VI-SEM –CSE(MODEL QUESTION PAPER-1)
CST-602-INTERNET & WEB TECHNOLOGY

FULL MARK : 80 Time: 3hrs

Answer any Five including Q.no.1 &2
Figures in the right hand margin indicates marks

1.	Answer **ALL** questions.	(2X10)
(a)	How many bits are there in IP address ?	
(b)	Name two types of internet connectivity ?.	
(c)	What is URL.	
(d)	Explain dotted decimal notation?	
(e)	Define UDP.	
(f)	What is internet.	
(g)	What do you mean by WWW.	
(h)	Define CGI perl.	
(i)	What is POP3 & IMAP.	
(j)	Define end points.	
2.	Answer any **SIX** questions	(5X6)
(a)	Define XML. What are the applications and rules of XML.	
(b)	What do you mean by TELNET ? Explain how it works.	
(c)	What is FTP ? Write the FTP process model by specifying FTP client and server.	
(d)	Explain the routing mechanism of E-mail.	
(e)	Describe the concepts of HTTP protocol.	
(f)	Write the concept of DTD and explain it with example.	
(g)	Differentiate between direct and indirect delivery.	
(h)	State the properties of reliable delivery service.	
3.	Explain the mapping of domain name to address with examples.	(10)
4.	Define internet datagram. Write the fields of datagram format.	(10)
5.	State and explain TCP/IP internet layering model by suitable diagram.	(10)
6.	Why congestion occurs? Write the techniques to resolve /reduce congestion.	(10)
7.	Write shot notes on any **TWO** a)VB Script. (c) firewall. b)IMAP (d) Java script	(5X2)

VI-SEM –CSE(MODEL ANSWER PAPER-1)
CST-602-INTERNET & WEB TECHNOLOGY

1. a. Internet Protocol version 4 (IPv4) defines an IP address as a 32-bit number.

b. DSL and wireless are two types internet connectivity used.

c. Uniform Resource Locator (URL) is another name for a web address. URLs are made of letters, numbers. and other symbols in a standard form.

d. Dot-decimal notation is a presentation format for numerical data expressed as a string of decimal numbers each separated by a full stop. For example, the hexadecimal number 0xFF000000 may be expressed in dot-decimal notation as 255.0. 0.0

e.UDP (User Datagram Protocol) is a communications protocol that is used for establishing connections between applications on the internet. It speeds up transmissions by enabling the transfer of data before an agreement is provided by the receiver.

f. The Internet, sometimes called simply "the Net," is a worldwide system of computer networks a network of networks in which users at any one computer can, if they have permission, get information from any other computer.

g. The World Wide Web (WWW) is a network of online content that is formatted in HTML and accessed via HTTP. The term refers to all the interlinked HTML pages that can be accessed over the Internet.

h. CGI(Common Gateway Interface) is a protocol for executing scripts via web requests. CGI is having a very simple concept, but creating a CGI application requires real programming skills.

i. POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server.

j. The endpoint is a device or node that is connected to the LAN or WAN and accepts communications back and forth across the network.

2.a. Extensible Markup Language (XML) is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

There are nine basic rules for building good XML:

-All XML must have a root element.

-All tags must be closed.

-All tags must be properly nested.

-Tag names have strict limits.

-Tag names are case sensitive.

-Tag names cannot contain spaces.

-Attribute values must appear within quotes ("").

-White space is preserved.

XML Applications:

-at Chemical Markup Language. ...

-at Work: Mathematical Markup Language. ...

-at Work: Synchronized Multimedia Integration Language. ...

-at Work: HTML+TIME. ...

-at Work: XHTML. ...

-at Work: Microsoft's .

b.

Telnet stands for Teletype Network, but it can also be used as a verb; 'to telnet' is to establish a connection using the Telnet protocol.

HOW IT WORKS: Telnet provides users with a bidirectional interactive text-oriented communication system utilizing a virtual terminal connection over 8 byte. User data is interspersed in-band with telnet control information over the transmission control protocol (TCP). Often, Telnet was used on a terminal to execute functions remotely.

The user connects to the server by using the Telnet protocol, which means entering Telnet into a command prompt by following this syntax: telnet hostname port. The user then executes commands on the server by using specific Telnet commands into the Telnet prompt. To end a session and log off, the user ends a Telnet command with Telnet.

c.

FTP stands for File Transfer Protocol and, as the name implies, it is a way of transferring files between computers.

A File Transfer Protocol client (FTP client) is a software utility that establishes a connection between a host computer and a remote server, typically an FTP server. An FTP client provides the dual-direction transfer of data and files between two computers over a TCP network or an Internet connection. An FTP client works on a client/server architecture, where the host computer is the client and the remote FTP server is the central server.

An FTP client primarily provides a reliable means to transfer data between a local and remote host. It works when the host computer connects to the FTP server by specifying the domain, IP address, username and password of that server. After the user authentication, a connection is established between both systems, and the host computer can upload data onto the FTP server. An FTP client generally supports one or multiple simultaneous file transfers. Moreover, most FTP clients have the ability to connect to multiple FTP servers simultaneously, providing status updates of the uploading process, and notifications about successful and failed transfers. Besides uploading, the host computer can also download files from the FTP server using the FTP client. An FTP server needs a TCP/IP network for functioning and is dependent on usage of dedicated servers with one or more FTP clients. In order to ensure that connections can be established at all times from the clients, An FTP server is an important component in FTP architecture and helps in exchanging of files over internet.

d. Email routing will help you keep track of important emails and make sure the right people are kept in the loop.

There's a lot of ways you can use email routing:

- Send sales inquiries to the right person or department
- Instantly sort large amounts of email
- Automatically copy emails to managers for oversight and accountability
- Selectively archive important emails

Email routing is performed based entirely on the destination address of the email message. An email address has the following format:*username* @ *domain*

e. HTTP is a protocol designed to transfer information between computers over WWW (World Wide Web).
Simply, HTTP (Hyper Text Transfer Protocol), is used for transferring information like document, file, image, video

between computers over Internet. HTTP stands for Hypertext Transfer Protocol. (HyperText Transfer Protocol) The communications protocol used to connect to Web servers on the Internet or on a local network (intranet). Its primary function is to establish a connection with the server and send HTML pages back to the user's browser. It is also used to download files from the server either to the browser or to any other requesting application that uses HTTP.

Addresses of websites begin with an http:// prefix; however, Web browsers typically default to the HTTP protocol. For example, typing www.yahoo.com is the same as typing http://www.yahoo.com. In fact, only yahoo.com has to be typed in.

A Stateless Connection

HTTP is a "stateless" request/response system. The connection is maintained between client and server only for the immediate request, and the connection is closed. After the HTTP client establishes a TCP connection with the server and sends it a request command, the server sends back its response and closes the connection.
The first version of HTTP caused considerable overhead. Each time a graphics file on the page was requested, a new protocol connection had to be established between the browser and the server. In HTTP Version 1.1, multiple files could be downloaded with the same connection. It also improved caching and made it easier to create virtual hosts (multiple websites on the same server).

f. DTD stands for Document Type Definition. It defines the legal building blocks of an XML document. It is used to define document structure with a list of legal elements and attributes. The purpose of a DTD is to define the structure of an XML document. It defines the structure with a list of legal elements: The DTD above is interpreted like this:

- !DOCTYPE note defines that the root element of the document is note
- !ELEMENT note defines that the note element must contain the elements: "to, from, heading, body"
- !ELEMENT to defines the to element to be of type "#PCDATA"
- !ELEMENT from defines the from element to be of type "#PCDATA"
- !ELEMENT heading defines the heading element to be of type "#PCDATA"
- !ELEMENT body defines the body element to be of type "#PCDATA"

g.

Direct Delivery:

In a direct delivery, the final destination of the packet is a host connected to the same physical network as the deliverer. Direct delivery occurs when the source and destination of the packet are located on the same physical network or when the delivery is between the last router and the destination host. The sender can easily determine if the delivery is direct. It can extract the network address of the destination (using the mask) and compare this address with the addresses of the networks to which it is connected. If a match is found, the delivery is direct.

Indirect Delivery:

If the destination host is not on the same network as the deliverer, the packet is delivered indirectly. In an indirect delivery, the packet goes from router to router until it reaches the one connected to the same physical network as its final destination.

h. Properties of Reliable Delivery Service

1. Stream Orientation: Stream delivery service on destination passes to the receiver exact same sequence of bytes that the sender passes it to the source.

2. Virtual Circuit Connection: Protocol software on both the ends communicate by verifying that the transfer is authorized and both sides are ready. Once all details have been settled, the protocol modules inform the application programs that the connection has been established and that transfer can begin.

3. Buffered transfer : When transferring data, each application uses whatever size pieces it finds convenient, which can be as small as a single octet.

4. Unstructured stream : Application programs using the stream service must understand stream content and agree on stream format before they initiate a connection.

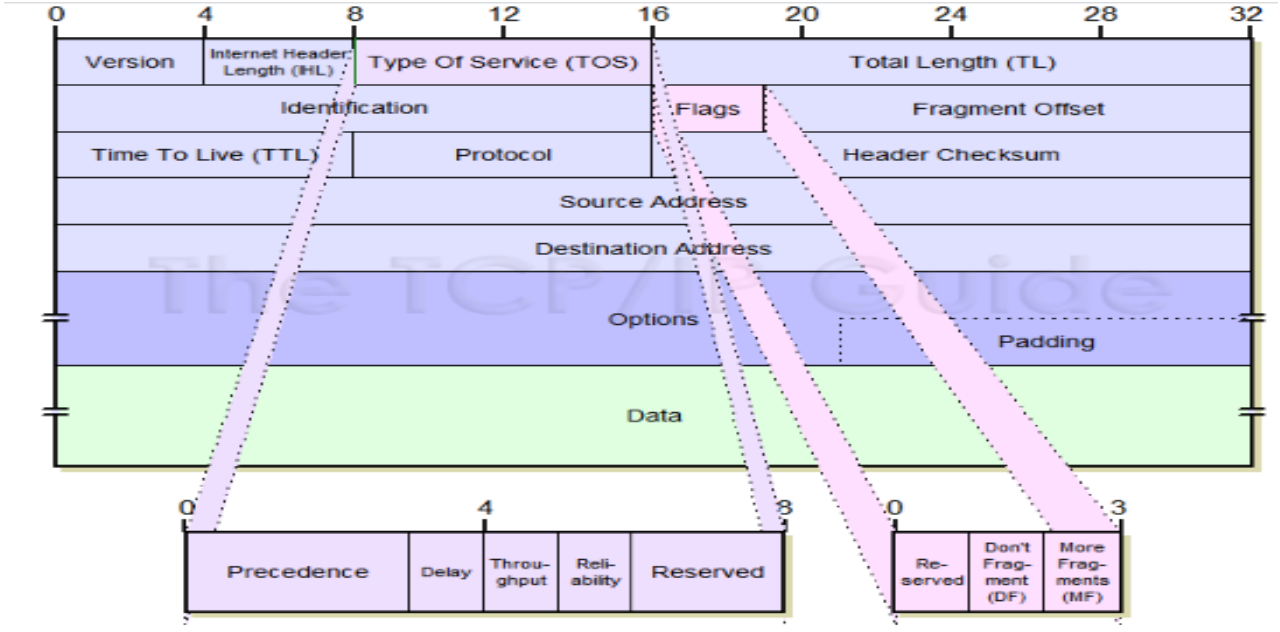
5. Full duplex connection : A full duplex connection consists of two independent streams flowing in opposite directions, with no apparent interaction. The advantage of a full duplex connection is that the underlying protocol software can send control information for one stream back to the source in datagrams carrying data in the opposite direction. Such piggybacking reduces network traffic.

3. One of the most fundamental instruments of the internet is the Domain Name System, or DNS. (Although many people think "DNS" stands for "Domain Name Server," it really stands for "Domain Name System.") DNS is a protocol within the set of standards for how computers exchange data on the internet and on many private networks, known as the TCP/IP protocol suite. Its purpose is vital, as it helps convert easy-to-understand domain names like "howstuffworks.com" into an Internet Protocol (IP) address, such as 70.42.251.42 that computers use to identify each other on the network. It is, in short, a system of matching names with numbers. Computers and other network devices on the internet use an IP address to route your request to the site you're trying to reach. This is similar to dialing a phone number to connect to the person you're trying to call. Thanks to DNS, though, you don't have to keep your own address book of IP addresses. Instead, you just connect through a domain name server, also called a DNS server or name server, which manages a massive database that maps domain names to IP addresses. Whether you're accessing a website or sending e-mail, your computer uses a DNS server to look up the domain name you're trying to access. The proper term for this process is DNS name resolution, and you would say that the DNS server resolves the domain name to the IP address. Without DNS servers, the internet would shut down very quickly. But how does your computer know what DNS server to use? Typically, when you connect to your home network, internet service provider (ISP) or WiFi network, the modem or router that assigns your computer's network address also sends some important network configuration information to your computer or mobile device. That configuration includes one or more DNS servers that the device should use when translating DNS names to IP address.

So far, you've read about some important DNS basics. The rest of this article dives deeper into domain name servers and name resolution. It even includes an introduction to managing your own DNS server. Let's start by looking at how IP addresses are structured and how that's important to the name resolution process. When a user types a human-readable address into the browser, the operating system’s DNS client will check for information in a local cache. If the requested address isn’t there, it will look for a DNS server in the local area network (LAN). When the local DNS server receives the query, and the requested domain name is found, it will return the result.For example the DNS provides mapping between human-readable names (like www.amazon.com) and their associated IP addresses (like 205.251.242.103). DNS can be best compared to a phone book where you look up the phone numbers listed by easier-to-remember names. DNS comes under the application layer protocol.

If the name is not found, the local server will forward the query to a DNS cache server, often provided by the Internet Service Provider (ISP). Since the DNS server's cache contains a temporary store of DNS records, it will quickly respond to requests. These DNS cache servers are called *not authoritative DNS servers* as they provide request resolution based in a cached value acquired from *authoritative DNS servers*. An Authoritative Root Name Server maintains and provides a list of authoritative name servers for each of the top-level domains (.com, .org, etc.).An Authoritative Top Level Domain Name Server maintains and provides a list of authoritative name servers for all domains. Its job is to query name servers to find and return the authoritative name server for the requested domain.

4. A datagram is a basic transfer unit associated with a packet-switched network. Datagrams provide a connectionless communication service across a packet-switched network. The delivery, arrival time, and order of arrival of datagrams need not be guaranteed by the network. Its format is given below:



Version: Identifies the version of IP used to generate the datagram. For IPv4, this is of course the number 4. The purpose of this field is to ensure compatibility between devices that may be running different versions of IP. In general, a device running an older version of IP will reject datagrams created by newer implementations, under the assumption that the older version may not be able to interpret the newer datagram correctly.
Internet Header Length (IHL): Specifies the length of the IP header, in 32-bit words. This includes the length of any options fields and padding.
Type Of Service (TOS): A field designed to carry information to provide quality of service features, such as prioritized delivery, for IP datagrams
Total Length (TL): Specifies the total length of the IP datagram, in bytes. Since this field is 16 bits wide, the maximum length of an IP datagram is 65,535 bytes, though most are much smaller.
Identification: This field contains a 16-bit value that is common to each of the fragments belonging to a particular message; for datagrams originally sent unfragmented it is still filled in, so it can be used if the datagram must be fragmented by a router during delivery.
Each datagram has two components, a header and a data payload. The header contains all the information sufficient for routing from the originating equipment to the destination without relying on prior exchanges between the equipment and the network. Headers may include source and destination addresses as well as a type field. The payload is the data to be transported. This process of nesting data payloads in a tagged header is called encapsulation. The internet layer is a datagram service provided by an IP. For example, UDP is run by a datagram service on the internet layer. IP is an entirely connectionless, best effort, unreliable, message delivery service. TCP is a higher level protocol running on top of IP that provides a reliable connection-oriented service.
5. TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of Defence's Project Research Agency (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.
The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact untill the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer.

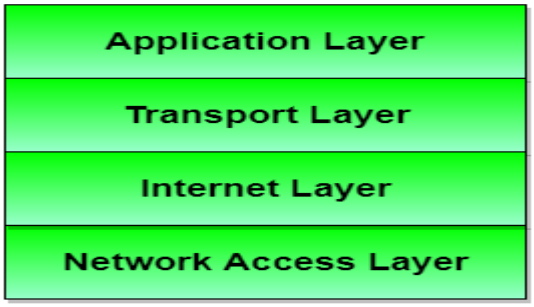
Layer 1: Host-to-network Layer

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

Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.

4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.
6. The various functions performed by the Internet Layer are:
    - Delivering IP packets
    - Performing routing
    - Avoiding congestion



Layer 3: Transport Layer

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

Layer 4: Application Layer

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

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

6. 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.

Congestion Control techniques in Computer Networks

Congestion control refers to the techniques used to control or prevent congestion. Congestion control techniques can be broadly classified into two categories:

Open Loop Congestion Control:

Open loop congestion control policies are applied to prevent congestion before it happens. The congestion control is handled either by the source or the destination.

Policies adopted by open loop congestion control :-

1. Retransmission Policy :
   It is the policy in which retransmission of the packets are taken care. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. This transmission may increase the congestion in the network.
   To prevent congestion, retransmission timers must be designed to prevent congestion and also able to optimize efficiency.
2. Window Policy :
   The type of window at the sender side may also affect the congestion. Several packets in the Go-back-n window are resent, although some packets may be received successfully at the receiver side. This duplication may increase the congestion in the network and making it worse.
   Therefore, Selective repeat window should be adopted as it sends the specific packet that may have been lost.
3. Discarding Policy :
   A good discarding policy adopted by the routers is that the routers may prevent congestion and at the same time partially discards the corrupted or less sensitive package and also able to maintain the quality of a message.
   In case of audio file transmission, routers can discard less sensitive packets to prevent congestion and also maintain the quality of the audio file.
4. Acknowledgment Policy :
   Since acknowledgement are also the part of the load in network, the acknowledgment policy imposed by the receiver may also affect congestion. Several approaches can be used to prevent congestion related to acknowledgment.
   The receiver should send acknowledgement for N packets rather than sending acknowledgement for a single packet. The receiver should send a acknowledgment only if it has to sent a packet or a timer expires.
5. Admission Policy :
   In admission policy a mechanism should be used to prevent congestion. Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of a congestion or there is

a congestion in the network, router should deny establishing a virtual network connection to prevent further congestion.

All the above policies are adopted to prevent congestion before it happens in the network.

Closed Loop Congestion Control:

Closed loop congestion control technique is used to treat or alleviate congestion after it happens. Several techniques are used by different protocols; some of them are:

1. Backpressure :
   Backpressure is a technique in which a congested node stop receiving packet from upstream node. This may cause the upstream node or nodes to become congested and rejects receiving data from above nodes. Backpressure is a node-to-node congestion control technique that propagate in the opposite direction of data flow. In above diagram the 3rd node is congested and stops receiving packets as a result 2nd node may be get congested due to slowing down of the output data flow. Similarly 1st node may get congested and informs the source to slow down.
2. Choke Packet Technique :
   Choke packet technique is applicable to both virtual networks as well as datagram subnets. A choke packet is a packet sent by a node to the source to inform it of congestion. Each router monitor its resources and the utilization at each of its output lines. whenever the resource utilization exceeds the threshold value which is set by the administrator, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic. The intermediate nodes through which the packets has traveled are not warned about congestion.

3. Implicit Signaling :
   In implicit signaling, there is no communication between the congested nodes and the source. The source guesses that there is congestion in a network. For example when sender sends several packets and there is no acknowledgment for a while, one assumption is that there is a congestion.
4. Explicit Signaling :
   In explicit signaling, if a node experiences congestion it can explicitly sends a packet to the source or destination to inform about congestion. The difference between choke packet and explicit signaling is that the signal is included in the packets that carry data rather than creating different packet as in case of choke packet technique.
   Explicit signaling can occur in either forward or backward direction.
   - Forward Signaling : In forward signaling signal is sent in the direction of the congestion. The destination is warned about congestion. The reciever in this case adopt policies to prevent further congestion.
   - Backward Signaling : In backward signaling signal is sent in the opposite direction of the congestion. The source is warned about congestion and it needs to slow down.

7.a. VBSCRIPT:

It is used in Windows Operating System and is a client-side scripting language similar to Visual Basic. It gives different functionalities to the web pages and designs the user interaction in a different manner. It is easy to learn and windows administrators find it easy to use than any other scripting languages. It is an un-typed language and developer cannot define the data types in advance in the scripts. VB Script is not case sensitive and has an extension of .vbs in the language. It works similar to JavaScript when employed on the client side in Internet Explorer. The executable instructions of the VBScript are included in the HTML pages and it also directly interacts with the DOM (Document Object Model) of the page to do things that are not possible by HTML alone. But there is no built-in support for it in other browsers such as Mozilla Firefox or Google Chrome or Opera, etc. which is why you might either need to install an

extension to interpret the VBScript or most developers go with JavaScript to achieve cross-browser compatibility. It is also used in developing the Windows Applications. Any standalone VBScript will have a .vbs extension.

b. IMAP allows you to access your email wherever you are, from any device. When you read an email message using IMAP, you aren't actually downloading or storing it on your computer; instead, you're reading it from the email service. As a result, you can check your email from different devices, anywhere in the world: your phone, a computer, a friend's computer.IMAP only downloads a message when you click on it, and attachments aren't automatically downloaded. This way you're able to check your messages a lot more quickly than POP. The easiest way to understand how IMAP works is by thinking of it as an intermediary between your email client and your email server. Email servers are always used when sending and receiving email messages. With IMAP, though, they remain on the server unless you explicitly delete them from it. When you sign into an email client like Microsoft Outlook, it contacts the email server using IMAP. The headers of all of your email messages are then displayed.

c. A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet. Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices. Firewalls can either be software or hardware, though it's best to have both. A software firewall is a program installed on each computer and regulates traffic through port numbers and applications, while a physical firewall is a piece of equipment installed between your network and gateway.

d. JavaScript is an object orient programming language designed to make web development easier and more attractive. In most cases, JavaScript is used to create responsive, interactive elements for web pages.JavaScript is a text-based programming language used both on the client-side and server-side that allows you to make web pages interactive. Where HTML and CSS are languages that give structure and style to web pages, JavaScript gives web pages interactive elements that engage a user.It is used because as below:

- JavaScript is the only programming language native to the web browser
- JavaScript is the most popular language
- There's a low threshold to get started
- It's a fun language to learn.