HTTP (HYPERTEXT TRANSFER PROTOCOL)

- ✓ The HyperText Transfer Protocol (HTTP) is used to define how the client-server programs can be written to retrieve web pages from the Web.
- ✓ It is a protocol used to access the data on the World Wide Web (WWW).
- ✓ The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.
- ✓ HTTP is a stateless request/response protocol that governs client/server communication.
- ✓ An HTTP client sends a request; an HTTP server returns a response.

Features of HTTP

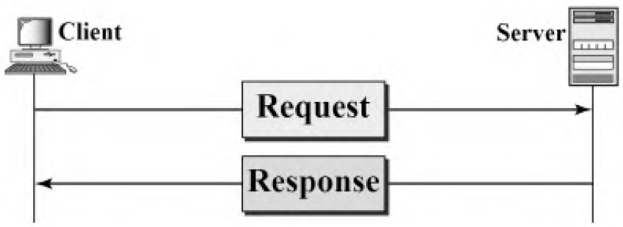
1. Connectionless protocol
2. Media independent
3. Stateless

HTTP REQUEST AND RESPONSE MESSAGES

The HTTP protocol defines the format of the request and response messages.

Request Message: The request message is sent by the client that consists of a request line, headers, and sometimes a body.

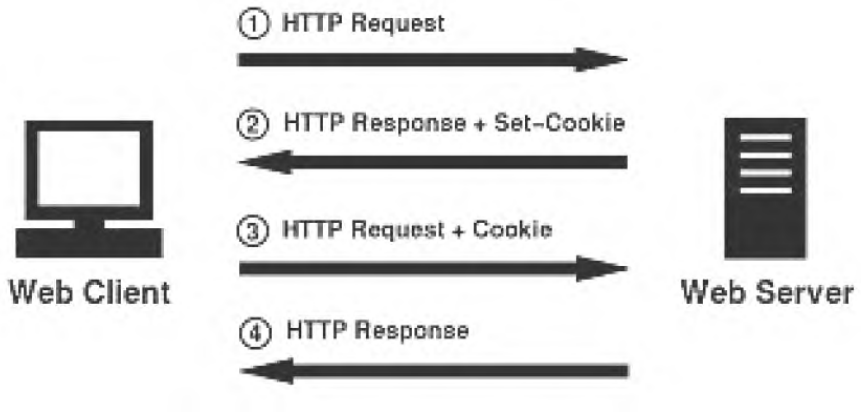
Response Message: The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body.



HTTP COOKIES

- ✓ An HTTP cookie (also called web cookie, Internet cookie, browser cookie, or simply cookie) is a small piece of data sent from a website and stored on the user's computer by the user's web browser while the user is browsing.
- ✓ HTTP is stateless , Cookies are used to add State.

- ✓ Cookies were designed to be a reliable mechanism for websites to remember stateful information (such as items added in the shopping cart in an online store) or to record the user's browsing activity (including clicking particular buttons, logging in, or recording which pages were visited in the past).



Components of Cookie

A cookie consists of the following components:

1. Name
2. Value
3. Zero or more attributes (name/value pairs). Attributes store information such as the cookie's expiration, domain, and flags

Types of Cookies

1.Authentication cookies These are the most common method used by web servers to know whether the user is logged in or not, and which account they are logged in with. Without such a mechanism, the site would not know whether to send a page containing sensitive information, or require the user to authenticate themselves by logging in.

2.Tracking cookies These are commonly used as ways to compile individuals browsing histories.

3.Session cookie

A session cookie exists only in temporary memory while the user navigates the website. Web browsers normally delete session cookies when the user closes the browser.

4.Persistent cookie

Instead of expiring when the web browser is closed as session cookies do, a persistent cookie expires at a specific date or after a specific length of time.This means that, for the cookie's entire lifespan , its information will be transmitted to the server every time the user visits the

website that it belongs to, or every time the user views a resource belonging to that website from another website.

HTTP CACHING

- HTTP Caching enables the client to retrieve document faster and reduces load on the server.
- HTTP Caching is implemented at Proxy server, ISP router and Browser.
- Server sets expiration date (Expires header) for each page, beyond which it is not cached.
- HTTP Cache document is returned to client only if it is an updated copy by checking against If-Modified-Since header.
- If cache document is out-of-date, then request is forwarded to the server and response is cached along the way.

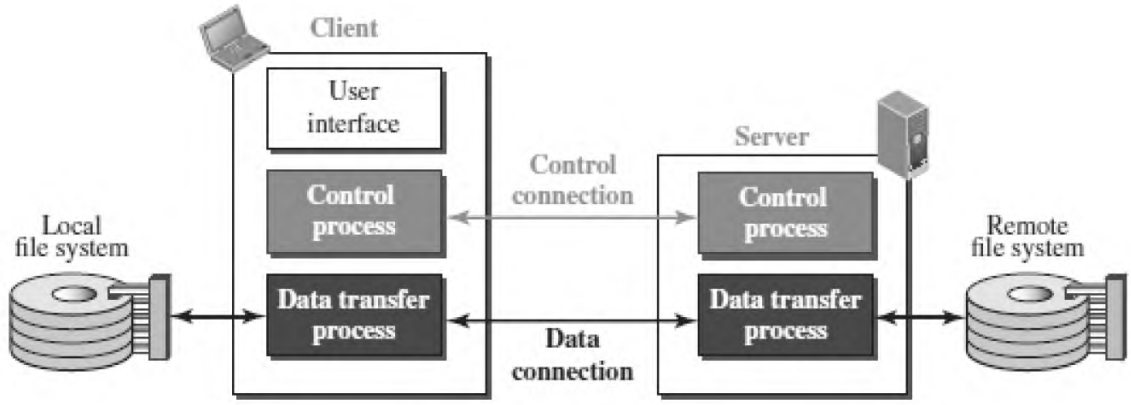
HTTP SECURITY

- HTTP does not provide security.
- However HTTP can be run over the Secure Socket Layer (SSL).
- In this case, HTTP is referred to as HTTPS.
- HTTPS provides confidentiality, client and server authentication, and data integrity.

FTP (FILE TRANSFER PROTOCOL)

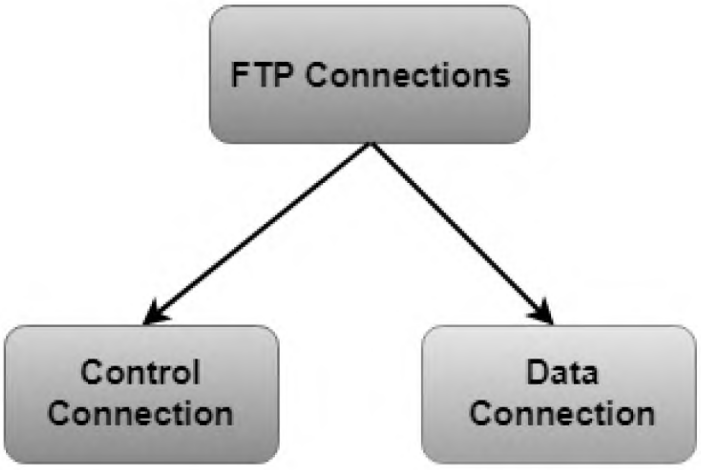
- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other servers.
- Although we can transfer files using HTTP, FTP is a better choice to transfer large files or to transfer files using different formats.

FTP MECHANISM



FTP CONNECTIONS

- There are two types of connections in FTP - Control Connection and Data Connection.
- The two connections in FTP have different lifetimes.
- The control connection remains connected during the entire interactive FTP session.
- The data connection is opened and then closed for each file transfer activity. When a user starts an FTP session, the control connection opens.
- While the control connection is open, the data connection can be opened and closed multiple times if several files are transferred.



Control Connection:

- The control connection uses very simple rules for communication. o Through control connection, we can transfer a line of command or line of response at a time.
- The control connection is made between the control processes.
- The control connection remains connected during the entire interactive FTP session.

Data Connection:

- The Data Connection uses very complex rules as data types may vary.
- The data connection is made between data transfer processes.
- The data connection opens when a command comes for transferring the files and closes when the file is transferred.

FTP COMMUNICATION

- FTP Communication is achieved through commands and responses.
- FTP Commands are sent from the client to the server
- FTP responses are sent from the server to the client.
- FTP Commands are in the form of ASCII uppercase, which may or may not be followed by an argument.

FTP TRANSMISSION MODE

- FTP can transfer a file across the data connection using one of the following three transmission modes: stream mode, block mode, or compressed mode.
- The stream mode is the default mode; data are delivered from FTP to TCP as a continuous stream of bytes.
- In the block mode, data can be delivered from FTP to TCP in blocks.
- In the compressed mode, data can be compressed and delivered from FTP to TCP.

FTP SECURITY

- FTP requires a password, the password is sent in plaintext which is unencrypted. This means it can be intercepted and used by an attacker.
- The data transfer connection also transfers data in plaintext, which is insecure.
- To be secure, one can add a Secure Socket Layer between the FTP application layer and the TCP layer.