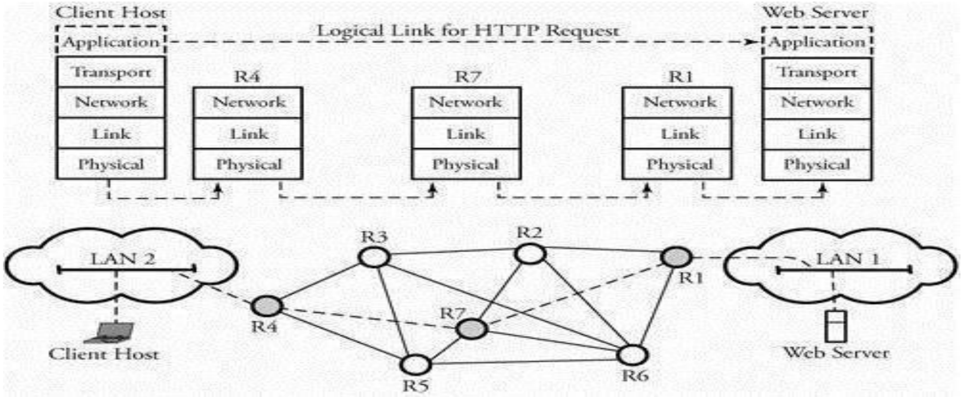
Module 5

An application layer protocol defines how application processes (clients and servers), running on different end systems, pass messages to each other. Inparticular, an application layer protocol defines:

- The types of messages, e.g., request messages and response messages.
- The syntax of the various message types, i.e., the fields in the message and how the fields are delineated.
- The semantics of the fields, i.e., the meaning of the information that the field is supposed to contain;
- Rules for determining when and how a process sends messages and responds to messages.



Client and Server Model

A client/server model provides specific computational services, such as partial-time usage services to multiple machines. Reliable communication protocols, such as TCP, allow interactive use of remote servers as well. For example, we can build a server that provides remote

image-processing services to clients. Implementing such a communication service requires a server loaded with the application protocol to accept requests and a client to make such requests. To invoke remote image processing, a user first executes a client program establishing a TCP connection to a server. Then, the client begins transmitting pieces of a raw image to the server. The server processes the received objects and sends the results back.

Domain Name Server (DNS) in Application Layer

DNS is a host name to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.

Requirement

Every host is identified by the IP address but remembering numbers is very difficult for the people and also the IP addresses are not static therefore a mapping is required to change the domain name to IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.

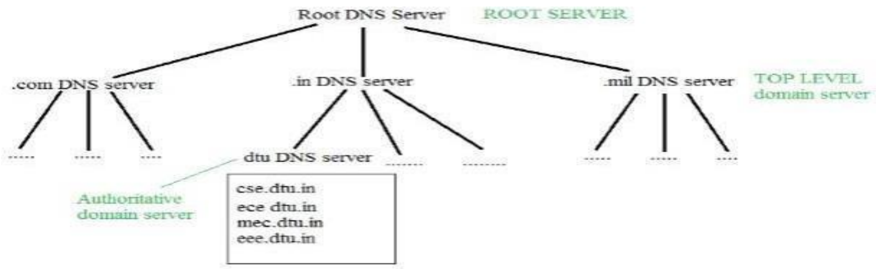
Domain

There are various kinds of DOMAIN :

1. Generic domain: .com(commercial) .edu(educational) .mil(military) .org(non profit organization) .net(similar to commercial) all these are generic domain.

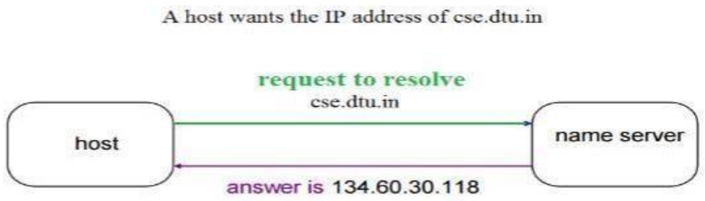
2. Country domain :.in (india) .us .uk
3. Inverse domain if we want to know what is the domain name of the website. Ip to domain name mapping.So DNS can provide both the mapping for example to find the ip addresses of geeksforgeeks.org then we have to type nslookup www.geeksforgeeks.org.

Organization of Domain



It is Very difficult to find out the ip address associated to a website because there are millions of websites and with all those websites we should be able to generate the ip address immediately, there should not be a lot of delay for that to happen organization of database is very important.
DNS record – Domain name, ip address what is the validity?? what is the time to live ?? and all the information related to that domain name. These records are stored in tree like structure.
Namespace – Set of possible names, flat or hierarchical . Naming system maintains a collection of bindings of names to values – given a name, a resolution mechanism returns the corresponding value –
Name server – It is an implementation of the resolution mechanism.. DNS (Domain Name System) = Name service in Internet – Zone is an administrative unit, domain is a subtree.

Name to Address Resolution



The host request the DNS name server to resolve the domain name. And the name server returns the IP address corresponding to that domain name to the host so that the host can future connect to that IP address.

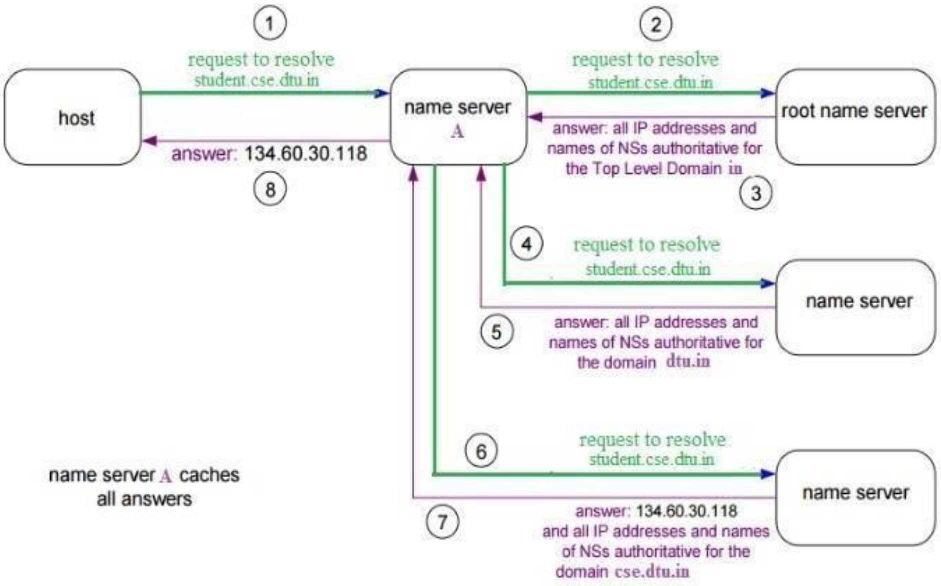
Hierarchy of Name Servers

Root name servers – It is contacted by name servers that can not resolve the name. It contacts authoritative name server if name mapping is not known. It then gets the mapping and return the IP address to the host.

Top level server – It is responsible for com, org, edu etc and all top level country domains like uk, fr, ca, in etc. They have info about authoritative domain servers and know names and IP addresses of each authoritative name server for the secondlevel domains.

Authoritative name servers This is organization's DNS server, providing authoritative hostName to IP mapping for organization servers. It can be maintained by organization or service provider. In order to reach cse.dtu.in we have to ask the root DNS server, then it will point out to the top level domain server and then to authoritative domain name server which actually contains the IP address. So the authoritative domain server will return the associative ip address.

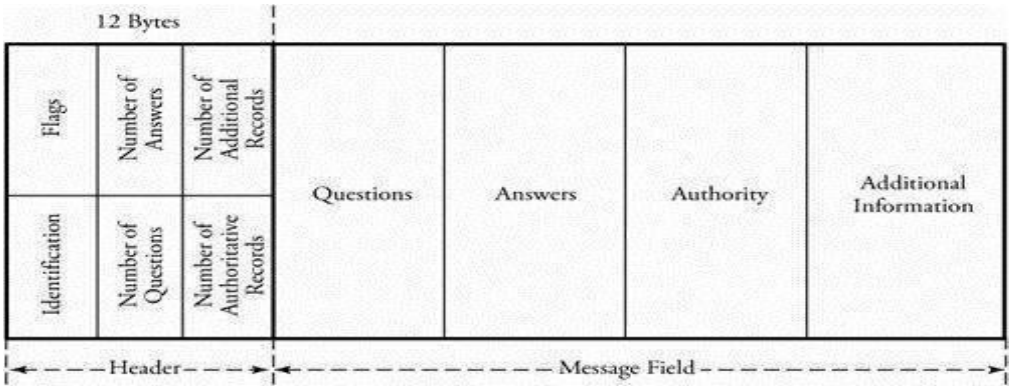
Domain Name Server


1
request to resolve student.cse.dtu.in
2
request to resolve student.cse.dtu.in
host
name server A
root name server
answer: 134.60.30.118
8
answer: all IP addresses and names of NSs authoritative for the Top Level Domain in
3
4
request to resolve student.cse.dtu.in
name server
5
answer: all IP addresses and names of NSs authoritative for the domain dtu.in
6
request to resolve student.cse.dtu.in
name server
name server A caches all answers
7
answer: 134.60.30.118 and all IP addresses and names of NSs authoritative for the domain cse.dtu.in

The client machine sends a request to the local name server, which , if root does not find the address in its database, sends a request to the root name server , which in turn, will route the query to an intermediate or authoritative name server. The root name server can also contain some hostName to IP address mappings . The intermediate name server always knows who the authoritative name server is. So finally the IP address is returned to the local name server which in turn returns the IP address to the host.

DNS Message Format

DNS communication is made possible through query and reply messages. Both message types have the 12-byte header format.



DNS message format

The header has six fields as follows. A client uses the identification field to match the reply with the query. This field may appear with a different number each time a client transmits a query. The server copies this number in its reply. The flags field contains subfields that represent the type of the message, such as the type of answer requested or requested DNS recursive or iterative mapping. The number of questions field indicates how many queries are in the question portion of the message. The number of answers shows how many answers are in the answer field. For the query message, this field contains all zeros. The number of authoritative records field consists of the number of authoritative records in the authority portion of a reply message. Similarly, this field is filled by zeros for a query message. Finally, the number of additional records field records are in the additional information portion of a reply message and is similarly filled by zeros in a query message.

Remote Login Protocols

A client/server model can create a mechanism that allows a user to establish a session on the remote machine and then run its applications. This application is known as remote login . A user may want to run such applications at a remote site, with results to be transferred back to its local site. For example, an employee working at home can log in to his/her work server to access application programs for doing a project. This can be done by a client/server application program for the desired service. Two remote login protocols are TELNET and SSH.

TELNET (Terminal Network):

- TELNET is client-server application that allows a user to log onto remote machine and lets the user to access any application program on a remote computer.
- TELNET uses the NVT (Network Virtual Terminal) system to encode characters on the local system.

- On the server (remote) machine, NVT decodes the characters to a form acceptable to the remote machine.
- TELNET is a protocol that provides a general, bi-directional, eight-bit byte oriented communications facility.
- Many application protocols are built upon the TELNET protocol □ Telnet services are used on PORT 23.

SSH protocol(Secure Shell)

The SSH protocol (also referred to as Secure Shell) is a method for secure remote login from one computer to another. It provides several alternative options for strong authentication, and it protects the communications security and integrity with strong encryption. It is a secure alternative to the non-protected login protocols (such as telnet, rlogin) and insecure file transfer methods (such as FTP).

TYPICAL USES OF THE SSH PROTOCOL

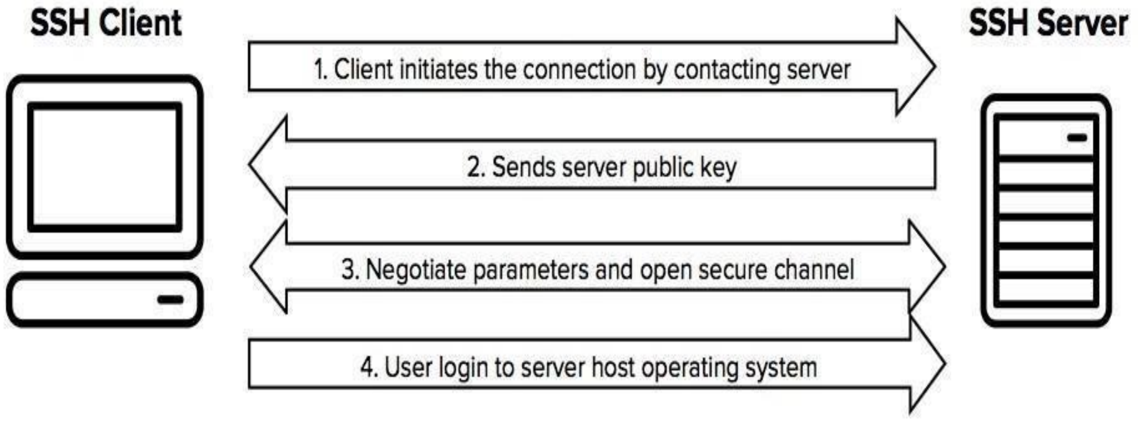
The protocol is used in corporate networks for:

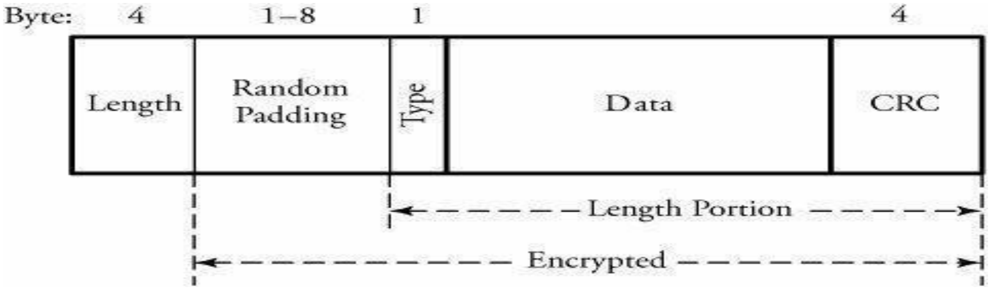
- providing secure access for users and automated processes
- interactive and automated file transfers
- issuing remote commands
- managing network infrastructure and other mission-critical system components.

HOW DOES THE SSH PROTOCOL WORK

The protocol works in the client-server model, which means that the connection is established by the SSH client connecting to the SSH server. The SSH client drives the connection setup process and uses public key cryptography to verify the identity of the SSH server. After the setup phase the SSH protocol uses strong symmetric encryption and hashing algorithms to ensure the privacy and integrity of the data that is exchanged between the client and server.

The figure below presents a simplified setup flow of a secure shell connection.


SSH Client
SSH Server
1. Client initiates the connection by contacting server
2. Sends server public key
3. Negotiate parameters and open secure channel
4. User login to server host operating system



The format of an SSH packet

- Length indicates the size of the packet, not including the length field or the variablelength random padding field that follows it.
- Padding causes an intrusion to be more difficult. ○ Type identifies the type of message. ○ CRC , or cyclic redundancy check, is an error-detection field .

When encryption is enabled, all fields except length are encrypted. SSH also permits optional compression of the data, which is useful when SSH is used in low-bandwidth situations. In such cases, the client and the server negotiate compression, and only the type and data fields are compressed.

File Transfer Protocol

- The File Transfer Protocol (FTP) is the most widely used protocol for file transfer over the network. FTP uses TCP/IP for communication and it works on TCP port 21. FTP works on Client/Server Model where a client requests file from Server and server sends requested resource back to the client.

- FTP uses out-of-band controlling i.e. FTP uses TCP port 20 for exchanging controlling information and the actual data is sent over TCP port 21.
- The client requests the server for a file. When the server receives a request for a file, it opens a TCP connection for the client and transfers the file. After the transfer is complete, the server closes the connection. For a second file, client requests again and the server reopens a new TCP connection.

- FTP is the standard mechanism provided by TCP/IP for copying a file from one host to another.
- FTP differs form other client-server applications because it establishes 2 connections between hosts.
- Two connections are: Data Connection and Control Connection.
- Data Connection uses PORT 20 for the purpose and control connection uses PORT 21 for the purpose.

- FTP is built on a client-server architecture and uses separate control and data connections between the client and the server.
- One connection is used for data transfer, the other for control information (commandsand responses).
- It transfer data reliably and efficiently.

Secure Copy Protocol(SCP)

Secure Copy, or SCP, does not use FTP or SSL to transfer files, rather Secure Copy handles the file transfer and relies on the SSH protocol to provide authentication and security for both credentials and data. Unfortunately, SCP doesn't have file management capabilities -- certainly a cause of concern. When an SCP client sends a request to download files or directories, the server feeds the client with its subdirectories and files, causing a server-driven download. This makes the protocol a security risk if the server is malicious or has been compromised. You will find that SCP is being replaced by the more comprehensive and platform-independent SFTP protocol, which is also based on SSH.

Email and Simple Mail Transfer Protocol

The Simple Mail Transfer Protocol (SMTP) is used to transfer electronic mail from one user to another. This task is done by means of email client software (User Agents) the user is using. User Agents help the user to type and format the email and store it until internet is available. When an email is submitted to send, the sending process is handled by Message Transfer Agent which is normally comes inbuilt in email client software.

Message Transfer Agent uses SMTP to forward the email to another Message Transfer Agent (Server side). While SMTP is used by end user to only send the emails, the Servers normally use SMTP to send as well as receive emails. SMTP uses TCP port number 25 and 587.

Client software uses Internet Message Access Protocol (IMAP) or POP protocols to receive emails.

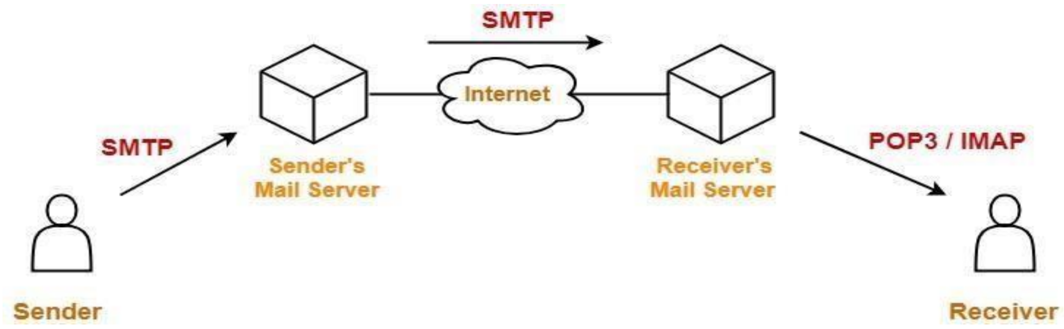
- One of the most popular network service is electronic mail (e-mail).
- The TCP/IP protocol that supports electronic mail on the Internet is called Simple Mail Transfer Protocol (SMTP).
- SMTP transfers messages from senders&apos; mail servers to the recipients&apos; mail servers using TCP connections.
- Users based on e-mail addresses.
- SMTP provides services for mail exchange between users on the same or different computers.
- Following the client/server model:

  ○ SMTP has two sides: a client side which executes on a sender&apos;s mail server, and server side which executes on recipient&apos;s mail server. ○ Both the client and server sides of SMTP run on every mail server.

○ When a mail server sends mail (to other mail servers), it acts as an SMTP client. ○ When a mail server receives mail (from other mail servers) it acts as an SMTP server.

Working-

- SMTP server is always on a listening mode.
- Client initiates a TCP connection with the SMTP server.
- SMTP server listens for a connection and initiates a connection on that port.
- The connection is established.
- Client informs the SMTP server that it would like to send a mail.
- Assuming the server is OK, client sends the mail to its mail server.
- Client's mail server use DNS to get the IP Address of receiver's mail server.
- Then, SMTP transfers the mail from sender's mail server to the receiver's mail server.



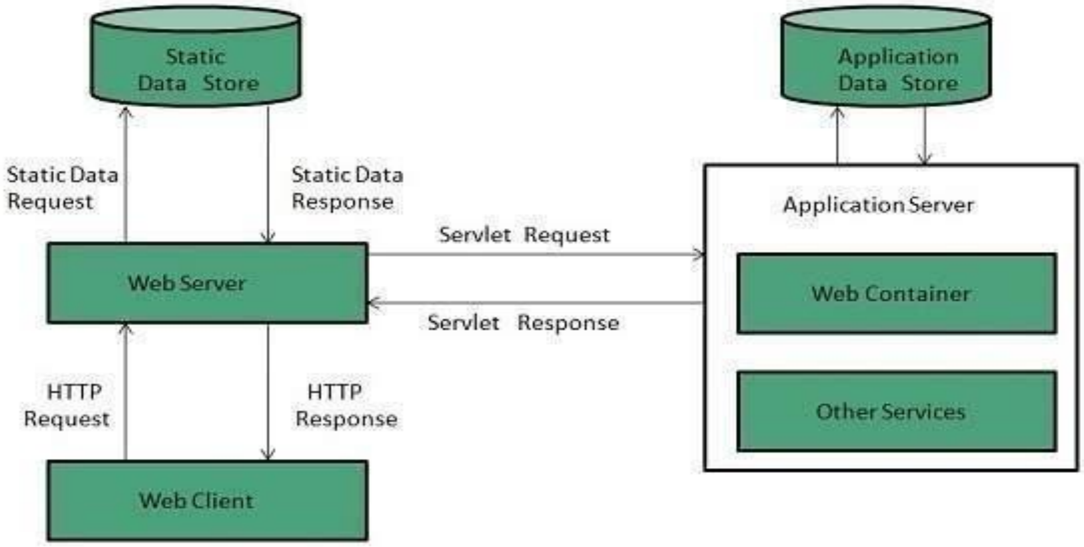
World Wide Web and Proxy Server(Web Caching)

Web server is a computer where the web content is stored. Basically web server is used to host the web sites but there exists other web servers also such as gaming, storage, FTP, email etc.

Web Server Working

Web server respond to the client request in either of the following two ways:

- Sending the file to the client associated with the requested URL.
- Generating response by invoking a script and communicating with database



Key Points

- When client sends request for a web page, the web server search for the requested page if requested page is found then it will send it to client with an HTTP response.
- If the requested web page is not found, web server will the send an **HTTP response:Error 404 Not found.**
- If client has requested for some other resources then the web server will contact to the application server and data store to construct the HTTP response.

A **Web cache** (or **HTTP cache**) is an information technology for the temporary storage (caching) of Web documents, such as Web pages, images, and other types of Web multimedia, to reduce server lag. A Web cache system stores copies of documents passing through it; subsequent requests may be satisfied from the cache if certain conditions are met. A Web cache system can refer either to an appliance or to a computer program.

What Is Caching?

Caching is the term for storing reusable responses in order to make subsequent requests faster. There are many different types of caching available, each of which has its own characteristics.

Application caches and memory caches are both popular for their ability to speed up certain responses. Web caching, the focus of this guide, is a different type of cache. Web caching is a core design feature of the HTTP protocol meant to minimize network traffic while improving the perceived responsiveness of the system as a whole. Caches are found at every level of a content's journey from the original server to the browser. Web caching works by caching the HTTP responses for requests according to certain rules. Subsequent requests for cached content can then be fulfilled from a cache closer to the user instead of sending the request all the way back to the web server.

Benefits

Effective caching aids both content consumers and content providers. Some of the benefits that caching brings to content delivery are:

- **Decreased network costs**: Content can be cached at various points in the network path between the content consumer and content origin. When the content is cached closer to the consumer, requests will not cause much additional network activity beyond the cache.
- **Improved responsiveness**: Caching enables content to be retrieved faster because an entire network round trip is not necessary. Caches maintained close to the user, like the browser cache, can make this retrieval nearly instantaneous.
- **Increased performance on the same hardware**: For the server where the content originated, more performance can be squeezed from the same hardware by allowing aggressive caching. The content owner can leverage the powerful servers along the delivery path to take the brunt of certain content loads.
- **Availability of content during network interruptions**: With certain policies, caching can be used to serve content to end users even when it may be unavailable for short periods of time from the origin servers.

Hyper Text Transfer Protocol (HTTP)

The Hyper Text Transfer Protocol (HTTP) is the foundation of World Wide Web. Hypertext is well organized documentation system which uses hyperlinks to link the pages in the text documents. HTTP works on client server model. When a user wants to access any HTTP page on the internet, the client machine at user end initiates a TCP connection to server on port 80. When the server accepts the client request, the client is authorized to access web pages.

To access the web pages, a client normally uses web browsers, who are responsible for initiating, maintaining, and closing TCP connections. HTTP is a stateless protocol, which means the Server maintains no information about earlier requests by clients.

- This is a protocol used mainly to access data on the World Wide Web (www).
- The Hypertext Transfer Protocol (HTTP) the Web&apos;s main application-layer protocol although current browsers can access other types of servers
- A respository of information spread all over the world and linked together.
- The HTIP protocol transfer data in the form of plain text, hyper text, audio, video and so on.
- HTTP utilizes TCP connections to send client requests and server replies.
- it is a synchronous protocol which works by making both persistent and non persistent

HTTP versions

- HTTP 1.0 uses non persistent HTTP. At most one object can be sent over a single TCP connection.
- HTTP 1.1 uses persistent HTTP. In this version, multiple objects can be sent over a single TCP connection