14IT505

Hall Ticket Number:

III/IV B.Tech (Regular) DEGREE EXAMINATION

NOVEMBER,2017 | **Information Technology**

Fifth Semester | **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) What is meant by Data Communication?

Ans: Data communications (DC) is the process of using computing and communication technologies to Transfer data from one place to another, and vice versa.

b) What is the necessity of Protocol Architecture?

Ans: When computers, terminals, and/or other data processing devices exchange data, the procedures involved Can be quite complex. There must be a data path between the two computers, either directly or via a Communication network. But more is needed .Typical tasks to be performed are as follow:

1. The source system must either activate the direct data communication path or inform the communication
2. Network of the identity of the desired destination system.

c) Write various Error Detection methods.

Ans: There are three types of Error Detection methods

Vertical Redundancy Check (VRC)

Cyclic redundancy check(CRC)

Parity check

d) What is meant by store and forward packet switching?

Ans: Store and forward is a data communication technique in which a message transmitted from a source nodeis sto at an intermediary device before being forwarded to the destination node .The store and forward process enables ren hosts, data connectivity and transmission, even if there is no direct connection betweenthe source and destination no

e) Write Uses of flooding algorithm.

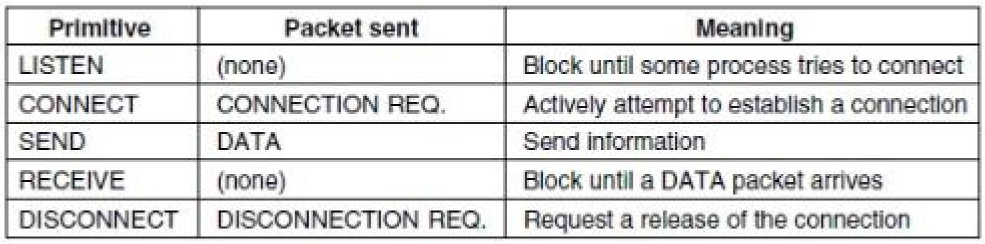
Ans: Flooding is a simple routing *algorithm* in which every incoming packet is transmitted through every Outgoing link. **Flooding algorithms** are also useful for solving many mathematical problems, including maze Problems and many problems in graph theory.

f) Briefly describe IP addresses.

Ans: An Internet Protocol address (IP address) is a logical numeric address that is assigned to every single Computer, printer, switch, router or any other device that is part of a TCP/IP-based network.

g) Write various simple transport service primitives.

Ans:



Primitive	Packet sent	Meaning
LISTEN	(none)	Block until some process tries to connect
CONNECT	CONNECTION REQ.	Actively attempt to establish a connection
SEND	DATA	Send information
RECEIVE	(none)	Block until a DATA packet arrives
DISCONNECT	DISCONNECTION REQ.	Request a release of the connection

h) What is meant by upward multiplexing?

Ans: In upward multiplexing, the different transport connections are multiplexed in to one network connection.

- These transport connections are grouped by the transport layer as per their destinations.
- It then maps the groups with the minimum number of network connections possible.
- The upward multiplexing is quite useful where the network connections come very expensive.

i) What is Remote Procedure Call?

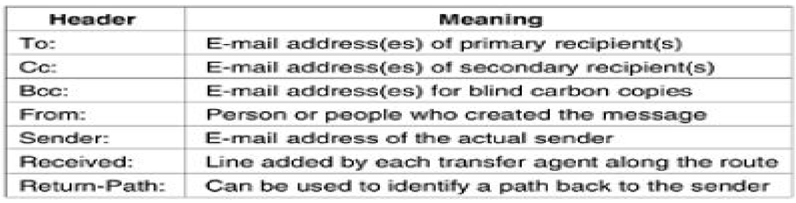
Ans: RPC is a powerful technique for constructing distributed, client-server based applications. It is based on extending the notion of conventional, or local procedure calling, so that the called procedure need not exist in the same address space as the calling procedure.

j) Briefly write about Name servers.

Ans: A name server is a specialized server on the Internet that handles queries or questions from your local Computer, about the location of a domain name's various services.

k) Write Message Format of Electronic Mail.

Figure 7-9. RFC 822 header fields related to message transport.



Header	Meaning
To:	E-mail address(es) of primary recipient(s)
Cc:	E-mail address(es) of secondary recipient(s)
Bcc:	E-mail address(es) for blind carbon copies
From:	Person or people who created the message
Sender:	E-mail address of the actual sender
Received:	Line added by each transfer agent along the route
Return-Path:	Can be used to identify a path back to the sender

l) Uses of HTTP.

The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed,**collaborative**, and Hypermedia information systems. HTTP is the foundation of **data communication** for the World Wide Web. Hypertext is **structured** text that uses**logical** links (hyperlinks) between nodes containing text.

UNIT – I

2.a Explain the TCP/IP Protocol architecture. **6M**

Types of layer----------2m

Diagram-----------------2m

Operation description—2m

Ans:

The TCP/IP Protocol architecture Developed by the US Defense Advanced Research Project Agency (DARPA) for its packet switched network (ARPANET)

Used by the global Internet

This model contains five Layers.

Application layer: Support for user applications,e.g. http, SMPT **2M**

Host to host or transport layer: Reliable delivery of data, Ordering of delivery

Internet layer: Systems may be attached to different networks, Routing functions across Multiple networks, Implemented in end systems and routers.

Network access layer: Exchange of data between end system and network, Destination address provision Invoking services like priority.

Physical layer: Physical interface between data transmission device (e.g. computer) and transmission Medium or network, Characteristics of transmission medium, Signal levels and data rates.

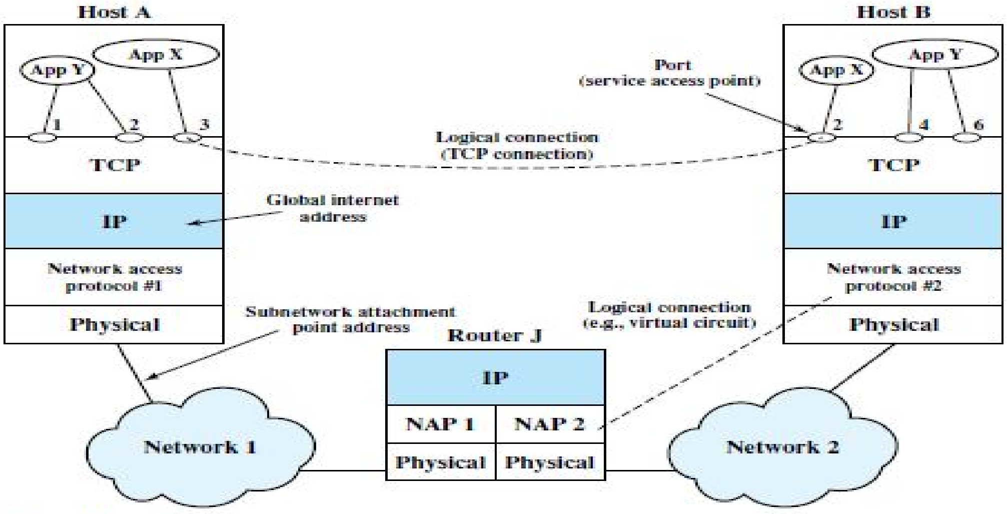

Host A
App Y
App X
1
2
3
TCP
IP
Network access protocol #1
Physical
Host B
App X
App Y
2
4
6
TCP
IP
Network access protocol #2
Physical
Port (service access point)
Logical connection (TCP connection)
Global internet address
Subnetwork attachment point address
Logical connection (e.g., virtual circuit)
Router J
IP
NAP 1
NAP 2
Physical
Physical
Network 1
Network 2

Figure 2.1 TCP/IP Concepts

Figure:2M

Operation2M

Figure 2.1 indicates how these protocols are configured for communications. Tomake clear that the total communications facility may consist of multiple networks,the constituent networks are usually referred to as **sub networks**. Some sort of networkaccess protocol, such as the Ethernet logic, is used to connect a computer to asub network. This protocol enables the host to send data across the sub network toanother host or, if the target host is on another sub network, to a router that will forwardthe data. IP is implemented in all of the end systems and the routers. It acts asa relay to move a block of data from one host, through one or more routers, toanother host. TCP is implemented only in the end systems; it keeps track of theblocks of data to assure that all are delivered reliably to the appropriate application.

2b) Compare OSI and TCP/IP Protocol architecture. 6M

Each difference ------------------------ 1m

Ans:

OSI(Open System Interconnection)	**TCP/IP(Transmission Control Protocol / Internet Protocol)**
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	5. TCP/IP model is, in a way implementation of the OSI model.
6. Network layer of OSI model provides both connection oriented and connectionless service.	6. The Network layer in TCP/IP model provides connectionless service.

(OR)

3a) Describe Asynchronous and Synchronous Transmission in detail.6M

Description for Synchronous transmission:---------------3m

Description for Asynchronous transmission:------------3m

Ans:

Synchronous transmission:3m

Synchronous transmission is, therefore, defined as the process by which data or signal is transferred from one application system or device to another at constant periods or intervals, usually monitored by a clock. This means that the transmitting and receiving systems send and receive data at the same rate or speed. They are in sync. An example of this is copying data from one file location to another:

Asynchronous Transmission: 3M

In the case of **asynchronous transmission**, the data or signals being transmitted and received are not done in synchronization. The time interval between the sending and receiving devices enable transmission and reception at their own pace. This means the data sending 'transmitter' may not be at the same rate as the data receptor. This mode of transmission is not monitored by the same rate and the transmission is said to be asynchronous. For example, observe the data transfer:

3b) Explain High-Level Data Link Control.6M
Basic Characteristics------------------------------------2m
Frame structure--2m
Operation description diagram-----------------------2m

Ans:

The most important data link control protocol is HDLC (ISO 3009, ISO 4335). Not only is HDLC widely used, but it is the basis for many other important data link control protocols, which use the same or similar formats and the same mechanisms as employed in HDLC.

Basic Characteristics2m

To satisfy a variety of applications, HDLC defines three types of stations, two link configurations, and three data transfer modes of operation. The three station types are

Primary station: Responsible for controlling the operation of the link. Frames issued by the primary are called commands.

Secondary station: Operates under the control of the primary station. Frames issued by a secondary are called responses. The primary maintains a separate logical link with each secondary station on the line.

Combined station: Combines the features of primary and secondary. A combined station may issue both commands and responses. The two link configurations are

Unbalanced configuration: Consists of one primary and one or more secondary stations and supports both full-duplex and half-duplex transmission.

Balanced configuration: Consists of two combined stations and supports both full-duplex and half-duplex transmission.

The three data transfer modes are

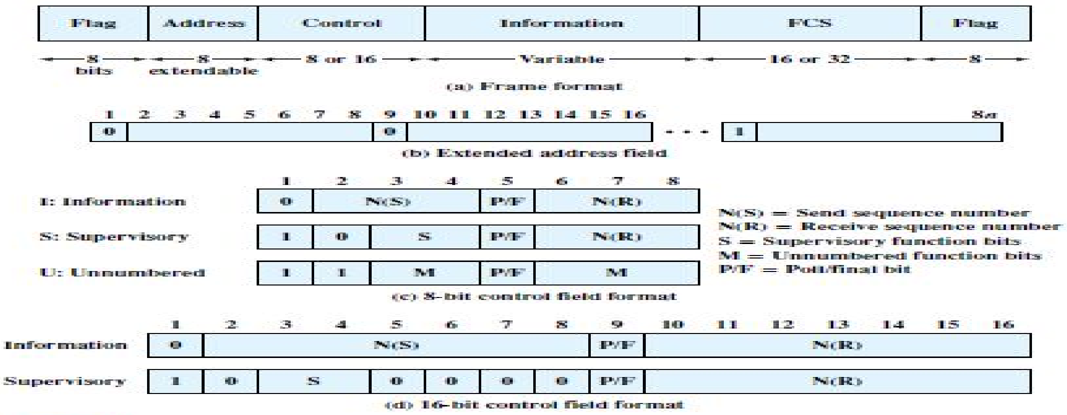
Normal response mode (NRM): Used with an unbalanced configuration. Theprimary may initiatedata transfer to a secondary, but a secondary may onlytransmit data in response to a command from the primary.

Asynchronous balanced mode (ABM): Used with a balanced configuration.Either combined station may initiate transmission without receiving permissionfrom the other combined station.

Asynchronous response mode (ARM): Used with an unbalanced configuration.The secondary may initiate transmission without explicit permission ofthe primary. The primary still retains responsibility for the line, including initialization,error recovery, and logical disconnection.

Frame Structure2m

HDLC uses synchronous transmission. All transmissions are in the form of frames,and asingle frame format suffices for all types of data and control exchanges.Figure 7.7 depicts the structure of the HDLC frame. The flag, address, and controlfields that precede theinformation field are known as a **header**. The FCS andflag fields following the data field are referred to as a **trailer**.



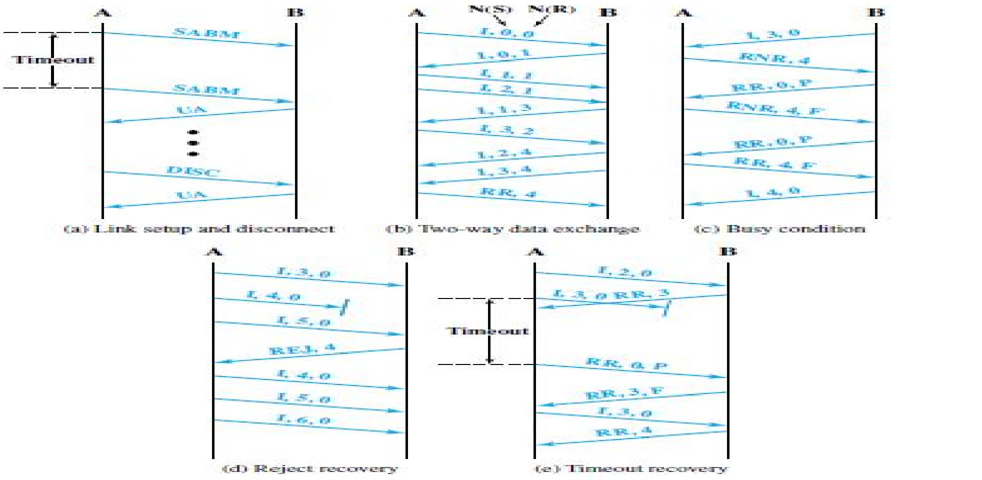
(a) Frame format

(b) Extended address field

(c) 8-bit control field format

(d) 16-bit control field format

Figure 7.7



(a) Link setup and disconnect

(b) Two-way data exchange

(c) Busy condition

(d) Reject recovery

(e) Timeout recovery

Figure 7.9 Examples of HDLC Operation

UNIT – II

4a) State Optimality principal and Illustrate Shortest Path routing algorithm with figure6M
Definition---------------1m
Description-------------2m
Diagram-----------------3m

Ans:

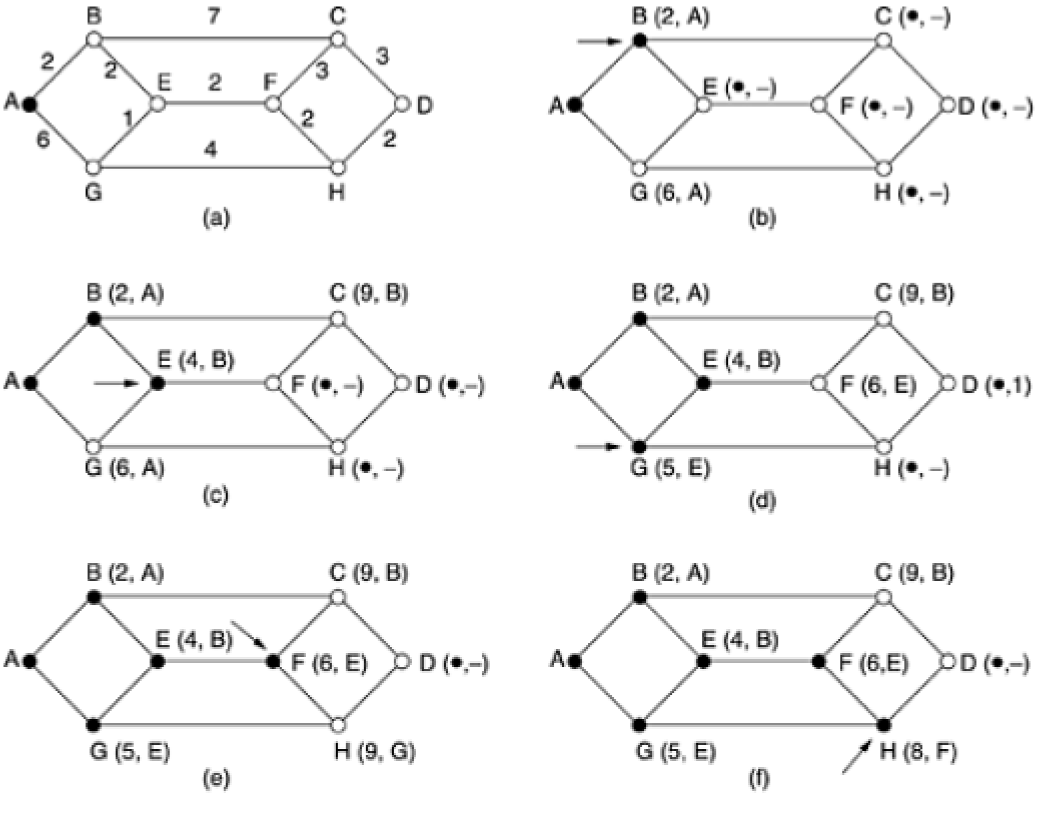
Optimality principal: The **optimality principle**. It states that if router *J* is on the optimal path from router *I* to router *K*, then the optimal path from *J* to *K* also falls along the same route.**1M**

Description: **2M**

The concept of a **shortest path** deserves some explanation. One way of measuring path length is the number of hops. Using this metric, the paths *ABC* and *ABE* in Fig. 5-7 are equally long. Another metric is the geographic distance in kilometers, in which case *ABC* is clearly much longer than *ABE* (assuming the figure is drawn to scale).

Several algorithms for computing the shortest path between two nodes of a graph are known. This one is due to Dijkstra (1959). Each node is labeled (in parentheses) with its distance from the source node along the best known path. Initially, no paths are known, so all nodes are labeled with infinity. As the algorithm proceeds and paths are found, the labels may change, reflecting better paths. A label may be either tentative or permanent. Initially, all labels are tentative. When it is discovered that a label represents the shortest possible path from the source to that node, it is made permanent and never changed thereafter.

Figure 5-7. The first five steps used in computing the shortest path from* A *to* D*. The arrows indicate the working node.3M



4b) Explain Link State Routing algorithm in detail6M
Five steps---1M
Description for Five steps--------------------------5M

Ans:

The idea behind link state routing is simple and can be stated as five parts. Each router must do the following: **1M**

Discover its neighbors and learn their network addresses.
Measure the delay or cost to each of its neighbors.
Construct a packet telling all it has just learned.
Send this packet to all other routers.
Compute the shortest path to every other router.

arning about the Neighbors 1M

a router is booted, its first task is to learn who its neighbors are. It accomplishes this goal by sending a ecial HELLO packet on each point-to-point line.

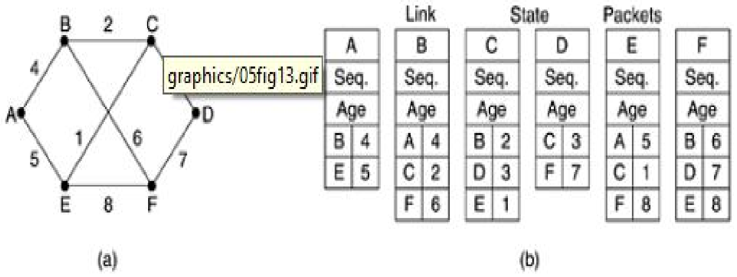
Measuring Line Cost ***1M***

The link state routing algorithm requires each router to know, or at least have a reasonable estimate of, the delay to each of its neighbors. The most direct way to determine this delay is to send over the line a special ECHO packet that the other side is required to send back immediately.

Building Link State Packets ***1M***

Once the information needed for the exchange has been collected, the next step is for each router to build a packet containing all the data. The packet starts with the identity of the sender, followed by a sequence number and age, and a list of neighbors. For each neighbor, the delay to that neighbor is given.

Figure 5-13. (a) A subnet. (b) The link state packets for this subnet.



Link State Packets

A	B	C	D	E	F
Seq.	Seq.	Seq.	Seq.	Seq.	Seq.
Age	Age	Age	Age	Age	Age
B 4	A 4	B 2	C 3	A 5	B 6
E 5	C 2	D 3	F 7	C 1	D 7
	F 6	E 1		F 8	E 8

Distributing the Link State Packets ***1M***

First we will describe the basic distribution algorithm. Later we will give some refinements. The fundamental idea is to use flooding to distribute the link state packets. To keep the flood in check, each packet contains a sequence number that is incremented for each new packet sent.

Computing the New Routes ***1M***

Once a router has accumulated a full set of link state packets, it can construct the entire subnet graph because every link is represented. Now Dijkstra's algorithm can be run locally to construct the shortest path to all possible destinations. The results of this algorithm can be installed in the routing tables, and normal operation resumed.

(OR)

5a) Describe Load shedding and Jitter Control.8M

Description for Load Shedding-----------------4M

Description for Jitter Control------------------ 2M

Load Shedding: **4M**

Ans:

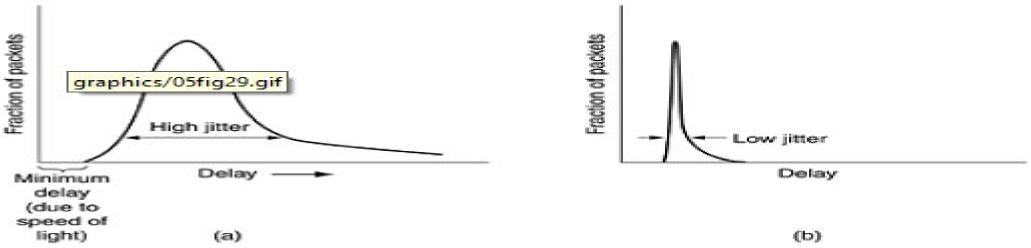
Load shedding is a fancy way of saying that when routers are being inundated by packets that they cannot handle, they just throw them away. This is what routers do when they run out of buffers. If they must throw away a packet then they can at least try to pick the best packets to pitch. This depends on the application and on the error strategy used in the data link layer. The application. Getting the application to mark packets with priority requires some incentive like cheaper transmission rates for lower priority packets .It appears to be better for routers to start dropping packets as soon as congestion seems likely, rather than wait for congestion to take over.

Jitter Control: **2M**

Some applications such as audio and video streaming, it does not matter much if the packets take 20 msec or 30 msec to be delivered, as long as the transit time is constant. The variation (i.e., standard deviation) in the packet arrival times is called **jitter**.

2M

Figure 5-29. (a) High jitter. (b) Low jitter.



5b) Explain various Techniques for achieving good quality of service.4M

List of Techniques for achieving Good quality of Service - 1M
Description for any one Technique 3M
Ans:

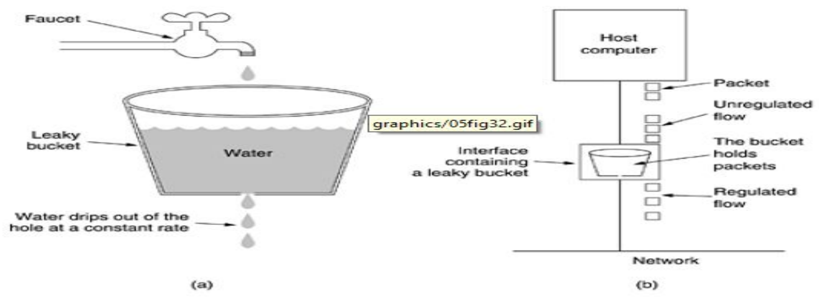
Overprovisioning
Buffering
Traffic shaping
The leaky Bucket Algorithm
The Token Bucket Algorithm
Resource Reservation
Admission Control
Proportional Routing
Packet Scheduling

Traffic shaping1M

Traffic shaping, which smooths out the traffic on the server side, rather than on the client side. Traffic shaping is about regulating the average *rate* (and burstiness) of data transmission.

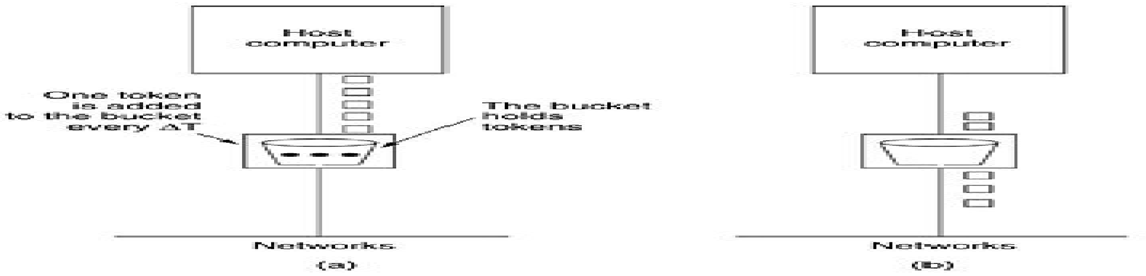
The Leaky Bucket Algorithm:*Imagine a bucket with a small hole in the bottom. No matter at what rate water enters the bucket, the outflow is at a constant rate, ρ, when there is any water in the bucket, and zero when the bucket is empty. Also, once the bucket is full, any additional water entering is spills over the sides and is lost***1M**

Figure 5-32. (a) A leaky bucket with water. (b) A leaky bucket with packets.



The Token Bucket Algorithm 1M

The leaky bucket algorithm enforces a rigid output pattern at the average rate, no matter how bursty the traffic is. For many applications, it is better to allow the output to speed up somewhat when large bursts arrive, so a more flexible algorithm is needed, preferably one that never loses data. One such algorithm is the **token bucket algorithm**.



UNIT – III

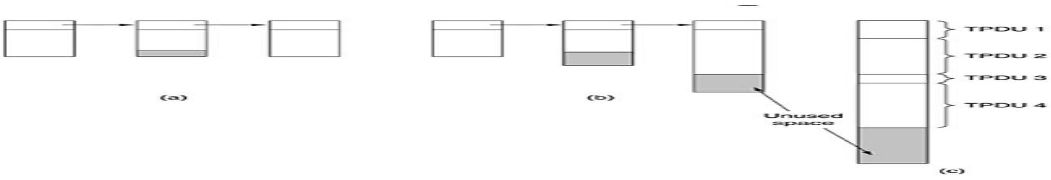
6a) Describe Flow Control and Buffering6M
Description-------------------------------------- 3
Digarm-- 3

Ans:

In the computer network, each node has a certain amount of processor memory available for buffers. Which limits the flow of data in the computer network. Flow control is a function for the control of the data flow within an OSI layer or between adjacent layers. Flow control is a function for the control of the data flow within an OSI layer or between adjacent layers.

Different approaches for buffer organization
Chained fixed-size buffers
Chained variable-sized buffers
One large circular buffer per connection

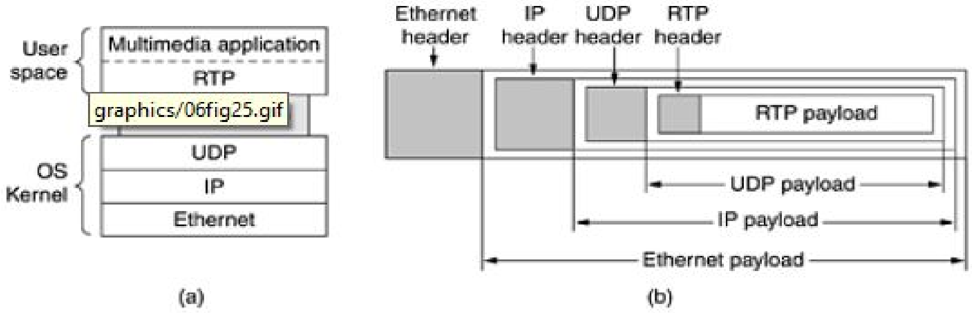
Figure: 3M



(a)Chained fixed-size buffers. (b) Chained variable-sized buffers. (c) One large circular buffer per connection.

6b) Explain in detail about the Real Time transport protocol. 6M
Description-------------------- 3M
Diagram------------------------ 3M
Ans: Client-server RPC is one area in which UDP is widely used. Another one is real-time multimedia applications. In particular, as Internet radio, Internet telephony, music-on-demand, videoconferencing, video-on-demand, and other multimedia applications became more commonplace, people discovered that each application was reinventing more or less the same real-time transport protocol. It gradually became clear that having a generic real-time transport protocol for multiple applications would be a good idea. Thus was **RTP** (**Real-time Transport Protocol**) born.
Diagram **3M**

Figure 6-25. (a) The position of RTP in the protocol stack. (b) Packet nesting.

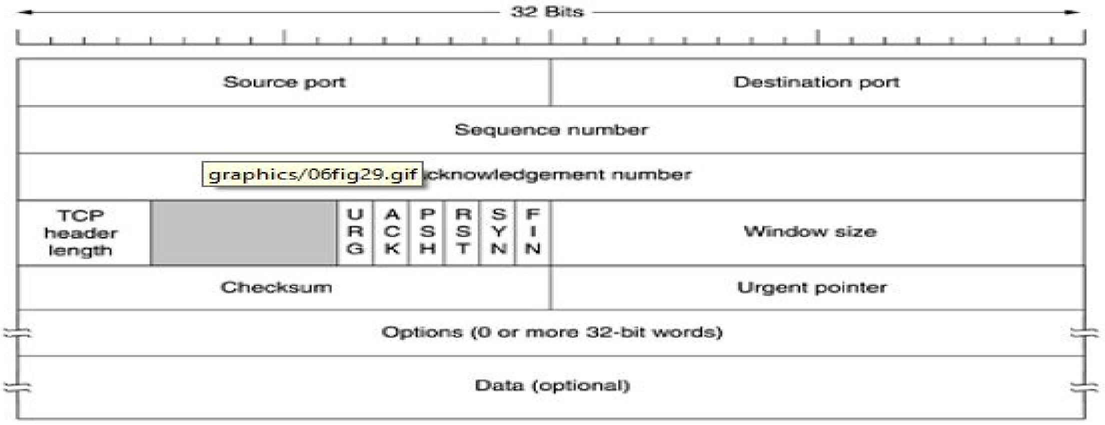


The basic function of RTP is to multiplex several real-time data streams onto a single stream of UDP packets. The UDP stream can be sent to a single destination (unicasting) or to multiple destinations (multicasting). Because RTP just uses normal UDP, its packets are not treated specially by the routers unless some normal IP quality-of-service features are enabled. In particular, there are no special guarantees about delivery, jitter, etc.

(OR)

7a) Describe TCP protocol and TCP Segment header.6M
TCP protocol Description------------------------------- 3M
TCP Segment headerDiagram------------------------- 3M
TCP protocol Description: 3M
Ans:
TCP (**Transmission Control Protocol**) was specifically designed to provide a reliable end-to-end byte stream over an unreliable internetwork. An internetwork differs from a single network because different parts may have wildly different topologies, bandwidths, delays, packet sizes, and other parameters. TCP was designed to dynamically adapt to properties of the internetwork and to be robust in the face of many kinds of failures.
The basic protocol used by TCP entities is the sliding window protocol. When a sender transmits a segment, it also starts a timer. When the segment arrives at the destination, the receiving TCP entity sends back a segment (with data if any exist, otherwise without data) bearing an acknowledgement number equal to the next sequence number it expects to receive. If the sender's timer goes off before the acknowledgement is received, the sender transmits the segment again.
TCP Segment header Diagram 3M

Figure 6-29. The TCP header.



The *Source port* and *Destination port* fields identify the local end points of the connection. The*Sequence number* and *Acknowledgement number* fields perform their usual functions. The *TCP header length* tells how many 32-bit words are contained in the TCP header. This information is needed because the *Options* field is of variable length, Now come six 1-bit flags. *URG* is set to 1 if the *Urgent pointer* is in use. The *Urgent pointer* is used to indicate a byte offset from the current sequence number at which urgent data are to be found. The *ACK* bit is set to 1 to indicate that the *Acknowledgement number* is valid. If *ACK* is 0,

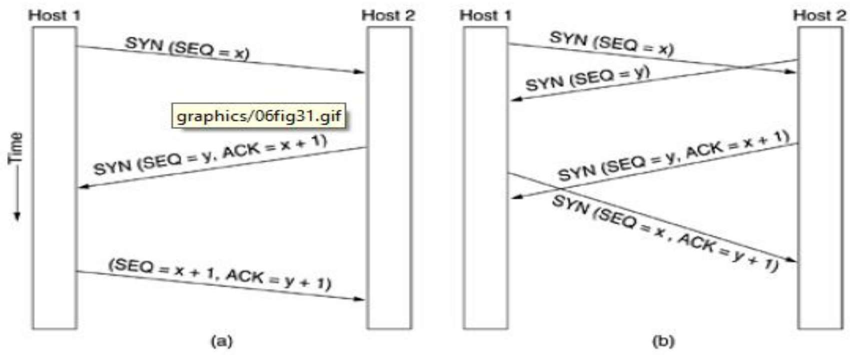
the segment does not contain an acknowledgement so the *Acknowledgement number* field is ignored.
The *PSH* bit indicates PUSHed data. The *RST* bit is used to reset a connection The *SYN* bit is used to establish connections. The *FIN* bit is used to release a connection. A*Checksum* is also provided for extra reliability.

7b) Illustrate TCP Connection establishment with relevant figure6M
TCP Connection establishment---------------------- 3M
TCP Connection establishment Diagram----------- 3M

Connections are established in TCP by means of the three-way handshake discussed in Sec. 6.2.2. To establish a connection, one side, say, the server, passively waits for an incoming connection by executing the LISTEN and ACCEPT primitives, 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.

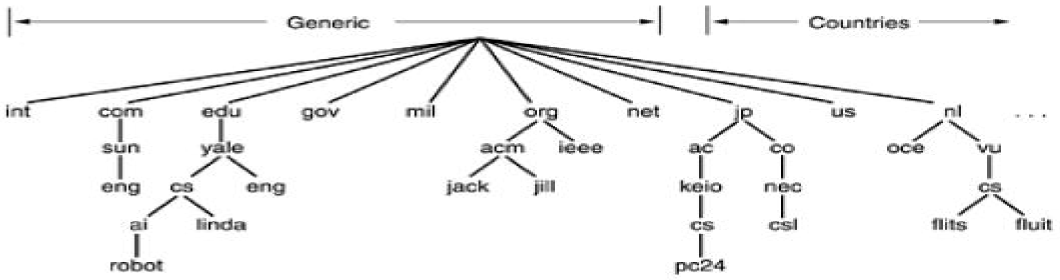
Figure 6-31. (a) TCP connection establishment in the normal case. (b) Call collision.


Host 1
Host 2
SYN (SEQ = x)
graphics/06fig31.gif
Time
SYN (SEQ = y, ACK = x + 1)
(SEQ = x + 1, ACK = y + 1)
(a)
Host 1
Host 2
SYN (SEQ = x)
SYN (SEQ = y)
SYN (SEQ = y, ACK = x + 1)
SYN (SEQ = x, ACK = y + 1)
(b)

UNIT – IV

8a) Explain DNS Name Space in detail. 6M
Description DNS Name Space---------------- 3M
Diagram for DNS Name Space---------------- 3M
Ans: DNS Name Space: 4M
The Internet is divided into over 200 top-level **domains**, where each domain covers many hosts. Each domain is partitioned into subdomains, and these are further partitioned, and so on. All these domains can be represented by a tree, as shown in Fig. 7-1. The leaves of the tree represent domains that have no subdomains (but do contain machines, of course). A leaf domain may contain a single host, or it may represent a company and contain thousandsof hosts.
Diagram for DNS Name Space 2M

Figure 7-1. A portion of the Internet domain name space.



The top-level domains come in two flavors: generic and countries. The original generic domains were *com (commercial)*, *edu* (educational institutions), *gov* (the U.S. Federal Government), *int* (certain international organizations), *mil* (the U.S. armed forces), *net* (network providers), and *org* (nonprofit organizations). The country domains include one entry for every country, as defined in ISO 3166. In November 2000, ICANN approved four new, general-purpose, top-level domains, namely, *biz* (businesses), *info* (information), *name* (people's names), and *pro* (professions, such as doctors and lawyers). In addition, three more specialized top-level domains were introduced at the request of certain industries. These are *aero* (aerospace industry), *coop* (co-operatives), and *museum* (museums). Other top-level domains will be added in the future.

8b) Describe Email Architecture and Services. 6M
Description for Email System-------------------3M
Services for Email System---------------------- 3M
Ans:

Email System: 3M

The Email System normally consist of two subsystems: the **user agents**, which allow people to read and send e-mail, and the **message transfer agents**, which move the messages from the source to thedestination. The user agents are local programs that provide a command-based, menu-based, or graphical method for interacting with the e-mail system. The message transfer agents are typically system **daemons**, that is, processes that run in the background. Their job is to move e-mail through the system.Typically, e-mail systems support five basic functions. Let us take a look at them.

Services for Email System: 3M

Composition refers to the process of creating messages and answers. Although any text editor can be used for the body of the message, the system itself can provide assistance with addressing and the numerous header fields attached to each message.

Transfer refers to moving messages from the originator to the recipient. In large part, this requires establishing a connection to the destination or some intermediate machine, outputting the message, and releasing the connection.

Reporting has to do with telling the originator what happened to the message. Was it delivered? Was it rejected? Was it lost?

Displaying incoming messages is needed so people can read their e-mail. Sometimes conversion is required or a special viewer must be invoked,

Disposition is the final step and concerns what the recipient does with the message after receiving it. Possibilities include throwing it away before reading, throwing it away after reading, saving it, and so on.

(OR)

9a) Write about DNS Resource Records. 6M
Description for DNS Resource Records-------------------------- 2M
Description for DNS Resource record five-tuple----------------- 2M
Description for DNS Resource record type table ---------------- 2M
Ans:

DNS Resource Records: 2M

Every domain, whether it is a single host or a top-level domain, can have a set of **resourcerecords**associated with it. For a single host, the most common resource record is just its IP address, but many other kinds of resource records also exist. When a resolver gives a domain name to DNS, what it gets back are the resource records associated with that name. Thus, the primary functionof DNS is to map domain names onto resource records. A resource record is a five-tuple.

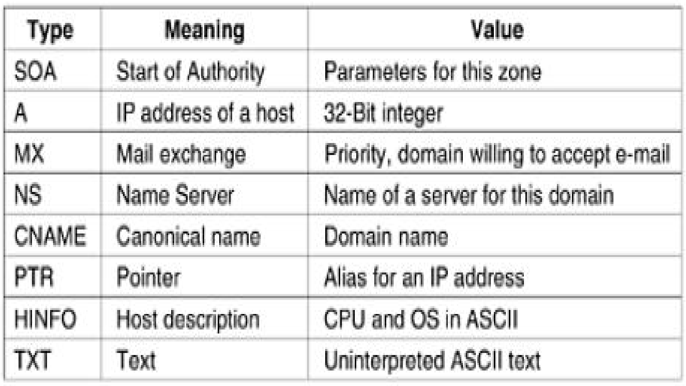
Domain_name Time_to_live Class Type Value 2M

The *Domain_name* tells the domain to which this record applies. Normally, many records existfor each domain and each copy of the database holds information about multiple domains.The *Time_to_live* field gives an indication of how stable the record is. Information that is highly stable is assigned a large Value, such as 86400 (the number of seconds in 1 day). Information that is highly volatile is assigned a small value,such as 60 (1 minute).The third field of every resource record is the *Class*. For Internet information, it is always *IN*. Finally, we have the *Value* field. This field can be a number, a domain name, or an ASCII string. The semantics depend on the record type.

DNS Resource record type table 2M

The *Type* field tells what kind of record this is. The most important types are listed in Fig. 7-2.

Figure 7-2. . The principal DNS resource record types for IPv4.



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

9b) Explain Static and Dynamic Web documents of world wide web.6M

Description for Static Documents---------------------------3M

Description for Dynamic Documents-----------------------3M

Ans:

Static documents: **3M**

A static web document resides in a file that it is associated with a web server. The author of a static document determines the contents at the time the document is written. Because the contents do not change, each request for a static document results in exactly the same response.

Static Advantages: simplicity, reliability and performance. The browser can place a copy in a cache on a local disk.

Static Disadvantages:inflexibility, changes are time consuming because they require a human to edit the file.

Dynamic documents **3M**

Dynamic documents: A dynamic web document does not exist in a predefined form. When a request arrives the web server runs an application program that creates the document. The server returns the output of the program as a response to the browser that requested the document. Because a fresh document is created for each request, the contents of a dynamic document can vary from one request to another.

Dynamic Advantages: ability to report current information (current stocks prices, current weather conditions, current availability of tickets for a concert). Because both static and dynamic documents use HTML, a browser does not know whether the server extracted the page from a disk file or obtained the page dynamically from a computer program.

Dynamic Disadvantages: increased cost and, like a static document, a dynamic document does not change after a browser retrieves a copy. Thus, information in a dynamic document begins to age as soon as it as been sent to the browser (stock prices). Server push. The server runs the programs periodically and sends the new document to the browser

Signature of the HOD.

Signature of the internal Examiner (B. Krishnaiah)

Name of the external Examiners	Name of the college	Dept.	Signature