Review of Web Technogies I

Unit 1

Protocol:

- A protocol is a set of rules and guidelines for communicating data. Rules are defined for each step and process during communication between two or more computers. Networks have to follow these rules to successfully transmit data.
- Example: HTTP,HTTPS,FTP,SMTP,TCP,IP,UDP etc.

HTTP

- HTTP (Hypertext Transfer Protocol) is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. As soon as a Web user opens their Web browser, the user is indirectly making use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP model.
- An HTTP session begins when a client’s browser requests a resource, such as a web page, from a remote Internet server. When the server responds by sending the page requested, the HTTP session for that object ends.

HTTPS

- HTTPS is the use of Secure Socket Layer (SSL) or Transport Layer Security (TLS) as a sub layer under regular HTTP application layering. HTTPS encrypts and decrypts user page requests as well as the pages that are returned by the Web server. The use of HTTPS protects against eavesdropping and man-in-the-middle attacks. HTTPS was developed by Netscape.

FTP

- File Transfer Protocol(FTP) is one of the original Internet services. FTP runs in TCP/IP’s Application layer and permits users to transfer files from a server to their client computer, and vice versa. The files can be documents, programs, or large database files.
- Using FTP we can easily upload and download files and distribute files on the internet with each other.

SMTP

- Simple Mail Transfer Protocol(SMTP) is the Internet protocol used to send e-mail to a server. To retrieve e-mail from a server, the client computer uses Post Office Protocol version 3(POP3).

TCP/IP

- Transmission Control Protocol(TCP/IP) which has become the core communications protocol for the Internet.
- TCP establishes the connections among sending and receiving Web computers, and makes sure that packets sent by one computer are received in the same sequence by the other, without any packets missing.
- IP provides the Internet’s addressing scheme and is responsible for the actual delivery 0f the packets.

UDP

- UDP (User Datagram Protocol) is an alternative communications protocol to Transmission Control Protocol (TCP) .
- Both UDP and TCP run on top of the Internet Protocol (IP) and are sometimes referred to as UDP/IP or TCP/IP. But there are important differences between the two.
- Where UDP enables process-to-process communication, TCP supports host-to-host communication. TCP sends individual packets and is considered a reliable transport medium; UDP sends messages, called datagrams, and is considered a best-effort mode of communications.
- In addition, where TCP provides error and flow control, no such mechanisms are supported in UDP. UDP is considered a connectionless protocol because it doesn't require a virtual circuit to be established before any data transfer occurs.

Web client

- The client, or user, side of the Web. It typically refers to the Web browser in the user's machine. It may also refer to plug-ins and helper applications that enhance the browser to support special services from the site. The term may imply the entire user machine or refer to a handheld device that provides Web access.

web server

- A **web server** is server software, or hardware , that can satisfy World Wide Web client requests. A web server can, in general, contain one or more websites. A web server processes incoming network requests over HTTP and several other related protocols.
- The primary function of a web server is to store, process and deliver web pages to clients. The communication between client and server takes place using the Hypertext Transfer Protocol (HTTP). Pages delivered are most frequently HTML documents, which may include images, style sheets and scripts in addition to the text content.

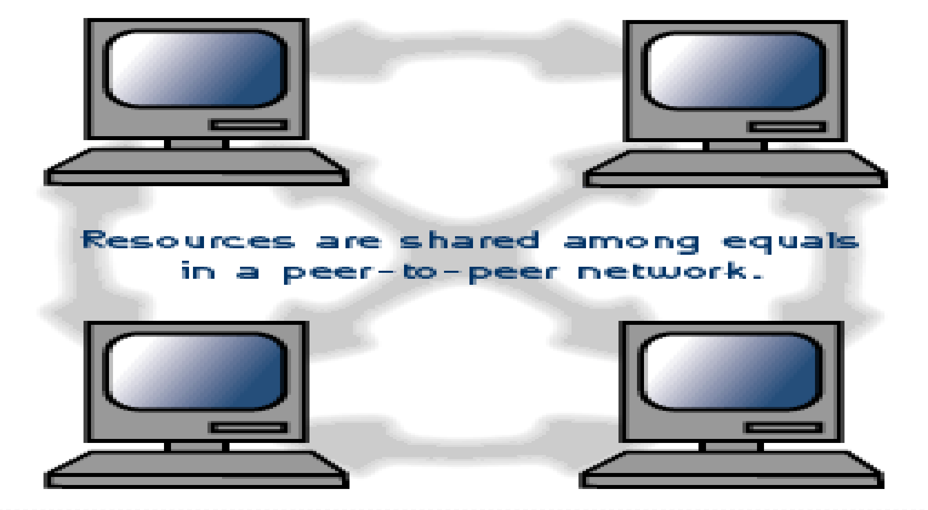
Network Architecture

- It's basically the physical and logical design which refers to the software, hardware, protocols and the media of transmission of data. Simply put, it refers to how computers are organized and how tasks are allocated among these computers.
- Types of network architectures are:

1) **peer-to-peer(P2P)**
2) **client/server(tiered)**.

Peer-to-Peer Architecture

- In a peer-to-peer network, tasks are allocated to every device on the network. Furthermore, there is no real hierarchy in this network, all computers are considered equal and all have the same abilities to use the resources available on this network. Instead of having a central server which would act as the shared drive, each computer that is connected to this network would act as the server for the files stored on



Advantages of a peer-to-peer network

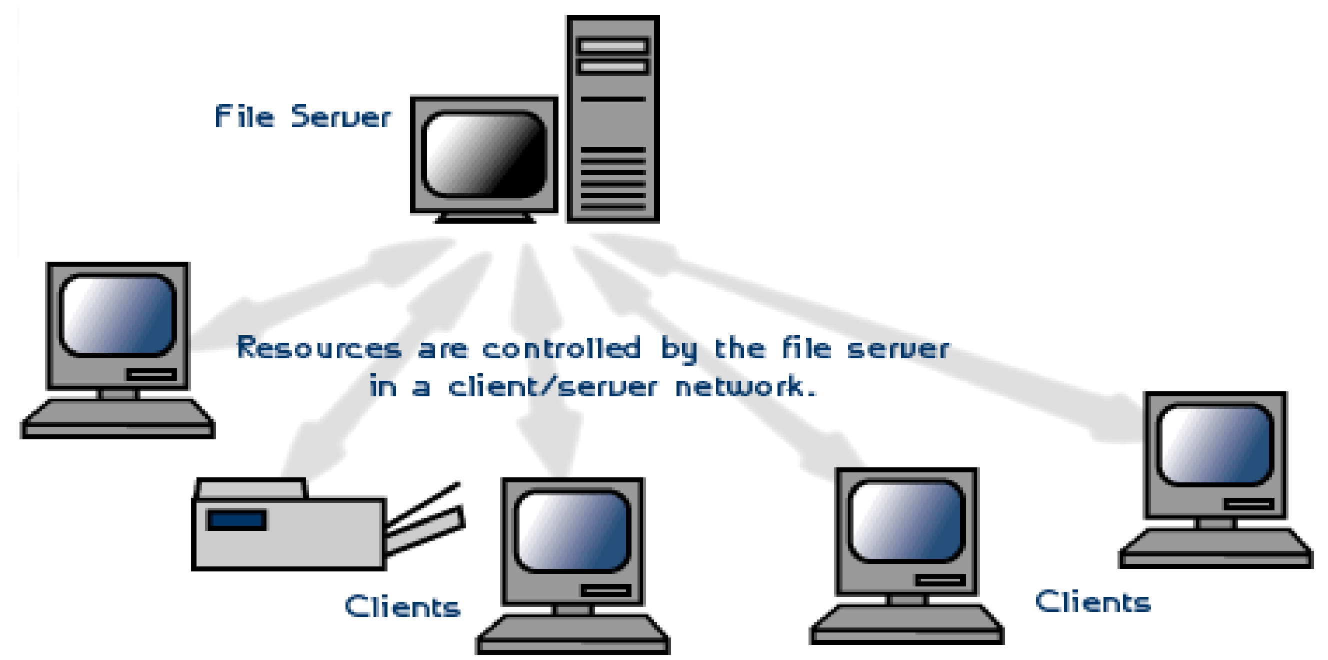
- Does not require a dedicated server which means its less costly.
- If one computer stops working, the other computers connected to the network will continue working.
- Installation and setup is quite painless because of the built-in support in modern operating systems.

Disadvantages of a peer-to-peer network

- Security and data backups are to be done to each individual computer.
- As the numbers of computers increases on a P2P network... performance, security, and access becomes a major headache.

Client/Server Architecture

- In a client/server network, a centralized, really powerful computer(server) acts as a hub in which other computers or workstations(clients) can connect to. This server is the heart of the system, which manages and provides resources to any client that requests them.


File Server
Resources are controlled by the file server in a client/server network.
Clients
Clients

Advantages of a client/server network

- Resources and data security are controlled through the server.
- Not restricted to a small number of computers.
- Server can be accessed anywhere and across multiple platforms.

Disadvantages of a client/server network

- Can become very costly due to the need of a server as well as networking devices such as hubs, routers, and switches.
- If and when the server goes down, the entire network will be affected.
- Technical staff needed to maintain and ensure network functions efficiently.

scripting language

- A **script** or **scripting language** is a computer language with a series of commands within a file that is capable of being executed without being compiled. Good examples of server-side scripting languages include Perl, PHP, and Python. The best example of a client side scripting language is JavaScript.

Difference between client side and server side scripting language

Basis for comparison	Server-side scripting	Client-side scripting
Basic	Works in the back end which could not be visible at the client end.	Works at the front end and script are visible among the users.
Processing	Requires server interaction.	Does not need interaction with the server.
Languages involved	PHP, ASP.net, Ruby on Rails, ColdFusion, Python, etc.	HTML, CSS, JavaScript, etc.
Affect	Could effectively customize the web pages and provide dynamic websites.	Can reduce the load to the server.
Security	Relatively secure.	Insecure