

## INTRODUCTION TO INTERNET TECHNOLOGY

### Multiple Choice Type Questions

1. In ..... the IP header of the original packet is also encrypted. [WBUT 2013]  
a) only tunnel mode      b) only transport mode  
c) both tunnel mode and transport mode    d) none of these

Answer: (a)

2. NAT stands for [WBUT 2013]  
a) Native Address Translation      b) Network Address Translation  
c) Network Address Transmission      d) Native Address Transmission

Answer: (b)

3. Which organization defines the Web Standards? [WBUT 2014]  
a) Apple Inc      b) World Wide Web Consortium (W3C)  
c) Microsoft Corporation      d) IBM Corporation

Answer: (b)

4. In telnet, the client echoes the character on the screen but does not send it until a whole line is completed in [WBUT 2014, 2018]  
a) default mode      b) character mode  
c) server mode      d) none of the mentioned

Answer: (a)

5. A web server by default runs on port [WBUT 2015]  
a) 23      b) 25      c) 80      d) 22

Answer: (c)

6. HTTP status code is [WBUT 2015, 2018]  
a) two-digit code      b) three-digit code  
c) four-digit code      d) five-digit code

Answer: (b)

7. Which of the following is a transport layer protocol in the TCP/IP protocol suit? [WBUT 2015]  
a) HTTP      b) UDP      c) SMTP      d) FTP

Answer: (b)

8. What type of protocol is HTTP? [WBUT 2017]  
a) State aware      b) Stateful  
c) Stateless      d) Connection oriented

Answer: (c)

9. Which of the following is not IPv6 address?  
a) Any cast      b) Multicast      c) Unicast  
d) Broadcast  
Answer: (d)
10. Maximum size of the data portion of the IP data gram is  
a) 65555B      b) 65535B      c) 65515B  
these  
d) none of  
Answer: (b)
11. In IPV4, what is length of the data field for given an HLEN value of 12 and length value of 40.000?  
a) 39.988      b) 40.012      c) 40.048      d) 39.952  
Answer: (d)
12. In IPv6 option length is  
a) 4      b) 5      c) 3      d) infinite  
Answer: (d)

#### Short Answer Type Questions

✓ 1. What is servlet? What do you understand by servlet API?  
Describe the life cycle of a servlet.

[WBUT 2016]

OR,

Explain the life cycle of a JAVA servlet.

[WBUT 2016, 2018]

Answer:

1<sup>st</sup> Part:

Servlets provide a component-based, platform-independent method for building Webbased applications, without the performance limitations of CGI programs. Servlets have access to the entire family of Java APIs, including the JDBC API to access enterprise databases.

2<sup>nd</sup> Part:

The Servlet API provides interfaces and classes that are required to build servlets. These interfaces and classes are group into the following two packages:

- javax.servlet
- javax.servlet.http

3<sup>rd</sup> part:

Servlets run on the web server platform as part of the same process as the web server itself. The web server is responsible for initializing, A web server communicates with a servlet through a simple interface, Javax.servlet.Servlet.  
This interface consists of three main methods:

- init()
- service()
- destroy()

and two ancillary methods:

- `getServletConfig()`
- `getServletInfo()`

#### *The init() method*

When a servlet is first loaded, its `init()` method is invoked. This allows the servlet to perform any setup processing such as opening files or establishing connections to their servers. If the servlet has been permanently installed in a server, it loads when the server starts to run.

The `init` method definition looks like this:

```
public void init() throws ServletException {  
    // Initialization code...  
}
```

#### *The service() method:*

The `service()` method is the heart of the servlet. Each request message from client results in single call to the servlet's `service()` method. Each time the server receives a request for a servlet, the server spawns a new thread and calls `service`. The `service()` method checks the HTTP request type (GET, POST, PUT, DELETE, etc.) and calls `doGet`, `doPost`, `doPut`, `doDelete`, etc. methods as appropriate.

Here is the signature of this method:

```
public void service(HttpServletRequest request, HttpServletResponse response)  
throws ServletException, IOException {  
}
```

The `service()` method is called by the container and `service` method invokes `doGet`, `doPost`, `doPut`, `doDelete`, etc. methods as appropriate. So you have nothing to do with `service()` method but you override either `doGet()` or `doPost()` depending on what type of request you receive from the client.

#### *The destroy() method:*

The `destroy()` method is called only once at the end of the life cycle of a servlet. This method gives your servlet a chance to close database connections, halt background threads, write cookie lists or hit counts to disk, and perform other such cleanup activities. After the `destroy()` method is called, the servlet object is marked for garbage collection. The `destroy` method definition looks like this:

```
public void destroy()  
{  
    //Finalization code...  
}
```

#### *2. Discuss an effective communication between a client and a server. [WBUT 2016]*

##### *Answer:*

The communications channel between a client and server is full-duplex: either side can send a message to the other at any time. This is canonically implemented over a TCP/IP socket interface, though other communications channels are often used, including Unix domain sockets, named pipes and shared memory. The channel must provide a reliable, ordered byte stream. When a client first connects to the server, a handshaking procedure

occurs to establish the channel, to verify that the client is authenticated to connect, and to set some communication parameters, such as the byte-endianness to be used. In the early days, it was assumed that the server was a highly capable machine and the client was not. Thus, interestingly, the client may ask the server to provide whichever endianness the client prefers: the server will byte-swap requests and responses as needed.

After that, the client sends request messages to the server, asking the server to perform an operation or to provide some information to the client. Clients typically accumulate requests in a buffer, sending them in batches for more efficient communication handling and context switching.

The server processes the requests from each client in the order received from that client. However, the server is typically multiplexing requests from multiple clients at any given time, and does not guarantee any ordering between clients unless special requests are made to ensure that. Both server and client keep track of the number of requests sent on their connection so far, and use that number as a sequence number for each request to identify it later.

The server sends responses to the client. Many requests from clients are simply handled by the server, and result in nothing being returned to the client if all goes well. If a request is defined to return information, the server sends a response called a reply to the client. The sequence number of the reply identifies the request to which the reply data is a response. Clients may have sent many requests at once to the server, and be waiting for the responses asynchronously. The replies will come back in order, but the client needs to remember the request sequence number to map the reply back to the request that was made.

If there is a problem handling a request, then the server will send an error response to the client. The error response includes the sequence number of the problematic packet, an error code and some additional details about what went wrong. Debugging a failure often involves determining the origin of the errant request. Error responses are usually received well after the client has moved on to later calls, due to the asynchronicity of the protocol; thus the sequence number is invaluable information for client server model.

**Q3. A block of address is given to a small organization. It is known that one of the addresses is 205.16.37.39/28. What is the first and last address in the block? What is 'subnet'? Is 'masking' required at all? What is the difference between default mask and subnet mask?** [WBUT 2016]

**Answer:**

IP address: 205.16.37.39/28

Subnet mask: /28: 11111111.11111111.11111111.11110000

= 255.255.255.240 ✓

205.16.37.39 ✓

AND 255.255.255.240

Network address 205.16.37.32

First address of the block- 205.16.37.32 ✓

Last address of the block- 205.16.37.47 ✓

**Subnet:**

A router uses a concept of masking to filter packets for a particular network, this outputs the Net ID. This property of IP addressing causes problem as the network grows. Also a large network is difficult to maintain and control. To overcome this problem, a concept known as subnets is used, which splits a network into several parts for internal use, but still acts like a single network to the outside world. This method or technique is called as subnet.

Masking is required when the network grows larger. For smaller networks masking is not required. Also modern routers make masking compulsory.

Subnetted or unsubnetted network the router needs to handle masking. For unsubnetted network the masking is done with default mask. For E.g.

- Class A: Default mask-255.0.0.0
- Class B: Default mask-255.255.0.0
- Class C: Default mask-255.255.255.0

For a subnetted network the masking is done with subnet mask. Subnet mask can be boundary level (with values 0 and 255) or non-boundary level (other than 0 and 255).

**4. What do you mean by Internet? Give a comparison for Intranet, Extranet and Internet.** [WBUT 2017]

**Answer:**

Internet: The internet is the largest computer network in the world, connecting millions of computers. A network can be considered as group of two or more computer systems linked together. Computer networks are basically of three main types LAN, MAN and WAN. Internet can be considered as a group of LAN, MAN and WAN and also WWW.

Intranet:

It is the private computer-network that uses internet protocols network connectivity and possibly the public telecommunication system and is owned and used by Private Network. Intranet can also proprietary protocols and services.

Extranet:

It is also a private network that uses internet protocols, network connectivity and public communication system but the system is not limited the organizations employees but can be accessed by trusted outside agencies also like suppliers, distributors, dealers who supply from official store company partners. These can be business partners, collaborators, branch office of companies or some other business houses.

Internet:

It is a public network that uses internet protocols, network connectivity and WWW to be used by everyone.

**5. State the difference between IPv4 and IPv6 packet format.** [WBUT 2017]

**Answer:**

An IPv4 header contains the following fields:

version :  
length:  
type of service :  
total length :  
Identification :  
Flags:  
fragment offset :  
time to live :  
Protocol :  
header checksum:  
Sender address and destination address  
Options  
Padding

Whereas the IPv6 packet format omits the following field:

header length as the length is constant in IPv6.

identification

flags

fragment offset as this is moved into fragmentation extension headers)

header checksum

IPv6 options improve over IPv4 by being placed in separate extension headers that are located between the IPv6 header and the transport-layer header in a packet. Another improvement is that IPv6 extension headers, unlike IPv4 options, can be of arbitrary length and the total amount of options that a packet carries is not limited to 40 bytes. By using extension headers, instead of a protocol specifier and options fields, newly defined extensions can be integrated more easily into IPv6.

#### Q6. Why is HTTP stateless?

[WBUT 2018]

**Answer:**

Interactions between the browser and the web server are governed by a strict set of rules called the hypertext transfer protocol or HTTP. This protocol describes the types of messages the server and the client can send to each other, the meanings of the various fields in those messages, the order in which those messages can be sent, and the way to handle various error conditions. The reason for having a strict set of detailed rules about the allowed interactions is to make it possible for different groups of implementers to build browsers and web server software that can interoperate seamlessly. Such a protocol is just an important special case of an interface that specifies how two parts of the system can interact. As long as the interface is not affected, the different parts can change independently. The implementers of web server software do not need to know about all the browsers implementations in the world, they just need to ensure that their software complies with the protocol. Similarly the implementers of browsers need to ensure that they comply with the protocol and the details of various web server implementations are hidden to them. The Internet has many other protocols that govern other applications

such as email or chat or infrastructure services not directly visible to users. HTTP is a request-reply protocol. The client first initiates a connection with the server, it sends a request with the name of the document it wants and the server sends a reply which normally includes the requested document. HTTP also allows the client to send to the server data the user submits. This feature of HTTP is used for example when you enter in your browser your credit card information and submit it to yatra.com before finalizing your purchase. HTTP conversations may also include other types of context information: the type of the browser, the image formats supported by the browser, etc. Each request-response pair is handled independently. This is why HTTP is called a stateless protocol. This property makes it easier to build fast and reliable servers.

**7. Write the steps required to create the DSN.**

[WBUT 2018]

**Answer:**

A Data Source Name (DSN) is the logical name that is used by Open Database Connectivity (ODBC) to refer to the drive and other information that is required to access data. The name is used by Internet Information Services (IIS) for a connection to an ODBC data source, such as a Microsoft SQL Server database. To set this name, use the ODBC tool in Control Panel.

When you use an ODBC DSN entry to externally store the connection string values, simplify the information that is needed in the connection string. When you do this, changes are made to the data source that are completely transparent to the code. This article describes how to create a system data source name in Windows XP.

**Create a System DSN in Windows XP**

1. Click **Start**, point to **Control Panel**, double-click **Administrative Tools**, and then double-click **Data Sources (ODBC)**.
2. Click the **System DSN** tab, and then click **Add**.
3. Click the database driver that corresponds with the database type to which you are connecting, and then click **Finish**.
4. Type the data source name. Make sure that you choose a name that you can remember. You will need to use this name later.
5. Click **Select**.
6. Click the correct database, and then click **OK**.
7. Click **OK**, and then click **OK**.

**8. What is the difference between DNS and NIS domains?**

[MODEL QUESTION]

**Answer:**

DNS provides a hierarchical hostname management system spanning the entire Internet, each level in the hierarchy designates authoritative name servers that contain maps of hostnames and IP addresses. Whereas NIS is a hostname management system spanning the entire Local Area Network. Mapping of DNS is on a larger scale whereas NIS mapping is on a smaller scale.

### ✓ DNS integration with NIS

. Hostnames are managed in a hierarchy. Each host manages its own name, so the hosts are the "leaf nodes" in this management tree. Hosts are grouped together into NIS or DNS domains, creating a two-level tree. DNS domains may be further grouped together by company, department, or physical location, adding more levels to the management hierarchy. NIS fits into the DNS management scheme at the lowest level in this hierarchy.

Within a single DNS domain, there may be many physical networks with several system administrators. NIS provides a system for the independent management of these small networks; NIS host map information can be combined to form the DNS host file.

So if an Internet DNS is used in conjunction with NIS, it is helpful to tie the NIS domain names to the DNS domain name. Joining NIS and DNS domain names also makes sense if you have a single DNS domain that spans several physical locations. Each office will have its own networks, and its own NIS domains, so using the DNS domain name in the NIS domain name indicates how these locations fit into the "big picture."

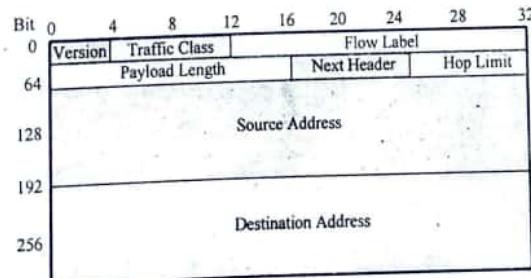
For example, the XYZ Company uses the DNS domain name xyz.com. It has five NIS domains in its company, which uses the XYZ.com DNS domain name. The NIS domain names use the DNS domain name as a suffix:

head-office.xyz.com  
office\_1.xyz.com  
office\_2.xyz.com  
office\_3.xyz.com  
office\_4.xyz.com

### Long Answer Type Questions

- ✓ 1. Draw the various fields in IPv6 packet header. What is the purpose of next header field? [WBUT 2013]

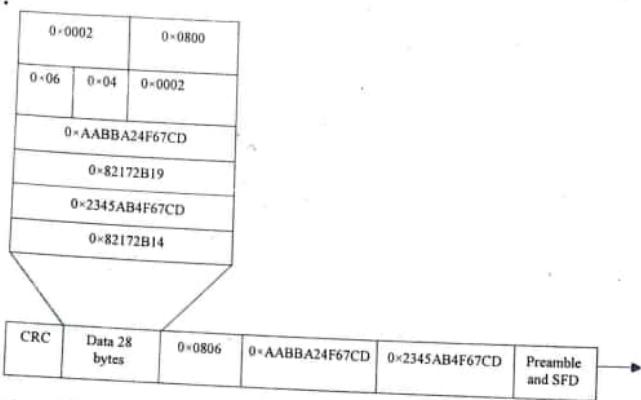
Answer:



Next header: Indicates either the first extension header (if present) or the protocol in the upper layer PDU (such as TCP, UDP, or ICMPv6). When indicating an upper layer protocol above the Internet layer, the same values used in the IPv4 Protocol field are used here.

**Q.** A router with IP address 125.45.23.12 and Ethernet physical address 23:45:AB:4F:67:CD has received a packet for a destination with IP address 125.11.78.10 and Ethernet physical address AA:BB:A2:4F:67:CD. Show the entries in the ARP request packet sent by the router. Encapsulate the ARP request packet in a data link frame. Fill in all the fields. [WBUT 2013]

Answer:



**3. a)** In a class B subnet, the IP address of one of the hosts and the mask are given below:

IP Address : 125.134.112.66  
Mask : 255.255.224.0 [WBUT 2013]

What are the first address (network address) and the last address (broadcast address) in this subnet?

**b)** An organization granted a block of address with the beginning address 14.24.74.0/24. There are 256 addresses in this block. The organization needs to have 11 subnets. 2 subnets each have 64 addresses, 2 subnets each have 32 addresses, 3 subnets each have 16 addresses, 4 subnets each have 4 addresses. Design the subnets. [WBUT 2013, 2015]

**c)** What are content in the header of DNS response packet if a query for rabi@xyz.au.ac.in (let us take IP is 10.3.4.5) and name of server IP is 10.0.0.1?

**d)** What is multicast addressing? Describe the working principle of transport gateway. [WBUT 2013]

Answer:

g) Network address- 125.134.96.0  
Broadcast address-125.134.127.255

**b)** Address block 14.24.74.0/24 and 256 addresses.

2 subnets each of 64

subnet 1: 14.24.74.0-14.24.74.63 subnet address/mask= 255.255.255.192

subnet 2: 14.24.74.64-14.24.74.127 subnet address/mask= 255.255.255.192

2 subnets of 32 address

subnet 3: 14.24.74.128-14.24.74.159 subnet address/mask= 255.255.255.224

subnet 4: 14.24.74.160-14.24.74.191 subnet address/mask= 255.255.255.224  
3 subnets of 16 address

subnet 5: 14.24.74.192-14.24.74.207 subnet address/mask= 255.255.255.240 ✓

subnet 6: 14.24.74.208-14.24.74.223 subnet address/mask= 255.255.255.240 ✓

subnet 7: 14.24.74.224-14.24.74.239 subnet address/mask= 255.255.255.240 ✓

4 subnets of 4 address

subnet 8: 14.24.74.240-14.24.74.243 subnet address/mask= 255.255.255.252 ✓

subnet 9: 14.24.74.244-14.24.74.247 subnet address/mask= 255.255.255.252 ✓

subnet 10: 14.24.74.248-14.24.74.251 subnet address/mask= 255.255.255.252 ✓

subnet 11: 14.24.74.252-14.24.74.255 subnet address/mask= 255.255.255.252 ✓

e)

	0x1333		0x8180
1	1		1
0	0		0
4	'r'	'a'	'b'
'l'	4	'x'	'y'
'z'	3	'a'	'u'
2	'a'	'c'	1
'T'	'n'	0	Contd. in next line
		1	0x10
5	0x0C	1	Contd. in next line
	1	12000	Contd. in next line
		4	10
3	4	5	

d) Multicast addressing – defines a group of computers that may or may not share the same prefix and may or may not be connected to the same physical network. It falls in Class D range of Classfull Ipv4 addressing, ranges from 224.0.0.0 to 239.255.255.255.

4. a) What is the meaning of the term 'Hypertext Transfer Protocol' in World Wide Web environment? [WBUT 2014]

b) What is URL? Explain different component of URL. [WBUT 2014, 2018]

c) Distinguish between GET and POST method in HTTP. [WBUT 2014, 2015]

OR,

Compare POST and GET methods.

[WBUT 2018]

Answer:

a) The Hyper-Text Transfer Protocol (HTTP) is the method used to transfer Web pages to the computer. With hypertext, a word or phrase can contain a link to another Web site that can be opened by clicking the link. The pages of the www are written using HTML.

b) URL stands for Universal resource locator. It is the unique address of resource/file residing at different computer, which can be accessed using browser.

A URL consists of four parts. These parts are the protocol, domain name, path, and filename with optional port number.

http://www.xyz.com:80

http:- This stands for the protocol hyper text transfer protocol used for www or internet.  
:// - This represents the domain name or address of the computer, that is permanently connected to Internet.

www- This field is not compulsory, this only stands for an indication that it is used for world wide web.

xyz.com – name of the resource (computer where it resides). This can be followed by a folder or file name in that computer. Followed by a period (.) and com. It stands for extension name which can be net, gov etc.

:80- Followed by an optional port number which is by default 80 for http. So we generally do not write it. However some sites can have specialized port numbers like 3082 etc. in that case the specific port number has to be written.

- e) GET and POST are two commonly used methods for a request-response between a client and server.

GET- Requests data from a specified resource

POST - Submits data to be processed to a specified resource

The difference between the two methods is as below:

	GET	POST
usage	GET index.html?name1 =value&name2=value HTTP /1.1 HOST:XYZ.com	POST /index.html HTTP/1.1 Host: about.com name=value1 & name2=value2
History	Parameters remain in browser history	Parameters are not saved in browser history
Restriction on data length	These is restriction on data length in GET as it adds the data to the URL (maximum URL length is 2048 characters)	No restrictions
Restriction on data type	Only ASCII characters allowed	No restrictions. Binary data is also allowed.
Security	GET is less secure compared to POST as data is sent as a part of the URL.	POST is somewhat safer than GET because the parameters are not stored in history or web server logs.
Visibility	Data is visible to everyone in the URL.	Data is not displayed in the URL.
Bookmarked	Can be marked	Can not be marked.
Cached	Can be cached	Not cached

5. a) Why MIME is used as an extension of SMTP for e-mail transferring system over network?

[WBUT 2014]

- b) Explain different stages of SMTP email delivery system with the help of a diagram.

[WBUT 2014, 2018]

Answer:

- Multipurpose Internet Mail Extensions (MIME) defines the standard format of mail messages on the Internet. Initially as defined in RFC 822 (1983), a mail message using SMTP can only comprise lines of ASCII text with the maximum length of each line set at

1000 characters. The sending user agent (UA) converts each character into NVT ASCII (i.e. into 8-bit form). However, as the use of Internet became widespread, demand for alternative message types, which can incorporate binary data and other media types such as audio and video including multimedia, increased. Moreover, messages can contain different languages and alphabets. This led to the introduction of the MIME standard as an extension to the RFC 822 standard. The corresponding RFCs are referred to as RFCs 2045/8. The aim of MIME is to allow alternative media types in messages using same message transfer system by adding a number of extra header fields to the existing ones. Thus MIME is an extension of SMTP.

b) The actual mail transfer is done through Mail Transfer Agents (MTAs). To send mail, a system must have a client MTA; and to receive mail, a system must have a server MTA. In the Internet, message transfer is done through a protocol (and software) named Simple Mail Transfer Protocol (SMTP). To send a message, we need a client SMTP and a server SMTP. In Fig.1 we show Alice sending an email to Bob with the SMTP clients and servers needed. Mail transfer occurs between the two mail servers, one at Alice's site and the other at Bob's site. The mail servers can belong to the ISPs to which Alice and Bob are subscribers, or they can belong to the companies where Alice and Bob work.

**Commands and Responses:** SMTP uses commands and responses to transfer messages between an MTA client and an MTA server. Each command or reply is terminated by a two-character (carriage return and line feed) end-of-line token.

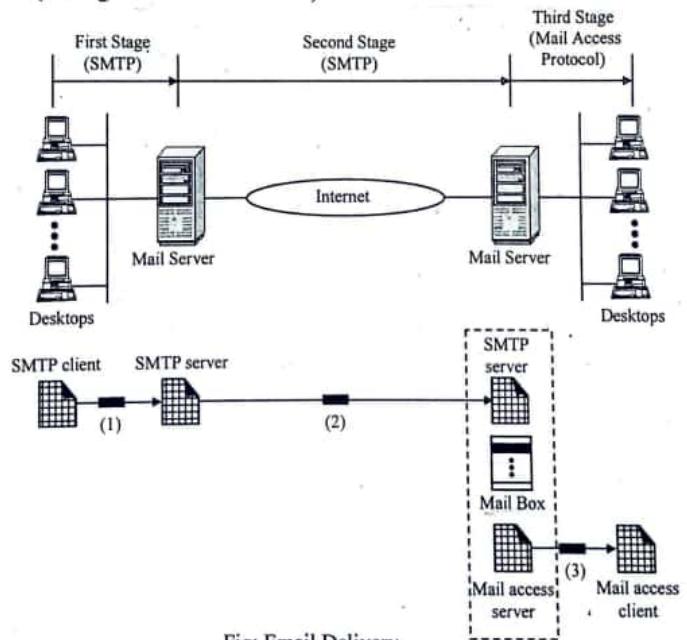


Fig: Email Delivery

- **First Stage:** Here, the email goes from the user agent to the local server. The mail does not go directly to the remote server because the remote server may not be available at all times. Therefore, the mail is stored in the local server until it can be sent. The user agent uses SMTP client software, and the local server uses SMTP server software.
  - **Second Stage:** In the second stage, the email is relayed by the local server, which now acts as the SMTP client, to the remote server, which is the SMTP server in this stage. The email is delivered to the remote server, not to the remote user agent. The reason is that SMTP messages must be received by a server that is always running since mail can arrive at any time. However, people often turn off their computers at the end of the day, and those with laptops or mobile computers do not normally have on all the time. So usually an organization (or ISP) assigns a computer to be the email server and run the SMTP server program. The email is received by this mail server and stored in the mailbox of the user for later retrieval.
  - **Third Stage:** In the third stage, the remote uses a mail access protocol such as POP3 or IMAP4 to access the mailbox and obtain the mail.

6. Explain briefly about the TCP/IP protocol suit.

[WBUT 2015]

**Answer:**

A majority of the internet uses a protocol suite called the Internet Protocol Suite also known as the TCP/IP protocol suite. This suite is a combination of protocols which encompasses a number of different protocols for different purpose and need. Because the two major protocols in this suites are TCP (Transmission Control Protocol) and IP (Internet Protocol), this is commonly termed as TCP/IP Protocol suite. This protocol suite has its own reference model which it follows over the internet.

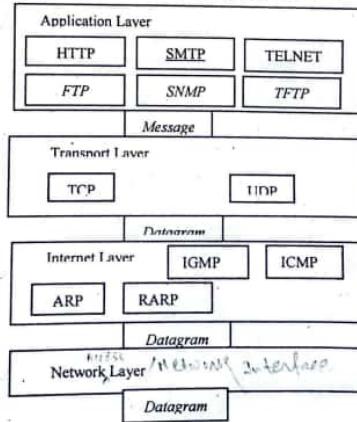


Fig: Different protocols in the four layers of TCP/IP

7. Discuss Congesting Policy. Congestion Avoidance and Congestion Detection in TCP with relevant diagrams. [WBUT 2016]

Answer:

Congestion, in the context of networks, refers to a network state where a node or link carries so much data that it may deteriorate network service quality, resulting in queuing delay, frame or data packet loss and the blocking of new connections. In a congested network, response time slows with reduced network throughput. Congestion occurs when bandwidth is insufficient and network data traffic exceeds capacity.

Data packet loss from congestion is partially countered by aggressive network protocol retransmission, which maintains a network congestion state after reducing the initial data load. This can create two stable states under the same data traffic load - one dealing with the initial load and the other maintaining reduced network throughput.

There are two strategies used generally for congestion control open-loop congestion control and closed-loop congestion control. The open-loop strategy attempts to solve the problem by providing a good design before the system is up and running. These solutions are generally static in nature as they do not take change according to the current state of operations of the system. They are also called as open-loop strategies which are further divided on the basis of whether these acts on source or destination ends. The second category is based on the concept of feedback. They are called as feedback strategies or closed-loop strategies. These solutions work by taking into consideration the system parameters and giving feedback to the portions of the subnet that can take action to reduce the congestion.

#### Congestion avoidance in TCP

Congestion can occur when data arrives on a large bandwidth link and gets sent out a smaller bandwidth link. Congestion can also occur when multiple input streams arrive at a router whose output capacity is less than the sum of the inputs. This leads to loss of packets and subsequent delays in transmission. Thus reducing bandwidth. Congestion avoidance is a way to deal with lost packets. Originally TCP did not have provision for handling congestion. Additive-increase/multiplicative-decrease (AIMD) was the first feedback control approach that is the primary mechanism for adjusting the rate of a TCP flow, i.e. answering the question "How fast should I send?". Though AIMD was never included as a part of TCP. There are 3 versions of TCP for congestion control

- TCP Tahoe
  - This is the original version of TCP congestion avoidance as implemented by Jacobson
  - Uses: *Slow Start*
  - and: *Fast Retransmit*
- TCP Reno
  - is equal to TCP Tahoe plus
  - *Fast Recovery*
- TCP Vegas
  - This is completely new implementation based on delay variation (instead of packet loss as in the previous 2 versions of TCP)

## POPULAR PUBLICATIONS

### Congestion detection in TCP

Two common ways to detect congestion are timeout and duplicate acknowledgement.

8. a) Describe IP datagram format.

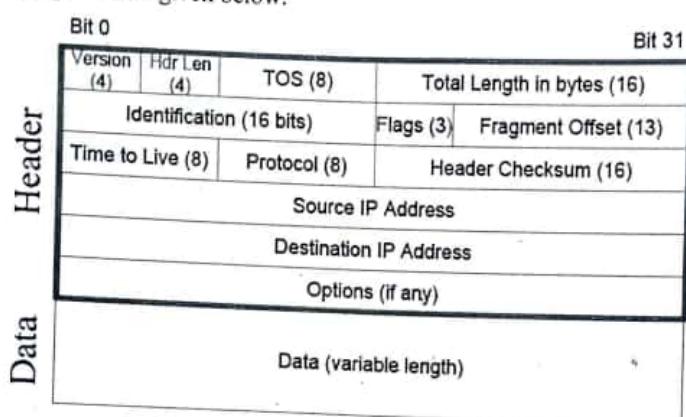
b) Compare and contrast between Distance vector routing and Link state routing.

c) Describe different types of link in OSPF protocol.

[WBUT 2017]

Answer:

a) The IP datagram is as given below:



Version: Version number of IP protocol. For IPv4 current version is Version 4, IPv6 has different header format.

Header Length (in 32 bit words): Indicates end of header and beginning of payload, If no options, Header length = 5

Type of Service (TOS): Allows different types of service to be requested

Packet Length (in Bytes): Unambiguously specify end of packet, Max packet size = 216 = 65,535 Bytes

Identification: All fragments of a single datagram have the same identification number.

Flags: 1st bit: reserved, must be zero, 2nd bit: DF -- Do Not Fragment, 3rd bit: MF -- More Fragments

Fragment Offset (in units of 8 bytes): Used for reassembly of packet, 1st fragment has offset = 0.

Time to Live: Initially set by sender (up to 255), decremented by each router, packet discard when TTL = 0 to avoid infinite routing loops

Protocol: Value indicates what is in the data field, Example: TCP or UDP

Header Checksum: Checks for error in the header only.

Source and Destination IP Addresses: Strings of 32 ones and zeros

Options : Example: timestamp, record route, source route

Identification: All fragments of a single datagram have the same identification number

b)

S. No	Distance vector routing	Link state routing
1	In distance vector routing each node has information only about the next hop	In link state routing, each node has a complete map of the topology
2	In distance vector routing the routing decisions are based on the least number of hops.	In link state routing decisions are based on the cost.
3	Distance vector routing makes poor routing decisions if directions are not completely correct	If a node fails, each node can calculate the new route
4	Full routing tables are updated periodically.	Only state of the links are updated, when there is an instance or trigger
5	Information given to only next node.	Link state information must be flooded to all nodes
6	E.g: Bellman ford.	E.g: Dijkstra

c) Types of link in OSPF protocol:

In OSPF, there are four types of links: point-to-point, transient, stub, and virtual. A point-to-point link connects two routers without any other host or router in between. It has Neighbor router ID as link ID. A transient link connects a network with several routers attached to it. The packets can enter and leave through any of the routers. It has IP address of destination router as link ID. A stub link connects to only one router. The data packets enter the network through this single router and leave the network through this same router. This is also considered as a special case of the transient network and it has link ID as IP Network. When the link between two routers is broken, the administrator may create a virtual link between them, using a longer path that probably goes through several routers.

9. a) What is the default mask and broadcast address for class B? Specify the private IP range for class A address.  
b) Why dynamic routing is preferred over static routing algorithm in a network, which changes continuously?  
c) Distinguish between GET and POST method in HTTP.  
d) What are the differences between TCP and UDP?

[WBUT 2017]

Answer:

a) Default mask of Class B address

255.255.0.0

Broadcast address of Class B address

As the Class B address range is from Class B IP Addresses range from 128.0.x.x to 191.255.x.x. So the default broadcast address of Class B can be said to be as 191.255.255.255. However, broadcast address is for a particular range for example Consider an IP range of 172.16.0.0 with a subnet of 255.255.224.0

In this range  
172.16.0.0 < Network Address  
172.16.0.1 - 172.16.31.254 < Usable Hosts  
172.16.31.255 < Broadcast Address  
Private IP range of Class A address  
10.0.0.0

b) Static routing are table mapping between source and destination before routing done by administrator. These mappings do not change unless the network administrator alters them. The algorithms then maps the incoming request to the destination from the table. They work well in environments where network traffic is relatively predictable and where network design is

relatively simple. Routing decisions in these algorithms are in no way based on current topology or traffic. As static routing systems cannot react to network changes, they generally constantly changing or dynamic networks.

Whereas the dynamic routing algorithms are more adaptable to changes in network and it adjusts to changing network circumstances by analyzing incoming routing update messages. If the message indicates that a network change has occurred, the dynamic routing algorithm recalculates routes and sends out new routing update messages.

### o) GET

The GET method sends the encoded user information appended to the page request. The page and the encoded information are separated by the ? character.

Example

[http://www.exa.edu/index.htm?name1 = val1&name2 = val2](http://www.exa.edu/index.htm?name1=val1&name2=val2)

The GET method produces a long string that appears in your server logs, in the browser's Location: box.

The GET method is restricted to send upto 1024 characters only.

We should not use GET method if we have password or other sensitive information to be sent to the server.

GET can't be used to send binary data, like images or documents, to the server.

The data sent by GET method can be accessed using QUERY\_STRING environment variable.

### POST

The POST method transfers information through HTTP headers. The information is encoded as described in case of GET method and put into a header called QUERY\_STRING

The POST method does not have any restriction on data size to be sent.

The POST method can be used to send ASCII as well as binary data.

The data sent by POST method goes through HTTP header so security depends on HTTP protocol. By using Secure HTTP (https) one can make sure that your information is secure.

d)

S. No	TCP	UDP
1	TCP is a connection oriented protocol	UDP is a connectionless oriented protocol
2	TCP assure reliable delivery of data to the destination.	UDP does not assure reliable delivery of data to the destination.
3	TCP provides extensive error checking mechanisms such as flow control and acknowledgment of data	UDP does not provides error checking mechanisms such as flow control and acknowledgment of data
4	Delivery of data is guaranteed if you are using TCP.	Delivery of data is not guaranteed if you are using UDP.
5	TCP is comparatively slow because of these extensive error checking mechanisms	UDP makes fast and best effort service to transmit data
6	Retransmission of lost packets is possible in TCP.	There is no retransmission of lost packets in UDP

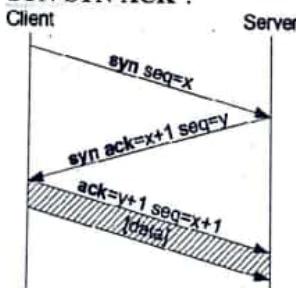
10. Write short notes on the following:

- a) Three-way handshaking of TCP connection establishment [WBUT 2014]
- b) Path vector routing [WBUT 2014, 2017]
- c) NAT [WBUT 2015]
- d) SMTP [WBUT 2015, 2018]
- e) Gateway [WBUT 2018]

Answer:

- a) TCP three-way handshake is the method used by TCP set up a TCP/IP connection over an Internet Protocol based network.

It's commonly referred to as "SYN-SYN-ACK".



Process

1. Host A sends a TCP SYNchronize packet to Host B
2. Host B receives A's SYN
3. Host B sends a SYNchronize-ACKnowledgement
4. Host A receives B's SYN-ACK
5. Host A sends ACKnowledge

6. Host B receives ACK.  
 7. TCP socket connection is ESTABLISHED.

**b) Path vector routing:**

Path vector routing does routing using path. It is useful for inter domain routing. In path vector routing for every AS there are one or more node, which acts in behalf of entire system. These may be called as Speaker node(s). This speaker creates routing table and advertises it to speaker nodes of neighbouring ASs. The routing table contains only the paths without any metric as shown in figure below.

Destination	Path
A1	AS1
A2	AS1
A3	AS1
A4	AS1

After receiving such table a neighbour speaker updates its own table by adding the nodes that are not in its routing table and adding the autonomous system that sent the table. This goes on and after some time each speaker has a table and knows how to reach each node in ASs. Optimum path obtained by path vector routing included optimum path of individual ASs and not any particular metric for the whole system.

**Advantages of path vector routing**

- 1) Creation of loop by distance vector routing can be avoided using path vector routing.
- 2) Policy routing can also be implemented using path vector.

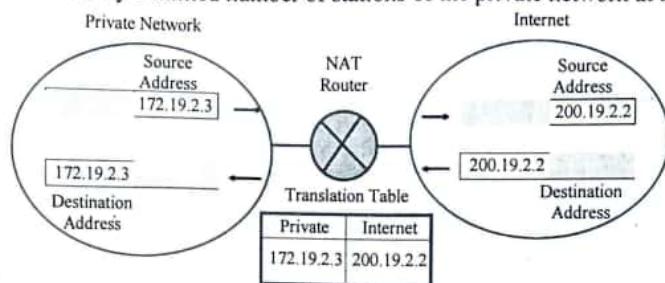
**c) NAT:**

With the increasing number of internet users requiring an unique IP address for each host, there is an acute shortage of IP addresses (until everybody moves to IPV6). The Network Address Translation (NAT) approach is a quick interim solution to this problem. NAT allows a large set of IP addresses to be used in an internal (private) network and a handful of addresses to be used for the external internet. The internet authorities has set aside three sets of addresses to be used as private addresses as shown in Table below.

Range of addresses	Total number
10.0.0.0 to 10.255.255.255	$2^{24}$
172.16.0.0 to 172.31.255.255	$2^{20}$
192.168.0.0 to 192.168.255.255	$2^{16}$

It may be noted that these addresses can be reused within different internal networks simultaneously, which in effect has helped to increase the lifespan of the IPV4. However, to make use of the concept, it is necessary to have a router to perform the operation of address translation between the private network and the internet. As shown in Fig below, the NAT router maintains a table with a pair of entries for private and internet address. The source address of all outgoing packets passing through the NAT router gets replaced by an internet address based on table look up. Similarly, the destination address of all

incoming packets passing through the NAT router gets replaced by the corresponding private address, as shown in the figure. The NAT can use a pool of internet addresses to have internet access by a limited number of stations of the private network at a time.



#### d) SMTP:

Simple Mail Transfer Protocol (SMTP) is internet's standard host-to-host mail transport protocol and traditionally operates over TCP, port 25. SMTP uses a style of asymmetric request-response protocol. The protocol is designed to be equally useful to either a computer or a human, though not too forgiving of the human. From the server's viewpoint, a clear set of commands is provided and well-documented in the RFC. For the human, all the commands are clearly terminated by newlines and a HELP command lists all of them. From the sender's viewpoint, the command replies always take the form of text lines, each starting with a three-digit code identifying the result of the operation, a continuation character to indicate another lines following, and then arbitrary text information designed to be informative to a human.

If mail delivery fails, sendmail (the most important SMTP implementation) will queue mail messages and retry delivery later. However, a backoff algorithm is used, and no mechanism exists to poll all Internet hosts for mail, nor does SMTP provide any mailbox facility, or any special features beyond mail transport. For these reasons, SMTP is not a good choice for hosts situated behind highly unpredictable lines (like modems). A better-connected host can be designated as a DNS mail exchanger, then arrange for a relay scheme. Currently, there are two main configurations in use. One is to configure POP mailboxes and a POP server on the exchange host, and let all users use POP-enabled mail clients. The other possibility is to arrange for a periodic SMTP mail transfer from the exchange host to another, local SMTP exchange host which has been queuing all the outbound mail. Of course, since this solution does not allow full-time Internet access, it is not too preferred.

#### e) Gateway:

A device which is used to connect networks using different protocols so that information can be passed from one system to the other. It is also called a Protocol Convertor. Gateways functions at the Network layer of the OSI model. As a consequence, it is known as a Layer-7 relay. But depending on situation may have to operate in all 7 layers of the OSI Model. The application level gateways can look into the content application layer packets such as email before forwarding it to the other side. This property has made

it suitable for use in Firewalls. Gateways are also multi-purpose connection devices. They are able to convert the format of data in one computing environment to a format that is usable in another computer environment (for example, AppleTalk and DECnet). The term gateway is sometimes used when referring to a router.

A Gateway many of the times is simply – Hardware-wise PC with Both Media Device Interface (NIC's) and some sort of Software that does the actual conversion of protocols and data packets.

**11. a) What is interior routing and exterior routing? Give example of both routing protocols. Explain any one interior routing protocol.**

**b) Discuss about the extra hop and hidden network problem that arises in internet due to the coexistence of participating and non-participating router.**

[MODEL QUESTION]

**Answer:**

a) An interior routing protocol works inside in an independent network system called as autonomous systems. The routing information is exchanged using an interior protocol chosen by the autonomous system's administration. These routing protocols determine the "best" route to each destination, and they distribute routing information among the systems on a network. There are several interior protocols OSPF, RIP, and EIGRP. Exterior routing protocols are used to exchange routing information between autonomous systems. The routing information passed between autonomous systems is called reachability information. Reachability information is simply information about which networks can be reached through a specific autonomous system. EGP and BGP are two exterior routing protocols.

**Routing Information Protocol:** The Routing Information Protocol (RIP) uses hop count as its metric. RIP is widely used for routing traffic in the global Internet and is an interior gateway protocol (IGP), thus it performs routing within a single autonomous system. These protocol sends update messages at regular intervals and when the network topology changes. After receiving a routing update that contains changes to an entry, it updates its routing table to reflect the new route, the metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send. RIP uses hop count as a single routing metric to measure the distance between the source and a destination network. Each hop in a path from source to destination is assigned a hop count value, typically 1. When a router receives a routing update that contains a new or changed destination network entry, the router adds 1 to the metric value indicated in the update and enters the network in the routing table. The IP address of the sender is used as the next hop. RIP uses several timers to regulate its performance such as a routing-update timer, a route-timeout timer, and a route-flush timer. The routing-update timer clocks the interval between periodic routing updates, it is set to 30 seconds, with a small random amount of time added whenever the timer is reset. This is done to help prevent

congestion, which could result from all routers simultaneously attempting to update their neighbors.

- b) An organization can not establish a total route by its own estimates as routing involves all other routers that are connected between source and destination. Moreover it also can not have more than one router per network. These constraints results in extra hop and hidden network problem, which are routing anomalies.

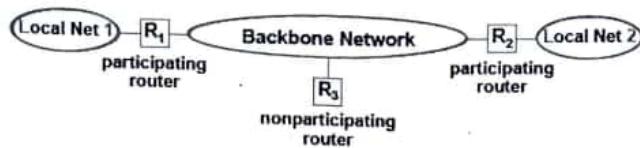


Fig: Participating and non participating routers

Constraints on the number of router involved in information exchange results into other routers which are connected to the back bone labeled as non participating router. Any datagram sent to nonparticipating router has to be forwarded to a participating router for a successful delivery as this non participating router does not have any information. But this result in adding one extra hop each time, this anomaly is called as extra hop problem. The extra hop problem can be solved by allowing even nonparticipating routers to make routing decisions. Also there should be mechanism that allows nonparticipating routers to obtain correct routing information automatically (without the overhead of participating fully in a routing exchange protocol). Now when a datagram is to be routed to a computer served by a non participating router it has to be routed to a participating router for final delivery. This is because non participating routers take help of participating router for sending and receiving information. The participating router will then redirect the datagram to non participating router for final delivery. This anomaly is called as hidden network problem and this caused because network services by non participating router is hidden to the backbone as it hidden from the backbone. To solve this problem of hidden network a mechanism is needed that allows nonparticipating routers to inform the other group about hidden networks.

**12. Describe link state routing algorithm and also state its advantages and disadvantages.** [MODEL QUESTION]

**Answer:**

Link state routing is a process by which each router shares knowledge about their neighbor with every router in the area. This knowledge is shared as following:

- Advertise about neighborhood: Instead of sending its entire routing table, a router sends information about its neighborhood only.
- Flooding: Each router sends this information to every other router on the internetwork, not just to its neighbors. It does so by a process of flooding. In Flooding, a router sends its information to all its neighbors (through all of its output ports). Every router sends such messages to each of its neighbor, and every router

## POPULAR PUBLICATIONS

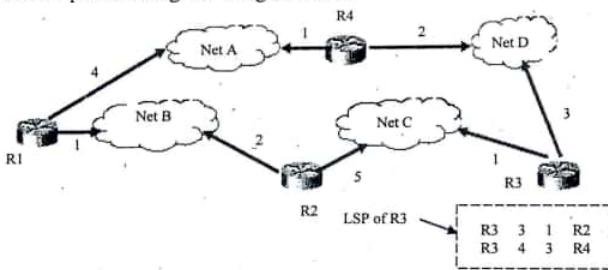
that receives the packet sends copies to its neighbor. Finally, every router has a copy of same information.

- c) Active response: Each outer sends out information about the neighbor when there is a change.

After a router is assured that its interfaces are functioning, it uses the OSPF Hello protocol (sends greeting messages) to acquire neighbors, which are routers with interfaces to a common network. The router sends hello packets to its neighbors and receives their hello packets. These messages are also known as greeting messages. It then prepares an LSP (Link State packet) based on the results of this Hello protocol.

A router gets its information about its neighbor by periodically sending them a short greeting packet. If neighbor responds to this greeting message as expected, it is assumed to be alive and functioning. If it does not, a change is assumed to have occurred and the sending router then alerts the rest of the network in its next LSP, about this neighbor being down.

**Advertising:** The process of router flooding the network with information about its neighborhood is known as Advertising. The basis of advertising is a short packet called a Link state Packet (LSP). An LSP usually contains 4 fields: the ID of the advertiser (Identifier of the router which advertises the message), ID of the destination network, The cost, and the ID of the neighbor router. Figure below shows the LSP of a router found after the Hello protocol as given in figure below.



Every router receives every LSP and then prepares a database, which represents a complete network topology. This Database is known as Link State Database also called as topological database. As every router receives the same LSPs, every router builds the same database. Every router uses it to calculate its routing table. If a router is added or deleted from the system, the whole database must be changed accordingly in all routers.

**Shortest Path calculation:** After gathering the Link State database, each router applies an algorithm called the Dijkstra algorithm to calculate the shortest distance between any two nodes. The Dijkstra's algorithm calculates the shortest path between two points on a network using a graph made up of nodes and arcs, where nodes are the Routers and the network, while connection between router and network is refer to as arcs.

### Main advantages:

- 1) Link state convergence occurs faster than distance vector convergence.

- 2) They use a hierarchical structure that help limit the distance that an LSA (Links State Advertisement) travels, and this reduces the likelihood that a change in the network will impact every router.
- 3) They use multicasts (instead of broadcasts) to share routing information.
- 4) They support classless routing.

**13. How is statelessness of HTTP overcome to run E-commerce applications on Web?**

[MODEL QUESTION]

**Answer:**

Statelessness can be overcome by implementing session tracking and management in the program running on the server side.

There are three typical solutions to this problem.

- cookies. You can use HTTP cookies to store information about a shopping session, and each subsequent connection can look up the current session and then extract information about that session from some location on the server machine. This is an excellent alternative, and is the most widely used approach. However, even though Servlets have a high-level and easy-to-use interface to cookies, there are still a number of relatively tedious details that need to be handled:
  - Extracting the cookie that stores the session identifier from the other cookies (there may be many, after all),
  - Setting an appropriate expiration time for the cookie (sessions interrupted by 24 hours probably should be reset), and
  - Associating information on the server with the session identifier (there may be far too much information to actually store it in the cookie, plus sensitive data like credit card numbers should never go in cookies).
- URL Rewriting. You can append some extra data on the end of each URL that identifies the session, and the server can associate that session identifier with data it has stored about that session. This is also an excellent solution, and even has the advantage that it works with browsers that do not support cookies or where the user has disabled cookies. However, it has most of the same problems as cookies, namely that the Server-Side program has a lot of straightforward but tedious processing to do. In addition, you have to be very careful that every URL returned to the user (even via indirect means like Location fields in server redirects) has the extra information appended. And, if the user leaves the session and comes back via a bookmark or link, the session information can be lost.
- Hidden form fields. HTML forms have an entry that looks like the following: <INPUT TYPE="HIDDEN" NAME="session" VALUE="...">>. This means that, when the form is submitted, the specified name and value are included in the GET or POST data. This can be used to store information about the session. However, it has the major disadvantage that it only works if every page is dynamically generated, since the whole point is that each session has a unique identifier.

## HTML, XML, CGI SCRIPTS

### Multiple Choice Type Questions

1. Which HTML attribute is used to define inline styles?  
a) style      b) font      c) styles      d) div  
Answer: (a)
2. XML was designed to serve the ..... purpose.  
a) format data      b) display data  
c) transport data      d) none of these  
Answer: (c)
3. What does a Markup tag tell the web browser?  
a) how to organize the page      b) how to display message box on page  
c) how to display the page      d) none of these  
Answer: (b)
4. HTML documents are saved in  
a) ASCII text      b) machine language codes  
c) special binary format      d) none of these  
Answer: (a)
5. Which of the following is correct regarding meta tag in HTML?  
a) <meta>...</meta>      b) <meta name = " "/>  
c) <metadata>...</metadata>      d) <metadata name = " "/>  
Answer: (b)
6. Which of the following methods is used to get meta information of a resource?  
a) TOP      b) HEAD      c) GET      d) GRAB  
Answer: (b)
7. DHTML is for  
a) model      b) view      c) controller      d) servlet  
Answer: (b)
8. Which of the following is recommended XML?  
a) W3C      b) Microsoft      c) Sun      d) IEEE  
Answer: (a)
9. Which of the following technologies is used to display XML data?  
a) CSS      b) XPath      c) XQuery      d) XHTML  
Answer: (a)

10. Which of the following is an invalid CSS selector?  
a) Title selectors      b) HEAD selectors  
c) TAG selectors      d) Id selectors [WBUT 2015]  
Answer: (b)
11. A declaration is terminated by a  
a) } - end curly bracket      b) . - period  
c) ; - semi colon      d) ! - exclamation sign [WBUT 2015]  
Answer: (c)
12. The correct HTML tag for the biggest heading is  
a) <h6>      b) <heading small>      c) <small heading>      d) <h1> [WBUT 2016]  
Answer: (d)
13. The ..... in XML is equivalent to the schema in database.  
a) Element      b) Attribute      c) Parser      d) DTD [WBUT 2016, 2018]  
Answer: (d)
14. An XML parser is used to ..... the contents of an XML document. [WBUT 2016]  
a) display      b) read but not interpret  
c) read and interpret      d) none of these  
Answer: (c)
15. Which statement is true?  
a) XML tags are case sensitive      b) XML documents must have a root tag  
c) XML elements must be properly closed      d) All the statements are true [WBUT 2016]  
Answer: (d)
16. Which statement is true?  
a) All the statements are true      b) All XML elements must have a closing tag  
c) All XML elements must be in lower case      d) All XML documents must have a DTD [WBUT 2017]  
Answer: (a)
17. Which HTML attribute is used to define inline styles?  
a) Class      b) Styles      c) Style      d) Font [WBUT 2017]  
Answer: (c)

#### Short Answer Type Questions

- Q. Compare between SAX and DOM approach in respect of XML parsing. [WBUT 2013]

**Answer:**

SAX	DOM
1. Parses node by node.	1. Stores the entire XML documents into memory before processing.
2. Event based parser (Sequence of events)	2. Tree model parser (Tree of nodes)
3. No memory constraints as it does not store the XML content in the memory	3. Has memory constraints since it loads the whole XML file before parsing
4. SAX is read only i.e. can't insert or delete the node	4. DOM is read and write (can insert or delete the node)
5. Use SAX parser when memory content is large	5. If the XML content is small then prefer DOM parser
6. SAX reads the XML file from top to bottom and backward navigation is not possible	6. Backward and forward search is possible for searching the tags and evaluation of the information inside the tags. So this gives the ease of navigation
7. Faster at runtime	7. Slower at runtime
8. Doesn't preserve comments	8. Preserves comments.

2. a) State different types of lists with examples in HTML.  
b) State the use of <pre> and <del> tags.

[WBUT 2014]

**Answer:**

- a) There are three types of lists in HTML:

- **Ordered Lists:** These are sometimes called numbered lists, and list items that have a specific numerical order or ranking. This list is created by <ol> tag. The numbering starts at one and is incremented by one for each successive ordered list element tagged with <li>. You can use *type* attribute to specify the type of numbers you like (Attributes: type = I|A|a|I|i). By default it's a generic numbers. You can also use *start* attribute to specify the beginning of any index. For example:

```
<ol>
    <li>Entry 1</li>
    <li>Entry 2</li>
    <li>Entry 3</li>
</ol>
```

- **Unordered Lists:** These are sometimes called bulleted lists, because they have small bullet icons in front of the list items. They are for lists that don't have a required order. Use the <ul> tag (the ending </ul> tag is required) to create a list with bullets instead of numbers. Just like with the ordered list, the elements are created with the <li> tag. For example:

```
<ul>
    <li>Entry 1</li>
    <li>Entry 2</li>
    <li>Entry 3</li>
</ul>
```

- **Definition Lists:** These are lists of items that have two parts, a term to be defined and the definition. This creates lists similar to a dictionary or glossary. There are three tags associated with the definition list:

- i) <dl> to define the list
- ii) <dt> to define the definition term
- iii) <dd> to define the definition of the term

Here is how a definition list looks:

```
<dl>
  <dt>This is a definition term</dt>
  <dd>And this is the definition</dd>
  <dt>term 2</dt>
  <dd>definition 2</dd>
  <dt>term 3</dt>
  <dd>definition 3</dd>
</dl>
```

b) **Use of pre tag:** Sometimes you want your text to follow the exact format of how it is written in the HTML document. In those cases, you can use the preformatted tag (<pre>). Any text between the opening <pre> tag and the closing <pre> tag will preserve the formatting of the source document.

**Use of del tag:** The *HTML Deleted Text Element* (<del>) represents a range of text that has been deleted from a document. This element is often (but need not be) rendered with strike-through text.

```
<html>
  <head><title>Use of del tag in html</title>
  </head>
  <body>
    <p><del>This text has been deleted</del>, here is the rest
       of the paragraph.
    </p>
  </body>
</html>
```

3. a) What is the difference between class selector and id selector in CSS.

b) Give coding example for inline styles of CSS.

[WBUT 2014]

**Answer:**

- i) The difference between class selector and id selector is that an id selector can be called only once in a document, but a class selector can be called multiple times in a document.
- ii) The id selector uses the id attribute of the HTML element, and is defined with a "#". But, the class selector uses the HTML class attribute, and is defined with a ".".
- iii) The second difference is that id can be called by Javascript's getElementById function.

**b) Coding example for inline styles of CSS:**

```
<html>
<body>
<h1 style="color:red; margin-left:30px;">This is a heading.</h1>
<p>This is an example of inline styles .</p>
</body>
</html>
```

- 4. Why do we need to have a dynamic webpage? What is the advantage of using style sheet in formatting the different elements of webpages in a website? How can we link a style sheet to a webpage?** [WBUT 2016]

**Answer:**

A dynamic web page is a web page with web content that varies based on specific parameters provided by a user or a computer program. Dynamic webpages manage the content in the website effectively and thereby make the site more attractive which in turn will attract more customers to the site. Also dynamic web designs empower the owners with the ability to upload information on their own, through password protected administrative platforms.

**Benefits/Advantages of CSS:**

- 1) We can write CSS once and then reuse as many times in the same pages. Thus it saves time.
- 2) If using CSS the pages load faster. If we are using CSS we do not need to write HTML tag attributes every time. So less code and faster download times.
- 3) CSS allows easy maintenance as to make a global change simply change the style, and all the elements in all the web pages will be updated automatically.
- 4) CSS has a much wider array of attributes than HTML
- 5) CSS allow content to be optimized for more than one type of device.

There are four different ways of inserting a CSS styles in webpage.

**1) Embedded or Internal CSS:** Using the <style> Element:

We can put CSS rules into an HTML document using the <style> element. This tag is placed inside <head>...</head> tags. A generic syntax:

```
<head> <style type="text/css" media="..."> Style Rules ..... </style> </head>
```

**2) Inline CSS:** Uses the style Attribute of any HTML element to define style rules. These rules will be applied to that element only.

Generic syntax:

```
<element style="...style rules....">
```

**3) External CSS:** Uses the <link> Element to include an external stylesheet file in the HTML document. An external style sheet is a separate text file with .css extension. Define all the Style rules within this text file and then you can include this file in any HTML document using <link> element.

Generic syntax of including external CSS file:

```
<head> <link type="text/css" href="..." media="..." /> </head>
```

4) **Imported CSS:** Uses @import Rule to import an external stylesheet in a manner similar to the <link> element.

Generic syntax of @import rule.  
<head> <@import "URL";> </head>

5. What are the XML schemas? How they are better than DTDs? [WBUT 2017]

Answer:

1<sup>st</sup> part:

XML Schema is commonly known as XML Schema Definition (XSD). It is used to describe and validate the structure and the content of XML data. XML schema defines the elements, attributes and data types. Schema element supports Namespaces. It is similar to a database schema that describes the data in a database.

Syntax

You need to declare a schema in your XML document as follows –

Example

The following example shows how to use schema –

The following example shows how to use schema –

```
<?xml version = "1.0" encoding = "UTF-8"?>
<x:schema xmlns:x = "http://www.w3.org/2001/XMLSchema">
  <x:element name = "contact">
    <x:complexType>
      <x:sequence>
        <x:element name = "name" type = "x:string" />
        <x:element name = "company" type = "x:string" />
        <x:element name = "phone" type = "x:int" />
      </x:sequence>
    </x:complexType>
  </x:element>
</x:schema>
```

The basic idea behind XML Schemas is that they describe the legitimate format that an XML document can take.

2<sup>nd</sup> Part: XML schemes are better than DTD for the following reasons:

1) XML schemas use XML Syntax, so we don't have to learn a new language, we can use our XML editor to edit our schema files, so we can use our XML parser to parse our schema file.

2) Support for primitive (build in) data types (e.g., xsd:integer, xsd:string, xsd:data and so on), which facilitates using XML in conjunction with other typed-data, including relational data.

3) The ability to define custom data types, using object-oriented data modeling principles: encapsulation, inheritance and substitution.

4) XML Schemas are extensible; so we can reuse our schema in other Schemas.

6. Describe the anatomy of an XML document.

[MODEL QUESTION]

Answer:

A simple XML file with its anatomy described

```
<? xml version = "1.0"?>
< p e r s o n >
<sex> female </sex >
<name>
<first name> James </first name>
    <last name> Smith </last name>
</ name>
< address city = " Kolkata " zip = "700026" > </address>
< /person >
```

In the above example

- The first line of the file identified the document as an xml document and indicates the version of the xml. It is not mandatory to use in your document but it is always good to add.
- The first tag <person> is called the root element. Every XML document must have a root element. Every opening tag must have a closing tag </person>. All the rest of the elements are present in between the <person> and </person> tags.
- The other elements <sex>, <first name> and <last name> are called child elements.
- <first name> and <last name> are again child element of element <name>
- The <address> tag has got attributes describing the address tag.
- Attributes are "city", "zip".

#### Long Answer Type Questions

a) Using the FORM tag of HTML create a registration form containing the below mentioned fields:

[WBUT 2013]

- i) First Name (Using text boxes)
- ii) Last Name (Using text boxes)
- iii) E-mail ID (Using text boxes)
- iv) Gender (Using radio button)
- v) Hobbies (Using check boxes)
- vi) Submit Button and Rest Button.

OR,

Design a HTML form for registration to a website for a specific service. The form should contain at least one instance of the following form elements:

- i) Text Box
- ii) Check Box
- iii) Select Box
- iv) Submit and Rest Button
- v) Radio Button

[WBUT 2018]

b) In your browser there will be a textbox to enter your name. There will be a SUBMIT button. If your name field is empty then on submit this will give an alert that your name field is empty. If your name is more than 10 characters long then it

will give an alert to enter your name properly. Else it will display your name in capital, bold and in red colour.  
[WBUT 2013]

Answer:

a)

```
<html>
<head><title>Welcome to Registration Page</title></head>
<body>
<form>
<pre>
First Name <input type="text" size="10" maxlength="40"
name="name"><br />
Last Name <input type="text" size="10" maxlength="40"
name="name"><br />
Email ID <input type="text" size="10" maxlength="40"
name="name"><br />
Gender <input type="radio" name="Registration"
value="Male">Male<br />
<input type="radio" name="Registration"
value="Female">Female<br />
Hobbies
<input type="checkbox" name="Registration"
value="Drawing">Drawing<br />
<input type="checkbox" name="Registration"
value="Singing">Singing<br />
<input type="checkbox" name="Registration"
value="Dancing">Dancing<br />
</pre>
<button type="submit" name="Registration"
value="Submit">Submit</button>
<input type="reset" value="Reset" />
</form>
</body>
</html>
```

b)

```
<html>
<head>
<script type="text/javascript">

function abc()
{
    var name=document.getElementById("name").value;
    if(name=="")
        alert("Your name field is empty!");
    else if(name.length > 10)
        alert("Enter your name properly!");
    else
        {
```

#### SYLLABUS PUBLICATIONS

```
        name=name.toUpperCase();
        name=name.bold();
        document.write(name.fontcolor("red"));
    }

</script>
</head>
<body>
<input type='text' title='Name' id='name'>
<input type='submit' onclick='abc()' value='Submit'>
</body>
</html>
```

- 2 a) What is XML? What is the basic structure of an XML document?  
b) Create an XML document which has a root element emp. Root element contains more than one No. of employee element. Each employee has sub-element empname, id, gender and address. Address has the sub-element street, city, region, postalcode, countrycode. Street has two sub-elements street1 and street2. Countrycode has an attribute c\_id. Write an external DTD to validate this XML.

Answer:

[WBUT 2013]

a) XML, stands for Extensible Markup Language, is a framework for defining markup languages. In contrast to HTML, there is no fixed collection of markup tags in XML. Instead, XML lets us define our own tags, tailored for the kind of information that we wish to represent. XML's purpose is to aid information systems in sharing structured data, especially via the Internet, to encode documents, and to serialize data.

- The prolog and
- The content.

Other than the above two it can contain optionally:

- Attributes.
- Entity References.
- Comments.

The **prolog or head** of the document usually contains the administrative metadata about the rest of document. It is the first structural element. It will have information such as:

- Version of XML is used,
- The character set standard used,
- The DTD Document types Definition, either through a link to an external file or internally.

Content is usually divided into two parts,

- The structural markup and
- Content contained in the markup, which is usually plain text.

<?xml version="1.0" encoding="iso-8859-1"?>

- <?xml declares to a processor that this is where the XML document begins.

ITECH-CS-34

- version="1.0" declares which recommended version of XML the document should be evaluated in, version can be 1.1 also.
- encoding="iso-8859-1" identifies the standardized character set that is being used to write the markup and content of the XML.

b) emp.dtd

```
<!ELEMENT emp (empname, id, gender, address*)>
<!ELEMENT empname (#PCDATA)>
<!ELEMENT id (#PCDATA)>
<!ELEMENT gender (#PCDATA)>
<!ELEMENT address (street*, city, region, postalcode,
countrycode*)>
<!ELEMENT street (street1,street2)*>
<!ELEMENT city (#PCDATA)>
<!ELEMENT region (#PCDATA)>
<!ELEMENT postalcode (#PCDATA)>
<!ELEMENT countrycode (c_id)>
```

employee.xml

```
<?xml version="1.0"?>
<!DOCTYPE note SYSTEM "emp.dtd">
<emp>
  <empname>Ram</empname>
  <id>001</id>
  <gender>Male</gender>
  <address>
    <street>
      <street1>street1:kalyani A</street1>
      <street2>street2:kalyani B</street2>
    </street>
    <city>Kalyani</city>
    <region>Kalyani</region>
    <postalcode>741235</postalcode>
    <countrycode>
      <c_id>KYL</c_id>
    </countrycode>
  </address>
</emp>
```

3. a) Write down the features of scripting language. How markup language is different from scripting language?

b) Create a HTML page with the following features.

Hyperlink, List and Form.

[WBUT 2015]

Answer:

a) A markup language is simply a set of tags that are used to "mark up" text documents so that sections of text can be logically arranged and labeled. These documents can be viewed as plain text, or, more commonly, are viewed through a browser. The browser

parses the document, looking for markup tags, and it then arranges the text and/or formats it according to the values in the tags.

Scripting languages, on the other hand, are interpreted at run-time. This means that every time you want to run the program, a separate program needs to read the code, interpret it, and then follow the instructions in the code. Compiled code has already been interpreted into machine language, so it will typically execute faster because the conversion into machine language has already been done.

b)

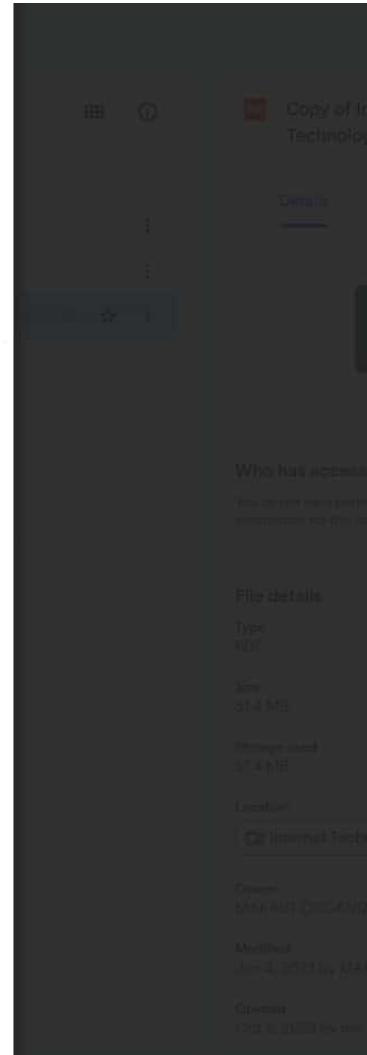
```
<html>
<body>
<h2>Introduction to Hyperlink</h2>
<p><a href="#C4">Jump to Chapter 4</a></p>
<h2>Chapter 1</h2>
<p>This chapter explains 1</p>
<h2>Chapter 2</h2>
<p>This chapter explains 2</p>
<h2>Chapter 3</h2>
<p>This chapter explains 3</p>
<h2 id="C4">Chapter 4</h2>
<p>This chapter explains 4</p>
<h2>Chapter 5</h2>
<p>This chapter explains 5</p>
<h2>Introduction to Unordered List without Bullets.....</h2>
<ul style="list-style-type:none">
    <li>Coffee</li>
    <li>Tea</li>
    <li>Milk</li>
</ul>
<h2> Introduction to Ordered List.....</h2>
<ol>
    <li>Coffee</li>
    <li>Tea</li>
    <li>Milk</li>
</ol>
<h2> Introduction to Forms....</h2>
<form>
    First name:<br>
    <input type="text" name="firstname">
    <br>
    Last name:<br>
    <input type="text" name="lastname">
</form>
</body>
</html>
```

Q Search HOME Shared with me BCA Shared with me > BCA

Name ↑

Copy of internet technology

Copy of internet technology.pdf



Why XML is superior to HTML. What are the different types of parser used in XML?

Search in Drive

Shared with me > BCA

Downloaded 29

Copy of Internet Technology.pdf

Copy of Internet Technology.pdf

**Answer:**

XML allows authors and providers to design their own document markup instead of being limited by HTML. For the following reason we can say XML is superior than HTML:

- Information content can be richer and easier to use, because the descriptive and hypertext linking abilities of XML are much greater than those available in HTML.
- XML can provide more and better facilities for browser presentation and performance, using XSLT and CSS stylesheets; *(Standard Generalized Markup Language)*
- It removes many of the underlying complexities of SGML-format HTML (which led to them being ignored and broken) in favour of a more flexible model, so writing programs to handle XML is much easier than doing the same for all the old broken HTML.
- Information becomes more accessible and reusable, because the more flexible markup of XML can be used by any XML software instead of being restricted to specific manufacturers as has become the case with HTML.
- XML files can be used outside the Web as well, in existing document-handling environments (e.g. publishing).

**XML parser**

XML Parser provides way how to access or modify data present in an XML document. Java provides multiple options to parse XML document. Following are various types of parsers which are commonly used to parse XML documents.

- **Dom Parser** - Parses the document by loading the complete contents of the document and creating its complete hierarchical tree in memory.
- **SAX Parser** - Parses the document on event based triggers. Does not load the complete document into the memory.
- **JDOM Parser** - Parses the document in similar fashion to DOM parser but in more easier way.
- **StAX Parser** - Parses the document in similar fashion to SAX parser but in more efficient way.
- **XPath Parser** - Parses the XML based on expression and is used extensively in conjunction with XSLT.
- **DOM4J Parser** - A java library to parse XML, XPath and XSLT using Java Collections Framework, provides support for DOM, SAX and JAXP.

5. a) Explain an internal valid XML document with an example. [WBUT 2016]  
b) Write down the rules for creating a well formed XML document.  
c) Write the differences between DOM and SAX parser in XML.  
d) Explain the following:  
(i) <!ELEMENT section (title + para(note | code\*)>  
(ii) <!ATTLIST sign signature file CDATA #IMPLIED email CDATA# required>

Copy of Internet Technology.pdf

Details

Who has access

File details

Type: PDF

Size: 51.4 MB

Storage used: 51.4 MB

Last modified: April 1, 2016 by MAHANTESH DABIR

Owner: MAHANTESH DABIR

Modified: April 1, 2016 by MAHANTESH DABIR

Updated: April 1, 2016 by MAHANTESH DABIR

**Answer:**

- a) The XML Document Type Declaration, DTD, is a way to describe XML language precisely. An XML DTD can be either specified inside the document, or it can be kept in a separate document and then linked separately.

**Internal DTD Declaration**

If the DTD is declared inside the XML file, it should be wrapped in a DOCTYPE definition with the following syntax:

```
<!DOCTYPE root-element [element-declarations]>
```

**Example:**

```
<?xml version="1.0"?>
<!DOCTYPE note [
  <!ELEMENT note (to, from, heading, body)>
  <!ELEMENT to (#PCDATA)>
  <!ELEMENT from (#PCDATA)>
  <!ELEMENT heading (#PCDATA)>
  <!ELEMENT body (#PCDATA)>
]>
<note>
  <to>Ram</to>
  <from>Syam</from>
  <heading>Reminder</heading>
  <body> Let's go for Shopping</body>
</note>
```

- b) XML documents, minimum, are made of two parts:

- The prolog and
- The content.

Other than the above two it can contain optionally:

- Attributes.
- Entity References.
- Comments.

The prolog or head of the document usually contains the administrative metadata about the rest of document. It is the first structural element. It will have information such as:

- Version of XML is used,
- The character set standard used,
- The DTD Document types Definition, either through a link to an external file or internally.

Content is usually divided into two parts,

- The structural markup and
- Content contained in the markup, which is usually plain text.

```
<?xml version="1.0" encoding="iso-8859-1"?>
```

- <?xml declares to a processor that this is where the XML document begins.
- version="1.0" declares which recommended version of XML the document should be evaluated in, version can be 1.1 also.

- encoding="iso-8859-1" identifies the standardized character set that is being used to write the markup and content of the XML.

**c) Refer to Question No. 1 of Short Answer Type Questions.**

**(i) (i) <!ELEMENT section (title + para(note | code\*)>**

Explanation: Here **section** is an element name and **section** must contain a "title" element and a "para" element which must contain either a "note" or a "code". "code" can occur zero or more times inside the "para" element.

**(ii) <!ATTLIST sign signaturefile CDATA #IMPLIED email CDATA #REQUIRED>**

Explanation: The above list is an attribute-list declaration where **sign** is an element name and **signaturefile** and **email** are two attributes in **sign** elements. **signaturefile** is **#IMPLIED** as we don't want to force the author to include an attribute, and we don't have an option for a default value. **email** is **#REQUIRED** as we don't have an option for a default value, but still want to force the attribute to be present.

**6. Prepare an XML document for the following table with internal DTD definition:  
[WBUT 2018]**

NAME	STU_ID	Department
Mr. XYZ	STU1	SCE
Mr. ABC	STU2	I.T.

**Answer:**

```
<?xml version="1.0"?>
<!DOCTYPE STUDENT [
<!ELEMENT STUDENT (NAME, STUD_ID, Department)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT STUD_ID (#PCDATA)>
<!ELEMENT Department (#PCDATA)>
]>
<STUDENT>
  <NAME>Ms. XYZ</NAME>
  <STUD_ID>STU1</STUD_ID>
  <Department>SCE</Department>
  <NAME>Mr. ABC</NAME>
  <STUD_ID>STU2</STUD_ID>
  <Department>I.T.</Department>
</STUDENT>
```

**7. Illustrate the basic tags of a HTML page with an example.  
[WBUT 2018]**

**Answer:**

The basic structure for all HTML documents is simple and should include the following minimum elements or tags:

- <html> - The main container for HTML pages ✓ ✓
- <head> - The container for page header information ✓ ✓
- <title> - The title of the page ✓ ✓

- **<body>** - The main body of the page

Remember that before an opening `<html>` tag, an XHTML document can contain the optional XML declaration, and it should always contain a DOCTYPE declaration indicating which version of XHTML it uses.

An HTML document starts and ends with `<html>` and `>/html>` tags. These tags tell the browser that the entire document is composed in HTML. Inside these two tags, the document is split into two sections:

- The `<head>...</head>` elements, which contain information about the document such as title of the document, author of the document etc. Information inside this tag does not display outside.
  - The `<title>...</title>` elements, which element is a child of the `<head>` element. It specifies a title for every page that you write inside the `<title>` element.
- The `<body>...</body>` elements, which contain the real content of the document that you see on your screen.

In spite of the above four tags there are lots tags available in HTML. We discuss some tags among them.

#### Example:

```
<html>
    <head>
        <title> My first page </title>
    </head>
    <body text="white" bgcolor="blue">
        This is a html page.
        <i>This is italic</i> and this is <b> bold</b>.
    </body>
</html>
```

#### Heading Tag

One of the earliest means of formatting text was the heading tag. It is available in six levels of importance from `<h1>` down to `<h6>`, as shown in the following code and in Figure. You might think of these headers as headlines for chunks of text.

```
<html>
    <head>
        <title>Header Example</title>
    </head>
    <body>
        <h1>This is an example of a level 1 header. </h1>
        <h2>This is an example of a level 2 header.</h2>
        <h3>This is an example of a level 3 header.</h3>
        <h4>This is an example of a level 4 header.</h4>
        <h5>This is an example of a level 5 header.</h5>
        <h6>This is an example of a level 6 header.</h6>
    </body>
```

The `<p>` element offers a way to structure your text. The `p` tag signifies a paragraph break. The paragraph breaks cause the browser to skip a line. Also, the `p` tag is considered a *container* tag because its opening and closing tags should be used to contain paragraphs of content.

Each paragraph of text should go in between an opening `<p>` and closing `</p>` tag. `</p>` tag as shown below in the example:

```
<p>Here is a paragraph of text.</p>
<p>Here is a second paragraph of text.</p>
<p>Here is a third paragraph of text.</p>
```

You can use `align` attribute to align your paragraphs.

```
<p align="left">This is left aligned.</p>
<p align="center">This is center aligned.</p>
<p align="right">This is right aligned.</p>
<p align="justify">This is justified. This works when you have multiple lines in
your paragraph and you want to justify all the lines so that they can look more
nice.</p>
```

#### ✓ Line break:

The `br` tag inserts a simple line break. Whenever you use the `<br />` element, anything following it starts on the next line. This tag is an example of an **empty** element, where you do not need opening and closing tags, as there is nothing to go in between them. It tells the browser to drop down to the next line before continuing. If you insert multiple `br` tags, the browser will drop down several lines before continuing.

#### Example:

```
<p>
  Jack and Jill went up a hill <br />
  To catch a pail of water <br />
  Jack fell down and broke his crown <br />
  And Jill came tumbling after <br />
</p>
```

#### 8. Write short notes on the following:

- a) Image map
- b) HTML Image Map
- c) XML tree

[WBUT 2013]  
[WBUT 2014, 2017, 2018]  
[WBUT 2014]

#### Answer:

##### a) Image map:

An image map is an image that contains one or more clickable sections. These are referred to as hotspots and they function as hyperlinks. When only sections of an image are linked (as opposed to the entire image), the visitor's pointer only changes to the hand when he moves his mouse over one of the predefined hot spots on the image. Each *hot spot* within an image map can link to its own web page, if wanted. An image maps allows

Creating link to different URLs depending upon where we click on the image. It is useful for creating links on maps, diagrams, fancy buttons etc.

There are two parts of an image map.

- The image
- The map file: Defines the areas of the image and the URLs that correlate to different areas.

So image map is a single image that contains hot spots.

- When we click on the hot spots we go to a new location (URL).
- Requires loading of only one image from server hence load is reduced.

#### Types of image maps:

Depending on the way they are configured and the location where the processing is carried out, image maps can be classified as:

- Server Side: Traditional.
- Client Side: More efficient and supported by all browsers.

The `<map>` element contains a number of `<area>` elements that defines the clickable areas in the image map.

Following is the code for map:

```

<map name="image">
    <area shape="rect" coords="0,0,82,120" href="rect.htm"
    alt="Rectangule Link">
    <area shape="circle" coords="90,58,3" href="circle.htm"
    alt="Circle Link">
</map>
The <area> tag defines an area inside an image-map (an image-map is an image with clickable areas). The <area> element is always nested inside a <map> tag.
The following code shows this concept:

<map name="image">
    <area shape="rect" coords="0,0,82,120" href="rect.htm"
    alt="Rectangule Link">
    <area shape="circle" coords="90,58,3" href="circle.htm"
    alt="Circle Link">
</map>
```

#### HTML image map:

An image map is an image that contains one or more clickable sections. These are referred to as hotspots and they function as hyperlinks. When only sections of an image are linked (as opposed to the entire image), the visitor's pointer only changes to the hand

creating link to different URLs depending upon where we click on the image. It is useful for creating links on maps, diagrams, fancy buttons etc.

There are two parts of an image map.

- The image
- The map file: Defines the areas of the image and the URLs that correlate to different areas.

So image map is a single image that contains hot spots.

- When we click on the hot spots we go to a new location (URL).
- Requires loading of only one image from server hence load is reduced.

#### Types of image maps:

Depending on the way they are configured and the location where the processing is carried out, image maps can be classified as:

- **Server Side:** Traditional.
- **Client Side:** More efficient and supported by all browsers.

The `<map>` element contains a number of `<area>` elements that defines the clickable areas in the image map.

Following is the code for map:

```

<map name="image">
    <area shape="rect" coords="0,0,82,120" href="rect.htm" alt="Rectangule Link">
    <area shape="circle" coords="90,58,3" href="circle.htm" alt="Circle Link">
</map>
The <area> tag defines an area inside an image-map (an image-map is an image with clickable areas). The <area> element is always nested inside a <map> tag.
The following code shows this concept:

<map name="image">
    <area shape="rect" coords="0,0,82,120" href="rect.htm" alt="Rectangule Link">
    <area shape="circle" coords="90,58,3" href="circle.htm" alt="Circle Link">
</map>
```

#### c) XML Tree:

An XML document is always descriptive. The tree structure is often referred to as XML Tree and plays an important role to describe any XML document easily:

The tree structure contains root (parent) elements, child elements and so on. By using tree structure, you can get to know all succeeding branches and sub-branches starting from the

## POPULAR PUBLICATIONS

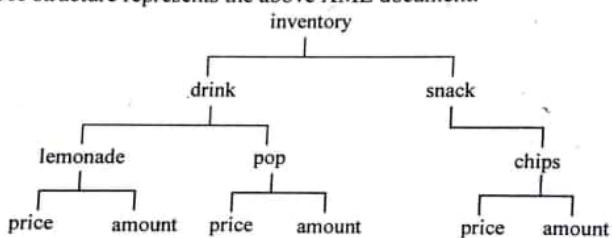
root. The parsing starts at the root, then moves down the first branch to an element, take the first branch from there, and so on to the leaf nodes.

### **Example**

Following example demonstrates simple XML tree structure:

```
<inventory>
    <drink>
        <lemonade>
            <price>$2.50</price>
            <amount>20</amount>
        </lemonade>
        <pop>
            <price>$1.50</price>
            <amount>10</amount>
        </pop>
    </drink>
    <snack>
        <chips>
            <price>$4.50</price>
            <amount>60</amount>
        </chips>
    </snack>
</inventory>
```

Following tree structure represents the above XML document:



In the above diagram, there is a root element named as <inventory>. Inside the inventory element, there are two branches named <drink> and <snack>. Inside <drink> element, there are two sub branches named <lemonade> and <pop>. And <snack> element has another sub element named <chips>. Inside <lemonade>, <pop> and <chips> elements have two sub branches named <price> and <amount>.

9. a) Show the typical Request and Response format used in HTTP protocol.
- b) What is the significance of method field in an HTTP request?
- c) Create an HTML page with the following features: Hyperlink, navigation buttons, tables, forms. [MODEL QUESTION]

**Answer:**

a) **HTTP Request**

A HTTP request is a collection of lines sent to the server by the browser. It includes:

**A request line:** This is a line specifying the type of document requested, the method which must be applied, and the version of the protocol used. The line is made up of three elements which must be separated by a space: the method, URL, and the version of the protocol used by the client (generally HTTP/1.0). A HTTP request therefore has the following syntax(<crlf> meaning carriage return and line feed):

```
METHOD URL VERSION<crlf>
HEADER: Value<crlf>
...
HEADER: Value<crlf>
Empty line <crlf>
```

**The request header fields:** This is a collection of optional lines allowing additional information about the request and/or the client to be given (browser, operating system, etc.). Each of these lines is composed of a name describing the header type, followed by a colon (:) and the value of the header.

**The body of the request:** This is a collection of optional lines which must be separated from preceding lines by an empty line and for example allowing data to be sent by a POST command during the sending of data to the server using a form.

**Here is an example of a HTTP request:**

```
GET http://www.mywebsite.com/ HTTP/1.0
Accept: text/html
If-Modified-Since: Saturday, 15-January-2000 14:37:11 GMT
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 95)
```

#### **HTTP Response**

A HTTP response is a collection of lines sent to the server by the browser.

It includes:

**A status line:** This is a line specifying the protocol version used and the status of the request being processed using a code and explanatory text. The line is made up of three elements which must be separated by a space: the version of the protocol used, the status code, and the meaning of the code.

A HTTP response therefore has the following:

syntax :  
VERSION-HTTP CODE EXPLANATION<crlf>
HEADER: Value<crlf>
...
HEADER: Value<crlf>
Empty line <crlf>

**The response header fields:** This is a collection of optional lines allowing additional information about the response and/or the client to be given (browser, operating system, etc.). Each of these lines is composed of a name describing the header type, followed by a colon (:) and the value of the header.

**The body of the response:** This contains the requested document.

b) HTTP defines nine **methods** (sometimes referred to as "verbs") indicating the desired action to be performed on the identified **resource**. What this resource represents, whether pre-existing data or data that is generated dynamically, depends on the implementation of the server. Often, the resource corresponds to a file or the output of an executable residing on the server.

1. HEAD
2. GET
3. POST
4. PUT
5. DELETE
6. TRACE
7. OPTIONS
8. CONNECT
9. PATCH

c)

```
<html>
<title>HTML with Hyperlink, navigation buttons, tables, forms
</title>
<body bgcolor="#FFFFFF">
<form>
Navigation buttons utilizing history go
<br>
<input type="button" value="Back" onClick="history.go(-1)">
<input type="button" value="Forward" onClick="history.go(1)">
<input type="button" value="Refresh" onClick="history.go(0)">
</form>
<p>
<a href="http://www.google.com/">Google</a> This is a link to a
website on the World Wide Web.
</p>
<table border="1">
<tr>
<td>row 1, cell 1</td>
<td>row 1, cell 2</td>
</tr>
<tr>
<td>row 2, cell 1</td>
<td>row 2, cell 2</td>
</tr>
</table>
</body>
</html>
```

10. Write the differences between XML and HTML.

[MODEL QUESTION]

**Answer:**

HTML (Hypertext Markup Language) has been around for a very long time and has been used extensively in webpage design that although it is already rare to see webpages written solely in HTML, it is considered as basic knowledge to the whole process of creating webpages.

XML (Extensible Markup Language), on the other hand is a more recent and much less known technology compared to HTML. XML was created as an adaptation of SGML (Standard Generalized Markup Language) for use in the World Wide Web. XML is a more structured and strict markup language compared to HTML that allowed users to create their own definitions and modularized code. It was made to create a standardized specifications for creating custom mark-up languages which are now known as XML dialects. Since XML was adapted from SGML it contains a lot of code and techniques that were originally from SGML like its strictness and a so called well-formedness. Certain rules should always be considered when creating code that is based on XML. There is even a well formed declaration with every document to state what type of document it is and to what rules should the processing be based on. This is very different compared to the very relaxed coding that is used in HTML.

When you process an HTML page, you would have some sort of result regardless of what the input was. The HTML processor tries to make sense of what was in the document and makes an output which it thinks best represents the input data. This is not true comes to XML. XML employs an error handling mechanism that is considered as "draconian". Whenever the XML processor encounters something that it cannot comprehend, it just creates an error report and terminates the processing of the file. That leaves you with an error box and no result at all unlike in HTML.

To put it in perspective, HTML is a markup language used to quickly and easily display some manner of output. It does not concern itself with correctness of the input and just tries to create an output based on the input file. XML on the other hand is a very strict markup language which is not usually used to create content. Its primary use is as a tool for creating other markup languages that create the needed content.

## PERL, JAVA SCRIPT, COOKIES, JAVA APPLETS

### Multiple Choice Type Questions

1. Which of the following is not an applet life cycle method?  
a) init ()      b) run ()      c) destroy ()      d) paint ()  
Answer: (b)

[WBUT 2013]

2. Variables are declared in Java Script using which of the following? [WBUT 2016]  
a) dim      b) var      c) function      d) variable  
Answer: (b)

3. PERL stands for  
a) Practical Extraction and Report Language  
b) Practical Example and Report Language  
c) Practical Expert on Report Language  
d) Practical Extraction and Reading Language  
Answer: (a)

[WBUT 2017]

4. Cookie is created and sent by  
a) Web browser      b) Web server  
c) Application server      d) Strut platform  
Answer: (b)

[WBUT 2017]

5. Cookies are stored in  
a) Web Server      b) Web Browser  
c) Application Server      d) Database Server  
Answer: (b)

[WBUT 2018]

6. PERL is a  
a) High level, cross-platform language  
b) High level, Platform Independent language  
c) Middle level, cross-platform language  
d) Middle level, Platform Independent language.  
Answer: (a)

[MODEL QUESTION]

7. Javascript's default object is  
a) navigator      b) documents      c) window      d) browser  
Answer: (c)

[MODEL QUESTION]

8. Applet is based on the concept of  
a) server push      b) server pull      c) client push      d) client pull  
Answer: (d)

[MODEL QUESTION]

### Short Answer Type Questions

1. a) What is associative array in PERL?

[WBUT 2013]

b) Write a program to find length of a string in PERL?

Answer:

a) Ordinary list arrays allow us to access their element by number. The first element of array @car is \$car[0]. The second element is \$car[1], and so on. But Perl also allows us to create arrays which are accessed by string. These are called *associative arrays*. To define an associative array we use the usual parenthesis notation, but the array itself is prefixed by a % sign. Suppose we want to create an array of people and their ages. It would look like this:

```
%ages = ("Sachin", 39,  
          "Rahul", 38,  
          "Dhoni", 27);
```

b)

```
my $strVar = "A simple example of a string variable";  
my $strLength = length($strVar);  
print "Our string has $strLength characters\n";
```

2. What are the advantages of JavaScript over HTML?

[WBUT 2013]

Answer:

The advantages of JavaScript over HTML is that, JavaScript enhances HTML by making it dynamic. HTML as we know is static and therefore once an HTML document has been created it cannot be changed.

JavaScript has two basic functionalities which are:

1. To build HTML dynamically as the web page is loaded and;
2. To monitor as well as react to User events.

3. What are the usage of: hover, active and: focus dynamic pseudo classes?

[WBUT 2014]

Answer:

**Hover pseudo-class:** The hover pseudo-class applies while the user designates an element (with some pointing device), but does not activate it. For example, a visual user agent could apply this pseudo-class when the cursor (mouse pointer) hovers over a box generated by the element. User agents not supporting interactive media do not have to support this pseudo-class. Some conforming user agents supporting interactive media may not be able to support this pseudo-class (e.g., a pen device).

**Active pseudo-class:** The active pseudo-class applies while an element is being activated by the user. For example, between the times the user presses the mouse button and releases it.

**Focus pseudo-class:** The focus pseudo-class applies while an element has the focus (accepts keyboard events or other forms of text input).

**4. What is cookie?**

[WBUT 2014, 2018]

**Answer:**

Cookies are the name given to the small text files your browser stores on your computer, which contain information relevant to the sites you have visited in the past. Another definition is that, cookie is a variable that is stored on the visitor's computer. Each time the same computer requests a page with a browser, it will send the cookie too. With JavaScript, you can both create and retrieve cookie values.

**5. Implement the following regular expression in Perl: a\*bc.**

[WBUT 2014]

**Answer:**

```
#!/usr/bin/ perl -w
# Regular Expression
print "Enter the string:";
chomp ($exp=<STDIN>);
if($exp =~ /a*bc/) {print "success\n"}
```

**6. Write a Java Script program to validate email id using regular expression.**

[WBUT 2015]

**Answer:**

```
<html>
<head>
<title>Check Email Address</title>
<script language="javascript">
function checkEmail(inputvalue){
    var pattern=/^([a-zA-Z0-9_.-])+@([a-zA-Z0-9_.-]+)\.([a-zA-
Z]+([a-zA-Z])+/";
    if(pattern.test(inputvalue)){
        alert("true");
    }else{
        alert("false");
    }
}
</script>
</head>
<body>
<form name="signupform">
Input your email: <input name="email" type="text" class="inputs"
id="email_address"
value="any@any.com" size="35" maxlength="255">
<input name="summit" type="submit" value="Check"
onClick="checkEmail(document.signupform.email.value)">
</form>
</body>
</html>
```

**7. a) What is Java applet?**

[WBUT 2015]

**b) Differentiate between java applet and application program.**

Answer:

- a) An Applet is a Java program that runs in a Web browser. They can be transported over the internet from one computer to another and run using the Applet Viewer or any web browser that supports Java. An applet like any application program can do many things for us. It can perform arithmetic operations, display graphics, play sounds, accept user input, create animations and play interactive games.

b)

Applet	Application
Small Program	Large Program
Used to run a program on client Browser	Can be executed on stand alone computer system
Applet is portable and can be executed by any JAVA supported browser.	Need JDK, JRE, JVM installed on client machine.
Applets are created by extending the <code>java.applet.Applet</code>	Applications are created by writing public static void <code>main(String[] s)</code> method.
Applet application has 5 methods which will be automatically invoked on occurrence of specific event	Application has a single start point which is main method
Example: <pre>import java.awt.*; import java.applet.*; public class NewApplet extends Applet {     public void init() { }     public void start() { }     public void stop() { }     public void destroy(){ }     public void paint(Graphics g) { }</pre>	<pre>public class NewApplication {     public static void main(String args[ ]) { } }</pre>

8. What are the different technologies available to make a webpage dynamic? Why does Java play a vital role in dynamic webpage creation? [WBUT 2016]

Answer:

Different technologies available to make a webpage dynamic are:

PHP, Javascript, or Actionscript to create dynamic pages.

One can also use frameworks like Ruby on Rails, Django for creating dynamic webpages.

#### Server-Side Dynamic Web Page

It is created by using server-side scripting. There are server-side scripting parameters that determine how to assemble a new web page which also include setting up of more client-side processing.

#### Client-Side Dynamic Web Page

It is processed using client side scripting such as JavaScript. And then passed in to Document Object Model (DOM).

JavaScript makes a website more interactive and user friendly. JavaScript helps easy navigation of the website and helps designers to guide the visitors with additional information or guide them through walkthroughs. Visual effects can also be achieved with JavaScript. JavaScript can be used effectively to create special effects like rollover for images.

JavaScript stands unique as it brings out all the special functionalities in the client's browser instead of the site's server. The role of JavaScript can never be denied as JavaScript can act as both object oriented language and procedural language.

**Q. Write a brief note on the role of Java Script in client side data validation with suitable examples. State also briefly the need of client side validation.**

[WBUT 2016]

**Answer:**

**1<sup>st</sup> Part:**

JavaScript scripting language is used as a client-side method for validation and other simple tasks. JavaScript isn't a fully fledged programming language like PHP; it can't connect to databases, it's limited as to which system resources it can interact with, and it can't do most tasks a web database application requires. However, JavaScript is good for interacting with a <form> and for controlling the display of data to the user.

Common uses of JavaScript in web database applications include:

- Validation of <form> data, the main topic of this section.
- Simple interaction with <form> data; e.g., JavaScript is often used to calculate values and display these in a data-entry widget.
- Enhancing user interactions by adding dynamic elements to a web page. Common features include pull-down menus, mouseover changes to the presentation (rollovers), and dialog boxes.
- Customizing the browser and using information from the browser to enhance presentation.

Most of these techniques are oriented around events. An event is an action that occurs—such as a mouse passing over an object or a user clicking on a button—and that can be trapped through JavaScript code.

**A simple JavaScript example to check if a <form> field is empty:**

```
<html>
<head>
  <title>Simple JavaScript Example</title>
<script type="text/javascript">
<!-- Hide the script from old browsers
function containsblanks(s)
{
  for(var i = 0; i &lt; s.value.length; i++)</pre>
```

```
        alert('The field must not contain whitespace');
        return false;
    }
}
return true;
// end hiding -->
</script>
</head>
<body>
<h2>Username Form</h2>
<form onSubmit="return(containsblanks(this.userName));"
method="post" action="test.php">
<input type="text" name="userName" size=10>
<input type="submit" value="SUBMIT">
</form>
</body>
</html>
```

**2<sup>nd</sup> part:**

In the Client Side Validation you can provide a better user experience by responding quickly at the browser level. When you perform a Client Side Validation, all the user inputs validated in the user's browser itself. Client Side validation does not require a round trip to the server, so the network traffic which will help your server perform better. This type of validation is done on the browser side using script languages such as JavaScript, VBScript or HTML5 attributes.

For example, if the user enters an invalid email format, you can show an error message immediately before the user move to the next field, so the user can correct every field before they submit the form.

Mostly the Client Side Validation depends on the JavaScript Language, so if users turn JavaScript off, it can easily bypass and submit dangerous input to the server. So the Client Side Validation cannot protect your application from malicious attacks on your server resources and databases.

**10. Write a simple servlet program which will return the current date and time.  
[WBUT 2018]**

**Answer:**

```
import java.io.*;
import java.text.*;
import java.util.Date;
import javax.servlet.*;
import javax.servlet.http.*;
public class CurrentDate extends HttpServlet {
public void doGet(HttpServletRequest request, HttpServletResponse
response) throws ServletException, IOException {
// Set response content type
```

```
PrintWriter out = response.getWriter();
String title = "Display Current Date & Time";
Date dNow = new Date();
SimpleDateFormat ft = new SimpleDateFormat ("E yyyy.MM.dd 'at'
hh:mm:ss a zzz");
String docType = "<!doctype html public \"-//w3c//dtd html 4.0. "
+
"transitional//en\\>\\n";
out.println(docType +
"<html>\\n" +
"<head><title>" + title + "</title></head>\\n" +
"<body bgcolor = \"#f0f0f0\\>\\n" +
"<h1 align = \"center\\>" + title + "</h1>\\n" +
"<h2 align = \"center\\>" + ft.format(dNow) + "</h2>\\n" +
"</body>
</html>";
);
}
}
```

**Output:**

Display Current Date & Time  
Mon 2010.06.21 at 10:06:44 PM GMT+04:00

**11. Create a JSP page to find the factorial of a number.**

[WBUT 2018]

**Answer:**

First install Netbeans Software. Then choose new project(web application). Now select a index.jsp page within "Web pages". and paste the following code to create a simple html page(i.e. your index page)

CODE:

```
<%--  
Document : index  
Created on : 12 Oct, 2012, 7:35:11 PM  
Author : nested code team  
--%>  
<%@page contentType="text/html" pageEncoding="UTF-8"%>  
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01  
Transitional//EN"  
"http://www.w3.org/TR/html4/loose.dtd">  
<html>  
<head>  
<meta http-equiv="Content-Type" content="text/html;  
charset=UTF-  
8">  
<title>JSP Page</title>  
</head>
```

```
<form action="fact.jsp ">
<h1>Enter the no :: <input type=text name=n ><br><br>
<input type=submit value="Submit"></h1>
</form></center>
</body>
</html>
```

Now we have to create the "fact.jsp" page, so choose again a new jsp page and give the name as "fact.jsp". Now paste the following code.

```
<HTML>
<HEAD>
<TITLE>Recursion</TITLE>
</HEAD>
<BODY>
<H1>factorial number Using Recursion</H1>
<%!
int numberfactorial(int number)
{
if (number == 1) {
return number;
}
else {
return number * numberfactorial(number - 1);
}
%>
<%
out.println("The factorial of 5 is " + numberfactorial(5));
%>
</BODY>
</HTML>
```

12. Write a function to create a cookie in JavaScript.

[MODEL QUESTION]

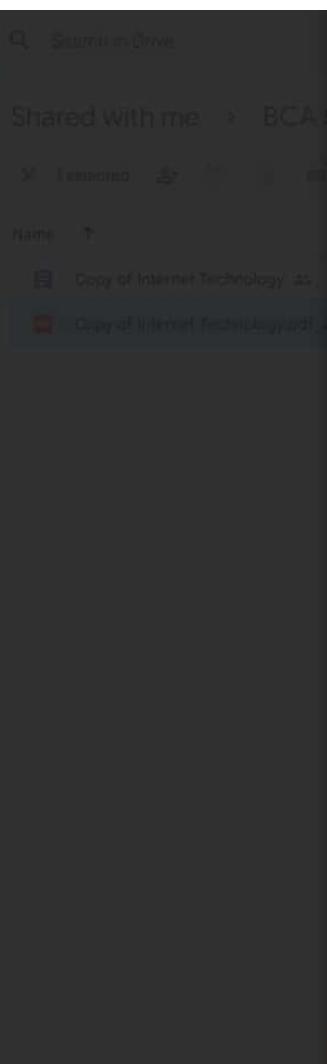
Answer:

```
function createCookie(name, value, days) {
    if (days) {
        var date = new Date();
        date.setTime(date.getTime()+(days*24*60*60*1000));
        var expires = "; expires=" + date.toGMTString();
    }
    else var expires = "";
    document.cookie = name + "=" + value + expires + "; path=/";
}
```

#### Long Answer Type Questions

Explain the life cycle of an applet using requisite figure.

IWBUT 2013. 2015

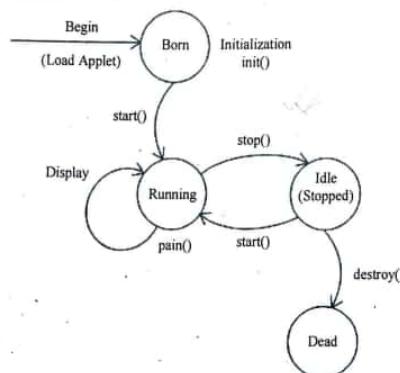


**Answer:**

Every Java applet inherits a set of default behavior from the Applet class. As a result, when an Applet is loaded, it undergoes a series of changes in its state as shown in figure. The applet states include:

- Born or Initialization state
  - Running or Start state
  - Idle or Stop state
  - Dead or Destroyed state

#### An Applet State transition diagram:



### Initialization state

The life cycle of an applet is begin on that time when the applet is first loaded into the browser. The init() method is called only one time in the life cycle on an applet. We can enter into the initialization stage by overriding the Applet class's init() method. The signature of the method is as follows:

```
public void init()
{
    .....
}
```

#### **Running or Start state**

Applet enters the running state when the system calls the start() method of Applet class. The start method of an applet is called after the initialization method init(). This method may be called multiple times when the Applet needs to be started or restarted. To provide our own start() code we have to override the Applet class's start() method. The signature of the method is as follows:

```
    public void start()  
    {
```

```
.....  
}
```

#### Idle or Stop state

An applet becomes idle when it is stopped from running. Stopping occurs automatically when we leave the page containing the currently running applet. We can do so by calling the stop methods explicitly. If we want to stop the applet explicitly, we should override the Applet class's stop method. The signature of the method is as follows:

```
public void stop()  
{  
.....  
}
```

#### Dead or Destroyed state

The applet is said to be dead when it is removed from memory. It occurs automatically by invoking the destroy() method when we quit the browser. The destroy() method is called only one time in the life cycle of Applet like init() method. The signature of the method is as follows:

```
public void destroy()  
{  
.....  
}
```

#### Paint or Display State

It is to be noted that the display state is not considered as a part of the applet's life cycle. The paint() method is defined in the Applet class and is inherited from the Component class, a super class of Applet.

The paint( ) method has one parameter of type Graphics. This parameter will contain the graphics context, which describes the graphics environment in which the applet is running. The signature of the method is as follows:

```
public void paint(Graphics g)  
{  
.....  
}
```

2. a) What is Applet? Discuss life-cycle of an Applet.

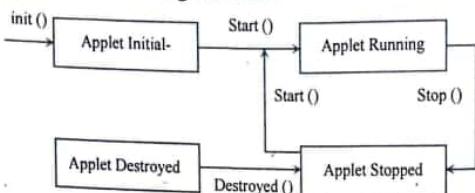
[WBUT 2016]

Answer:

1<sup>st</sup> Part:

An applet is a software component that typically runs inside some kind of container. The most common example of a container for Java applets is a Web browser such as IE or Firefox. Thus an applet can be thought of as a special kind of Java program which is used for internet programming. The applets reside in a server and they can be downloaded from the server to the client machine and executed on client machine provided that the browser is enabled with Java technology.

The applet life cycle is shown in figure below.



Each applet has four states - Born state, Running state, Idle state (may or may not) and Dead state.

**Born State:** When the class is executed the init function is automatically invoked. At this stage an applet is said to be born. This state is also called initialization state. During the applet life cycle, the born state occurs only once. The init function is defined within an applet. However, it can be overridden by the program. This function is used to initialize instance members, to load the required fonts, to initialize objects, to load pictures, to load back colors, etc.

**Running State:** After initialization, this state will automatically occur by invoking the start method of applet class which again calls the run method and which calls the paint method. The running state also occurs from idle state when the applet is reloaded.

**Idle State:** The idle state will make the execution of the applet to be halted temporarily. applet moves to this state when the currently executed applet is minimized or when the user switches over to another page.

At this point the stop method is invoked. From the idle state the applet can move to the running state.

**Dead State:** When the applet programs terminate, the destroy function is invoked which makes an applet to be in dead state.

b) Write a PERL script to show current date.

[WBUT 2016]

Answer:

```
#!/usr/local/bin/perl  
($day, $month, $year) = (localtime)[3,4,5];  
printf("The current date is %04d %02d %02d\n", $day, $month+1,  
$year+1900)
```

3. Write short notes on the following:

- a) Java socket
- b) Java application

[WBUT 2013, 2017]

[WBUT 2013]

Answer:

a) Java socket:

Java's socket model is derived from BSD (UNIX) sockets, introduced in the early 1980s for interprocess communication using IP.

Before start of communication, a connection or socket has to be established between the two hosts. There are five components in a socket: Protocol used, Source IP address, Source port number, Destination IP address, Destination port number.

#### ***Source and Destination IP address or Internet addresses:***

These are like an id to any machine, IP addresses are a 32-bit number, often represented as a "quad" of four 8-bit numbers separated by periods. They are organized into classes A, B, C, D, and E. IP address are manipulated in Java by the use of the InetAddress class. InetAddress takes care of the Domain Name System (DNS) look-up and reverse look-up. IP addresses can be specified by either the host name or the raw IP address. InetAddress provides methods to `getByName()`, `getAllByName()`, `getLocalHost()`, `getAddress()` for manipulating the IP address.

**Port numbers:** The port number field of an IP packet is specified as a 16-bit unsigned integer.

Port means a virtual opening, valid port numbers range from 1 through 65535. Some port numbers 1 to 10,000 reserved by IP for well-known services so we can not use it in our program. A well-known service is a service that is widely implemented which resides at a published, "well-known", port like HTTP uses port 80.

**Protocol:** A varied set of protocols can be used for transmission of data between one machine to another. TCP and UDP are most commonly used.

Typically for writing a Client-server program we need to write two sets of program one for server and another for client. The discussion below creates a UDP server and UDP client.

#### **b) Java application:**

A java application is fundamentally a computer program that is programmed using the java language. An example of such is java applets; a small programs that can run under numerous operating systems, as they are cross-platform. They are commonly used to provide better functionalities in WebPages. In spite of this, there is lots of java application. For example different mobile apps, android apps, games, facebook apps, etc. Java is widely used to make this application nowadays.

#### ***Developing General Java Applications***

The following short tutorial takes you through some of the basic steps of developing a Java SE application in NetBeans IDE. This tutorial assumes you already have some familiarity with developing Java applications. Along the way, you will see some of the IDE features that simplify application development.

You will create an application that converts several words into a single word that contains one letter from each of the other words. The resulting word is called an acrostic.

### **Creating a Java Application Project**

1. Choose File > New Project. Under Categories, select Java. Under Projects, select Java Application. Click Next.
2. Under Project Name, type MyApp. Make sure the Project Location is set to *NetBeansProjects*.
3. (Optional) Check the Use Dedicated Folder for Storing Libraries checkbox.
4. Enter acrostic. Main as the main class.
5. Ensure that the Create Main Class checkbox is checked.
6. Click Finish. The MyApp project is displayed in the Project window and Main.java opens in the Source Editor.

- 4. a) Explain different objects possible in Javascript. [MODEL QUESTION]**  
**b) What is the advantage of client-side scripting over server-side scripting?**  
**c) Write a javascript code to calculate factorial of a number.**

**Answer:**

a) The different types of built-in Javascript objects are Array object, Boolean object, Date object, Math object, Number object, String object and RegExp object. The most common ones are described below.

An **array** is a special variable, which can hold more than one value, at a time. Each element in the array has its own ID so that it can be easily accessed. The following code creates an array object called myCars:

```
var myCars=new Array();
```

The **date** object is a very powerful standalone object that you will use often.

Use the following syntax to create a date object:

```
var ObjectName = new Date (parameters)
```

where ObjectName is the name of the object, new is the object construction keyword parameters are optional and can define a specific date. The date object you create is a snapshot of an exact millisecond in time. It contains information on both date and time. It is important to understand that once the date object is created, the date and time that it contains does not change unless acted on by one of its many methods. If the parameters are left the object then contains the date and time that the computer clock is at.

### **String object**

When one declares and manipulates strings in JavaScript, one always writes them with single quotes' or double quotes "around them. This tells the browser that it is dealing with a string.

b) Many times the user has to submit some data to the server with help of a form. It is human to make mistakes when such data are entered in the HTML form. Now every time the data gets submitted the checking can be done in the server itself, but if there are mistakes the server has to send back response asking user to fill up again. Hence the overhead of sending data with mistakes and then getting proper response. sending back

should be left in the client side, to reduce the overhead and also to reduce unnecessary work from the server, who can then concentrate solely on the business logic part.

c)

```
function factorial(n) {
    if ((n == 0) || (n == 1))
        return 1
    else {
        result = (n * factorial(n-1) )
        return result
    }
}
```

**5. What is sessions? Why is a session object considered more secure and advantageous than cookies?**

[MODEL QUESTION]

**Answer:**

The Session object stores information needed for a particular user's session on the web server. It is automatically created every time when a servlet page from the web site or web application is requested by a user who does not already have a session, and it remains available until the session expires. The Session object is user specific. It can be used to store variables specific to a particular user and webserver will maintain these variables when the client moves across pages within your web site.

A site that ought to have much higher security standards might let users skip user name and passwords via cookies. For example, some of the big on-line bookstores use cookies to remember users, and let you order without reentering much of your personal information. However, they do not actually display the full credit card number, and only let you send books to an address that was entered when you did enter the credit card in full or use the username and password. As a result, someone using the person's computer (or stealing their cookie file) could do no more harm than sending a big book order to the credit card owner's address, where it could be refused. However, smaller companies might not be so careful, and access to someone's computer or cookie file could result in loss of valuable personal information. Even worse, incompetent sites might embed credit card or other sensitive information directly in the cookies themselves, rather than using innocuous identifiers which are only linked to real users on the server. So often session object is preferred over cookies.

**6. What are the advantages and disadvantages of applet?**

[MODEL QUESTION]

**Answer:**

**Advantages**

- it is simple to make and is cross platform
- the same applet can work on "all" installed versions of Java at the same time, rather than just the latest plug-in version only. However, if an applet requires a later version of the JRE the client will be forced to wait during the large download.
- it is supported by most web browsers

- it will cache in most web browsers, so will be quick to load when returning to a web page but may get stuck in the cache and have issues when new versions come out.
- it can have full access to the machine it is running on if the user agrees
- it can improve with use: after a first applet is run, the JVM is already running and starts quickly, benefitting regular users of Java but the JVM will need to restart each time the browser starts fresh.
- it can run at a speed that is comparable to (but generally slower than) other compiled languages such as C++, but many times faster than JavaScript
- it can move the work from the server to the client, making a web solution more scalable with the number of users/clients
- developers can develop and debug an applet direct simply by creating a main routine (either in the applet's class or in a separate class) and call init() and start() on the applet, thus allowing for development in their favorite J2SE development environment. All one has to do after that is re-test the applet in the appletviewer program or a web browser to ensure it conforms to security restrictions.

#### ***Disadvantages***

- It requires the Java plug-in, which is not available by default on all web browsers.
- It cannot start until the Java Virtual Machine is running, and this may have significant startup time the first time it is used.
- If untrusted, it has severely limited access to the user's system – in particular having no direct access to the client's disk or clipboard.
- Some organizations only allow software installed by the administrators.  
As a result, many users cannot view applets by default.

#### **7. Write short notes on the following:**

#### **[MODEL QUESTION]**

a) PERL

b) JavaScript

**Answer:**

a) PERL:

Perl is a family of high-level, general-purpose, interpreted, dynamic programming languages which can be used for a large variety of tasks. In the web development environment, Perl is a very powerful way to create dynamic web pages. A typical simple use of Perl would be for extracting information from a text file and printing out a report or for converting a text file into another form. But Perl provides a large number of tools for quite complicated problems, including systems programming. Programs written in Perl are called Perl scripts.

The process of creating a Perl script goes like this:

- Write a script in the Perl language
- Upload the script to a place in your website which allows scripts to run (typically the cgi-bin)
- Set the permissions of the script to allow anyone to run it

## INTERNET TECHNOLOGY

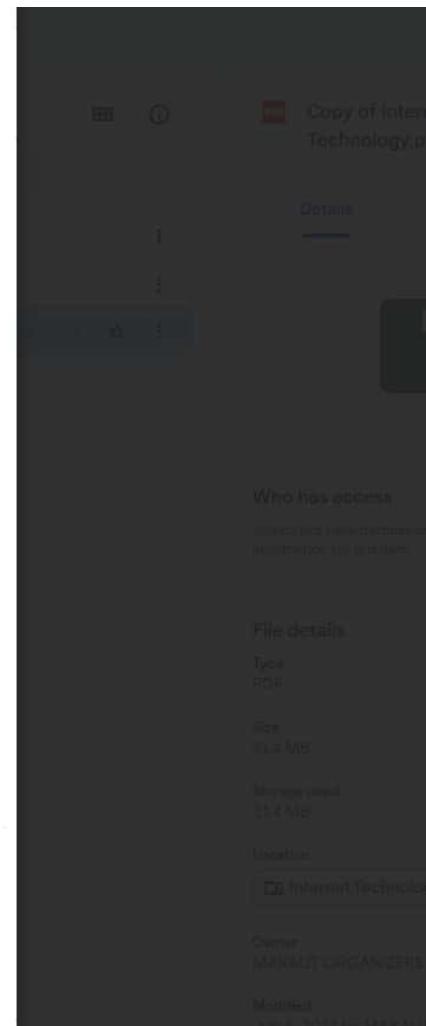
### **Example:**

```
#!/usr/bin/perl
print "Content-type: text/html\n\n";
print "<html><head><title>Test Page</title></head><body>";
print "Hello World!";
print "</body></html>";
```

### **b) JavaScript:**

JavaScript is a scripting language that was designed to add interactivity to HTML pages and is usually embedded directly into HTML pages. JavaScript is an interpreted language and everyone can use JavaScript without purchasing a license. Some of the features of Javascript are:

- **JavaScript gives HTML designers a programming tool** - HTML authors are normally not programmers, but JavaScript is a scripting language with a very simple syntax.
- **JavaScript can put dynamic text into an HTML page** - A JavaScript statement like this: document.write("<h1>" + name + "</h1>") can write a variable text into an HTML page
- **JavaScript can react to events** - A JavaScript can be set to execute when something happens, like when a page has finished loading or when a user clicks on an HTML element
- **JavaScript can read and write HTML elements** - A JavaScript can read and change the content of an HTML element
- **JavaScript can be used to validate data** - A JavaScript can be used to validate form data before it is submitted to a server. This saves the server from extra processing
- **JavaScript can be used to detect the visitor's browser** - A JavaScript can be used to detect the visitor's browser, and - depending on the browser - load another page specifically designed for that browser
- **JavaScript can be used to create cookies** - A JavaScript can be used to store and retrieve information on the visitor's computer.



## **NETWORK SECURITY**

### **Multiple Choice Type Questions**

1. Cookie is created and sent by  
 a) web server  
 b) application server  
 c) web browser  
 d) database server

Answer: (a) [WBUT 2013]

2. SSL layer is located between ..... and .....  
 a) transport layer, network layer  
 b) application layer, transport layer  
 c) data-link layer, physical layer  
 d) network layer, data-link layer

Answer: (b) [WBUT 2013]

3. Firewall is a specialized form of a  
 a) bridge                    b) disk  
 c) printer                    d) router

Answer: (d) [WBUT 2013]

4. RMI is one type of  
 a) distributed object application  
 b) scripting language  
 c) server side data validation technique  
 d) none of these

Answer: (c) [WBUT 2013]

5. Which of the following is tree view parser?  
 a) SAX  
 b) DOM  
 c) both (a) and (b)  
 d) none of these

Answer: (b) [WBUT 2014]

6. ..... programs can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly.  
 a) Zombie  
 b) Worm  
 c) Trojan Horses  
 d) Logic Bomb

Answer: (c) [WBUT 2014]

7. A remote object must be an instance of  
 a) java.rmi.RemoteObject  
 b) java.io.Serializable  
 c) java.lang.Cloneable  
 d) java.rmi.Remote

Answer: (d) [WBUT 2015]

8. Which of the following technologies is not a part of J2EE architecture?  
 a) JSP  
 b) Servlet  
 c) EJB  
 d) COBRA

Answer: (d) [WBUT 2016]

9. EJB contains  
a) unique interface  
c) two interfaces  
b) four interfaces  
d) no interface  
Answer: (c) [WBUT 2016]
10. The JSP tags are interpreted by  
a) JSP compiler  
c) JSP debugger  
b) JSP engine  
d) None of these  
Answer: (a) [WBUT 2016]
11. Which of the following protocols is stateless in nature?  
a) FTP b) HTTP c) TCP d) UUCP  
Answer: (b) [WBUT 2016]
12. After a servlet is destroyed garbage collection is performed by  
a) the server b) the servlet c) HTTP d) JVM  
Answer: (d) [WBUT 2016]
13. Which of the following is the intra domain routing protocol?  
a) RIP b) OSPF c) BGP d) None of these  
Answer: (a) and (b) [WBUT 2017]
14. RIP is based on  
a) Link State Routing b) Distance Vector Routing  
c) Path Vector Routing d) none of these  
Answer: (b) [WBUT 2017]
15. The position of SSL in TCP/IP protocol suite is  
a) between transport and internet layer  
b) between data link and physical layer  
c) between application and transport layer  
d) none of these  
Answer: (c) [WBUT 2017, 2018]

#### Short Answer Type Questions

1. a) What is the purpose of 'Time to Live' field of IPv4 datagram format?  
b) How salt makes dictionary attack difficult?  
c) Write the names of the components of VPN.  
Answer: [WBUT 2013]  
a) 'Time to Live' field in the datagram format specifies how long the datagram is allowed to "live" on the network, in terms of router hops. Each router decrements the value of the TTL field (reduces it by one) prior to transmitting it. If the TTL field drops to zero, the datagram is assumed to have taken too long a route and is discarded.

b) Salting a password means adding bits of information ("salt") to the given password before hashing it, so that the password is not merely guessable by a standard rainbow table, as the hashes are not of simple words anymore. Adding salts to the password make table, as without dictionary attacks for cracking large numbers of passwords much slower. As without salts, an attacker who is cracking many passwords at the same time only needs to hash each password guess once, and compare it to all the hashes. However, with salts, each password will likely have a different salt, thus each guess would have to be hashed separately for each salt, which is much slower since hashing is generally computationally expensive.

c) The components of VPN are VPN server, VPN client, tunnel, VPN connection, tunneling protocols, tunneled data, transit internetwork.

[WBUT 2013]

2. What do you mean by DOM? Explain briefly.

Answer:

The Document Object Model (DOM) is an application programming interface (*API*) for valid *HTML* and well-formed *XML* documents. It defines the logical structure of documents and the way a document is accessed and manipulated. In the DOM specification, the term "document" is used in the broad sense - increasingly, *XML* is being used as a way of representing many different kinds of information that may be stored in diverse systems, and much of this would traditionally be seen as data rather than as documents. Nevertheless, *XML* presents this data as documents, and the DOM may be used to manage this data.

With the Document Object Model, programmers can build documents, navigate their structure, and add, modify, or delete elements and content. Anything found in an *HTML* or *XML* document can be accessed, changed, deleted, or added using the Document Object Model, with a few exceptions - in particular, the DOM *interfaces* for the *XML* internal and external subsets have not yet been specified.

3. Design a firewall to block all traffic from 10.0.0.0/24 except port 23, 80 of TCP.

[WBUT 2013]

Answer:

```
# ipfwadm -a deny -P all -S 10.0.0.0/24 -D 0.0.0.0/24  
# ipfwadm -a accept -P tcp -S 10.0.0.0/24 -D 0/0 23  
# ipfwadm -a accept -P tcp -S 10.0.0.0/24 -D 0/0 80
```

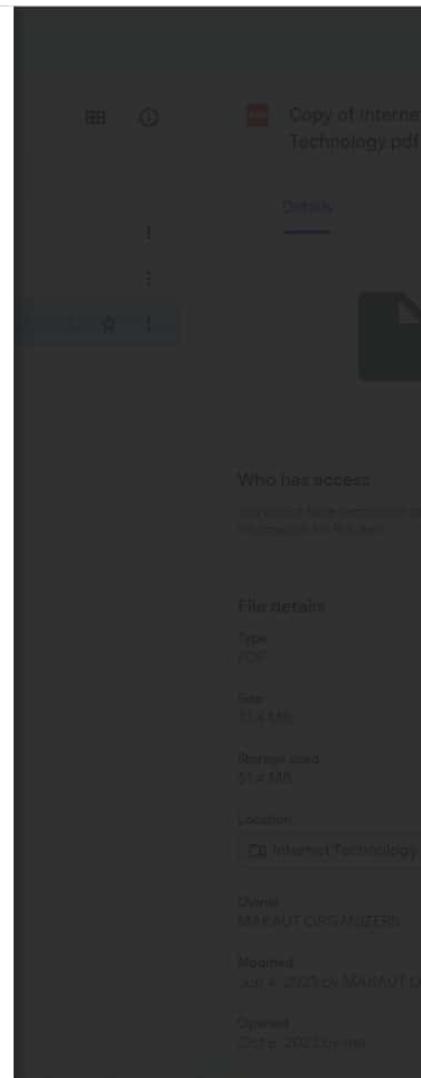
4. What do you mean by spoofing?

[WBUT 2014]

Answer:

Using IP spoofing attack an intruder can manipulate TCP/IP packets. Spoofing attack is done by pretending as a trusted user and gains the user's access privileges. The attacker may either use an IP address that is within the range of IP addresses for the network or use an authorized external IP address that is trusted and provides access to specified resources on the network.

Normally, an IP spoofing attack is limited to the injection of data or commands into an



Search in Drive

Shared with me > BCA

Name

Copy of Internet Technology

Copy of Internet Technology.pdf

Copy of Internet Technology.pdf

network connection. Spoofing can be of several types like IP Spoofing, e-mail spoofing, web spoofing etc.

6. a) What is Denial-of-service attack?  
b) Discuss briefly about proxy firewall.

[WBUT 2014, 2018]

Answer:

a) An attack in which a user or organization is deprived of the services of a resource that they would normally expect to have. The loss of service is related to a specific network service, such as e-mail or DNS. Attacks against DNS can force the loss of all services since names cannot be resolved. Denial of service (DoS) attacks has become a major threat to current computer networks. Denial of service implies that an attacker disables or corrupts networks, systems, or services with the intent to deny services to intended users. DoS attacks involve either crashing the system or slowing it down to the point that it is unusable. DoS can also be as simple as deleting or corrupting information. In most cases, performing the attack simply involves running a hack or script. The attacker does not need prior access to the target because a way to access it is all that is usually required. There are different types of DoS attacks like Buffer Overflow Attacks, SYN Flood Attack, Teardrop Attacks, Smurf Attack, DNS Attacks, Email Attacks, Physical Infrastructure Attacks.

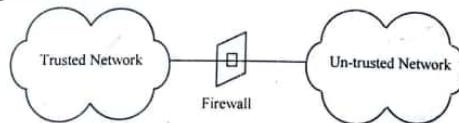
b) Proxy firewall is a firewall where proxy software runs on the firewall machine. These types of firewall are also called application level proxy. The proxy software running on the firewall acts on behalf of the users of an organisation. This program monitors all requests from users and allows access to only designated addresses outside. Limits use of certain browsers and disallow use of some protocols with known security holes. Now proxy firewall is the initiator of all sessions and thus knows every activity - thus ensuring security. It replaces the source address of transaction requestor with its own IP address, thus ensuring that others on Internet see only firewall's IP address and all other IP addresses of organization are hidden.

6. a) What is firewall?  
b) Briefly explain any two types of firewall.

[WBUT 2015]

Answer:

a) Firewall is a device which sits in between trusted network and untrusted network as shown in figure below. It allows only trusted data to enter and go through it as per the policy of the organization.



So firewalls serve as one of the key components of keeping networked computers safe and secure.

Copy of Internet Technology.pdf

Details

Who has access

File details

Type: PDF

Size: 21.1 MB

Modified: 16/1/2018 by MARYAM IDRIS

Opened: 16/1/2018 by MARYAM IDRIS

Owner: MARYAM IDRIS

b) Three types of firewalls are there to control traffic flows viz. packet filtering, application filtering and packet inspection.

- Packet-filtering firewalls validate packets based on protocol, source and/or destination IP addresses, source and/or destination port numbers, time range, Differentiate Services Code Point (DSCP), type of service (ToS), and various other parameters within the IP header.
- Application firewalls, as indicated by the name, work at Layer 7, or the application layer of the OSI model. These devices act on behalf of a client for requested services. This is also known as Proxy firewalls.

[WBUT 2015]

7. a) What is network congestion?

b) Describe congestion control strategies.

Answer:

a) Congestion, in the context of networks, refers to a network state where a node or link carries so much data that it may deteriorate network service quality, resulting in queuing delay, frame or data packet loss and the blocking of new connections. In a congested network, response time slows with reduced network throughput. Congestion occurs when bandwidth is insufficient and network data traffic exceeds capacity.

Data packet loss from congestion is partially countered by aggressive network protocol retransmission, which maintains a network congestion state after reducing the initial data load. This can create two stable states under the same data traffic load - one dealing with the initial load and the other maintaining reduced network throughput.

b) There are two strategies used generally for congestion control open-loop congestion control and closed-loop congestion control. The open-loop strategy attempts to solve the problem by providing a good design before the system is up and running. These solutions are generally static in nature as they do not take change according to the current state of operations of the system. They are also called as open-loop strategies which are further divided on the basis of whether these acts on source or destination ends. The second category is based on the concept of feedback. They are called as feedback strategies or closed-loop strategies. These solutions work by taking into consideration the system parameters and giving feedback to the portions of the subnet that can take action to reduce the congestion.

[WBUT 2015]

8. Describe different types of TCP Timers.

Answer:

TCP has to maintain a number of timers inside. All of them can be maintained by a single timer list. The four types of TCP timers are retransmission timer, persistence timer, keep-alive timer and time-waited timer.

Retransmission timer - Used to control a lost or discarded segment. This timer tells how long to wait for an ACK of a previously sent segment before retransmission. This depends on distance and network traffic density.

**Keep-alive timer** - There is a keep-alive timer that prevents long idle connections between two TCP's.

**Time-waited timer** - This timer is used during connection termination. When TCP closes a connection it is not really closed until this timer times out. It allows for FIN segments to be received.

9. With neat diagram differentiate between local and remote login. [WBUT 2015]

Answer:



10. What is the difference between Worm and Trojan Horse? [WBUT 2017]

Answer:

A worm, similar to a virus by design, spreads from computer to computer but unlike a virus, has the capability to travel without any human action by taking advantage of file or information transport features on the system which allows it to travel unaided. The biggest danger with a worm is its capability to replicate itself on a system and hence could send out hundreds or thousands of copies of itself, creating a huge devastating effect.

A Trojan horse is a program that appears to have some useful or benign purpose, but really masks some hidden malicious functionality. A Trojan horse can be only controlled locally. Trojan horses are one of the most common methods a computer criminal uses to infect your computer and collect personal information from your computer.

11. A network IP address is given as 192.168.110.25/27. Find the subnet mask, network address and no. of host possible in the network. [WBUT 2017]

Answer:

For the IP address 192.168.11.25/27,

Subnet mask is : 255.255.255.224

Network address: 192.168.110.0 ✓

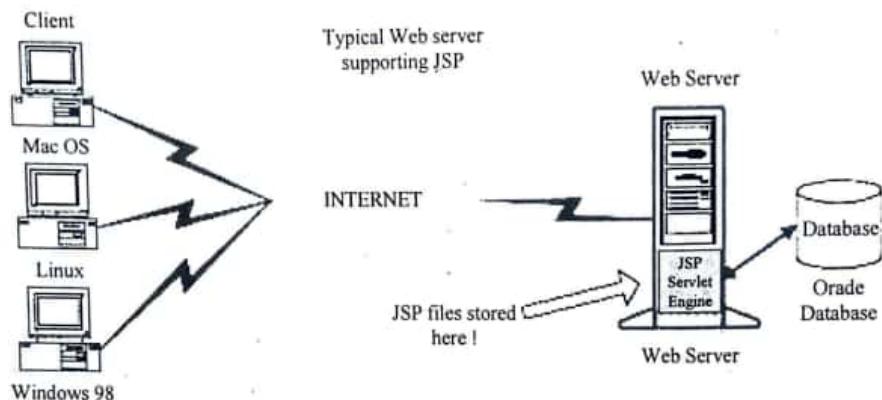
Broadcast address: 192.168.110.31

No. of host possible: 30

12. Briefly explain JSP architecture.

[WBUT 2018]

JSP's are built on top of SUN's servlet technology, JSPs are essentially as HTML page with special JSP tags embedded. These JSP tags can contain Java code.



#### **Steps required for a JSP Request**

1. The user goes to a website made using JSP. The user goes to a JSP page (ending with .jsp). The web browser makes the request via internet.
2. The JSP request gets sent to the web server.
3. The web server recognizes that the file required is special (.jsp), therefore passes to the JSP file to the JSP servlet engine.
4. If the JSP file has been called first time, the JSP file is parsed, otherwise go to step 7.
5. The next step is to generate a special servlet from the JSP file. All the HTML tags required is converted to println statement.
6. The servlet source code is compiled into class file.
7. The servlet is instantiated, calling init() and service() method.
8. HTML from the servlet output is sent via internet.
9. HTML result is displayed on the user's web browser.

#### **13. What is Web container? What is servlet engine?**

[WBUT 2018]

**Answer:**

**Web Container:** Web Container is an java application that controls servlet. Servlet do not have a main() method, So they require a container to load them. Container is a place where servlet gets deployed. When a client sends a request to web server that contain a servlet, server sends that request to container rather than to servlet directly. Container then finds out the requested servlet and pass the Http Request and response to servlet and loads the servlet methods i.e. doGet() or do Post(). Example of a web container is Tomcat.

**Servlet Engine:** To serve dynamic content, a Web server can include or call on a servlet engine, which is a program that takes a client request for a dynamic page and activates a Java class--the servlet--that provides the dynamic content. The content is typically derived from queries to the database, normally using a JDBC connection.

A servlet engine is almost always separate architecturally from the web server. For example, the Apache Web server can use the JServ servlet engine, which supports the Servlet 2.0 specification, or the newer Tomcat servlet engine, which supports the Java Servlet specification version 2.2.

The Oracle Servlet Engine running in the Oracle Java Virtual Machine (OJVM) is a servlet engine that works in conjunction with the Oracle HTTP Server, using the mod\_ose module.

**14. What is firewall rule chain? How does it work? How can we create user define rule chain?** [MODEL QUESTION]

**Answer:**

Firewall rule chain is a set of specific rules for filtering or restricting load in a network or node. The chain/rule can be based on source/destination ports, protocol, address etc. which verifies the incoming or outgoing packet with the rule chain set. If the packet matches the rule then based on the rule target either packet is allowed/drop/reject. Other than inbuilt chain, users can have their own rule / chain suitable for its customized needs. This user defined chain gives more effectiveness to the system.

**15. Explain how Security Association in IPSec is used in VPN Technology.** [MODEL QUESTION]

**Answer:**

Security Association is a relationship between two or more entities that describes how the entities will use security services to communicate securely. IPSec VPNs uses Internet Security association to provide key exchange while establishing and maintaining an IPSec connection. SA is established between a client and VPN gateway. The SA specifies the IPsec protocol to be used as well as cryptographic algorithms, cryptographic keys and their lifetime. IPSec provides many options for performing network encryption and authentication. Each IPSec connection can provide encryption, integrity, authenticity, or all three. When the security service is determined, the two IPSec peers must determine exactly which algorithms to use (for example, DES or 3DES for encryption, MD5 or SHA for integrity). After deciding on the algorithms, the two devices must share session keys. As you can see, there is quite a bit of information to manage. The security association is the method that IPSec uses to track all the particulars concerning a given IPSec communication session.

**16. Draw the IP security authentication header.** [MODEL QUESTION]

**Answer:**

**AH header:**

01	02	03	04	05	06	07	08	09	10	11	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	3	3
01	02	03	04	05	06	07	08	09	10	11	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8
Next header																											
Length																											
0																											
Security Parameters Index																											
Sequence number																											
Authentication Data :::																											

**Next header.** 8 bits.  
Specifies the next encapsulated protocol.  
**Length.** 8 bits.  
Size of the AH header in 32 bit words - 2. May be cleared to zero.  
**SPI, Security Parameters Index.** 32 bits.  
Contains a pseudo random value used to identify the security association for this datagram. If cleared to zero, a security association does not exist. Values in the range 1 to 255 are reserved.  
**Sequence number.** 32 bits.  
**Authentication Data.** Variable-length.  
This field must contain a multiple of 32 bit words.

**17. What are the functions provided by RTP?**

[MODEL QUESTION]

**Answer:**

The functions provided by RTP include:

1. Sequencing
2. Payload Identification
3. Frame Indication
4. Source Identification
5. Intra-media Synchronization

**Long Answer Type Questions**

**1. What is java RMI? Why is RMI useful under modern computing environment?**  
[WBUT 2013]

**Answer:**

Remote Method Invocation, abbreviated as RMI, provides support for distributed objects in Java, i.e. it allows objects to invoke methods on remote objects. The calling objects can use the exact same syntax as for local invocations.

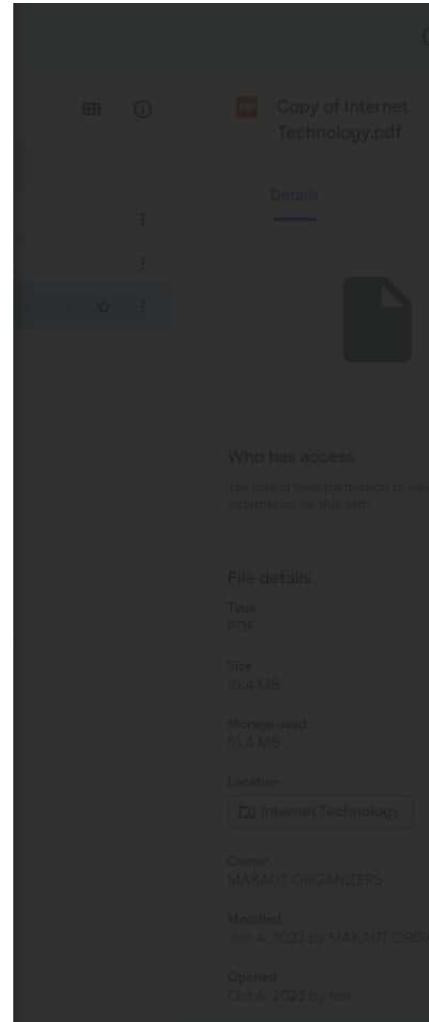
The Java RMI model has two general requirements. The first requirement is that the RMI model shall be simple and easy to use and the second requirement is that the model shall fit into the Java language in a natural way.

Using RMI we can restrict from unauthorized access by designing security policies. RMI present object collections using an object manager with name binding services. This program is called rmiregistry. RMI offers object (fields/methods). The interface for the object must be publicly shared between the client and server. These features of RMI is useful in modern computing environment.

2. a) What do you mean by the term 'DNS'? Explain DNS Recursive Resolution technique with a diagram.  
b) What is the significance of NVT in TELNET remote login procedure? Describe different types of operational mode in TELNET.  
[WBUT 2014]

OR,

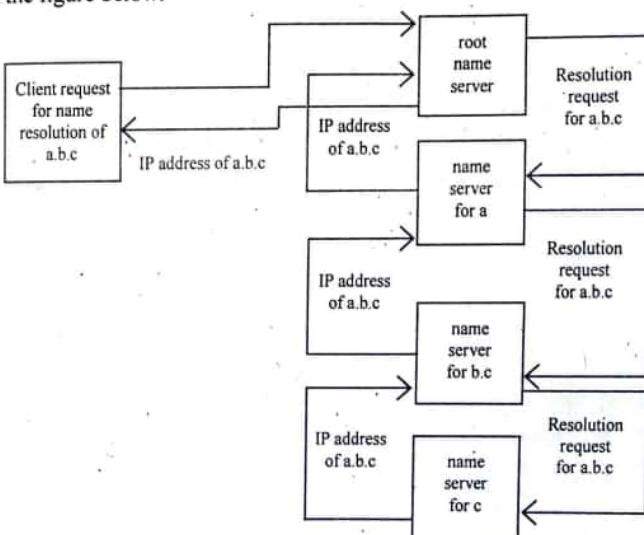
What is NVT? Why NVTs are required?  
[WBUT 2015]



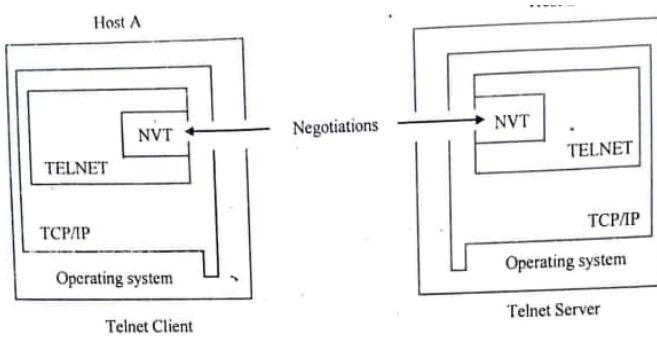
**Answer:**

a) DNS stands for Domain Name System. It is a distributed database system that is used to resolve host name to IP address. In Internet any host is identified by its IP address uniquely. Remembering each IP address is very difficult for users thus names are used to identify the hosts. But the Internet again understand the IP address the resolve of the name to IP address is done by the DNS.

There are two types of name resolution techniques, 1) Iterative and 2) Recursive. In recursive name resolution when a client sends a name resolution request to a name server, it responses back with the IP address if it has the answer. If it does not have the answer then it takes the responsibility of finding the answer on behalf of the client. It sends the request to other server, which in turn sends it recursively to another server if it does not have the answer. Finally the original root server gets the answer back and sends it to original client. Thus the original client sends only one request and eventually gets back the answer. Consider a client needs to resolve a.b.c the recursive resolution of the name is shown in the figure below.



b) Telnet is used for remote login across the Internet. The telnet client connects to telnet server through port 23. Both the telnet sessions opens a network virtual terminal (NVT). An NVT is an imaginary device having a basic structure common to a wide range of real terminals. Each host maps its own terminal characteristics to those of an NVT, and assumes that every other host will do the same. The NVT has a "printer" (or display) and a "keyboard". The keyboard produces outgoing data, which is sent over the TELNET connection. The printer receives the incoming data. The data representation is 7-bit ASCII.



The different types of operating mode of telnet are:

- 1) **Half-duplex:** This is the default mode used by NVT. It requires a GO AHEAD (GA) from the server before accepting user input. The user input is echoed locally from the NVT keyboard to the NVT printer so that only completed lines are sent from the client to the server.
- 2) **Character at a time:** Each character we typed is sent by itself to the server. The server echoes most characters, unless the application on the server turns echoing off. The problems with this mode are perceptible delays in echoing across long delay networks and the high volume of network traffic. It uses a combination of ECHO and SUPPRESS GO AHEAD.
- 3) **Line at a time:** Each line is transmitted at a time. When either of the ECHO or SUPPRESS GO AHEAD options are disabled, the operation is done line-by-line.
- 4) **Linemode:** It sends line by line. Though it looks as if it is same as Line at a time mode but Linemode is the appropriate and legal mode of operation.

3. a) What is classless addressing scheme? How does NAT work?  
 b) What do you mean about the term 'Subnet'? Why masking is necessary?  
 Distinguish between default mask and subnet mask.  
 c) A block of address is granted to a small organization. We know that one of the addresses is 205.16.37.39/28. What is the first and last addresses in the block?

[WBUT 2014]

**Answer:**

- a) CIDR eliminates the traditional concept of Class A, Class B, and Class C network addresses and replaces them with the generalized concept of a "network-prefix." Routers use the network-prefix, rather than the first 3 bits of the IP address, to determine the dividing point between the network number and the host number. As a result, CIDR supports the deployment of arbitrarily sized networks rather than the standard 8-bit, 16-bit, or 24-bit network numbers associated with classful addressing.

(not globally unique) addresses in the internal network into legal addresses, before packets are forwarded to another network.

As part of this capability, NAT can be configured to advertise only one address for the entire network to the outside world. This provides additional security by effectively hiding the entire internal network behind that address. NAT offers the dual functions of security and address conservation and is typically implemented in remote-access environments.

Basically, NAT allows a single device, such as a router, to act as an agent between the Internet (or public network) and a local network (or private network), which means that only a single unique IP address is required to represent an entire group of computers to anything outside their network.

b) Associated with IP address there are another type of address for e.g. 255.255.255.0, 255.255.0.0, 255.0.0.0 called subnet address. This allows identifying the dividing a network into small networks. So subnet means dividing a network into small networks. Subnet address is also used to find which portion of the IP address identifies the network and which identifies specific host. This is called as masking.

With the advent of subnetting, one can no longer rely on the definition of the IP address classes to determine the network ID in the IP address. A new value is needed to define which part of the IP address is the network ID and which part is the host ID regardless of whether class-based or subnetted network IDs are being used.

RFC 950 defines the use of a *subnet mask* (also referred to as an address mask) as a 32-bit value that is used to distinguish the network ID from the host ID in an arbitrary IP address. The bits of the subnet mask are defined as follows:

- All bits that correspond to the network ID are set to 1.
- All bits that correspond to the host ID are set to 0.

Each host on a TCP/IP network requires a subnet mask even on a single segment network. Either a default subnet mask, which is used when using class-based network IDs, or a custom subnet mask, which is used when subnetting or supernetting, is configured on each TCP/IP node.

Subnet masks are frequently expressed in dotted decimal notation. After the bits are set for the network ID and host ID portion, the resulting 32-bit number is converted to dotted decimal notation. Note that even though expressed in dotted decimal notation, a subnet mask is not an IP address.

A default subnet mask is based on the IP address classes and is used on TCP/IP networks that are not divided into subnets. Table 1 lists the default subnet masks using the dotted decimal notation for the subnet mask.

**Table 1 Default Subnet Masks (Dotted Decimal Notation)**

Address Class	Bits for Subnet Mask	Subnet Mask
Class A	1111111 00000000 00000000 00000000	255.0.0.0
Class B	11111111 11111111 00000000 00000000	255.255.0.0
Class C	11111111 11111111 11111111 00000000	255.255.255.0

Custom subnet masks are those that differ from these default subnet masks when we are doing subnetting or supernetting. For example, 138.96.58.0 is an 8-bit subnetted class B network ID. Eight bits of the class-based host ID are being used to express subnetted network IDs. The subnet mask uses a total of 24 bits (255.255.255.0) to define the subnetted network ID. The subnetted network ID and its corresponding subnet mask is then expressed in dotted decimal notation as:

138.96.58.0, 255.255.255.0

- c) One of the IP is: 205.16.37.39/28  
So subnet address is: 255.255.255.240  
Subnet id is: 205.16.37.32  
Broadcast is: 205.16.37.47  
Host address range is: 205.16.37.33 - 205.16.37.46  
First address is: 205.16.37.33  
Last address is: 205.16.37.46

4. a) Discuss the basic principle of security. Explain active attack passive with example.  
b) Differentiate between virus and worm. What is IP sniffing and IP spoofing? [WBUT 2015]

Answer:

a) 1<sup>st</sup> part:

Basic principles of security are

- **Confidentiality:** The sender encrypts the packets before transmitting them over the Internet.
- **Data integrity:** The receiver verifies the packets received from the sender to ensure they are not tampered during transmission.
- **Data origin authentication:** The receiver authenticates the legality of the sender.
- **Anti-replay:** The receiver examines the packets and rejects outdated or repeated packets.

2<sup>nd</sup> part:

An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target.

Types of active attacks:

- In a **masquerade attack**, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen login IDs and passwords, through finding security gaps in programs or through bypassing the authentication mechanism.
- In a **session replay attack**, a hacker steals an authorized user's log in information by stealing the session ID. The intruder gains access and the ability to do anything the authorized user can do on the website.