# Sixth Semester Theory Examination 2009-10

## COMPUTER NETWORKS

**Time : 3 Hours** **Total Marks : 100**

*Note : (i) Attempt **all** questions.*

*(ii) You may make suitable assumptions where necessary.*

**1. Attempt *any four* of the following :**

**Q. 1. (a) Which OSI layer handles each of the following ?**

**(i) Framing (ii) Routing**

**Ans. (i) Framing :** Framing is done by Data Link Layer. It is a technique to break the bit stream into discrete frames and compute the checksum for the same. When a frame arrives at the destination, the checksum is recomputed. If the newly checksum is different from the one contained in the frame, the data link layer knows that an error has occurred and deals with it.

**(ii) Routing :** They have access to network layer addresses and contain software that enables them to determine which of several possible paths between those addresses is the best for a particular transmission. Routers operate in the physical, data link and network layers of the OSI model.

Routers relay packets among multiple interconnected networks. They route packets from one network to any of a number of potential destination networks on an internet.

**Q. 1. (b) What are the two reasons for using layered protocols ?**

**Ans.** The following are the two main reasons for using layered protocols :

1. It helps to prevent changes in one layer from affecting other layers. This helps to expedite technology development.

2. Work loads can be evenly distributed which means that multiple activities can be conducted in parallel thereby reducing the time taken to develop, debug, optimize and package new technologies ready for production implementation.

**Q. 1. (c) How much minimum bandwidth is required to digitally transmit a analog stream which is generated at 50 kHz after Manchester encoding ?**

**Ans.** We know that

A sampling rate of twice of the frequency.

So, sampling rate = $2 \times 50000$

$= 100000$

samples/seconds

A analog signal require twice the bandwidth of the original signal.

So, B.W. = $2 \times 50000 = 100000$

B.W. = 100 kHz

So, 100 kHz bandwidth is required to digitally transmit a analog stream.

**Q. 1. (d) State with reasons if circuit switching is better suited for real time traffic.**

**Ans.** Circuit switching is not an efficient method for routing any kind of data, whether it is digital voice or user data. The circuit is wasted much of the time because no transmission is using the bandwidth of the circuit 100 percent of the time. Any time there are idle period on the circuit, the circuit is being wasted. It would be much more efficient to have a transmission facility capable of transmitting many different conversations over the same circuit at the same time.

Circuit switching enables performance guarantees such as guaranteed maximum delay, which is essential for real time applications like voice conversations. It is also much easier to do detailed accounting for circuit-switched network usage.

**Q. 1. (e) What are the number of cable links required for $n$ devices connected in mesh, ring, bus and star topology ?**

**Ans. Mesh :** In a mesh topology, every device has a dedicated point-to-point link to every other device. A fully connected mesh network has $\frac{n(n-1)}{2}$ physical channels to link $n$ devices and to accomodate that many links, every device on the network must have $n-1$ input/output ports.

**Ring :** In a ring topology, each device has a dedicated point-to-point line configuration only with the two devices on either side of it.

To connect $n$ devices in a ring topology, we need $n$ cable links. An eight-device ring needs eight cable links.

**Star :** In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub.

To connect $n$ devices in a star topology, we need $(n-1)$ cable links.

**Bus :** One long cable acts as a backbone to link all the devices in the network. Nodes are

connected to the bus cable by drop lines and taps.

If we consider bus as device, then $(n-1)$ cable links are required; otherwise $n$ links are required.

**2. Attempt *any four* parts of the following :**

**Q. 2. (a) Write three major problems with CDMA (Code Division Multiple Access).**

**Ans.** The three major problems with CDMA are :

1. As one of the major problems facing the development of telecommunications, bandwidth demand has driven the search for protocols that could be used to maximize bandwidth efficiency. Multiple accesses enable multiple signals to occupy a single communication channel.

2. The near-far problem is common in CDMA. It is a condition in which a strong signal captures a receiver making it impossible for the receiver to detect a weaker signal. It is very difficult in CDMA systems where transmitters share transmission frequencies and transmission time.

3. Third problem is the antenna volume. An antenna is supposed to occupy a certain volume in order to operate in a particular frequency. That is, the phone needs a certain space inside its housing for an internal antenna. Usually the space is limited, therefore smaller antennas are always desirable. Also, since an antenna requires a bigger volume for a lower frequency, the handset using a comparably low frequency range for a CDMA band requires more volume. That is, designing internal antennas for the handset using the lower frequency ranges can be more challenging.

**Q. 2. (b) 128 input callers are to be connected to 128 outputs. Using the 3-stage switching structure. If there are 16 first stage and third stage matrices then how many cross points are needed if the structure is to be non-blocking.**

**Ans.** Let us compare the number of cross points in a 128 by 128 single. Stage cross bar switch with the 128-by-128 multistage switch. In the single stage switch, we need 16384 crosspoint $(128 \times 128)$.

In multistage switch or three stage switch using we need.

- 16 first stage switch, each with 32 crosspoints $(8 \times 4)$, for a total of 512 crosspoints at the first stage.
- 6 second-stage switches, each with 16 crosspoints $(4 \times 4)$, for a total of 96 crosspoints at the first stage.
- 16 third stage switches, each with 32 crosspoints $(8 \times 4)$, for a total of 512 crosspoints at last stage.

The total number of crosspoints required by our multistage switch is 1120.

**Q. 2. (c) What are the problems encountered when IEEE 802.4 LAN as source is connected to IEEE 802.3 LAN as destination ?**

**Ans.** IEEE 802.4 is also referred to as taken Bus or Ethernet Bus. There were two main problems with 802.3, first due to probabilistic MAC protocol, with a bad luck a station might have to wait for a long time to transmit and secondly 802.3 frames do not have priorities which made it unsuited for real-time systems.

Ethernet (IEEE 802.3) is not a suitable protocol for this purpose because the number of collisions is not predictable and the delay in sending data from the control centre to the computers along the assembly line is not a fixed value.

**Q. 2. (d) What is the band rate of the standard 10 Mbps 802.3 LAN ? Explain your answer ?**

**Ans.** 10 Mbps Ethernet uses Manchester encoding where each symbol is represented by 2 bit sequence. Hence, the bits/symbol is 2.

Since, Data rate = bits/symbol × symbol/seconds.

Symbols/seconds = band rate = 5 mega band.

**Q. 2. (e) Explain the binary exponential back off algorithm ?**

**Ans.** Binary exponential backoff algorithm is used in 802.3. Medium Access Control (MAC) sublayer protocol. It is used to try to minimize the probability of collision. When 2 or more devices detect that the network is idle and end up trying to send packets at the same time a collision happens. If the station has a collision for 1st time it would wait for 0 or 1 time dot before trying again, as per this algorithm. After the second collision both will pick up either 0, 1, 2 or 3. When third time collision happens the number of slots to wait is chosen at random from 0 to $2^3 - 1$. After 1 collision the random number will be between $2^i - 1$. After 10 collisions have been reached, the randomisation interval is frozen at 1023. After 16 collisions the controllers makes the station stop contesting and reports failure.

**3. Attempt *any two* parts of the following :**

**Q. 3. (a) What are the network number,**

**subnet number, and host number for address 135.104. 192.100, mask 255.255.128.0 ?**

Ans. IP address 135.104.192.100
Mask 255.255.128.0
Network number = 135.104
Subnet number = 135.104.128.0
Host number = 16, 484

Because IP address is a class B address since 135 (base 10) = × 87 = 10000111 (base 2).

and the subnet number is 1 since the high-order bit of the octel 192 is a 1;

Here 192 = 11000000 (base 2) = × CO,

The host number is ×4064 or 16, 484 (base 10).

**Q. 3. (b) (i) Explain ARP (address resolution protocol) and RARP (reverse ARP) ? What is an ARP-cache ?**

**Ans. ARP :** ARP is a protocol used by the Internet protocol, specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol. The protocol operates below the network layer as a part of the interface between the OSI network and OSI data link layer.

For two machines on a given network to communicate, they must know the other machine's physical addresses. By broadcasting ARPs, a host can dynamically discover the MAC-layer address corresponding to a particular IP network-layer address.

The term address resolution refers to the process of finding an address of a computer in a network. The address is "resolved" using a protocol in which a piece of information is sent by a client process executing on the local computer to a server process executing on a remote computer. The information received by the server allows the server to uniquely identify the network system for which the address was required and therefore to provide the required address. The address resolution procedure is completed when the client receives a response from the server containing the required address.

**RARP :** It is the logical inverse of ARP, might be used by diskless workstations that donot know their addresses when they boot. RARP relies on the presence of a RARP server with table entries of MAC-layer-to-IP address mappings.

RARP allows a physical machine in a LAN to request its IP address from a gateway servers ARP table or cache. A network administrator creates a table in a LAN's gateway router that maps the physical machine (or MAC address) addresses to corresponding IP address. When a new machine is set up, its RARP client program requests from the RARP server on the router to be sent its IP address. Assuming that on entry has been set up in the router table, the RARP server will return the IP address to the machine, which can store it for future use. RARP is available for Ethernet, FDDI and taken ring LAN.

**ARP Cache :** To reduce the number of address resolution requests, a client normally caches resolved addresses for a short period of time. The ARP cache is of a finite size, and would become full of incomplete and obsolete entries for computers that are not in use if it was allowed to grow without check. The ARP cache is therefore periodically flushed of all entries. This deletes unused entries and frees space in the cache. It also removes any unsuccessful attempts to contact computers, which are not currently running.

**Q. 3. (b) (ii) Is CIDR network prefix visible outside IP network ? Justify.**

**Ans.** CIDR notation uses a syntax of specifying IP addresses for IPv4 and IPv6, using the base address of the network followed by a slash and the size of the routing prefix, *e.g.*, 192.168.0.0/16 (IPv4).

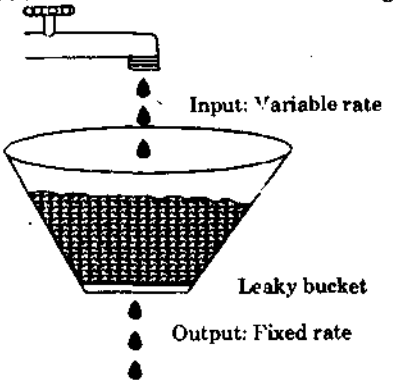
An IP address is part of a CIDR block and is said to match the CIDR prefix if the initial N bits of the address and the CIDR prefix are the same. Thus, understanding CIDR requires that IP address be visualized in binary. Since the length of an IPv4 address has 32 bits, an N-bit CIDR prefix leaves 32-N bits unmatched, meaning that $2^{32-N}$ IPv4 addresses match a given N-bit CIDR prefix. Shorter CIDR prefixes match more addresses, while longer CIDR prefixes match fewer. An address can match multiple CIDR prefixes of different lengths.

CIDR is also used with IPv6 addresses and the syntax semantic is identical. A prefix length can range from 0 to 128, due to the larger number of bits in the address, however, by convention a subnet on broadcast MAC layer networks always has 64-bit host identifiers. Larger prefixes are rarely used even on print-to-print links.

**Q. 3. (c) (i) What are the limitations of leaky bucket algorithm ? How are they resolved ?**

**Ans. Limitations of leaky bucket algorithms :** The behaviour of a switch in a Frame Relay network can be simulated by a leaky bucket. If a bucket has a small hole at the

bottom, the water leaks from the bucket at a constant rate as long as there is water in the bucket. The rate at which the water leaks does not depend on the rate at which the water is input to the bucket. The input rate can vary, but the output rate remains constant (see Fig.)




It is obvious that if more water enters the bucket than is leaked, the time will come when the bucket overflows. The same situation occurs in a packet-switched network such as Frame Relay that does not use flow control. Each switch can send data out at a certain rate. If data are received faster than transmitted, the switch can be congested and discard some frames.

How can the leaky bucket control bursty input ? Imagine water is leaking at the rate of 2 gallons per minute. If we have an input burst with a rate of 10 gallons per minute for a duration of 12 seconds and then nothing during the next 48 seconds, what should be the capacity of the bucket to avoid overflow ? We can find the capacity using the following calculation :

Total water during the burst duration
$= 10 \times (12 / 60) = 2$ gallons.

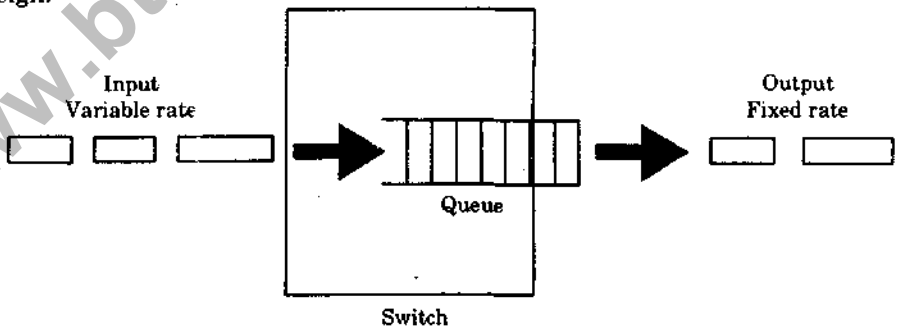
If the capacity of the bucket is two gallons, it can hold the water for the duration of the burst and let it leak continuously for a period of one minute. Note that the capacity can be slightly less than two gallons because some of the water is leaking out during the burst interval. It is customary to use the upper limit.

We can apply the idea to each output interface of each switch in Frame Relay. The output is a fixed rate (1.544 Mbps for example), while the input can be bursty. The switch can use a queue (buffer) to serve as the bucket. The bursty data can be stored in the queue and then sent at the fixed rate.

For example, imagine a switch with only one input and one output interface. If the data rate at the output interface is 1.544 Mbps and the input data are bursty with a rate of 40 Mbps for the duration of 100 milliseconds (and nothing else until the next second), what should be the size of the queue ?

40 Mbps × (100/1000) = 4 megabits

The output interface should have a queue (buffer) of 4 million bits or half a million bytes. Figure shows the design.




But how can we control the output data rate to be always less than a fixed rate (for example, 1.544 Mbps) in a packet-switched network where the size of each packet can be different ? We can use a counter and clock. At the tick of the clock (the beginning of the second, for example), the counter is set to the amount of data that can be output in one tick (usually in bytes). The algorithm then checks the size of the frame at the front of the queue. If the size is less than or equal to the value of the counter, the packet is sent; if the size is greater than the value of the counter, the packet is left in the queue and waits for the next tick of the clock. So example are clear that we can resoled if.

**Q. 3. (c) (ii) Write a brief note on traffic shaping ?**

**Ans.** Traffic shaping is a mechanism to control the amount and the rate of the traffic sent to the network to improve Qos. It is a method used for congestion control. (Congestion control is a method to manage network and internetwork traffic to improve through put). It

helps the packets to be transmitted at a more predictable rate. This approach to congestion management is widely used in ATM networks and is referred to as traffic shaping.

Two algorithms used for this are :

1. The leaky bucket algorithm.
2. The token bucket algorithm.

**4. Attempt *any two* parts of the following :**

**Q. 4. (a) Explain TCP congestion control algorithm in Internet ?**

**Ans. Nagle's Algorithm :** To solve the problem of congestion of WAN, the Nagle algorithm is used. The Nagle algorithm says that when TCP connection has outstanding data that has not yet been acknowledged, small segment cannot be sent until the outstanding data is acknowledged. Instead small amounts of data are collected by TCP and sent in a single segment when the acknowledgement arrives. The Nagle algorithm is self clocking. The faster the ACKs come back, the faster the data is sent. But on a slow WAN, where it is desired is reduce the number of tiny grams, fewer segments are sent. Nagle's algorithm is widely used by TCP implementations. The example is X window system server. Mouse movements must be delivered without delay to provide real time feedback for control called a sliding window protocol working is same as sliding window protocol in data link layer.

The problem occurs when data is passed to the sending entity in large blocks, but an interactive application on receiving side reads data 1 byte at a time. Initially buffer on receiving side is full and sender knows this (*i.e.*, has a window of size 0). Then the interactive application reads one character from TCP stream. This is good for TCP, so it sends a window update to the sender that it is all right to send a byte. The sender obligies and sends 1 byte. The buffer is now full so receives acknowledgement of 1-byte segment but sets a window too. This behaviour can go on forever.

**Q. 4. (b) Explain TCP segment header ? Also discuss the TCP connection management ?**

**Ans. The TCP Segment :** The scope of the services provided by TCP requires that the segment header be extensive (see Fig.). A comparison of the TCP segment format with that of a UDP user datagram shows the differences between the two protocols. TCP provides a comprehensive range of reliability functions but sacrifices speed (connections must be established, acknowledgements waited for, etc.). Because of its smaller frame size, UDP is much faster than TCP, but at the expense of reliability. The description of each field is in order.

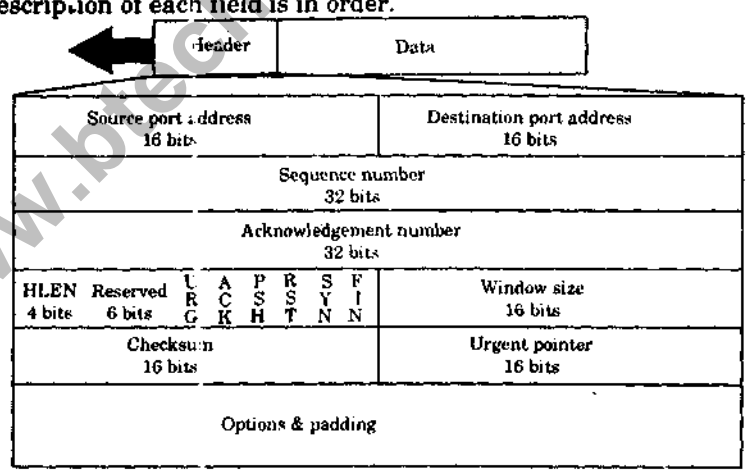



**Fig. TCP segment format.**

- **Source port address.** The source port address defines the application program in the source computer.
- **Destination port address.** The destination port address defines the application program in the destination computer.
- **Sequence number.** A stream of data from the application from the application program may be devided into two or more TCP segments. The sequence number field shows the position of data in the original data stream.
- **Acknowledgement number.**
- **Header Length (HLEN)**
- **Reserved.**
- **Control.**
- Window size
- Check sum
- Urgent Pointer

• Option and Padding.

**TCP Connection Management :** Transport layer connection-oriented protocols are responsible for the series of communications required to establish a connection, maintain it as data is sent over it and then terminate the connection when it is no longer required.

**Three-way handshake :**

**Step 1 :** Client end system sends TCP SYN control segment to server.

• Specifies initial seq #.

**Step 2 :** Server end system receives SYN, replies with SYNACK control segment.

• ACKs received SYN.
• Allocates buffers.
• Specifies server → receiver initial seq. #.

**Q. 4. (c) Discuss various QoS (quality of services) primitives looked at transport layer.**

**Ans. The quality of service (QoS)** defines a set of attributes related to the performance of the connection. For each connection, the user can request a particular attribute. Each service class is associated with a set of the attributes. We can categorize the attributes into those related to the user and those related to the network. Figure shows the two categories and some important attributes in each category.

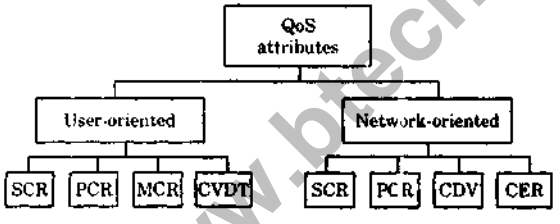


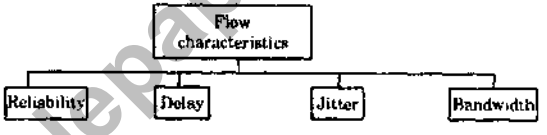

**Figure : Qos**

**User Related Attributes :** User related attributes are those attributes that define how fast the user wants to send data. These are negotiated at the time of contract between a user and a network. The following are some user-related attributes :

- **SCR.** The **sustained cell rate (SCR)** is the average cell rate over a long time interval. The actual cell rate may be lower or higher than this value, but the average should be equal to or less than the SCR.
- **PCR.** The **peak cell rate (PCR)** defines the sender's maximum cell rate. The user's cell rate can sometimes reach this peak, as long as the SCR is maintained.
- **CVDT.** The **cell variation delay tolerance (CVDT)** is a measure of the variation in cell transmission times. For example, if the CVDT is 5 ns, this means that the difference between the minimum and the maximum delays in delivering the cells should not exceed 5 ns.

**Various Quality of Services Primitives looked at Transport Layer :** Quality of service (QoS) is an internetworking issue that has been discussed more than defined. We can informally define quality of service as something a flow seeks to attain.

**Flow Characteristics :** Traditionally, four type of characteristics are attributed to a flow, reliability, delay, jitter, and bandwidth, as shown in figure.




**Reliability :** Reliability is a characteristic that a flow needs. Lack of reliability means losing a packet or acknowledgement, which entails retransmission. However, the sensitivity of application programs to reliability is not the same. For example it is more important that electronic mail, the transfer, and Internet access have reliable transmissions than telephony or audio conferencing.

**Delay :** Source-to-destination delay is another flow characteristic. Again applications can tolerate delay in different degrees. In this case, telephony, audio conferencing, video conferencing, and remote log-in need minimum delay, while delay in file transfer or e-mail is less important.

**Jitter :** Jitter is the variation in delay for packets belonging to the same flow. For example, if four packets depart at times 0, 1, 2, 3 and arrive at 20, 21, 22, 23, all have the same delay, 20 units of time. On the other hand, if the above four packets arrive at 21, 23, 21 and 28, they will have different delays : 21, 22, 19 and 24.

For applications such as audio and video, the first case is completely acceptable; the second case is not. For these applications, it does not matter if the packets arrive with a short or long delay as long as the delay is the same for all packets. For this application, the second case is not acceptable.

Jitter is defined as the variation in the packet delay high jitter means the difference between delays is large; low jitter means the

variation is small.

**Bandwidth :** Different applications need different bandwidths in video conferencing we need to send millions of bits per second to refresh a color screen while the total number of bits in an e-mail may not reach even a million.

**5. Attempt *any two* parts of the following :**

**Q. 5. (a) (i) When web pages are sent out, they are prefixed by MIME headers. Why ?**

**Ans.** A mail message was defined as a block of plain text preceded by specially defined headers specifying routing or other information about the message (*e.g.*, where the message was from, who it was to, whom copies were sent to, etc.). This specification said little about the format of message content. At the time, e-mail messages were plain text files so that concerns about the format of content were unwarranted.

Today there is enormous demand for e-mail that can deliver messages containing components such as HTML text documents, image files, sound and even video data in addition to regular text. However, such messages can be widely communicated only if all mail-handling programs share a standard for constructing, encoding and transporting such complex, multipurpose, messages.

The MIME protocol provides this common standard. MIME provides an extensive format for including multimedia components within a mail message. MIME defines several document headers, placed inside the document, that specify such things as the nature of a message, how the message parts are separated, the data content of each part and the encoding scheme used to encode each part.

**Q. 5. (a) (ii) Explain the difference between http and https protocols ?**

**Ans.** HTTP is hypertext transfer protocol which is responsible for transmitting and receiving information across the internet whereas HTTPS is secure http, which is used exchanging confidential information with a server, which needs to be secured in order to prevent unauthorized access.

HTTP is transmitted over the wire via PORT 80 (TCP). You normally use http when you are browsing the web, its not secure and so someone can eavesdrop on the conversation between your computer and the web server. HTTP can support the client asking for a particular file to be sent only if it has been updated after a certain date and time. This would be used if the client has already retrieved a copy of a file by that name from that server, but wants to check to see if it has been updated since then. The server responds either with the updated file, with a message to say the file has not been changed or with a message that the file no longer exists.

HTTPS (Hypertext Transfer Protocol over secure socket layer or HTTP over SSL) is a web protocol developed by netape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the web server. HTTPS is really just the use of Neticape's SSL as a sublayer under its regular HTTP application layering. HTTPS uses port 443. SSL uses a 40-bit key size for the RC4 stream encryption algorithm, new-age browsers use 128-bit key size which is more secure than the former, it is considered an adequate degree of encryption for commercial exchange HTTPs is normally used in login pages, shopping etc.

**Q. 5. (b) What is the difference between active and dynamic web page ? Explain the structure of interface between access of a database over webpages ?**

**Ans.** Difference between static and Dynamic webpages :

1. Static webpages contain the same prebuilt content each time the page is loaded, while the content of dynamic webpages can be generated on the fly.

2. Static webpages include HTML but dynamic webpages include java, JSP.

3. Dynamic pages contain "server-side" code, which allows the server to generate unique content each time the page is loaded. For example : the server may display the current time and date on the webpage.

4. We can easily identify static and Dynamic webpages through their file extensions in the url.

Static webpages contains extension = ".htm" or ".html",

Dynamic webpages contains extension = ".php", ".asp", or ".jsp".

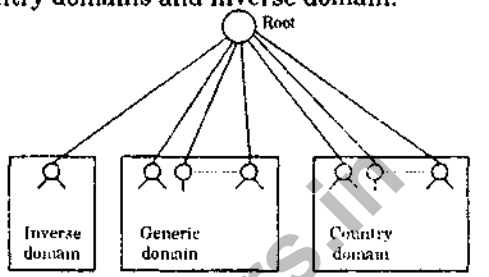
Applications are usually broken into logical chunks called "tiers", where every tier is assigned a role. Traditional applications consist only of 1 tier, which resides on the client machine, but web applications tend themselves to a n-tiered approach by nature. Though many variations are possible, the most common

structure is the 3-tier application. In its most common form, the three tiers are called presentation, application and storage, in this order. A web browser is the first tier, an engine using some dynamic web content technology is the middle tier making queries and updates against the database and generates a user interface. For more complex applications, a 3-tier solution may fall short and you may need a n-tiered approach, where the greatest benefit is breaking the business logic which resides on the application tier or adding an integration tier that separates the data tier from the rest of tiers by providing an easy-to-use interface to access the data. For example, you would access the client data by calling a "list clients ()" function instead of making a SQL query directly against the client table on the database. That allows us to replace the underlying database without changing the other tiers.

**Q. 5. (c) Write short notes on :**

**(i) DNS (ii) SNMP (iii) XML**

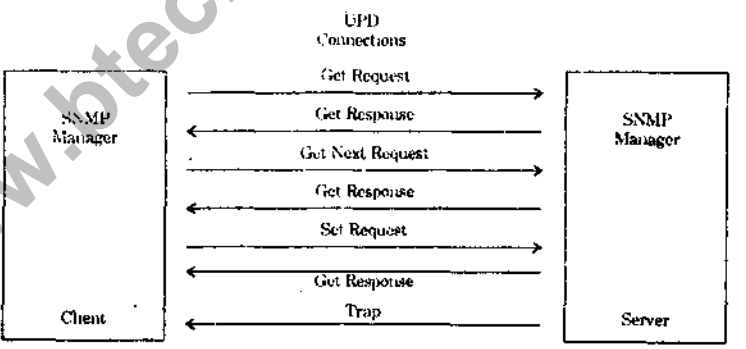
**Ans. (i) DNS :** To identify an entity, TCP/IP protocol use the IP address, which uniquely identifies the connection of a host to the Internet. However; people refer to use names instead of addresses. Therefore, we need a system that can map a name to an address and conversely an address to a name. In TCP/IP, this is the Domain Name System (DNS). DNS is a protocol that can be used in different platforms. In the Internet, the domain name space (tree) is divided into three different sections : generic domains, country domains and inverse domain.




**(ii) SNMP :** The Simple Network Management Protocol (SNMP) is a framework for managing devices in a Internet using the TCP/IP protocol suite. It provides a set of fundamental operations for monitoring and maintaining an Internet. SNMP is an application-level protocol in which a few manager stations control a set of agent. SNMP frees management tasks from both the physical characteristics of the managed devices and the underlying networking technology.

It can be used in a heterogenous internet mode of different LANs and WANs connected by routers or gateways made by different manufacturers.

SNMP defines five message : Get Request, Get Next Request, Set Request, Get Response and Trap.




**(iii) XML :** "XML is a cross-platform, software and hardware independent tool for transmitting information". XML is a W3C recommendations. It stands for Extensible Markup Language (XML). It is a markup language much like HTML used to describe data.

1. XML stands for extensible markup language.

2. XML is markup language much like HTML.

3. XML was designed to describe data.

4. XML tags are not predefined. You must define your own tags.

5. XML uses document type definition or XML schema to describe the data.