Internet Technologies

The Internet is the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide. **It is a *network of networks* that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies**. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide Web (WWW), electronic mail, telephony, and file sharing.

Topology

A Network Topology is the arrangement with which computer systems or network devices are connected to each other. Topologies may define both physical and logical aspect of the network. Both logical and physical topologies could be same or different in a same network.

1. Point-to-Point

Point-to-point networks contains exactly two hosts such as computer, switches or routers, servers connected back to back using a single piece of cable. Often, the receiving end of one host is connected to sending end of the other and vice-versa. If the hosts are connected point-to-point logically, then may have multiple intermediate devices. But the end hosts are unaware of underlying network and see each other as if they are connected directly.

2. Bus Topology

In case of Bus topology, all devices share single communication line or cable.Bus topology may have problem while multiple hosts sending data at the same time. Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue. It is one of the simple forms of networking where a failure of a device does not affect the other devices. But failure of the shared communication line can make all other devices stop functioning.

3. Star Topology

All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection. That is, there exists a point to point connection between hosts and hub. The hub device can be any of the following:

4. Ring Topology

In ring topology, each host machine connects to exactly two other machines, creating a circular network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data

travels through all intermediate hosts. To connect one more host in the existing structure, the administrator may need only one more extra cable.

5. Mesh Topology

In this type of topology, a host is connected to one or multiple hosts.This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only.

6. Tree Topology

Also known as Hierarchical Topology, this is the most common form of network topology in use presently.This topology imitates as extended Star topology and inherits properties of bus topology.This topology divides the network in to multiple levels/layers of network. Mainly in LANs, a network is bifurcated into three types of network devices. The lowermost is access-layer where computers are attached. The middle layer is known as distribution layer, which works as mediator between upper layer and lower layer. The highest layer is known as core layer, and is central point of the network, i.e. root of the tree from which all nodes fork.

7. Daisy Chain

This topology connects all the hosts in a linear fashion. Similar to Ring topology, all hosts are connected to two hosts only, except the end hosts.Means, if the end hosts in daisy chain are connected then it represents Ring topology.

8. Hybrid Topology

A network structure whose design contains more than one topology is said to be hybrid topology. Hybrid topology inherits merits and demerits of all the incorporating topologies.

Computer Networks Types

Generally, networks are distinguished based on their geographical span. A network can be as small as distance between your mobile phone and its Bluetooth headphone and as large as the internet itself, covering the whole geographical world,

1. Personal Area Network

A Personal Area Network (PAN) is smallest network which is very personal to a user. This may include Bluetooth enabled devices or infra-red enabled devices. PAN has connectivity range up to 10 meters. PAN may include wireless computer keyboard and mouse, Bluetooth enabled headphones, wireless printers and TV remotes.

2. Local Area Network

A computer network spanned inside a building and operated under single administrative system is generally termed as Local Area Network (LAN). Usually,LAN covers an organization' offices, schools, colleges or universities. Number of systems connected in LAN may vary from as least as two to as much as 16 million.

LAN provides a useful way of sharing the resources between end users.The resources such as printers, file servers, scanners, and internet are easily sharable among computers.

3. Metropolitan Area Network

The Metropolitan Area Network (MAN) generally expands throughout a city such as cable TV network. It can be in the form of Ethernet,Token-ring, ATM, or Fiber Distributed Data Interface (FDDI).

Metro Ethernet is a service which is provided by ISPs. This service enables its users to expand their Local Area Networks. For example, MAN can help an organization to connect all of its offices in a city.

4. Wide Area Network

As the name suggests,the Wide Area Network (WAN) covers a wide area which may span across provinces and even a whole country. Generally, telecommunication networks are Wide Area Network. These networks provide connectivity to MANs and LANs. Since they are equipped with very high speed backbone, WANs use very expensive network equipment.

A **Protocol** is a standard used to define a method of exchanging data over a computer network, such as local area network, Internet, Intranet, etc. Each protocol has its own method of how data is formatted when sent and what to do with it once received, how that data is compressed, or how to check for errors in the data.

One of the most common and known protocols is HTTP (HyperText Transfer Protocol), which is a protocol used to transmit data over the world wide web (Internet).

Basic Protocols:-

1. Transmission Control Protocol (TCP)

TCP is a connection oriented protocol and offers end-to-end packet delivery. It acts as back bone for connection.It exhibits the following key features:

- Transmission Control Protocol (TCP) corresponds to the Transport Layer of OSI Model.
- TCP is a reliable and connection oriented protocol.

2. Internet Protocol (IP)

Internet Protocol is **connectionless** and **unreliable** protocol. It ensures no guarantee of successfully transmission of data.

In order to make it reliable, it must be paired with reliable protocol such as TCP at the transport layer.

Internet protocol transmits the data in form of a datagram as shown in the following diagram:

3. User Datagram Protocol (UDP)

Like IP, UDP is connectionless and unreliable protocol. It doesn't require making a connection with the host to exchange data. Since UDP is unreliable protocol, there is no mechanism for ensuring that data sent is received.

UDP transmits the data in form of a datagram. The UDP datagram consists of five parts as shown in the following diagram:

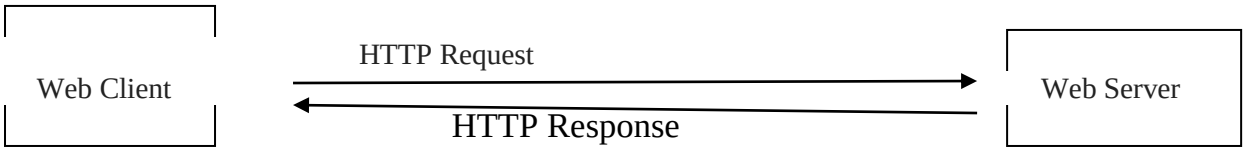
4. File Transfer Protocol (FTP)

FTP is used to copy files from one host to another. FTP offers the mechanism for the same in following manner:

- FTP creates two processes such as Control Process and Data Transfer Process at both ends i.e. at client as well as at server.

Client-Server Architecture:-

Client-server architecture (**client/server**) is a network **architecture** in which each computer or process on the network is either a **client** or a **server**. Servers are powerful computers or processes dedicated to managing disk drives (file servers), printers (print servers), or network traffic (network servers).



Basic Internet Terminologies

1. Browser

Beginning and advanced internet users all access the web through web browser software, which is included on computers and mobile devices at the time of purchase. Other browsers can be downloaded from the internet.

2. Webpage

A webpage is what you see in your browser when you are on the internet. Think of the webpage as a page in a magazine. You may see text, photos, images, diagrams, links, advertisements and more on any page you view.

3. URL

Uniform Resource Locators—URLs— are the web browser addresses of internet pages and files. With a URL, you can locate and bookmark specific pages and files for your web browser. URLs can be found all around us. They may be listed at the bottom of business cards, on TV screens during commercial breaks, linked in documents you read on the internet or delivered by one of the internet search engines. The format of a URL resembles this:

- http://www.examplewebsite.com/mypage

04. HTTP and HTTPS

Http is the acronym for "Hypertext Transfer Protocol," the data communication standard of web pages. When a web page has this prefix, the links, text and pictures should work properly in your web browser.

Https is the acronym for "Hypertext Transfer Protocol Secure." This indicates that the webpage has a special layer of encryption added to hide your personal information and passwords from others. Whenever you log in to your online bank account or a shopping site that you enter credit card information into, look for "https" in the URL for security.

05. HTML and XML

Hypertext Markup Language is the programming language of webpages. **HTML**commands your web browser to display text and graphics in a specific fashion. Beginning internet users don't need to know HTML coding to enjoy the webpages the programming language delivers to browsers.

XML is eXtensible Markup Language, a cousin to HTML. XML focuses on cataloging and databasing the text content of a web page.

XHTML is a combination of HTML and XML

6. IP Address

Your computer and every device that connects to the internet uses an Internet Protocol address for identification. In most cases, IP addresses are assigned automatically. Beginners don't usually need to assign an IP address. An IP address can look something like this:

- 202.3.104.55

7. Router

A router or router-modem combination is the hardware device that acts as the traffic cop for network signals arriving at your home or business from your ISP. A router can be wired or wireless or both.

8. Email

Email is electronic mail. It is the sending and receiving of typewritten messages from one screen to another. Email is usually handled by a webmail service—Gmail or Yahoo Mail, for example, or an installed software package such as Microsoft Outlook or Apple Mail.

9. Email Spam

Spam is the jargon name of unwanted and unsolicited email. Spam email comes in two main categories: high-volume advertising, which is annoying, and hackers attempting to lure you into divulging your passwords, which is dangerous.

10. Social Media

Social media is the broad term for any online tool that enables users to interact with thousands of other users. Facebook and Twitter are among the largest social networking sites. LinkedIn is a combination social and professional site. Other popular sites include YouTube, Google+, Instagram, Pinterest, Snapchat, Tumblr and Reddit.

11. E-Commerce

E-commerce is electronic commerce—the transaction of business selling and buying online. Every day, billions of dollars exchange hands through the internet and World Wide Web.

Internet shopping has exploded in popularity with internet users, to the detriment of traditional brick-and-mortar stores and malls. Every well-known retailer has a website that showcases and sells its products. Joining them are dozens of small sites that sell products and enormous sites that sell just about everything.

13. Encryption and Authentication

Encryption is the mathematical scrambling of data so that it is hidden from eavesdroppers. Encryption uses complex math formulas to turn private data into meaningless gobbledygook that only trusted readers can unscramble.

Encryption is the basis for how we use the internet as a pipeline to conduct trusted business, like online banking and online credit card purchasing. When reliable encryption is in place, your banking information and credit card numbers are kept private.

Authentication is directly related to encryption. Authentication is the complex way that computer systems verify that you are who you say you are.

14. Firewall

Firewall is a generic term to describe a barrier against destruction. In the case of computing, a firewall consists of software or hardware that protects your computer from hackers and viruses.

Computing firewalls range from small antivirus software packages to complex and expensive software and hardware solutions. Some firewalls are free. Many computers ship with a firewall you can activate. All the many kinds of computer firewalls offer some kind of safeguard against hackers vandalizing or taking over your computer system.

15. Malware

Malware is the broad term to describe any malicious software designed by hackers. Malware includes viruses, trojans, keyloggers, zombie programs and any other software that seeks to do one of four things:

- Vandalize your computer in some way
- Steal your private information
- Take remote control of your computer (zombie your computer) for other ends
- Manipulate you into purchasing something

16. Trojan

A trojan is a special kind of hacker program that relies on the user to welcome it and activate it. Named after the famous Trojan horse tale, a trojan program masquerades as a legitimate file or software program.

17. Phishing

Phishing is the use of convincing-looking emails and web pages to lure you into typing your account numbers and passwords/PINs. Often in the form of fake PayPal warning messages or fake bank login screens, phishing attacks can be convincing to anyone who is not trained to watch for the subtle clues. As a rule, smart users—beginners and long-time users alike—should distrust any email link that says "you should log in and confirm this."

18. Blogs

A blog is a modern online writer's column. Amateur and professional writers publish blogs on most every kind of topic: their hobby interests in paintball and tennis, their opinions on healthcare, their commentaries on celebrity gossip, photo blogs of favorite pictures or tech tips on using Microsoft Office. Absolutely anyone can start a blog.

Blogs are usually arranged chronologically and with less formality than a website. Many of them accept and respond to comments. Blogs vary in quality from amateurish to professional. Some savvy bloggers make reasonable incomes by selling advertising on their blog pages.

Cyber Crime:-

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers. Cybercrime may also be referred to as computer crime.

Message Switching

Message switching is a network switching technique in which data is routed in its entirety from the source node to the destination node, one hope at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are engaged or the network becomes blocked, the message-switched network stores and delays the message until ample resources become available for effective transmission of the message.

There are two types of message switching:-

1. Circuit Switching.
2. Packet Switching.

1. Circuit Switching :- In circuit switching network dedicated channel has to be established before the call is made between users. The channel is reserved between the users till the connection is active. For half duplex communication, one channel is allocated and for full duplex communication, two channels are allocated. It is mainly used for voice communication requiring real time services without any much delay.

2. **Packet Switching :-**In packet switching network unlike CS network, it is not required to establish the connection initially. The connection/channel is available to use by many users. But when capacity or number of users increases then it will lead to congestion in the network. Packet switched networks are mainly used for data and voice applications requiring non-real time scenarios.

Firewall is a barrier between Local Area Network (LAN) and the Internet. It allows keeping private resources confidential and minimizes the security risks. It controls network traffic, in both directions.

The following diagram depicts a sample firewall between LAN and the internet. The connection between the two is the point of vulnerability. Both hardware and the software can be used at this point to filter network traffic.

Types of Firewall

Firewall is categorized into three basic types −

- Packet filter (Stateless & Stateful)
- Application-level gateway
- Circuit-level gateway