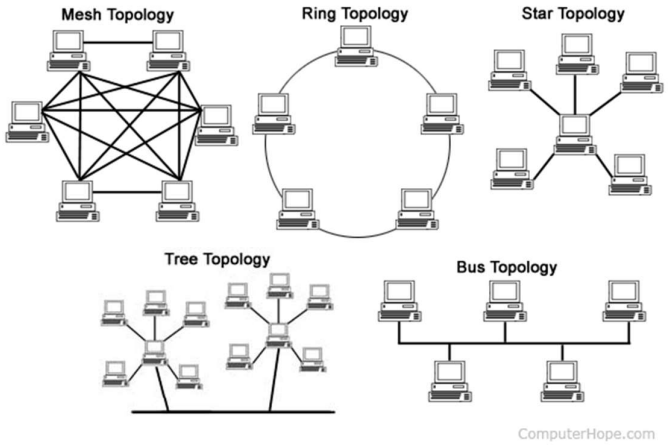
INTERNET FUNDAMENTALS

Network

- A network, in computing, is a group of two or more devices that can communicate.
- In practice, a network is comprised of a number of different computer systems connected by physical and/or wireless connections.
- The scale can range from a single PC sharing out basic peripherals to massive data centers located around the World, to the Internet itself.
- Regardless of scope, all networks allow computers and/or individuals to share information and resources.

Computer networks serve a number of purposes, some of which include:

- Communications such as email, instant messaging, chat rooms, etc.
- Shared hardware such as printers and input devices
- Shared data and information through the use of shared storage devices
- Shared software, which is achieved by running applications on remote computers



Some of the basic hardware components that can be used in networks include:

- Interface Cards: These allow computers to communicate over the network with a low-level addressing system using media access control (MAC) addresses to distinguish one computer from another.
- Repeaters: These are electronic devices that amplify communication signals and also filter noise from interfering with the signals.
- Hubs: These contain multiple ports, allowing a packet of information/data to be copied unmodified and sent to all computers on the network.
- Bridges: These connect network segments, which allows information to flow only to specific destinations
- Switches: These are devices that forward, make forwarding decisions and otherwise filter chunks of data communication between ports according to the MAC addresses in the packets of information. Routers: These are devices that forward packets between networks by processing the information in the packet.
- Firewalls: These reject network access requests from unsafe sources, but allow requests for safe ones.

There are various types of networks, which are classified according to specific characteristics such as connection types, whether they are wired or wireless, the scale of the network, and its architecture and topology. Network types include local area networks, wide area networks, metropolitan area networks and backbone networks.

Internet

- The internet is a globally connected network system that uses TCP/IP to transmit data via various types of media.
- The internet is a network of global exchanges – including private, public, business, academic and government networks – connected by guided, wireless and fiber-optic technologies.
- The terms internet and World Wide Web are often used interchangeably, but they are not exactly the same thing.
- The internet refers to the global communication system, including hardware and infrastructure, while the web is one of the services communicated over the internet.

History of Internet

- The internet originated with the U.S. government, which began building a computer network in the 1960s known as ARPANET.
- The system was replaced by new networks operated by commercial internet service providers in 1995.
- The internet was brought to the public on a larger scale at around this time.

Advantages:

- Global connection, i.e., keeps everyone around the connected.

Disadvantages:

- Not a secure form of network.
- No privacy to any information.
- Hacks and attacks are possible.

Intranet

- An intranet is a secure and private enterprise network that shares data or application resources via Internet Protocol (IP).
- An Intranet differs from the internet, which is a public network.
- Intranet, which refers to an enterprise's internal website or partial IT infrastructure, may host more than one private website and is a critical component for internal communication and collaboration.
- A company's intranet is based on Internet concepts and technology, but for private use.
- The term can refer to anything that is web-based but for private use, but typically means a company's shared web applications.
- For example, it is common for companies to store internal contact information, calendars, etc. on their intranet.

Advantages:

- Privacy maintained within a company or an organization.
- More secure than internet.

Disadvantages:

- Cost of installation is high.

Extranet

- An extranet is a controlled private network allowing customers, partners, vendors, suppliers and other businesses to gain information, typically about a specific company or educational institution, and do so without granting access to the organization's entire network.
- An extranet is often a private part of a website.
- It is restricted to select users through user IDs, passwords and other authentication mechanisms on a login page.
- An extranet may be viewed as an intranet mapped onto the public Internet or onto some other private network.

Advantages:

- The ability to exchange large volumes of data using electronic data interchange.
- Sharing product data or catalogues with business partners.
- Joint company collaboration and training.
- Sharing services such as online banking applications among affiliated banks.

Disadvantages:

- expensive implementation and maintenance if hosted internally and the potential for compromised sensitive or proprietary information.
- Alternately, it may be hosted by an application service provider.

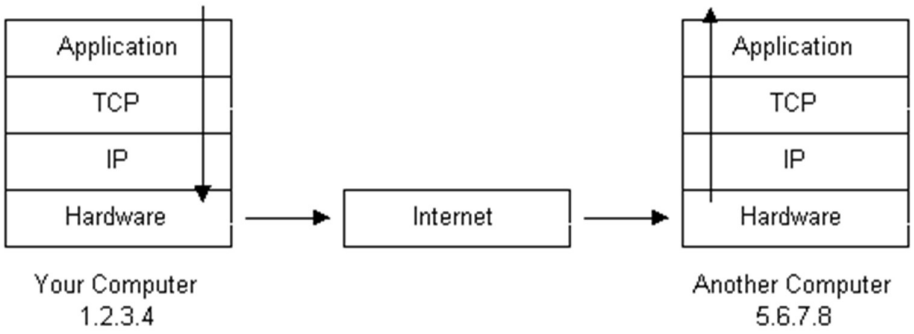
Working of the Internet

Important points:

- Electronic filing cabinets that simply store information and pass it on when requested are called servers.
- A computer that gets information from a server is called a client.
- When your computer connects over the Internet to a mail server at your ISP (Internet Service Provider) so you can read your messages, your computer is the client and the ISP computer is the server.
- When two computers on the Internet swap information back and forth on a more-or-less equal basis, they are known as peers.
- If you use an instant messaging program to chat to a friend, and you start swapping party photos back and forth, you're taking part in what's called peer-to-peer (P2P) communication.
- In P2P, the machines involved sometimes act as clients and sometimes as servers.
- For example, if you send a photo to your friend, your computer is the server (supplying the photo) and the friend's computer is the client (accessing the photo). If your friend sends you a photo in return, the two computers swap over roles.
- Apart from clients and servers, the Internet is also made up of intermediate computers called routers, whose job is really just to make connections between different systems.
- If you have several computers at home or school, you probably have a single router that connects them all to the Internet.
- The router is like the mailbox on the end of your street: it's your single point of entry to the worldwide network.

Working:

- TCP/IP, which stands for Transmission Control Protocol/Internet Protocol. It's the Internet's fundamental "control system" and it's really two systems in one. In the computer world, a "protocol" is simply a standard way of doing things—a tried and trusted method that everybody follows to ensure things get done properly.
- Internet Protocol (IP) is simply the Internet's addressing system.



- All the machines on the Internet—yours, mine, and everyone else's—are identified by an Internet Protocol (IP) address that takes the form of a series of digits separated by dots or colons.
- If all the machines have numeric addresses, every machine knows exactly how (and where) to contact every other machine.
- When it comes to websites, we usually refer to them by easy-to-remember names (like www.explainthatstuff.com) rather than their actual IP addresses—and there's a relatively simple system called DNS (Domain Name System) that enables a computer to look up the IP address for any given website.
- The other part of the control system, Transmission Control Protocol (TCP), sorts out how packets of data move back and forth between one computer (in other words, one IP address) and another.
- It's TCP that figures out how to get the data from the source to the destination, arranging for it to be broken into packets, transmitted, resent if they get lost, and reassembled into the correct order at the other end.

NOTE : In the original version of IP, known as IPv4, addresses consisted of four pairs of digits, such as 12.34.56.78 or 123.255.212.55, but the rapid growth in Internet use meant that all possible addresses were used up by January 2011. That has prompted the introduction of a new IP system with more addresses, which is known as IPv6, where each address is much longer and looks something like this: 123a:b716:7291:0da2:912c:0321:0ffe:1da2.

Internet Congestion

- Congestion, in the context of networks, refers to a network state where a node or link carries so much data that it may deteriorate network service quality, resulting in queuing delay, frame or data packet loss and the blocking of new connections.
- In a congested network, response time slows with reduced network throughput.
- Congestion = Load>Resorces
- 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.
- This can create two stable states under the same data traffic load - one dealing with the initial load and the other maintaining reduced network throughput.

Avoiding network congestion and collapse requires two major components:

- Routers capable of reordering or dropping data packets when received rates reach critical levels.
- Flow control mechanisms that respond appropriately when data flow rates reach critical levels.

Internet Culture

- Internet culture, or cyberculture, is the culture that has emerged, or is emerging, from the use of computer networks for communication, entertainment, and business.
- Internet culture is also the study of various social phenomena associated with the Internet and other new forms of the network communication,
- such as online communities, online multi-player gaming, wearable computing, social gaming, social media, mobile apps, augmented reality, and texting, and includes issues related to identity, privacy, and network formation.
- Cyberculture is a wide social and cultural movement closely linked to advanced information science and information technology, their emergence, development and rise to social and cultural prominence between the 1960s and the 1990s.

Business Culture on Internet

- The Internet has greatly changed the nature of work in connected segments of the world.
- For instance, work increasingly is performed outside of the traditional work place—a central office or factory—and more often in homes and other remote locations.
- The most cybercultured companies, moreover, more or less do away with the physical models of work, and are little more than interconnecting networks rather than physical, hierarchical organizations.
- Telecommuting allows workers to adjust their schedules to their own convenience and perform work in the comfort of their home offices.

Collaborative Computing and the Internet

- Collaborative computing is described as a phenomenon where modern technology tools facilitate and enhance group work that exists through distributed technology – where individuals collaborate from remote locations.
- Many different types of modern tools and technologies constitute collaborative programming resources.
- Some of the earliest systems focused on how to allow groups in distributed locations to view files, share information and chat amongst themselves in order to complete projects.
- As collaborative computing and general technology evolved, videoconferencing and multi-feature conferencing programs upped the ante in providing sophisticated platforms where remote teams could complete tasks like content management, or work on the full "life cycle" for a product or service.
- Much of the modern collaborative computing infrastructure offered to companies involves cutting down on face time, and replacing face-to-face meetings and interactions with digital ones.

Modes of connecting to the Internet

There exist several ways to connect to the internet. Following are these connection types available:

1. Dial-up Connection
2. ISDN
3. DSL
4. Cable TV Internet connections
5. Satellite Internet connections
6. Wireless Internet Connections

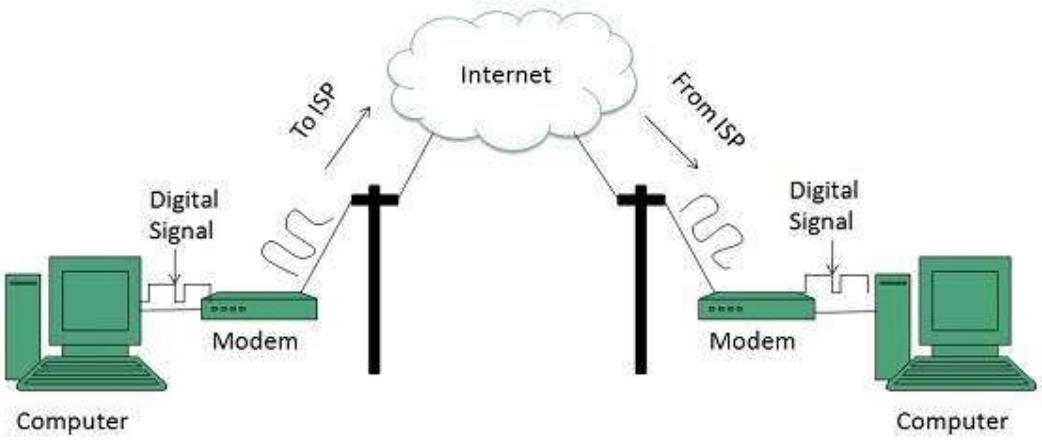
1. Dial-up Connection

Dial-up connection uses telephone line to connect PC to the internet. It requires a modem to setup dial-up connection. This modem works as an interface between PC and the telephone line.

There is also a communication program that instructs the modem to make a call to specific number provided by an ISP.
Dial-up connection uses either of the following protocols:

1. Serial Line Internet Protocol (SLIP)
2. Point to Point Protocol (PPP)

The following diagram shows the accessing internet using modem:



2. ISDN

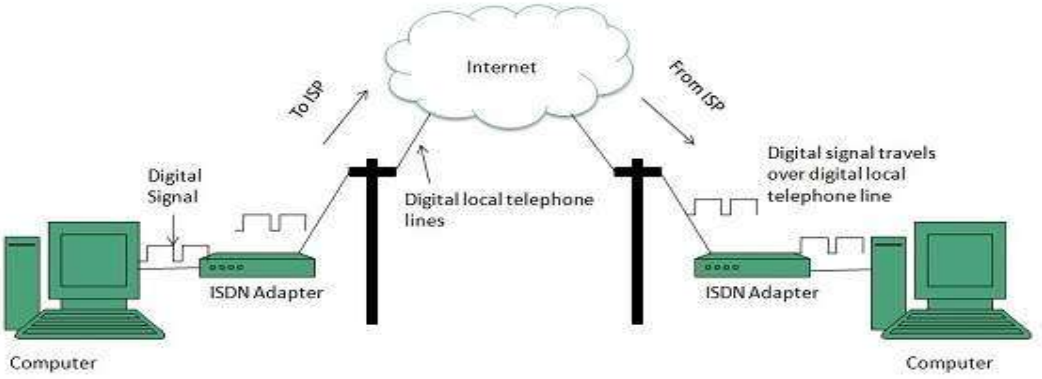
ISDN is acronym of **Integrated Services Digital Network.** It establishes the connection using the phone lines which carry digital signals instead of analog signals.
There are two techniques to deliver ISDN services:

1. Basic Rate Interface (BRI)
2. Primary Rate Interface (PRI)

Key points:

- The BRI ISDN consists of three distinct channels on a single ISDN line: t1o 64kbps B (Bearer) channel and one 16kbps D (Delta or Data) channels.
- The PRI ISDN consists of 23 B channels and one D channels with both have operating capacity of 64kbps individually making a total transmission rate of 1.54Mbps

The following diagram shows accessing internet using ISDN connection:



3. DSL

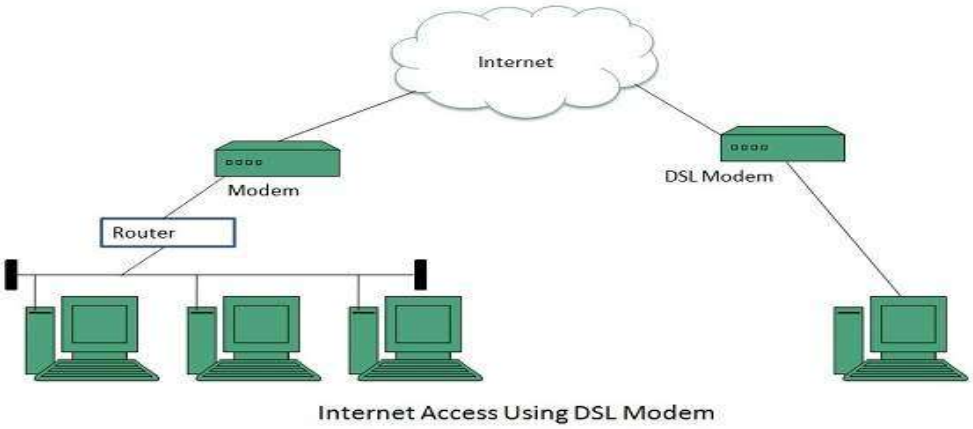
DSL is acronym of Digital Subscriber Line. It is a form of broadband connection as it provides connection over ordinary telephone lines.
Following are the several versions of DSL technique available today:

1. Asymmetric DSL (ADSL)
2. Symmetric DSL (SDSL)
3. High bit-rate DSL (HDSL)

4. Rate adaptive DSL (RDSL)
5. Very high bit-rate DSL (VDSL)
6. ISDN DSL (IDSL)

All of the above mentioned technologies differ in their upload and download speed, bit transfer rate and level of service.

The following diagram shows that how we can connect to internet using DSL technology:



Internet Access Using DSL Modem

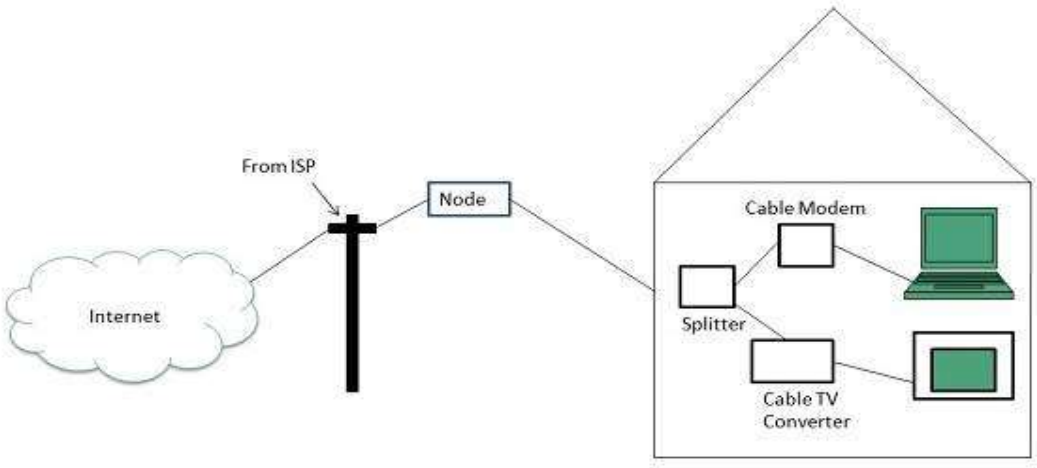
4. Cable TV Internet Connection

Cable TV Internet connection is provided through Cable TV lines. It uses coaxial cable which is capable of transferring data at much higher speed than common telephone line.

Key Points:

- A cable modem is used to access this service, provided by the cable operator.
- The Cable modem comprises of two connections: one for internet service and other for Cable TV signals.
- Since Cable TV internet connections share a set amount of bandwidth with a group of customers, therefore, data transfer rate also depends on number of customers using the internet at the same time.

The following diagram shows that how internet is accessed using Cable TV connection:

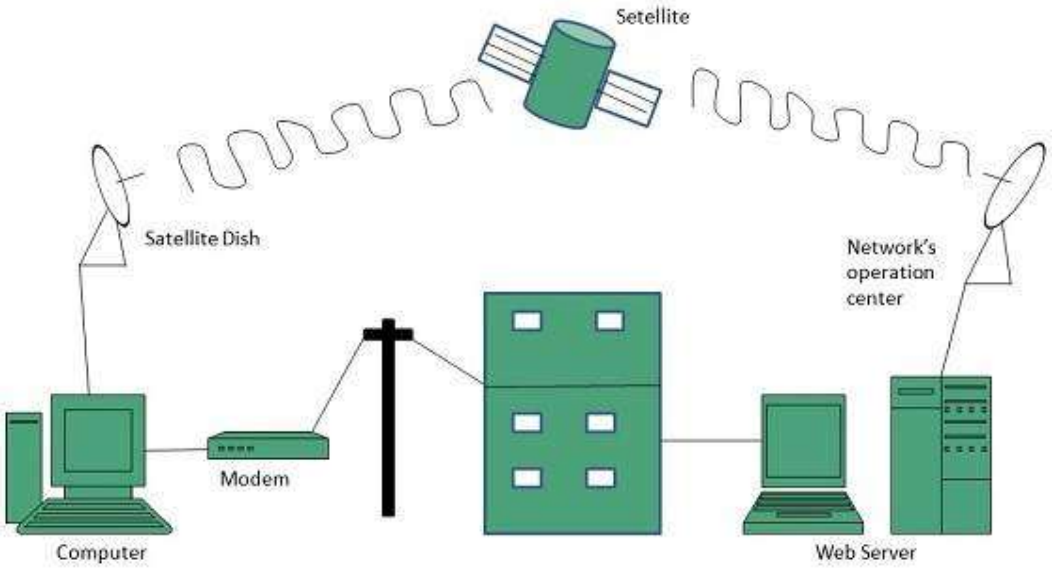


5. Satellite Internet Connection

Satellite Internet connection offers high speed connection to the internet. There are two types of satellite internet connection: one way connection or two way connection.

In one way connection, we can only download data but if we want to upload, we need a dialup access through ISP over telephone line.

In two way connection, we can download and upload the data by the satellite. It does not require any dialup connection.
The following diagram shows how internet is accessed using satellite internet connection:



6. Wireless Internet Connection

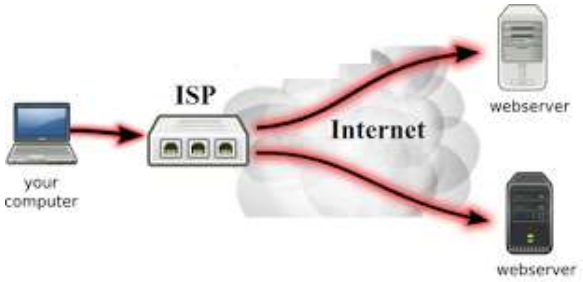
Wireless Internet Connection makes use of radio frequency bands to connect to the internet and offers a very high speed. The wireless internet connection can be obtained by either WiFi or Bluetooth.

Key Points:

- Wi Fi wireless technology is based on IEEE 802.11 standards which allow the electronic device to connect to the internet.
- Bluetooth wireless technology makes use of short-wavelength radio waves and helps to create personal area network (PAN).

Internet Service Providers (ISPs)

- An Internet service provider (ISP) is a company that provides customers with Internet access.
- Data may be transmitted using several technologies, including dial-up, DSL, cable modem, wireless or dedicated high-speed interconnects.
- ISPs connect to one another by forming backbones, which is another way of saying a main highway of communications.
- Typically, ISPs also provide their customers with the ability to communicate with one another by providing Internet email accounts, usually with numerous email addresses at the customer's discretion.
- Other services, such as telephone and television services, may be provided as well. The services and service combinations may be unique to each ISP.
- An Internet service provider is also known as an Internet access provider (IAP).



- Internet service providers may be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned.
- Internet services typically provided by ISPs include Internet access, Internet transit, domain name registration, web hosting, Usenet service, and colocation.

Internet Address (IP Address)

- An Internet Protocol address (IP address) is a logical numeric address that is assigned to every single computer, printer, switch, router or any other device that is part of a TCP/IP-based network.
- The IP address is the core component on which the networking architecture is built; no network exists without it.
- An IP address is a logical address that is used to uniquely identify every node in the network.
- Because IP addresses are logical, they can change.
- They are similar to addresses in a town or city because the IP address gives the network node an address so that it can communicate with other nodes or networks, just like mail is sent to friends and relatives.
- IP address is the most significant and important component in the networking phenomena that binds the World Wide Web together.

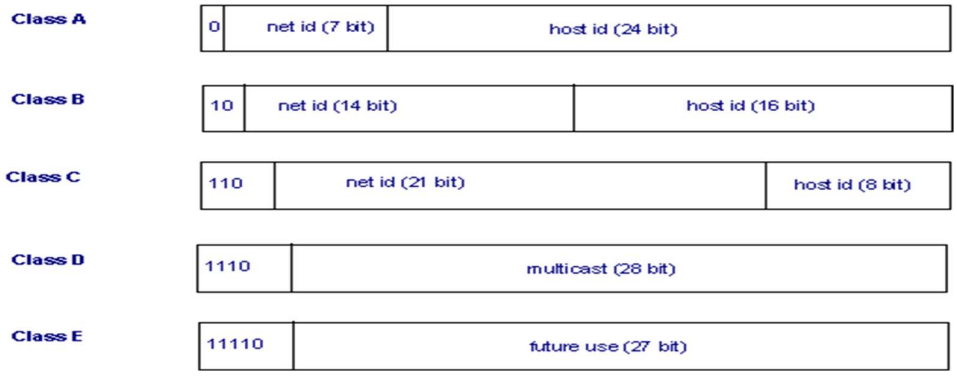
The numerals in an IP address are divided into 2 parts:

- The network part specifies which networks this address belongs to and
- The host part further pinpoints the exact location.

IP addresses falls into two types:

- Classfull IP addressing is a legacy scheme which divides the whole IP address pools into 5 distinct classes—A, B, C, D and E.
- Classless IP addressing has an arbitrary length of the prefixes.

Classes of IP Address:



Standard Address

1. IPv4:

- Internet Protocol Version 4 (IPv4) is the fourth revision of the Internet Protocol and a widely used protocol in data communication over different kinds of networks.
- IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet.
- It provides the logical connection between network devices by providing identification for each device.
- IPv4 uses 32-bit addresses for Ethernet communication in five classes: A, B, C, D and E.
- Classes A, B and C have a different bit length for addressing the network host.
- Class D addresses are reserved for multicasting, while class E addresses are reserved for future use.

2. IPv6:

- Internet Protocol Version 6 (IPv6) is an Internet Protocol (IP) used for carrying data in packets from a source to a destination over various networks.
- IPv6 is the enhanced version of IPv4 and can support very large numbers of nodes as compared to IPv4.
- It allows for 2128 possible node, or address, combinations.
- IPv6 is also known as Internet Protocol Next Generation (IPng).
- Released June 6, 2012, IPv6 was developed in hexadecimal format and contains 8 octets to provide large scalability.
- Like IPv4, IPv6 deals with address broadcasting without containing broadcast addresses in any class.

Domain Name

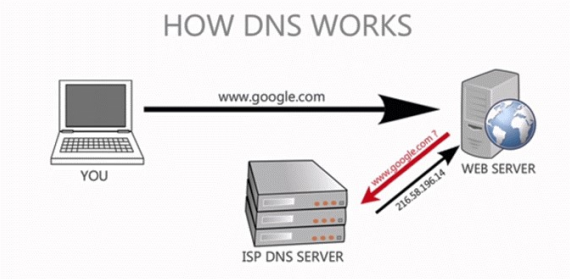
- A domain name is an Internet resource name that is universally understood by Web servers and online organizations and provides all pertinent destination information.
- To access an organization's Web-based services, website users must know the precise domain name.
- Domain names are used worldwide, particularly in the world of networks and data communication.

The following points explain how they work and how they are used:

- Domain names have two parts that are separated by a dot, such as example.com.
- A domain name can be used to identify a single IP address or group of IP addresses.
- A host or organization may use a domain name as an alternate IP address because domain names are alphanumeric (as opposed to all numbers), making them easier to memorize.
- A domain name is used as part of a URL to identify a website.
- The part that follows the dot is the top level domain (TLD), or group to which the domain name belongs. For example, .gov is the TLD for U.S. government domains.
- The IP address in the domain name's background is converted to a recognizable, alphanumeric domain name by a system known as the domain name system (DNS).

DNS Server (Domain Name System Server)

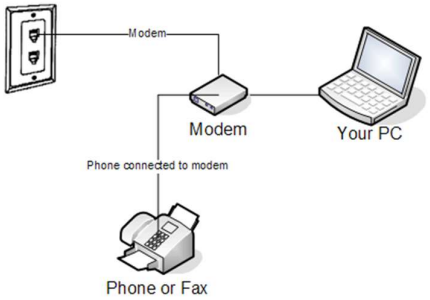
- Primarily designed to locate and deliver websites to end users over the Internet or a private network, a DNS server is developed on typical hardware but runs specialized DNS software.
- It is always connected to the Internet or a network.
- A DNS server stores a database of different domain names, network names, Internet hosts, DNS records and other related data.
- The most basic function of a DNS server is to translate a domain name into its respective IP address.
- During a domain name resolution query, DNS records are searched, and if found, the domain name record is returned.



- If the domain name is not registered or added to that DNS server, the query is then passed to other DNS servers until the domain name record is found.

Modem

- A modem is a network device that both modulates and demodulates analog carrier signals (called sine waves) for encoding and decoding digital information for processing.
- Modems accomplish both of these tasks simultaneously and, for this reason, the term modem is a combination of "modulate" and "demodulate."
- The most common use for modems is for both sending and receiving of the digital information between personal computers.
- This information used to be transmitted over telephone lines using V.92, the last dial-up standard, to an analog modem that would convert the signal back to a digital format for a computer to read.
- Now, access to the Internet more commonly takes place using high-speed broadband modems.



Types of Modem:

1. An external modem is a network device that is in a self-contained enclosure external to a computer. This is in contrast to an internal modem that is contained on a printed circuit board with a computer. External modems have lights indicating various modem functions and they can easily be moved from one computer system to another. The do, however, require one COM or USB port to operate.
   External modems are generally more expensive than internal modems, but they do offer portability between different computers.
   Some types of external modems include:
   - USB
   - Cable
   - DSL
   - External wireless modems
2. An internal modem is a network device that is contained on an expansion board that plugs into the motherboard. Unlike an external modem, an internal modem contains no lights to inform the user of its current function or changing modem states. Instead, the user must rely on the software that came with the modem.

Modem's Speed amd Time Continuum

- Cable Modem Speed is measured in Kilobits per second (KBPS).
- A cable modem speed test is a test by which the speed that your computer operates on the Internet can be gauged.
- Internet speed is measured in kilobits/second and for most people this means how fast data files can be downloaded.

The most accurate test available:

- There are now online services that can test your computer services overall speed, but they can also assist you in implementing measures to increase your performance speed as well.

- The cable modem speed test is administered by the services sending your computer a data file of a measure size.
- This file is then downloaded by your computer end then uploaded back to the sender.

Achieve maximum speed attainable:

- In this way, both your download speed and your upload speed is are combined to one figure that is your total result of the cable modem speed test.
- This is far better than testing only your download speed, which can be done by yourself by simply timing the speed of a file download with a stopwatch.
- Also, another benefit of using an online service is that they can automatically retest you as you are implements upgrades, until you have reached the maximum speed attainable.

Communication Software

- Communication software is an application or program designed to pass information from one system to another.
- Such software provides remote access to systems and transmits files in a multitude of formats between computers.
- Communication software forms a part of communication systems with software components classified according to functions within the Open Systems Interconnection Model (OSI Model).
- The best defined examples of communication software are file transfer protocol (FTP), messaging software and email.

Internet Tools

The major Internet tools and services are:

- Electronic mail (email)
- Newsgroups.
- Internet Relay Chat (IRC)
- Telnet and SSH.
- File Transfer Protocol (FTP and FTPS, SFTP)
- World Wide Web (www)

World Wide Web (WWW)

- 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.
- The World Wide Web was originally designed in 1991 by Tim Berners-Lee while he was a contractor at CERN.
- The World Wide Web is most often referred to simply as "the Web."
- The World Wide Web is what most people think of as the Internet. It is all the Web pages, pictures, videos and other online content that can be accessed via a Web browser.
- The Internet, in contrast, is the underlying network connection that allows us to send email and access the World Wide Web.

Web Browser

- A web browser is a software program that allows a user to locate, access, and display web pages.
- In common usage, a web browser is usually shortened to "browser."
- Browsers are used primarily for displaying and accessing websites on the internet, as well as other content created using languages such as Hypertext Markup Language (HTML) and Extensible Markup Language (XML).
- Browsers translate web pages and websites delivered using Hypertext Transfer Protocol (HTTP) into human-readable content.

- They also have the ability to display other protocols and prefixes, such as secure HTTP (HTTPS), File Transfer Protocol (FTP), email handling (mailto:), and files (file:).
- In addition, most browsers also support external plug-ins required to display active content, such as in-page video, audio and game content.

Examples of Web Browsers:

1. Internet Explorer

- Internet Explorer (IE) is a product from software giant Microsoft.
- This is the most commonly used browser in the universe.
- This was introduced in 1995 along with Windows 95 launch and it has passed Netscape popularity in 1998.

2. Google Chrome

- This web browser is developed by Google and its beta version was first released on September 2, 2008 for Microsoft Windows.
- Today, chrome is known to be one of the most popular web browser with its global share of more than 50%.

3. Mozilla Firefox

- Firefox is a new browser derived from Mozilla.
- It was released in 2004 and has grown to be the second most popular browser on the Internet.

4. Safari

- Safari is a web browser developed by Apple Inc. and included in Mac OS X. It was first released as a public beta in January 2003. Safari has very good support for latest technologies like XHTML, CSS2 etc.

Web Directories

- A web directory or link directory is an online list or catalog of websites. That is, it is a directory on the World Wide Web of (all or part of) the World Wide Web.
- A web directory includes entries about websites, including links to those websites, organized into categories and subcategories.
- Besides a link, each entry may include the title of the website, and a description of its contents.
- In most web directories, the entries are about whole websites, rather than individual pages within them (called "deep links"). Websites are often limited to inclusion in only a few categories.
- Web directories provide links in a structured list to make browsing easier.
- Many web directories combine searching and browsing by providing a search engine to search the directory.
- Unlike search engines, which base results on a database of entries gathered automatically by web crawler, most web directories are built manually by human editors.
- Many web directories allow site owners to submit their site for inclusion, and have editors review submissions for fitness.
- Web directories may be general in scope, or limited to particular subjects or fields. Entries may be listed for free, or by paid submission.

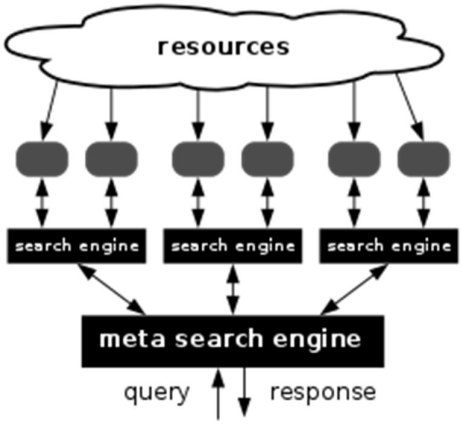
Search Engines

- Search engine is a service that allows Internet users to search for content via the World Wide Web (WWW).
- A user enters keywords or key phrases into a search engine and receives a list of Web content results in the form of websites, images, videos or other online data.

- The list of content returned via a search engine to a user is known as a search engine results page (SERP).
- First a spider/web crawler trolls the web for content that is added to the search engine's index. Then, when a user queries a search engine, relevant results are returned based on the search engine's algorithm. Early search engines were based largely on page content, but as websites learned to game the system, algorithms have become much more complex and search results returned can be based on literally hundreds of variables.
- Currently, Google and Microsoft's Bing control the vast majority of the market.

Meta Search Engines

- A meta search engine is a type of search engine that gives results based on a combination of results from other search engine databases.
- It specializes in concatenating databases from a variety of search engines and linking search results to relevant sources.
- Meta search engines use a complex algorithm that allows virtual databases to be generated on the fly.
- A virtual database "virtually" mirrors the physical database results of other search engines.
- All search result information and data are listed in a virtual database, and searches may be concentrated according to varied criteria.
- Thus, no two meta search engines are alike because they all operate with different criteria, such as news sites and newsgroups, depending on the algorithm designed to perform specified search functions.
- Examples are Metacrawler, Dogpile and Zoo, etc.



Search Strategies

- A search strategy is an organised structure of key terms used to search a database.
- The search strategy combines the key concepts of your search question in order to retrieve accurate results.

Your search strategy will account for all:

- possible search terms
- keywords and phrases
- truncated and wildcard variations of search terms
- subject headings (where applicable)

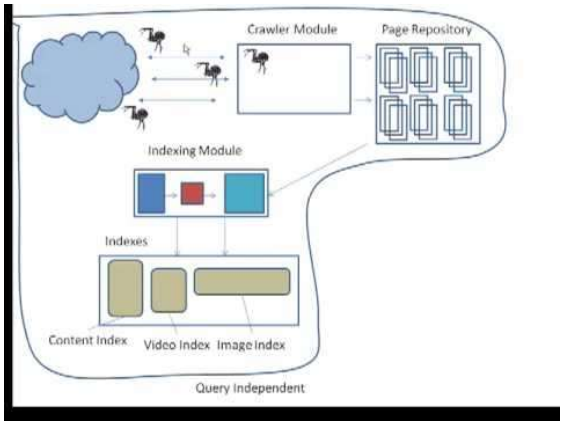
Search Strategy Techniques:

- Choosing search terms

- Searching with keywords
- Searching for exact phrases
- Using truncated and wildcard searches
- Searching with subject headings
- Using Boolean logic
- Citation searching

Working of Search Engines

- To find what you're after, a search engine will scan its index of webpages for content related to your search.
- A search engine makes this index using a program called a 'web crawler'. This automatically browses the web and stores information about the pages it visits.
- Every time a web crawler visits a webpage, it makes a copy of it and adds its URL to an index.
- Once this is done, the web crawler follows all the links on the page, repeating the process of copying, indexing and then following the links. It keeps doing this, building up a huge index of many webpages as it goes.
- Some websites stop web crawlers from visiting them. These pages will be left out of the index, along with pages that no-one links to.
- The information that the web crawler puts together is then used by search engines. It becomes the search engine's index. Every webpage recommended by a search engine has been visited by a web crawler.
- Search engines sort results to show you the ones they think are the most useful.
- PageRank is the best known algorithm which is used to improve web search results. The more links that point to a webpage, the more useful it will seem. This means it will appear higher up in the results.
- The webpages on the first page of results are those that PageRank thinks are the best.
- Search engines also pay attention to lots of other 'signals' when working out the order to show you results. For example how often the page is updated and if it is from a trustworthy domain.
- There are many search engines to choose from. Different search engines use different algorithms. This means that some sites will give their results in a different order, or they may even show completely different results altogether.



There are 3 basic stages, steps to how search engines work:

- Crawl – Content is discovered
- Indexing – Content is analysed and stored in a database
- Retrieval – User query is fetched and displayed

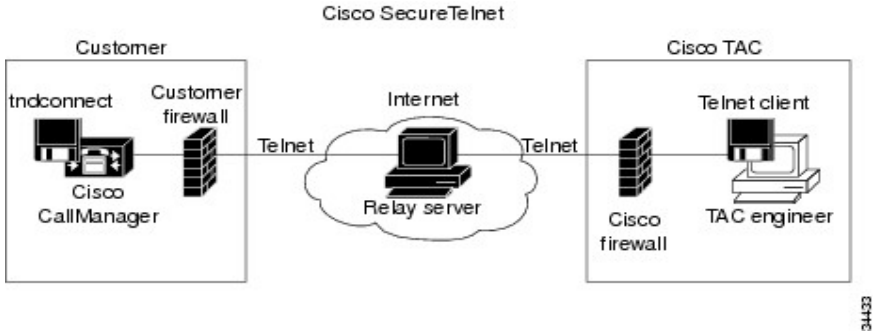
Types of search engines:

- Crawler-based – Software programs that crawl the web (Google, Yahoo)

- Hybrid – Combination of Crawler, directory results (Google, Yahoo)
- Meta – Combines all search engines results and compiles into one listing (metacrawler.com, dogpile.com)
- Directories – Human-edited (Yahoo-directory, Open-directory)

Telnet

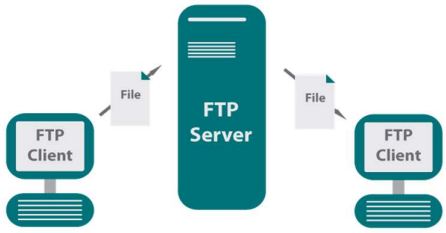
- Telnet (TN) is a networking protocol and software program used to access remote computers and terminals over the Internet or a TCP/IP computer network.
- Telnet was conceived in 1969 and standardized as one of the first Internet standards by the Internet Engineering Task Force (IETF).
- Designed for remote server access, management and client/server architectures, Telnet works through a purpose-built program that provides connectivity between a remote computer/server and host computer.
- Upon providing correct login and sign-in credentials, a user may access a remote system's privileged functionality.
- Additionally, Telnet's commands may be executed on a supported client or server device.
- Telnet sends all messages in clear text and has no specific security mechanisms. Thus, in many applications and services, Telnet has been replaced by Secure Shell (SSH).



FTP (File Transfer Protocol)

- File Transfer Protocol (FTP) is a client/server protocol used for transferring files to or exchanging files with a host computer.
- It may be authenticated with user names and passwords.
- Anonymous FTP allows users to access files, programs and other data from the Internet without the need for a user ID or password.
- Web sites are sometimes designed to allow users to use 'anonymous' or 'guest' as a user ID and an email address for a password.
- Publicly available flies are often found in a directory called pub and can be easily FTPed to a user's computer.
- FTP is also the Internet standard for moving or transferring files from one computer to another using TCP or IP networks.
- File Transfer Protocol is also known as RFC 959.
- An FTP server is a dedicated computer which provides an FTP service. This invites hackers and necessitates security hardware or software such as utilizing usernames, passwords and file access control.
- An FTP client is a computer application which accesses an FTP server. While doing so, users should block incoming FTP connection attempts using passive mode and should check for viruses on all downloaded files.

- An FTP site is a web site where users can easily upload or download specific files.

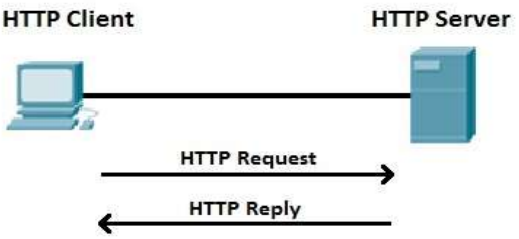


HTTP (HyperText Transfer Protocol)

- HyperText Transfer Protocol (HTTP) is an application-layer protocol used primarily on the World Wide Web.
- HTTP uses a client-server model where the web browser is the client and communicates with the webserver that hosts the website.
- The browser uses HTTP, which is carried over TCP/IP to communicate to the server and retrieve Web content for the user.
- HTTP is a widely used protocol and has been rapidly adopted over the Internet because of its simplicity.
- It is a stateless protocol, i.e., The client and server knows about each other just during the current request, if it closes and the two computers want to connect again, they need to provide information to one other a new, and the connection is handled as the very first one).
- It is also a connectionless protocol, i.e., After making the request the client disconnects from the server, then when the response is readythe server re-establishes the connection again and delivers the response.
- It can transfer any sort of data, as long as the two computers are able to read it.

A basic HTTP request involves the following steps:

- A connection to the HTTP server is opened.
- A request is sent to the server.
- Some processing is done by the server.
- A response from the server is sent back.
- The connection is closed.



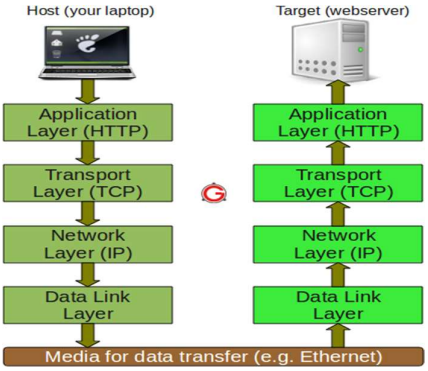
Gopher Commands

- Gopher is an application-layer protocol that provides the ability to extract and view Web documents stored on remote Web servers.
- Gopher was conceived in 1991 as one of the Internet's first data/file access protocols to run on top of a TCP/IP network.
- It was developed at University of Minnesota and is named after the school's mascot.
- Gopher was designed to access a Web server or database via the Internet.
- It requires that files be stored in a menu-style hierarchy on a Gopher server that is accessible through a Gopher-enabled client browser and/or directly.

- It initially supported only text-based file/document access but later came to support some image formats such as GIF and JPEG.
- Gopher was succeeded by the HTTP protocol and now has very few implementations.
- Gopher-based databases, servers or websites can be accessed through two search engines: Veronica and Jughead.

TCP/IP Protocol

- Transmission Control Protocol/Internet Protocol (TCP/IP) is the language a computer uses to access the internet.
- It consists of a suite of protocols designed to establish a network of networks to provide a host with access to the internet.
- TCP/IP is responsible for full-fledged data connectivity and transmitting the data end to end by providing other functions, including addressing, mapping and acknowledgment.
- TCP/IP contains four layers, which differ slightly from the OSI(Open Systems Interconnection) model.
- The technology is so common that one would rarely use the full name. In other words, in common usage the acronym is now the term itself.



- The TCP layer handles the message part. The message is broken down into smaller units, called packets, which are then transmitted over the network. The packets are received by the corresponding TCP layer in the receiver and reassembled into the original message.
- The IP layer is primarily concerned with the transmission portion. This is done by means of a unique IP address assigned to each and every active recipient on the network.
- TCP/IP is considered a stateless protocol suite because each client connection is newly made without regard to whether a previous connection had been established.

Working of TCP/IP:
The layers are:

- Process/Application Layer
- Host-to-Host/Transport Layer
- Internet Layer
- Network Access/Link Layer

1. Network Access/Link Layer –

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.

2. Internet Layer –

This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

i. IP – stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions:
IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
ii. ICMP – stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
iii. ARP – stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

3. Host-to-Host/Transport Layer –

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

i. Transmission Control Protocol (TCP) – It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
ii. User Datagram Protocol (UDP) – On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

4. Process/Application Layer –

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are :

i. HTTP and HTTPS – HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.
ii. SSH – SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
iii. NTP – NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync.

Browsers

- A web browser is a software program that allows a user to locate, access, and display web pages.
- In common usage, a web browser is usually shortened to "browser."
- Browsers are used primarily for displaying and accessing websites on the internet, as well as other content created using languages such as Hypertext Markup Language (HTML) and Extensible Markup Language (XML).

- Browsers translate web pages and websites delivered using Hypertext Transfer Protocol (HTTP) into human-readable content.
- They also have the ability to display other protocols and prefixes, such as secure HTTP (HTTPS), File Transfer Protocol (FTP), email handling (mailto:), and files (file:).
- In addition, most browsers also support external plug-ins required to display active content, such as in-page video, audio and game content.
- Common browsers include Internet Explorer from Microsoft, Firefox from Mozilla, Google Chrome, Safari from Apple, and Opera.

Coast to coast surfing

- The Web provides a means of accessing an enormous collection of information, including text, graphics, audio, video, movies, and so on.
- Information on the Web can be accessed in a nonlinear and experimental fashion.
- Unlike reading a book by flipping to the next page in a sequential order, you can "jump" from topic to topic via hyperlinks.
- This nonlinear approach to information gathering, or browsing is sometimes referred to as 'surfing the Web'.
- As a reader, you have the option to select what to explore next.

HyperText Markup Language

- Hypertext markup language (HTML) is the major markup language used to display Web pages on the Internet.
- In other words, Web pages are composed of HTML, which is used to display text, images or other resources through a Web browser.
- All HTML is plain text, meaning it is not compiled and may be read by humans.
- The file extension for an HTML file is .htm or .html.
- Web browsers receive HTML documents from a web server or from local storage and render the documents into multimedia web pages.
- HTML describes the structure of a web page semantically and originally included cues for the appearance of the document.
- HTML elements are the building blocks of HTML pages.
- With HTML constructs, images and other objects such as interactive forms may be embedded into the rendered page.
- HTML can embed programs written in a scripting language such as JavaScript, which affects the behavior and content of web pages.
- Inclusion of CSS defines the look and layout of content.

Using FrontPage Express

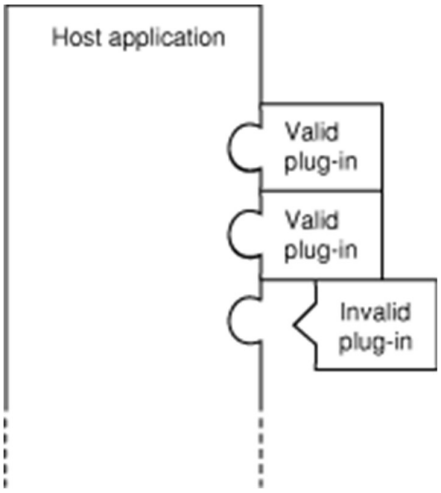
- FrontPage Express is the Microsoft software which allows you to design your own web pages.
- It works rather like a word processor.
- You type in what you want, where you want it, and you select letter size, colour and options like pictures and links.
- Then FrontPage Express turns it into HTML code for you.

Plug-ins

- A plug-in is an element of a software program that can be added to provide support for specific features or functionality.
- Plug-ins are commonly used in Internet browsers but also can be utilized in numerous other types of applications.
- In general, plug-ins are part of an array of software components known as add-ons.

- Programs may be changed by different kinds of add-ons in different ways.
- Plug-ins also can enable easier software upgrades or patches or additions by project collaborators.
- Plug-ins also can be a strategy for dealing with complex software licensing.
- One plug-in example is the range of customizable options common with browsers like Mozilla Firefox.

Architecture:



User Id (User Identification)

- User identification (user ID) is a logical entity used to identify a user on a software, system, website or within any generic IT environment.
- It is used within any IT enabled system to identify and distinguish between the users who access or use it.
- A user ID may also be termed as username or user identifier.
- User ID is one of the most common authentication mechanisms used within computing systems, networks, applications and over the Internet.
- Regardless of the type of user and the user's rights, each user has a unique identification that distinguishes it from other users.
- Typically in an authentication process, user ID is used in conjunction with a password.
- The end-user must provide both of the credentials correctly to gain access to the system or application.
- Moreover, system administrators use user IDs to assign rights, track user activity and manage overall operations on a particular system, network or application.

Password

- A password is a basic security mechanism that consists of a secret pass phrase created using alphabetic, numeric, alphanumeric and symbolic characters, or a combination.
- A password is used to restrict access to a system, application or service to only those users who have memorized or stored and/or are authorized to use it.
- A password may also be called an access code, PIN or secret code.
- A password is one of the most used access control procedures applied in virtually all digital and computing appliances.
- Generally, a password is used in combination with a user name and in most cases, an individual must provide both to gain access to a system, network or other password-protected area.
- In most applications and services, passwords are created by the user themselves and are typically separate for each different system or service used.

- In good security practices, a password should be between eight and 24 characters long, and include at least one capital letter, one number and one special character.

Email

- Electronic mail (email) is a digital mechanism for exchanging messages through Internet or intranet communication platforms.
- Email messages are relayed through email servers, which are provided by all Internet service providers (ISP).
- Emails are transmitted between two dedicated server folders: sender and recipient.
- A sender saves, sends or forwards email messages, whereas a recipient reads or downloads emails by accessing an email server.

Email messages are comprised of three components, as follows:

- Message envelope: Describes the email's electronic format
- Message header: Includes sender/recipient information and email subject line
- Message body: Includes text, image and file attachments

Email Address

- An email address is a unique identifier for an email account.
- It is used to both send and receive email messages over the Internet.
- Similar to physical mail, an email message requires an address for both the sender and recipient in order to be sent successfully.
- Every email address has two main parts: a username and domain name.
- The username comes first, followed by an at (@) symbol, followed by the domain name. In the example below, "mail" is the username and "techterms.com" is the domain name.
  For example, mail@techterms.com
- When a message is sent (typically through the SMTP protocol), the sending mail server checks for another mail server on the Internet that corresponds with the domain name of the recipient's address.
  For example, if someone sends a message to a user at techterms.com, the mail server will first make sure there is a mail server responding at techterms.com. If so, it will check with the mail server to see if the username is valid. If the user exists, the message will be delivered.

Message Components

E-mail Message comprises of different components:
E-mail Header, Greeting, Text, and Signature.
These components are described in the following diagram:

- E-mail Header

The first five lines of an E-mail message is called E-mail header. The header part comprises of following fields:

- From
- Date
- To
- Subject
- CC
- BCC

Therefore,

- FROM - The From field indicates the sender's address i.e. who sent the e-mail.
- DATE - The Date field indicates the date when the e-mail was sent.

- TO - The To field indicates the recipient's address i.e. to whom the e-mail is sent.
- SUBJECT - The Subject field indicates the purpose of e-mail. It should be precise and to the point.
- CC - CC stands for Carbon copy. It includes those recipient addresses whom we want to keep informed but not exactly the intended recipient.
- BCC - BCC stands for Black Carbon Copy. It is used when we do not want one or more of the recipients to know that someone else was copied on the message.
- GREETING - Greeting is the opening of the actual message. Eg. Hi Sir or Hi Guys etc.
- TEXT - It represents the actual content of the message.
- SIGNATURE - This is the final part of an e-mail message. It includes Name of Sender, Address, and Contact Number.

Advantages:
E-mail has prooved to be powerful and reliable medium of commmunication. Here are the benefits of E-mail:

- Reliable
- Convenience
- Speed
- Inexpensive
- Printable
- Global
- Generality

Disadvantages:
Apart from several benefits of E-mail, there also exists some disadvantages as discussed below:

- Forgery
- Overload
- Misdirection
- Junk
- No response

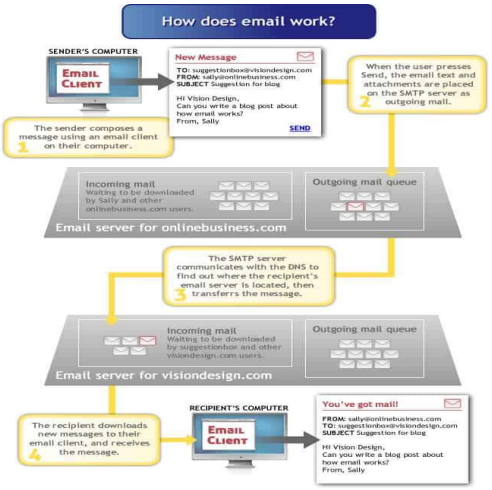
Message Composition

1. Click the Write icon on the center panel to display the Compose tab.
   The Compose tab contains the To, Cc and Subject fields.
2. Enter the email addresses of the recipients who should receive your message in the To field. Use a comma to separate multiple addresses.
   Alternatively, click the Address Book icon next to the To field to select the email address. To send a copy to a recipient, enter the email addresses in the Cc field or click the Address Book icon next to the Cc field to select email addresses.
   Convergence provides an address book auto completion feature. This feature needs to be enabled at the back-end Convergence server. When enabled, enter the first few characters of the display name of the recipient. The list of entries that closely match the entered characters from the Address Book appear in a drop-down list. See How Do I Add Contacts from Address Book?.
3. To send a blind copy to a recipient, click the Bcc icon. Optionally, click the Address Book icon next to the Bcc field to select email addresses from the saved list.
   The Bcc field appears. Enter the email address in the Bcc field.
4. Enter the subject of your message in the Subject field.
5. Click the Options icon in the top toolbar. The expanded message icons are shown.
6. From the priority drop-down list, select the required priority.

The priorities are Normal, Urgent, and Low. By default, the messages are sent with normal priority.

7. From the Receipt drop-down list, select an option.
   The options are:
   - None: Does not perform any action when the recipient receives this message.
   - Read: Sends a notification when the recipient reads the message.
   - Delivery: Sends a notification when this message is delivered to the recipient.
   - Delivery and Read: Sends a notification when your message is delivered and read by the recipient.
8. Select the Rich Text check box to include rich text features in the mail editor.
9. Click in the message text box and enter the text of the message.
   To attach a message to the mail, see Attaching Files to Messages.
10. Click Send to send the message.

Email Inner Working



- The sender composes a message using the email client on their computer.
- When the user sends the message, the email text and attachments are uploaded to the SMTP (Simple Mail Transfer Protocol) server as outgoing mail.
- All outgoing messages wait in the outgoing mail queue while the SMTP server communicates with the DNS (Domain Name Server–like a phone book for domain names and server IP addresses) to find out where the recipient's email server is located. If the SMTP server finds the recipient's email server, it will transfer the message and attachments. If the recipient's server can't be found, the sender will get a "Mail Failure" notification in their inbox.
- The next time the recipient clicks "Send & Receive," their email client will download all new messages from their own email server. You've got mail!

Email Management

Email management is a systematic approach to maximizing the efficiency of email practices and minimizing the negative effects that email handling can have on an individual's productivity and job satisfaction.

In the workplace, handling email ineffectively can waste a considerable amount of an employee's time and can also hamper other employees and negatively impact the organization as a whole. Email handling can account for more than 30 percent of an employee's work day, perhaps significantly more if handling behaviors are not optimized.

Tips for effective email management include:

- Limiting the number of times you process mail in a day.
- Limiting the amount of time you dedicate to processing email in a given session.
- Only keeping your email program open while you are actively dealing with it.

- Checking email only when you are going to process it.
- Deleting as many messages as possible immediately.
- Responding immediately to messages that can be answered very briefly.
- Moving messages to be dealt with later to a separate folder.
- Responding to only emails that require responses.
- Limiting recipients to as few individuals as possible.
- Keeping responses brief.
- Deleting all messages that are not archived after a specific amount of time.

Email management is typically categorized as a hard skill -- something that can be taught. However, because it has such a profound effect on employee productivity, email management is also considered a component of important soft skills such as time management, organization and communication.

MIME Types

MIME is acronym of **Multipurpose Internet Mail Extensions.** MIME compliant mailer allows us to send files other than simple text i.e. It allows us to send audio, video, images, document, and pdf files as an attachment to an email.

Suppose if you want to send a word processor document that has a group of tabular columns with complex formatting. If we transfer the file as text, all the formatting may be lost. MIME compliant mailer takes care of messy details and the message arrives as desired.

The following table describes commonly used MIME Types:

1.	Type	Subtype	Description	File extension(s)
2.	Application	postscript tex troff	Printable postscript document TEX document Printable troff document	.eps, .ps .tex .t, .tr, .roff
3.	Audio	aiff au midi real audio	Apple sound Sun Microsystems sound Musical Instrument Digital Interface Progressive Network sound	.aif, .aiff,.aifc .au, .snd .midi, .mid .ra, .ram
4.	image	gif jpeg png triff	Graphics Interchange Format Joint Photographic Experts Group Portable Network Graphics Tagged Image Modeling Language	.gif .jpeg, .jpg, .jpe .png .tiff, .tif
5.	Model	vrml	Virual reality Modelling Language	.wrl
6.	Text plain sgml	html	Hyper Text Markup Language Unformatted text Standard Generalized Markup language	.html, .htm .txt .sgml
7.	Video	avi mpeg quicktime sgi-movie	Microsoft Audio Video Interleaved Moving Pictures Expert Group Apple QuickTime movie silicon graphic movie	.avi .mpeg, .mpg .qt, .mov .movie

Newsgroups

- A newsgroup is an Internet-based discussion around an individual, entity, organization or topic.
- Newsgroups enable remotely connected users to share, discuss and learn about their topic of interest by exchanging text messages, images, videos and other forms of digital content.
- Newsgroups are also referred to as usenet newsgroups.
- Newsgroups were initially created in 1979 by some university students to exchange messages.
- Users can subscribe for free by submitting an email address, and the group generally consists of several topics/categories based around a main theme.
- The user/subscriber can post a message in a particular topic/category, which is either automatically visible in open newsgroups, or can only be viewed by approved members in moderated groups.
- All subscribers participating or following a particular topic/newsgroup will be notified of new messages and updates.
- Moreover, news/stories/topics in the newsgroup can be read through a downloadable news reader application.

Chat Rooms

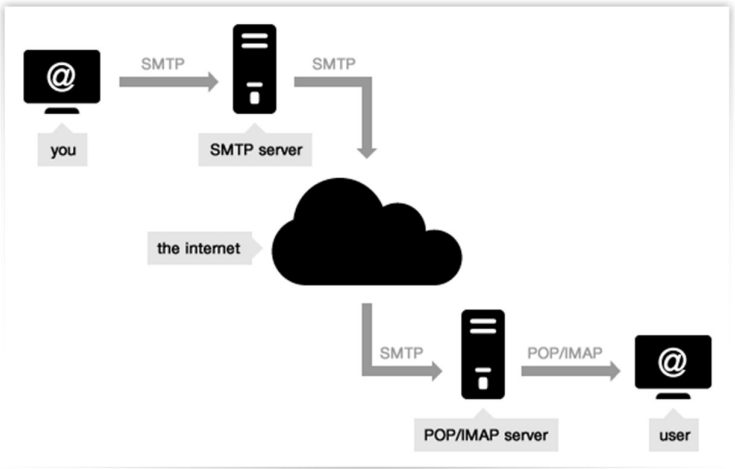
- A chat room is a designated virtual channel where users communicate with each other through the Internet, traditionally in plain text only.
- More recent developments in Web technology now allow the transmission of images and emoticons in a chat room as well.
- The term can mean online chatting, instant messaging and online forums using either synchronous or asynchronous conferencing.
- Some chat rooms require a username and password combination in order to log in or join a conversation, allowing for privacy among the users.
- From mIRC (Internet Relay Chat), one of the first popular chat clients, to Yahoo! Messenger, Skype and a slew of messaging applications available on the leading mobile platforms, the chat room has evolved to become an indispensable tool for modern communication.

Email Security

- Email security refers to the collective measures used to secure the access and content of an email account or service.
- It allows an individual or organization to protect the overall access to one or more email addresses/accounts.
- An email service provider implements email security to secure subscriber email accounts and data from hackers - at rest and in transit.
- Email security is a broad term that encompasses multiple techniques used to secure an email service.
- From an individual/end user standpoint, proactive email security measures include:
    1. Strong passwords
    2. Password rotations
    3. Spam filters
    4. Desktop-based anti-virus/anti-spam applications
- Similarly, a service provider ensures email security by using strong password and access control mechanisms on an email server; encrypting and digitally signing email messages when in the inbox or in transit to or from a subscriber email address.
- It also implements firewall and software-based spam filtering applications to restrict unsolicited, untrustworthy and malicious email messages from delivery to a user's inbox.

SMTP

- Simple Mail Transfer Protocol (SMTP) is the standard protocol for email services on a TCP/IP network.
- SMTP provides the ability to send and receive email messages.
- SMTP is an application-layer protocol that enables the transmission and delivery of email over the Internet.
- SMTP is created and maintained by the Internet Engineering Task Force (IETF).
- Simple Mail Transfer Protocol is also known as RFC 821 and RFC 2821.
- SMTP is one of the most common and popular protocols for email communication over the Internet and it provides intermediary network services between the remote email provider or organizational email server and the local user accessing it.
- SMTP is generally integrated within an email client application and is composed of four key components:
    1. Local user or client-end utility known as the mail user agent (MUA)
    2. Server known as mail submission agent (MSA)
    3. Mail transfer agent (MTA)
    4. Mail delivery agent (MDA)
- SMTP works by initiating a session between the user and server, whereas MTA and MDA provide domain searching and local delivery services.



PICO

- Pico (Pine composer) is a text editor for Unix and Unix-based computer systems used to create files.
- It is integrated with the Pine e-mail client, which was designed by the Office of Computing and Communications at the University of Washington.
- PICO is a very simple and easy-to-use text editor offering paragraph justification, cut/paste, and a spelling checker...".
- Pico does not support working with several files simultaneously and cannot perform a find and replace across multiple files.
- It also cannot copy text from one file to another (though it is possible to read text into the editor from a file in its working directory).
- Pico does support search and replace operations.
- Pico requires a video terminal emulation of VT – 100, VT – 200, VT – 210, or VT – 220.

PINE

- Pine is a freeware, text-based email client which was developed at the University of Washington.

- Pine is no longer under development, and has been replaced by the Alpine client, which is available under the Apache License.
- PINE is an easy to use interface to your Electronic Mailbox and Newsgroups service. It allows you to:
    1. Get specific online help for each task.
    2. Maintain an address book and use nicknames instead of long addresses.
    3. Send and receive messages to or from other users.
    4. Spell check your messages before sending them.
    5. Include a word processor document or other formatted and binary files attached to your message.
    6. Organize your messages in folders.
    7. Easily read and reply to articles on USENET newsgroups.
- General PINE Commands:
    1. ? - Show online help
    2. C - Compose a message
    3. I - Go to active FOLDER index
    4. L - Go to FOLDER LIST screen
    5. A - Go to ADDRESS BOOK
    6. S - SETUP functions
    7. Q - Quit Pine
- PINE supports the following Internet Protocols and specifications:
    1. SMTP (Simple Mail Transfer Protocol)
    2. MIME (Multipurpose Internet Mail Extension)
    3. IMAP (Internet Message Access Protocol)
    4. NNTP (Network News Transport Protocol)

Library Card Catalogue

- A library catalog or library catalogue is a register of all bibliographic items found in a library or group of libraries, such as a network of libraries at several locations.
- A bibliographic item can be any information entity (e.g., books, computer files, graphics, realia, cartographic materials, etc.) that is considered library material (e.g., a single novel in an anthology), or a group of library materials (e.g., a trilogy), or linked from the catalog (e.g., a webpage) as far as it is relevant to the catalog and to the users (patrons) of the library.
- Main Goals:

1. to enable a person to find a book of which either (Identifying objective)
    (i) the author
    (ii) the title
    (iii) the subject
    (iv) the date of publication
2. to show what the library has (Collocating objective)
    (i) by a given author
    (ii) on a given subject
    (iii) in a given kind of literature
3. to assist in the choice of a book (Evaluating objective)
    (i) as to its edition (bibliographically)
    (ii) as to its character (literary or topical)

Online catalogs:

- Online cataloguing through such systems as the Dynix software developed in 1983 and used widely through the late 1990s, has greatly enhanced the usability of catalogs, thanks to the rise of MARC standards (an acronym for MAchine Readable Cataloguing) in the 1960s.

- Rules governing the creation of MARC catalog records include not only formal cataloging rules such as Anglo-American Cataloguing Rules, second edition (AACR2), Resource Description and Access (RDA) but also rules specific to MARC, available from both the U.S. Library of Congress and the OCLC, the Online Computer Library Center global cooperative which builds and maintains WorldCat.
- MARC was originally used to automate the creation of physical catalog cards, but its use evolved into direct access to the MARC computer files during the search process.

OPACs have enhanced usability over traditional card formats because:

- The online catalog does not need to be sorted statically; the user can choose author, title, keyword, or systematic order dynamically.
- Most online catalogs allow searching for any word in a title or other field, increasing the ways to find a record.
- Many online catalogs allow links between several variants of an author's name.
- The elimination of paper cards has made the information more accessible to many people with disabilities, such as the visually impaired, wheelchair users, and those who suffer from mold allergies or other paper- or building-related problems.
- Physical storage space is considerably reduced.
- Updates are significantly more efficient.

Online Reference Works

- A reference work is a book or periodical (or its electronic equivalent) to which one can refer for information. The information is intended to be found quickly when needed.
- Reference works are usually referred to for particular pieces of information, rather than read beginning to end.
- The writing style used in these works is informative; the authors avoid use of the first person, and emphasize facts.
- Many reference works are compiled by a team of contributors whose work is coordinated by one or more editors rather than by an individual author.
- Indices are commonly provided in many types of reference work.
- For example, All Learn Academic Directories, Ask Oxford, Wikipedia, etc.

Web Server

- A web server is a system that delivers content or services to end users over the internet.
- A web server consists of a physical server, server operating system (OS) and software used to facilitate HTTP communication.
- A web server is also known as an internet server.
- The most simple definition is that a web server runs a website by returning HTML files over an HTTP connection.
- A web server is any internet server that responds to HTTP requests to deliver content and services.
- A web server's main purpose is to store web site files and broadcast them over the internet for you site visitor's to see. In essence, a web server is simply a powerful computer that stores and transmits data via the internet.
- There have been literally hundreds of web servers over the years, but Apache and Microsoft's IIS have emerged as two of the most popular systems.
- Dedicated computers and appliances may be referred to as Web servers as well.

Personal Web Server (PWS)

- Personal Web Server (PWS) is a web server application from Microsoft that allows a user to save, selectively publish and share posts on the World Wide Web or a local network.

- Designed for an individual PC and that enables the sharing of files and data to the network directly from the hard drive of the PC.
- Personal Web Server differs from all other types of Web servers in the way that it is controlled and operated by an individual rather than a company.
- Technically it is the same as a Web server, but conceptually it is quite different.
- PWS can be used to support Web pages if it is attached to a continuous Internet connection.
- It can also help websites to generate more traffic in an offline mode by staging websites before they are published globally.
- Personal Web Server can be implemented as a Web application, as an all-purpose Web server that can be personal or part of a small network, a website-hosting server working online (or offline) or simply a component of a computer.

Internet Information Services (IIS)

- Internet Information Services (IIS), formerly known as Internet Information Server, is a web server producted by Microsoft.
- It is a flexible, general-purpose web server from Microsoft that runs on Windows systems to serve requested HTML pages or files.
- An IIS web server accepts requests from remote client computers and returns the appropriate response. This basic functionality allows web servers to share and deliver information across local area networks, such as corporate intranets, and wide area networks, such as the internet.
- IIS is used with Microsoft Windows OSs and is the Microsoft-centric competition to Apache, the most popular webserver used with Unix/Linux-based systems.
- IIS was initially released for Windows NT and, along with ASP (Active-Server Pages), finally made a Windows-box a usable alternative for web-hosting.
- As of 2011, the most current version is IIS 7, which includes pretty much all modern features you'd expect to see in a webserver, including tight integration to ASP.NET.

Firewall

- A firewall is software used to maintain the security of a private network.
- Firewalls block unauthorized access to or from private networks and are often employed to prevent unauthorized Web users or illicit software from gaining access to private networks connected to the Internet.
- A firewall may be implemented using hardware, software, or a combination of both.
- A firewall is recognized as the first line of defense in securing sensitive information. For better safety, the data can be encrypted.

Firewalls generally use two or more of the following methods:

- Packet Filtering: Firewalls filter packets that attempt to enter or leave a network and either accept or reject them depending on the predefined set of filter rules.
- Application Gateway: The application gateway technique employs security methods applied to certain applications such as Telnet and File Transfer Protocol servers.
- Circuit-Level Gateway: A circuit-level gateway applies these methods when a connection such as Transmission Control Protocol is established and packets start to move.
- Proxy Servers: Proxy servers can mask real network addresses and intercept every message that enters or leaves a network.
- Stateful Inspection or Dynamic Packet Filtering: This method compares not just the header information, but also a packet's most important inbound and outbound data parts. These are then compared to a trusted information database for characteristic matches. This determines whether the information is authorized to cross the firewall into the network.

Digital Signature

- A digital signature guarantees the authenticity of an electronic document or message in digital communication and uses encryption techniques to provide proof of original and unmodified documentation.
- Digital signatures are used in e-commerce, software distribution, financial transactions and other situations that rely on forgery or tampering detection techniques.
- A digital signature is also known as an electronic signature.

A Digital signature is applied and verified, as follows:

- The document or message sender (signer) or public/private key supplier shares the public key with the end user(s).
- The sender, using his private key, appends the encrypted signature to the message or document.
- The end user decrypts the document and verifies the signature, which lets the end user know that the document is from the original sender.

Intrusion Detection System

- An intrusion detection system (IDS) is a type of security software designed to automatically alert administrators when someone or something is trying to compromise information system through malicious activities or through security policy violations.
- An IDS works by monitoring system activity through examining vulnerabilities in the system, the integrity of files and conducting an analysis of patterns based on already known attacks.
- It also automatically monitors the Internet to search for any of the latest threats which could result in a future attack.

There are three primary components of an IDS:

- Network Intrusion Detection System (NIDS): This does analysis for traffic on a whole subnet and will make a match to the traffic passing by to the attacks already known in a library of known attacks.
- Network Node Intrusion Detection System (NNIDS): This is similar to NIDS, but the traffic is only monitored on a single host, not a whole subnet.
- Host Intrusion Detection System (HIDS): This takes a “picture” of an entire system’s file set and compares it to a previous picture. If there are significant differences, such as missing files, it alerts the administrator.

Proxy Server

- A proxy server verifies and forwards incoming client requests to other servers for further communication.
- A proxy server is located between a client and a server where it acts as an intermediary between the two, such as a Web browser and a Web server.
- The proxy server's most important role is providing security.

A proxy server is used for many purposes, including:

- To provide internal system security
- To speed up resource access
- To apply access policies for tracking organizational Internet use or assessing employee progress.
- To bypass special controls, such as parental or security controls
- To scan for viruses and malware
- To circumvent regional restrictions

- To allow websites to make requests to externally hosted resources when cross-domain restrictions prohibit websites from linking to outside domains

Apache Web Server

- Apache Web Server is an open-source web server creation, deployment and management software.
- Initially developed by a group of software programmers, it is now maintained by the Apache Software Foundation.
- Apache Web Server is designed to create web servers that have the ability to host one or more HTTP-based websites.
- Notable features include the ability to support multiple programming languages, server-side scripting, an authentication mechanism and database support.