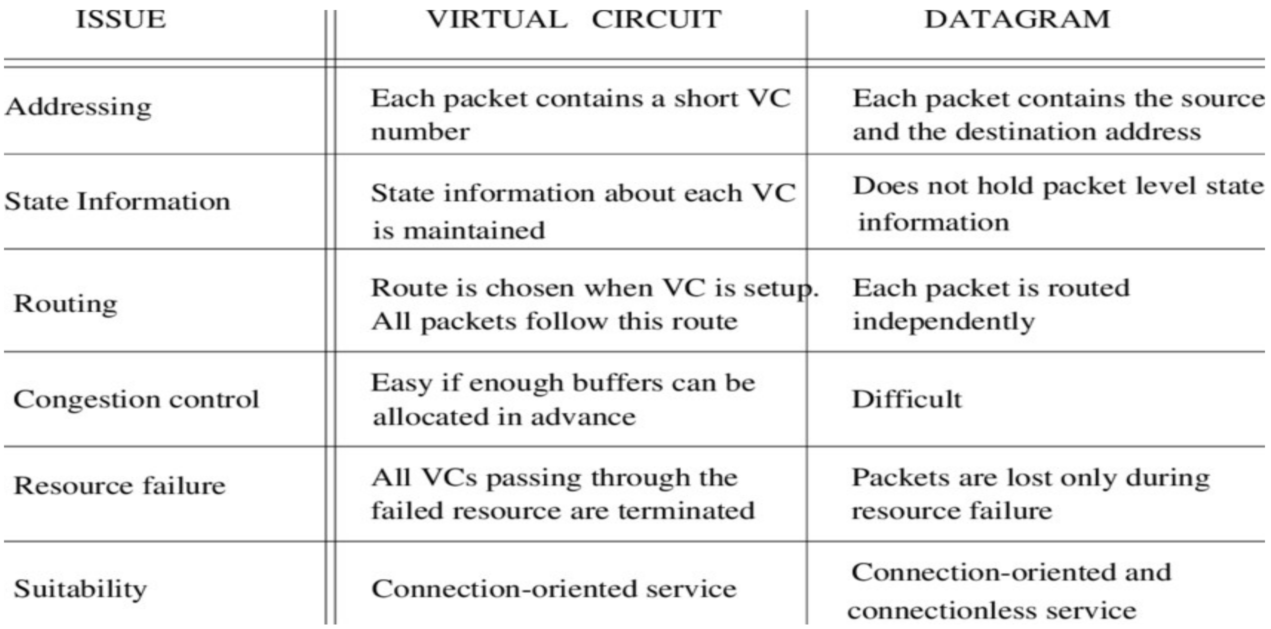
S.NO	SYNCHRONOUS TRANSMISSION	ASYNCHRONOUS TRANSMISSION
1.	In Synchronous transmission, Data is sent in form of blocks or frames.	In asynchronous transmission, Data is sent in form of byte or character.
2.	Synchronous transmission is fast.	Asynchronous transmission is slow.

3.	Synchronous transmission is costly.	Asynchronous transmission economical.
4.	In Synchronous transmission, time interval of transmission is constant.	In asynchronous transmission, time interval of transmission is not constant, it is random.
5.	In Synchronous transmission, There is no gap present between data.	In asynchronous transmission, There is present gap between data.

UNIT-II

4. (a) How virtual circuit subnet is different from datagram subnet? (6M)

Ans: 6-Points ---6M



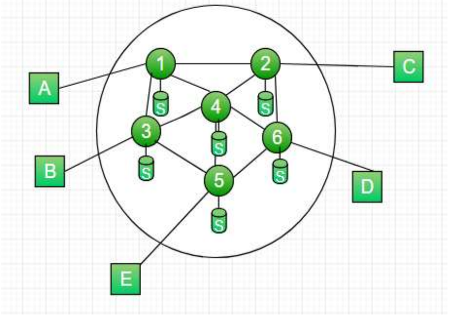
ISSUE	VIRTUAL CIRCUIT	DATAGRAM
Addressing	Each packet contains a short VC number	Each packet contains the source and the destination address
State Information	State information about each VC is maintained	Does not hold packet level state information
Routing	Route is chosen when VC is setup. All packets follow this route	Each packet is routed independently
Congestion control	Easy if enough buffers can be allocated in advance	Difficult
Resource failure	All VCs passing through the failed resource are terminated	Packets are lost only during resource failure
Suitability	Connection-oriented service	Connection-oriented and connectionless service

(b) Briefly explain flooding routing algorithm. (6M)

Ans: Diagram—2M Explanation—4M

Flooding –

- Requires no network information like topology, load condition ,cost of diff. paths
- Every incoming packet to a node is sent out on every outgoing like except the one it arrived on.
- For Example in the below figure
    - A incoming packet to (1) is sent out to (2),(3)
    - from (2) is sent to (6),(4) and from (3) it is sent to (4),(5)
    - from (4) it is sent to (6),(5),(3) , from (6) it is sent to (2),(4),(5),from (5) it is sent to (4),(3)



Characteristics –

- All possible routes between Source and Destination is tried. A packet will always get through if path exists
- As all routes are tried, there will be atleast one route which is the shortest
- All nodes directly or indirectly connected are visited

Limitations –

- Flooding generates vast number of duplicate pakects
- Suitable damping mechanism must be used

Hop-Count –

- A hop counter may be contained in the packet header which is decremented at each hop. with the packet being discarded when the counter becomes zero
- The sender initializes the hop counter. If no estimate is known, it is set to the full diameter of the subnet.
- Keep track of the packets which are responsible for flooding using a sequence number. Avoid sending them out a second time.

Selective Flooding: Routers do not send every incoming packet out on every line, only on those lines that go in approximately in the direction of the destination.

Advantages of Flooding :

- Highly Robust, emergency or immediate messages can be sent (eg military applications)
- Set up route in virtual circuit
- Flooding always chooses the shortest path
- Broadcast messages to all the nodes

(OR)

5. (a) How to avoid congestion in datagram subnet? Explain. (6M)

Definition -2M Causes—2M Solution ---2M

Ans:Problem: When too many packets are transmitted through a network, congestion occurs At very high traffic, performance collapses completely, and almost no packets are delivered.

Causes:bursty nature of traffic is the root cause → When part of the network no longer can cope a sudden increase of traffic, congestion builds upon. Other factors, such as lack of bandwidth, ill-configuration and slow routers can also bring up congestion.

Solution: congestion control, and two basic approaches – Open-loop: try to prevent congestion occurring by good design – Closed-loop: monitor the system to detect congestion, pass this information to where action can be taken, and adjust system operation to correct the problem

Prevention: Different policies at various layers can affect congestion are given below.

Transport

• Retransmission policy • Out-of-order caching policy • Acknowledgement policy
• Flow control policy• Timeout determination

Network

• Virtual circuit versus datagram • Packet queueing and service policy
• Packet discard policy • Routing algorithm
• Packet lifetime management

Data link

• Retransmission policy • Out-of-order caching policy • Acknowledgement policy
• Traffic shaping • Flow control

b) Write a short note IP classes. (6M)

IP Table ---3M Explanation ---3M

Ans: An IP address is a numeric identity of an interface. Just like a postal address provides a unique identity to a house, an IP address provides a unique identity to an interface.
IP network uses IP address to find the destination interface and delivers the IP packets. In order to receive IP packets, an interface needs a unique IP address. If multiple interfaces have same IP address, IP network will not work.

An IP address is 32 bits in length. These bits are divided in four parts. Each part is known as octets and contains and 8 bits.

An IP address can be written in three notations; dotted-decimal, binary and hexadecimal. Among these types, dotted-decimal is the most popular and frequently used method for writing an IP address.

In dotted-decimal notation, each byte (8 bits) of the 32 bits IP address is written in decimal equivalent. The four resulting decimal numbers are separated by a dot and written in a sequence. 10.10.10.10, 172.168.10.1, 192.168.1.1 and 200.0.0.1 are some examples of IP address in dotted-decimal notation.

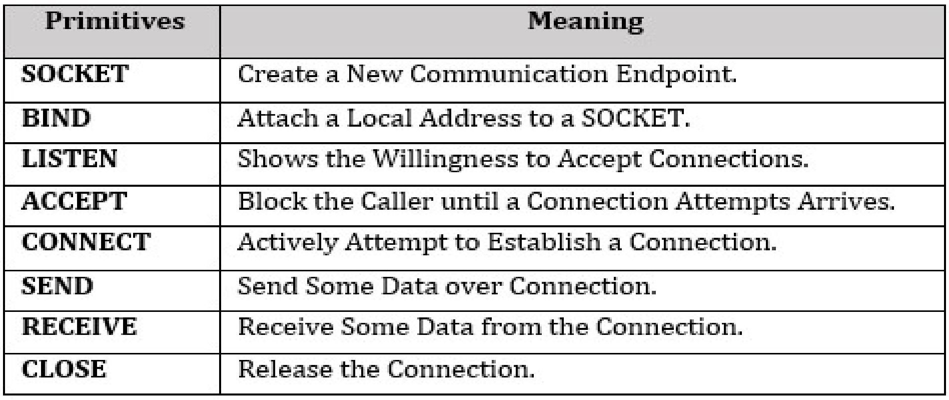
IP addresses are divided in following five classes:-

Class	Starting Address	Ending Address	Subnet mask
A	0.0.0.0	127.255.255.255	255.0.0.0
B	128.0.0.0	191.255.255.255	255.255.0.0
C	192.0.0.0	223.255.255.255	255.255.255.0
D	224.0.0.0	239.255.255.255	255.255.255.255
E	240.0.0.0	255.255.255.255	255.255.255.255

UNIT-III

6 (a) List out various Berkeley socket primitives for TCP. (4M)

Ans: Any 4 System calls—4M
Primitive used in Berkeley Socket:



Primitives	Meaning
SOCKET	Create a New Communication Endpoint.
BIND	Attach a Local Address to a SOCKET.
LISTEN	Shows the Willingness to Accept Connections.
ACCEPT	Block the Caller until a Connection Attempts Arrives.
CONNECT	Actively Attempt to Establish a Connection.
SEND	Send Some Data over Connection.
RECEIVE	Receive Some Data from the Connection.
CLOSE	Release the Connection.

(b). Derive the steps for Remote Procedure Call (RPC) with neat diagram. (8M)

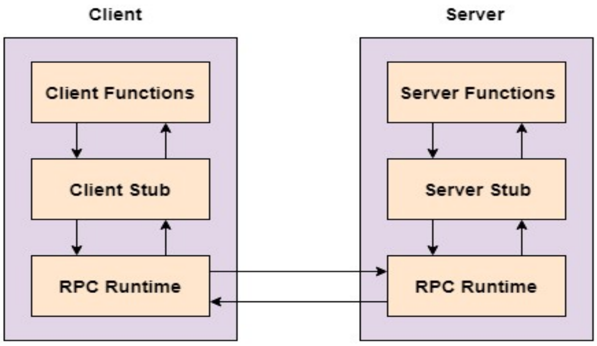
Ans: step by step procedure ---4M Diagram ---2M

A remote procedure call is an interprocess communication technique that is used for client-server based applications. It is also known as a subroutine call or a function call.

A client has a request message that the RPC translates and sends to the server. This request may be a procedure or a function call to a remote server. When the server receives the request, it sends the required response back to the client. The client is blocked while the server is processing the call and only resumed execution after the server is finished.

The sequence of events in a remote procedure call are given as follows:

- The client stub is called by the client.
- The client stub makes a system call to send the message to the server and puts the parameters in the message.
- The message is sent from the client to the server by the client's operating system.
- The message is passed to the server stub by the server operating system.
- The parameters are removed from the message by the server stub.
- Then, the server procedure is called by the server stub.



Advantages of Remote Procedure Call

- Remote procedure calls support process oriented and thread oriented models.
- The internal message passing mechanism of RPC is hidden from the user.
- The effort to re-write and re-develop the code is minimum in remote procedure calls.
- Remote procedure calls can be used in distributed environment as well as the local environment.
- Many of the protocol layers are omitted by RPC to improve performance.

Disadvantages of Remote Procedure Call

- The remote procedure call is a concept that can be implemented in different ways. It is not a standard.
- There is no flexibility in RPC for hardware architecture. It is only interaction based.
- There is an increase in costs because of remote procedure call.

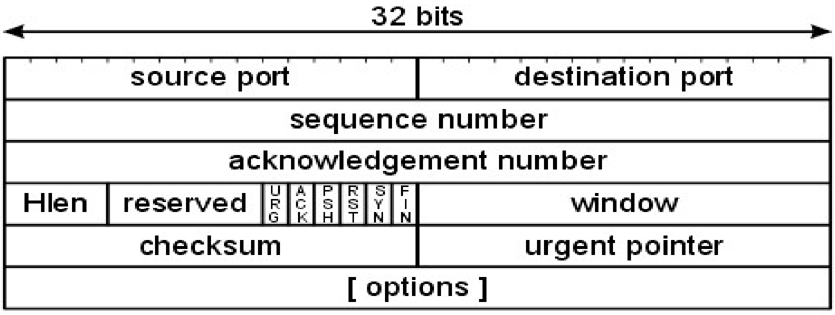
(OR)

7. (a) Briefly explain TCP segment header format with a neat diagram (8M)

Diagram – 4M Explanation---4M

Ans: Every segment begins with a fixed-format, 20-byte header. The fixed header may be followed by header options. After the options, if any, up to 65,535 - 20 - 20 = 65,495 data bytes may follow, where the first 20 refer to the IP header and the second to the TCP header. Segments without any data are legal and are commonly used for acknowledgements and control messages

TCP header format

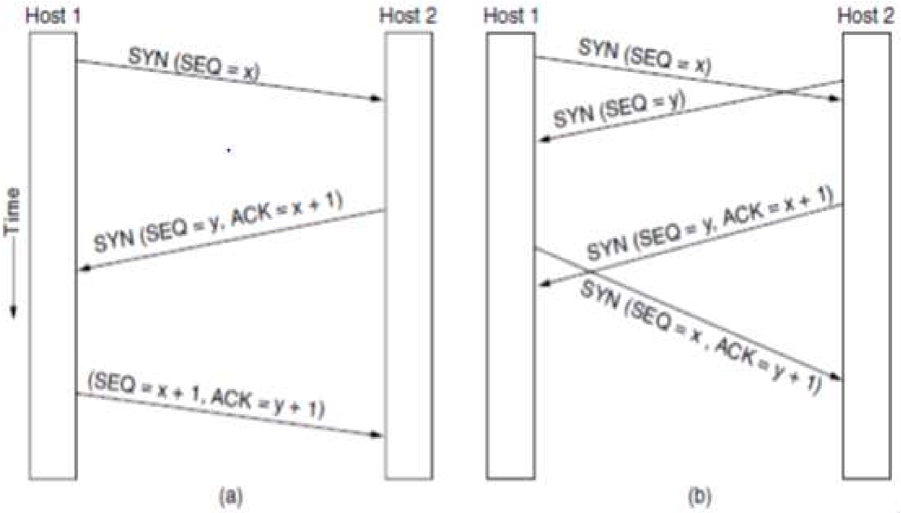


Source Port, Destination Port : Identify local end points of the connections
Sequence number: Specifies the sequence number of the segment
Acknowledgement Number: Specifies the next byte expected.
TCP header length: Tells how many 32-bit words are contained in TCP header
URG: It is set to 1 if URGENT pointer is in use, which indicates start of urgent data.
ACK: It is set to 1 to indicate that the acknowledgement number is valid.
PSH: Indicates pushed data
RST: It is used to reset a connection that has become confused due to reject an invalid segment or refuse anattempt to open a connection.
FIN: Used to release a connection.
SYN: Used to establish connections.

(b) Narrate TCP connection establishment. (4M)

Ans:Diagram – 2M Explanation---2M

- To establish a connection, one side, say the server, passively waits for an incoming connection by executing the LISTEN and ACCEPT primitives in that order, either specifying a specific source or nobody in particular.
- The other side, say, the client, executes a CONNECT primitive, specifying the IP address and port to which it wants to connect, the maximum TCP segment size it is willing to accept, and optionally some user data (e.g., a password).
- The CONNECT primitive sends a TCP segment with the SYN bit on and ACK bit off and waits for a response.
- When this segment arrives at the destination, the TCP entity there checks to see if there is a process that has done a LISTEN on the port given in the Destination port field. If not, it sends a reply with the RST bit on to reject the connection.
- If some process is listening to the port, that process is given the incoming TCP segment. It can either accept or reject the connection. If it accepts, an acknowledgement segment is sent back. The sequence of TCP segments sent in the normal case is shown in Fig below. Note that a SYN segment consumes 1 byte of sequence space so that it can be acknowledged unambiguously.


Host 1
Host 2
Host 1
Host 2
SYN (SEQ = x)
Time
SYN (SEQ = y, ACK = x + 1)
(SEQ = x + 1, ACK = y + 1)
SYN (SEQ = x)
SYN (SEQ = y)
SYN (SEQ = y, ACK = x + 1)
SYN (SEQ = x, ACK = y + 1)
(a)
(b)

a) TCP connection establishment in the normal case. (b) Simultaneous connection establishment on both sides.

UNIT-IV

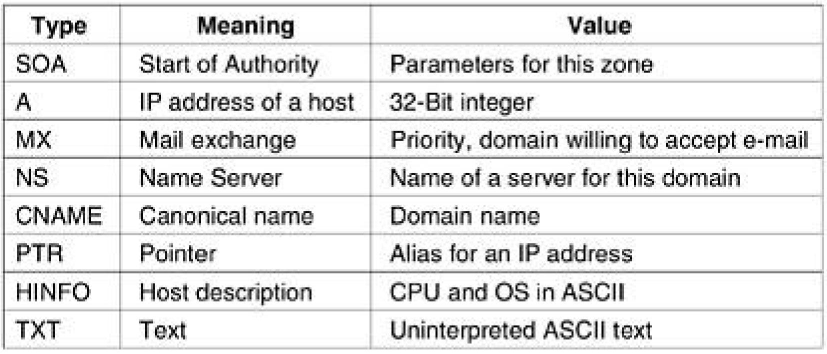
8 (a) Explain Domain resource records. . (6M)

Ans:Format –2M Types—2M Explanation—2M

Every domain can have a sent of resource records associated with it. For a single host, the most common resource record is just its IP address. When a resolver gives a domain name to DNS, it gets both the resource records associated with that name i.e., the real function of DNS is to map domain names into resource records. A resource record is a 5-tuple and its format is as follows:

Domain Name Time to live Type Class Value

Domain _name : Tells the domain to which this record applies.
Time- to- live : Gives an identification of how stable the record is (High Stable = 86400 i.e. no. of seconds /day) (High Volatile = 1 min)
Type: Tells what kind of record this is.
Class: It is IN for the internet information and codes for non internet information
Value: This field can be a number a domain name or an ASCII string.
The following table shows the various record types.



Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept e-mail
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

(b).What are the roles of the user agent? Explain all. (6M)

List-2M Explanation—4M

Ans:E-mail systems consist of two subsystems. They are:-
(1). User Agents, which allow people to read and send e-mail
(2). Message Transfer Agents, which move messages from source to destination
E-mail systems support 5 basic functions:-

a. Composition
b. Transfer
c. Reporting
d. Displaying
e. Disposition

THE USER AGENT

A user agent is normally a program (sometimes called a mail reader) that accepts a variety of commands for composing, receiving, and replying to messages, as well as for manipulating mailboxes.

SENDING E-MAIL

To send an e-mail message, a user must provide the message, the destination address, and possibly some other parameters. The message can be produced with a free-standing text editor, a word processing program, or possibly with a specialized text editor built into the user agent. The destination address must be in a format that the user agent can deal with. Many user agents expect addresses of the form user@dns-address.

READING E-MAIL

When a user agent is started up, it looks at the user's mailbox for incoming e-mail before displaying anything on the screen. Then it may announce the number of messages in the mailbox or display a one-line summary of each one and wait for a command.

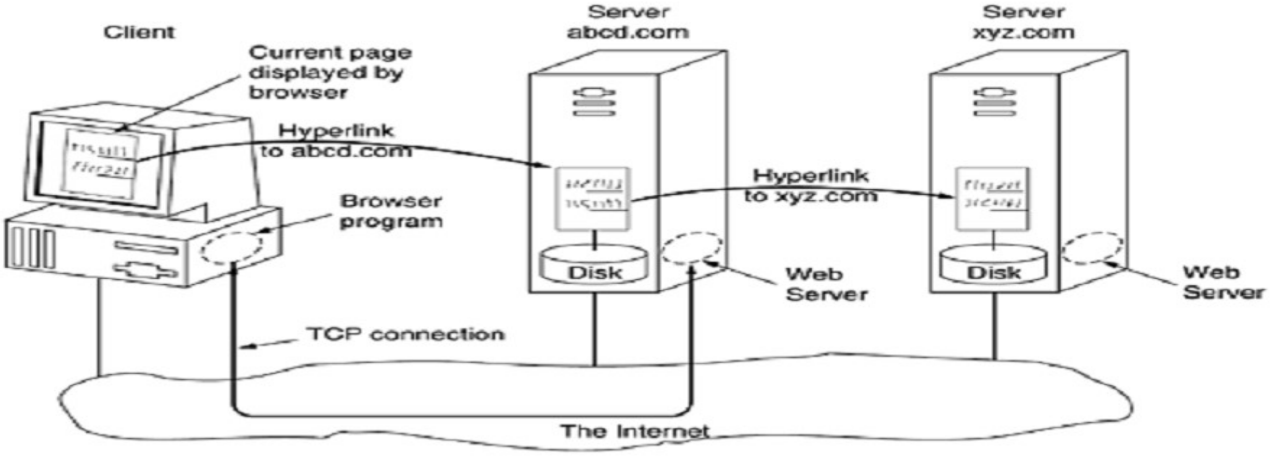
(OR)

(a). Narrate architecture of a Web with a neat diagram. (8M)

Diagram—4M clientside—2M Serverside—2M

Ans: The World Wide Web is an architectural framework for accessing linked documents spread out over millions of machines all over the Internet.

From the users' point of view, the Web consists of a vast, worldwide collection of documents or Web pages. Each page may contain links to other pages anywhere in the world. Users can follow a link by clicking on it, which then takes them to the page pointed to. This process can be repeated indefinitely. Pages are viewed with a program called a browser, of which Internet Explorer and Netscape Navigator are two popular ones. The browser fetches the page requested, interprets the text and formatting commands on it, and displays the page, properly formatted, on the screen. Strings of text that are links to other pages, called hyperlinks, are often highlighted, by underlining, displaying them in a special color, or both.



Here the browser is displaying a Web page on the client machine. When the user clicks on a line of text that is linked to a page on the *abcd.com* server, the browser follows the hyperlink by sending a message to the*abcd.com* server asking it for the page. When the page arrives, it is displayed. If this page contains a hyperlink to a page on the *xyz.com* server that is clicked on, the browser then sends a request to that machine for the page.

CLIENT SIDE

When an item is selected, the browser follows the hyperlink and fetches the page selected. Therefore, the
embedded hyperlink needs a way to name any other page on the Web. Pages are named using URLs (Uniform
Resource Locators).

The steps that occur at the client side are:

1 The browser determines the URL
2 The browser asks DNS for the IP address
3 DNS replies with the IP address
4 The browser makes a TCP connection to port 80 on the IP address
5 It sends a request asking for file
6 The site server sends the file
7 The TCP connection is released.
8 The browser fetches and displays all the text and images in the file.
9 Web pages are written in standard HTML language to make it understandable by all browsers.
10 The other way to extend a browser is to use a helper application. This is a complete program, running as aseparate process.

SERVER SIDE

The steps to be followed by the server side are:

1. Accept a TCP connection from a client (a browser).
2. Get the name of the file requested.
3. Get the file (from disk).
4. Return the file to the client.
5. Release the TCP connection.

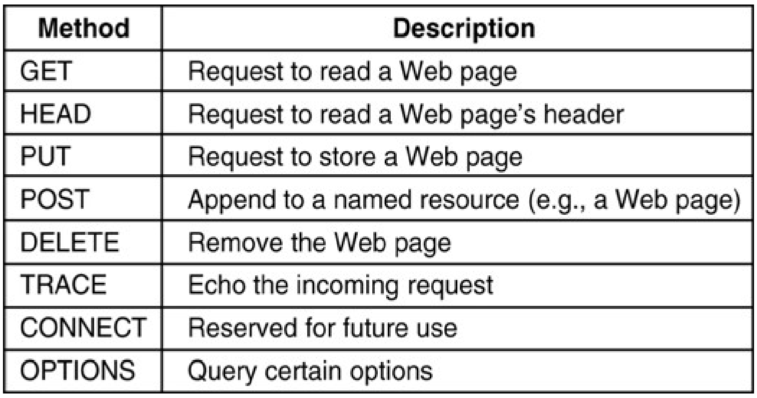
PROCESSING OF REQUEST

The processing of request on the web is as follows:

1. Resolve the name of the Web page requested.
2. Authenticate the client.
3. Perform access control on the client.
4. Perform access control on the Web page.
5. Check the cache.
6. Fetch the requested page from disk.
7. Determine the MIME type to include in the response.
8. Take care of miscellaneous odds and ends.
9. Return the reply to the client.
10. Make an entry in the server log.

b). List out the built-in HTTP request methods. **(4M)**

Ans: Any 4 mehods—4M



Method	Description
GET	Request to read a Web page
HEAD	Request to read a Web page’s header
PUT	Request to store a Web page
POST	Append to a named resource (e.g., a Web page)
DELETE	Remove the Web page
TRACE	Echo the incoming request
CONNECT	Reserved for future use
OPTIONS	Query certain options

Prepared by:

P. Ratna Prakash **Signature of HOD, IT**

I.T. Dept.