Unit 6: Internet & WWW

Contents: ***Internet*** *- Introduction to Internet and its Applications. Connecting to the Internet, Client/Server Technology, Internet as a Client/Server Technology, Email, Video-Conferencing, Internet Service Providers, Domain Name Server, Internet Address, Internet Protocols (IP, TCP, HTTP, FTP, SMTP, POP, Telnet, Gopher, WAIS), Introduction to Intranet, Internet vs. Intranet vs. Extranet, Advantages & Disadvantages of Intranet*

World Wide Web (WWW) *- World Wide Web and Its Evolution, Architecture of Web, Uniform Resource Locator (URL), Browsers, Search Engine, Web Servers: Apache, IIS, Proxy Server; HTTP Protocol, FTP protocol.*

Introduction to Internet

The Internet is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to serve billions of users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope that are linked by a broad array of electronic, wireless and optical networking technologies.

The Internet carries a vast range of information resources and services, such as the interlinked hypertext documents of the World Wide Web (WWW) and the infrastructure to support electronic mail

Application of Internet

1. **E-mail** - Email is now an essential communication tools in business. With e-mail you can send and receive instant electronic messages.
2. **24 hours a day - 7 days a week**: Internet is available,24x7 days for usage.
3. **Information** - Information is probably the biggest advantage internet is offering. There is a huge amount of information available on the internet for just about every subject, ranging from government law and services, trade fairs and conferences, market information, new ideas and technical support
4. **Services** - net banking, job searching, purchasing tickets, hotel reservations, guidance services
5. **E-commerce, Entertainment, Software downloads** etc.

Limitations of Internet

Theft of Personal information

Negative effects on family communication

Internet addiction

Children using the Internet

Virus threat, Spamming

Connecting to the Internet

Many home and small business users connect to the Internet via high-speed broadband Internet service. With broadband Internet service, your computer or mobile device usually is connected to the Internet the entire time it is powered on. Examples of broadband Internet service include cable, DSL, fiber, radio signals, and satellite.

1. Cable Internet service provides high-speed Internet access through the cable television network via a cable modem
2. DSL (digital subscriber line) provides high-speed Internet connections using regular copper telephone lines.
3. Fiber to the Premises (FTTP) uses fiber-optic cable to provide high-speed Internet access to home and business users.
4. Fixed wireless provides high-speed Internet connections using a dish-shaped antenna on your house or business to communicate with a tower location via radio signals.
5. A cellular radio network offers high-speed Internet connections to devices with built-in compatible.
6. A Wi-Fi (wireless fidelity) network uses radio signals to provide high-speed Internet connections to compatible or properly equipped wireless computers and devices.
7. Satellite Internet service provides high-speed Internet connections via satellite to a satellite dish that communicates with a satellite modem

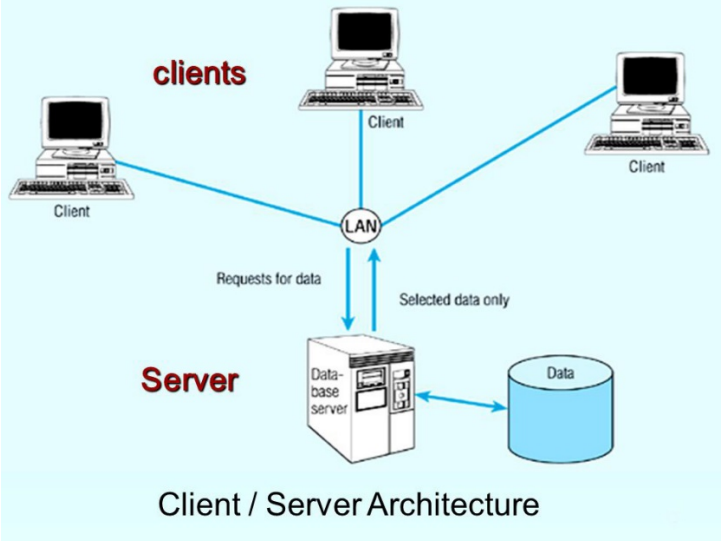
Client Server Technology

1. Client/Server is a term used to describe a computing model for the development of computerized systems. This model is based on the distribution of functions between two types of independent and autonomous processors: servers and clients.
2. A client is any process that requests specific services from server processes. A server is a process that provides requested services for clients. Client and server processes can reside in the same computer or indifferent computers connected by a network.

Client Server Architecture

The client server architecture has two major components; the client and the server.

- The Server is where all the processing, computing and data handling is happening, whereas the Client is where the user can access the services and resources given by the Server (Remote Server).
- The clients can make requests from the Server, and the Server will respond accordingly.
- Generally, there is only one server that handles the remote side. But to be on the safe side, we do use multiple servers will load balancing techniques



Client / Server Architecture

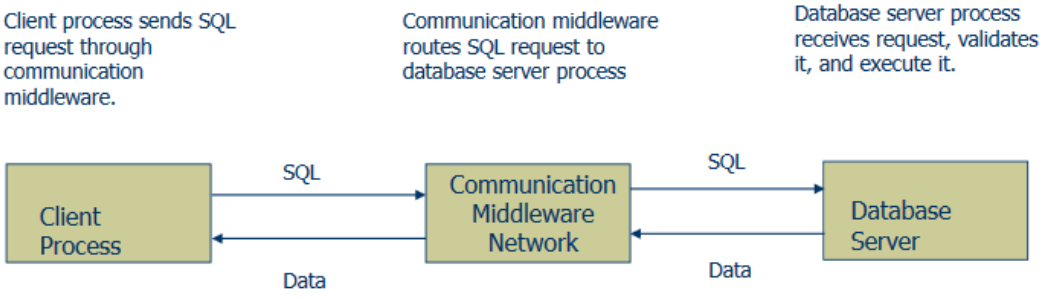
Advantages

1. Easier to Build and Maintain
2. Better Security
3. Stable

Disadvantages

1. Single point of failure
2. Less scalable

How Components Interact



Internet as client/server technology

- Internet is massive network of networks and world wide web is a system of interlinked hypertext documents accessed via the internet.

- To complete the flow of accessing information over the web there is need of client/server architecture.
- client/server describes the flow of information between two computer programs in which one computer program (client) makes a service request to another computer program (the server), which provide service requested by the client.
- Clients rely on servers for required resources. It is network architecture in which each computer or process on the network is either a client or a server. Hence, we could describe internet as client/server technology.

For example: When you check your bank account from a computer, a client program forwards a request to a server program at the bank. That program may in turn forward a request to its own client program which then sends a request to a database server at another bank computer. Once the account balance is retrieved from database, it is returned back to the client which in turn serves it back to the client in your computer, which then displays the information.

E-Mail (Electronic Mail)

One of the most popular Internet services is electronic mail (e-mail).

At the beginning of the Internet era, the messages sent by electronic mail were short and consisted of text only. But today, electronic mail is much more complex. It allows a message to include text, audio, and video. It also allows one message to be sent to one or more recipients.

Components of E-Mail Architecture

1. **User Agent** - The first component of an electronic mail system is the user agent. It provides service to the user to make the process of sending and receiving a message easier .It includes composing, reading, replying, forwarding and handling messages.
2. **Addresses** - To deliver mail, a mail handling system must use an addressing system with unique addresses. In the Internet, the address consists of two parts: a local part and a domain name, separated by an @ sign .
    a. **Local Part** - The local part defines the name of a special file, called the user mailbox, where all the mail received for a user is stored for retrieval by the message access agent.
    b. **Domain Name** - The second part of the address is the domain name. An organization usually selects one or more hosts to receive and send e-mail; the hosts are sometimes called mail servers or exchangers. The domain name assigned to each mail exchanger either comes from the DNS database or is a logical name (for example, the name of the organization).

Internet Service Providers

An Internet Service Provider (ISP) is a company such as Worldlink, Vianet etc that provides Internet access to companies, families, and even mobile users. ISPs use fiber-optics, satellite, copper wire, and other forms to provide Internet access to its customers.

The type of Internet access varies depending on what the customer requires. For home use, cable or DSL (digital subscriber line) is the perfect, affordable choice.

The amount of bandwidth is usually what drives the price. Bandwidth is the amount of data that can be sent through an internet connection in a given amount of time.

ISPs connect to one another by forming backbones, which is another way of saying a main highway of communications. Backbones usually consist of fiber-optic media.

Domain Name Server(DNS)

For communication to take place successfully, the sender and receiver both should have addresses and they should be known to each other . Addressing in the application program is different from that in other layers. There is a alias name of address of remote host. The application program uses an alias name instead of IP address.

To map a alias name onto an IP address, an application program calls a library procedure called the resolver, passing it the name as a parameter

The resolver sends a query containing the name to a local DNS server, which looks up the name and returns a response containing the IP address to the resolver, which then returns it to the caller.

The query and response messages are sent as UDP packets. Armed with the IP address, the program can then establish a TCP connection with the host or send it UDP packets

DNS Name Space

For the Internet, the top of the naming hierarchy is managed by an organization called ICANN (Internet Corporation for Assigned Names and Numbers).

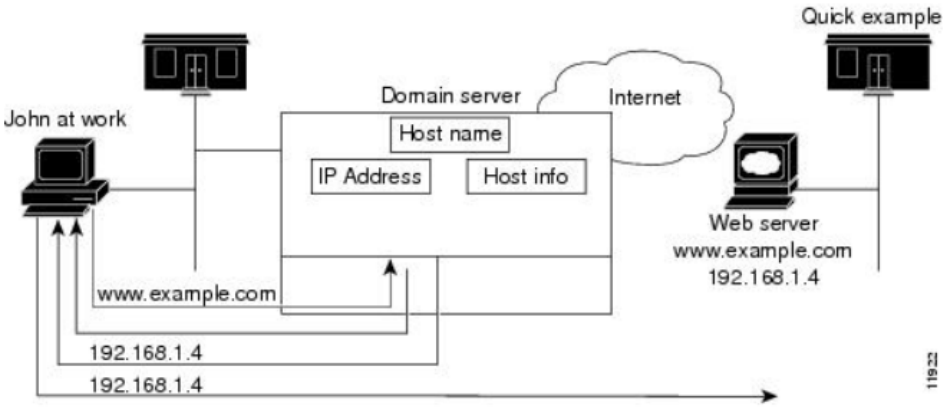
Conceptually, the Internet is divided into over 250 top-level domains, where each domain covers many hosts. Each domain is partitioned into subdomains, and these are further partitioned

The top-level domains come in two flavors: generic(eg. .com.,.edu,.net) and countries(.np,.au)

The country domains include one entry for every country, as defined in ISO 3166.

How DNS Works?

- John's workstation sends a request to the DNS server about the IP address of www.example.com.
- The DNS server checks its database to find that www.example.com corresponds to 192.168.1.4
- The server returns this address to John's browser.
- The browser uses the address to locate the website

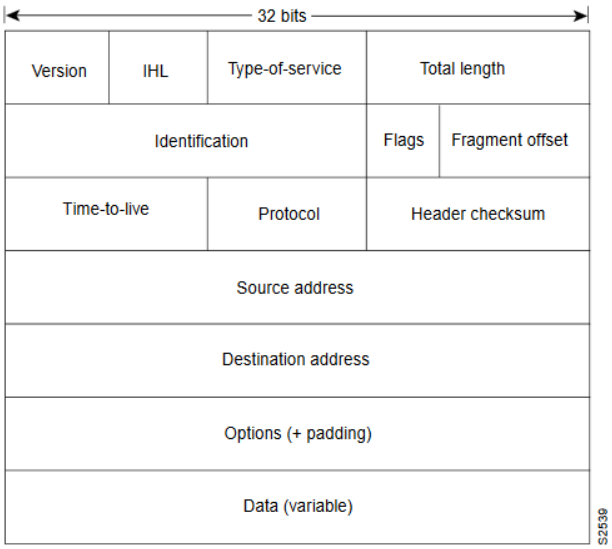


Intenet Protocol (IP)

- Internet Protocol (IP) is a network-layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be routed.
- IP is the primary network-layer protocol in the Internet protocol suite. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols.
- IP has two primary responsibilities: providing connectionless, best-effort delivery of datagrams through an internetwork and providing fragmentation and reassembly of datagrams to support data links with different maximum-transmission unit (MTU) sizes.
- IP includes a set of rules that embody the idea of unreliable packet delivery:
- How hosts and routers should process packets
- How and when error messages should be generated
- The conditions under which packets can be discarded.

IP Packet Format

IP packet contains several types of information, as illustrated in Figure



Internet Address (IP address, Domain Names, Electronic mail address, URL)

IP address

1. IPV4 Address

   An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet. IPv4 addresses are unique. They are unique in the sense that each address defines one, and only one, connection to the Internet. Two devices on the Internet can never have the same address at the same time.

   A protocol such as IPv4 that defines addresses has an address space. An address space is the total number of addresses used by the protocol. If a protocol uses N bits to define an address, the address space is 2N because each bit can have two different values (0 or 1) and N bits can have 2N values. IPv4 uses 32-bit addresses, which means that the address space is 2^32 or 4,294,967,296 (more than 4 billion).

   There are two prevalent notations to show an IPv4 address: binary notation and dotted decimal notation.

   Binary Notation :In binary notation, the IPv4 address is displayed as 32 bits. Each octet is often referred to as a byte. Eg. 01110101 10010101 00011101 00000010

   Dotted-Decimal Notation :To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes

   Eg: 117.149.29.2

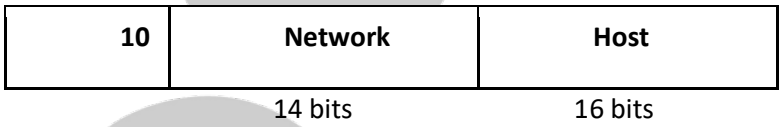
Classes of IP address

1. Class A Address

   The network field is 7 bit long and host field is 24 bit long. But the host numbers will range from 0.0.0.0 to 127.255.255.255.The 0 field in first field identifies that it is a class A network.

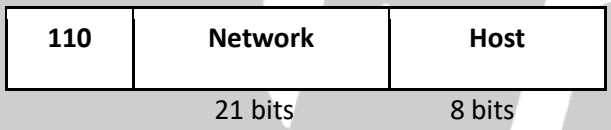
2. Class B Address

   The class B format is shown below. The first two fields identify the network and the number in the first field must be in range 128-192. Class b networks are large. IP address ranges from 128.0.0.0 to 191.255.255.255.



3. Class C address

   The class C format is as shown



   The IP address ranges from 192.0.0.0 to 223.255.255.255

4. Class D address

5. Class E address Format

Transmission control Protocol (TCP)

- The TCP provides reliable transmission of data in an IP environment. TCP corresponds to the transport layer (Layer 4) of the OSI reference model. Among the services TCP provides are stream data transfer, reliability, efficient flow control, full-duplex operation, and multiplexing

- TCP offers reliability by providing connection-oriented, end-to-end reliable packet delivery through an internetwork. It does this by sequencing bytes with a forwarding acknowledgment number that indicates to the destination the next byte the source expects to receive.
- TCP offers efficient flow control, which means that, when sending acknowledgments back to the source, the receiving TCP process indicates the highest sequence number it can receive without overflowing its internal buffers.
- Full-duplex operation means that TCP processes can both send and receive at the same time. Finally, TCP's multiplexing means that numerous simultaneous upper-layer conversations can be multiplexed over a single connection.
- To use reliable transport services, TCP hosts must establish a connection-oriented session with one another. Connection establishment is performed by using a "three-way handshake" mechanism.

SMTP

- The actual mail transfer is done through message transfer agents. To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA. The formal protocol that defines the MTA client and server in the Internet is called the Simple Mail Transfer Protocol (SMTP).
- SMTP is used two times, between the sender and the sender's mail server and between the two mail servers. SMTP simply defines how commands and responses must be sent back and forth.

- Commands and Responses

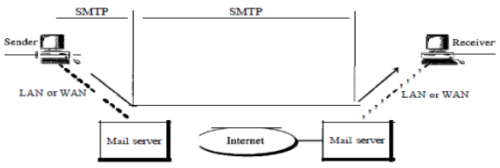


Fig: SMTP Range

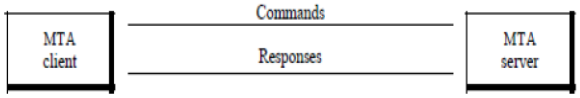


Fig: Command and Response

SMTP uses commands and responses to transfer messages between an MTA client and an MTA server.

Mail Transfer Phases

The process of transferring a mail message occurs in three phases: connection establishment, mail transfer, and connection termination.

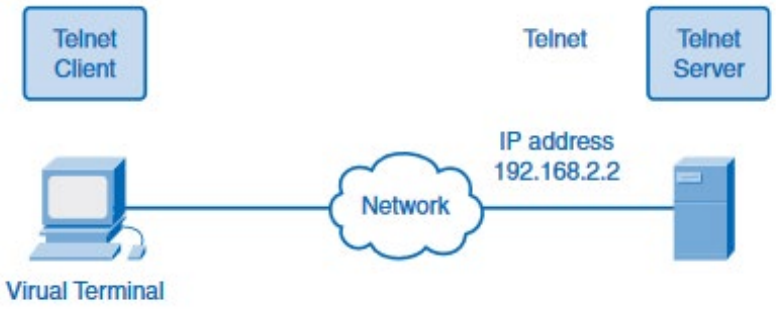
POP

- Post Office Protocol, version 3 (POP3) is simple and limited in functionality. The client POP3 software is installed on the recipient computer; the server POP3 software is installed on the mail server. Mail access starts with the client when the user needs to download e-mail from the mailbox on the mail server. The client opens a connection to the server on TCP port 110. It then sends its user name and password to access the mailbox. The user can then list and retrieve the mail messages, one by one.
- POP3 has two modes: the delete mode and the keep mode. In the delete mode, the mail is deleted from the mailbox after each retrieval. In the keep mode, the mail remains in the mailbox after retrieval. The delete mode is normally used when the user is working at her permanent computer and can save and organize the received mail after reading or replying. The keep mode is normally used when the user accesses her mail away from her primary computer (e.g., a laptop). The mail is read but kept in the system for later retrieval and organizing

TELNET

- TELNET is an abbreviation for TErminaL NETwork. It is the standard TCP/IP protocol for virtual terminal service as proposed by the International Organization for Standards (ISO).
- Telnet is a client/server protocol that provides a standard method of emulating text-based terminal devices over the data network. Both the protocol itself and the client software that implements the protocol are commonly referred to as Telnet
- A connection using Telnet is called a VTY(Virtual Terminal) session or connection. Telnet specifies how a VTY session is established and terminated. It also provides the syntax and order

of the commands used to initiate the Telnet session, and it provides control commands that can be issued during a session.

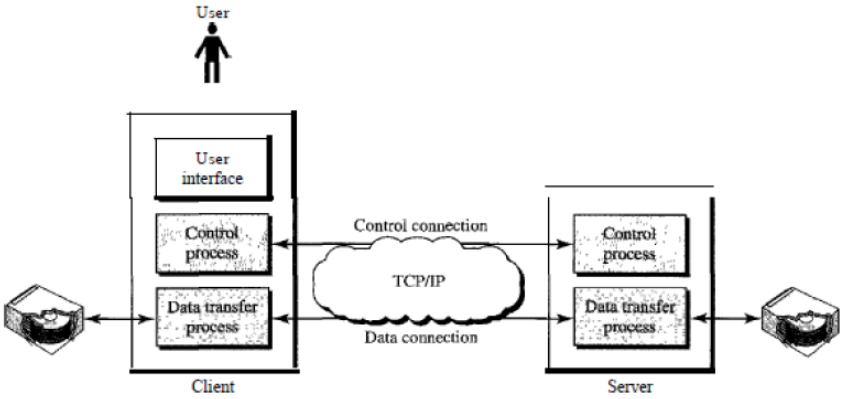


- Each Telnet command consists of at least 2 bytes. The first byte is a special character called the Interpret as Command (IAC)character. The IAC character defines the next byte as a command rather than text.
- Rather than using a physical device to connect to the server, Telnet uses software to create a virtual device that provides the same features of a terminal session with access to the server command-line interface (CLI).
- To support Telnet client connections, the server runs a service called the Telnet daemon. A virtual terminal connection is established from an end device using a Telnet client application.
- When a Telnet connection is established, users can perform any authorized function on the server, just as if they were using a command-line session on the server itself. If authorized, they can start and stop processes, configure the device, and even shut down the system.

FTP

- File Transfer Protocol (FTP) is the standard mechanism provided by TCP/IP for copying a file from one host to another. Although transferring files from one system to another seems simple and straightforward, some problems must be dealt with first. For example, two systems may use different file name conventions, two systems may have different ways to represent text and data.
- FTP differs from other client/server applications in that it establishes two connections between the hosts.
- One connection is used for data transfer, the other for control information (commands and responses). Separation of commands and data transfer makes FTP more efficient. The control connection uses very simple rules of communication. We need to transfer only a line of command or a line of response at a time.
- The data connection, on the other hand, needs more complex rules due to the variety of data types transferred. However, the difference in complexity is at the FTP level, not TCP. For TCP, both connections are treated the same. FTP uses two well-known TCP ports: Port 21 is used for the control connection, and port 20 is used for the data connection.

- The client has three components: user interface, client control process, and the client data transfer process. The server has two components: the server control process and the server data transfer process.
- The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.
- The data connection is made between the data transfer processes. The data connection is opened and then closed for each file transferred. It opens each time commands that involve transferring files are used, and it closes when the file is transferred



HTTP

- The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web. HTTP functions as a combination of FTP and SMTP. It is similar to FTP because it transfers files and uses the services of TCP. It uses only one TCP connection.
- There is no separate control connection; only data are transferred between the client and the server. HTTP is like SMTP because the data transferred between the client and the server look like SMTP messages.
- HTTP uses the services of TCP, HTTP itself is a stateless protocol. The client initializes the transaction by sending a request message. The server replies by sending a response.
- The formats of the request and response messages are similar. A request message consists of a request line, a header, and sometimes a body. A response message consists of a status line, a header, and sometimes a body.

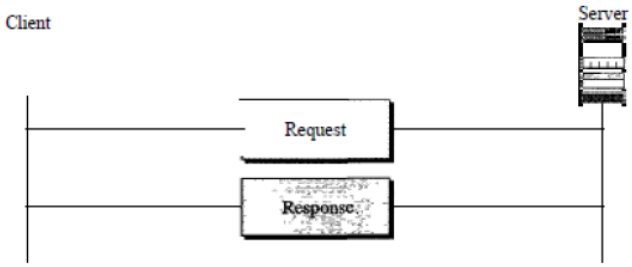


Fig: HTTP Transaction

Gopher

- 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

WAIS

- The Wide Area Information Server idea is based on a search model of information, rather than a browse one. Sites that run WAIS servers have created a collection of indexed data that can then be retrieved by searches on these indexes. The access protocol to WAIS servers is based on the standard developed for library searching by ANSI (American National Standards Institute) with the unlikely title, Z39.50 (aka Information Retrieval Service and Protocol Standard).
- WAIS has four parts (like most information services except the richer WWW): the client, the server, the database, and the protocol.
- Client programs (e.g. the X Windows client xwaisq) construct queries, and send them using the protocol to the appropriate server. The server responds, and includes a 'relevance' measure for the results of the search match to the query.
- The actual operation of the protocol is quite complex, as it permits exchanges to be broken into separate parts. WAIS permits retrieval of bibliographic, as well as contents (including images), data.
- A search request consists of seed words, or keys if you like, typed by a user into the client, together with a list of documents (identified by a unique global ID). The response is quite complex and includes a list of records, including the following fields:

    - Headline- basically a title/description
    - Rank- relative relevance of this document
    - Formats- list of formats available (text/postscript etc)
    - Document ID
    - Length

Intranet

- An Intranet is a private computer network that uses Internet protocols, network connectivity, and possibly the public telecommunication system to securely share part of an organization's information or operations with its employees.
- It uses the same concepts and technologies of the Internet (clients and servers) running on the TCP/IP protocol suite. HTTP, FTP and SMTP are very commonly used. Access to information is typically through browsers.
    - It is Platform independent.
    - No need to install special software on clients.
- Intranet Web servers differ from public Web servers in that the public must have the proper permissions and passwords to access the intranet of an organization.
- Intranets are designed to permit users who have access privileges to the internal LAN of the organization.
- Within an intranet, Web servers are installed in the network. Browser technology is used as the common front end to access information on servers such as financial, graphical, or text-based data.

Advantages

- Intranets help employees to quickly locate information and applications relevant to their roles and responsibilities.
- Standard interface, allowing "access from anywhere".
- Can serve as a powerful tool for communication within an organization.
- Permits information to be published.

Disadvantages

- Management does need to stop control of specific information, this problem can be minimized but with appropriate prudence.
- The other disadvantage of Intranet is security issue
- Intranet gathered everything in one location which is really good but if it is not prearranged then you will spoil everything.
- The cost of intranet is very high but has lots of advantages after implementing

Extranet

- An Extranet is a private network that uses Internet protocols, network connectivity, and possibly the public communication system to securely share part of an organization's information or operations with suppliers, partners, customers, or other businesses.
- It can be viewed as part of a company's Intranet that is extended to users outside the company.

- It is “a private internet over the Internet”. It is used to designate “private parts” of a website. Only registered users can navigate.
- It requires security and privacy.

    - Firewall server management
    - Issuance and use of digital certificates or similar means of authentication.
    - Encryption of messages.
    - Use of Virtual Private Networks (VPN) that tunnel through the public network.

    Advantages:

    - Can improve organization productivity.
    - Allows information to be viewed at times convenient for external
    - Information can be updated instantly.
    - Authorized users have immediate access to latest information.
    - Can improve relationships with customers

World Wide Web (WWW) and its evolution

The World Wide Web (WWW) allows computer users to position and view multimedia-based documents (i.e., documents with text, graphics, animations, audios and/or videos) on almost any subject.

Even though the Internet was developed more than three decades ago, the introduction of the WWW was a relatively recent event. In 1990, Tim Berners-Lee of CERN (the European Laboratory for Particle Physics) developed the World Wide Web and several communication protocols that form the backbone of the WWW.

The Internet and the World Wide Web will surely be listed among the most significant and profound creations of humankind. In the past, most computer applications ran on stand alone computers. (i.e., computers that were not connected to one another)

Today’s applications can be written to communicate among the world’s hundreds of millions of computers. The Internet makes our work easier by mixing computing and communications technologies. It makes information immediately and conveniently accessible worldwide. It makes it possible for individuals and small businesses to get worldwide contact

In the last decade, the Internet and World Wide Web have altered the way people communicate, conduct business and manage their daily lives. They are changing the nature of the way business is done.

Evolution

- March 1989 First proposal written at CERN by Tim Berners-Lee.
- October 1990 Tim Berners-Lee and Robert Cailliau submit revised proposal at CERN.
- November 1990 First prototype developed at CERN for the NeXT .
- March 1991 Prototype line mode browser available at CERN.

- January 1991 First HTTP servers outside of CERN set up including servers at SLAC and NIKHEF.
- July 1992 Viola browser for X-windows developed by P. Wei at Berkeley.
- November 1992 Midas browser (developed at SLAC) available for X-windows.
- January 1993 Around 50 known HTTP servers.
- August 1993 O'Reilly hosts first WWW Wizards Workshop in Cambridge, Mass. Approximately 40 attends
- February 1993 NCSA releases first alpha version of "Mosaic for X. "
- September 1993 NCSA releases working versions of Mosaic browser for X-windows, PC/Windows and Macintosh platforms.
- October 1993 Over 500 known HTTP servers.
- December 1993 John Markov writes a page and a half on WWW and Mosaic in the New York Times business section. Guardian (UK) publishes a page on WWW.
- May 1994 First International WWW Conference, CERN, Geneva, Switzer-land. Approximately 400 attended
- June 1994cOver 1500 registered HTTPcservers.
- July 1994MIT/CERN agreement to start WWW Organization.
- October 1994 Second International WWW Conference, Chicago, Illinois, with over 1500 attendees

Architecture of Web

Uniform resource Locator (URL)

- A URL (Uniform Resource Locator) is a unique identifier used to locate a resource on the internet. It is also referred to as a web address. URLs consist of multiple parts -- including a protocol and domain name -- that tell a web browser how and where to retrieve a resource.
- End users use URLs by typing them directly into the address bar of a browser or by clicking a hyperlink found on a webpage, bookmark list, in an email or from another application.
- A URL is the most common type of Uniform Resource Identifier (URI). URIs are strings of characters used to identify a resource over a network. URLs are essential to navigating the internet.
- URL protocols include HTTP (Hypertext Transfer Protocol) and HTTPS (HTTP Secure) for web resources, mailto for email addresses, ftp for files on a File Transfer Protocol (FTP) server, and telnet for a session to access remote computers. Most URL protocols are followed by a colon and two forward slashes; mailto is followed only by a colon.
- **Parts of an URL**

  http://host.company.com:80/a/b/c.html?user=Alice&year=2008#p2

  - **Scheme (http:)**: identifies protocol used to fetch the content.
  - **Host name (//host.company.com)**: name of a machine to connect to.
  - **Server's port number (80)**: allows multiple servers to run on the same machine.
  - **Hierarchical portion (/a/b/c.html)**: used by server to find content.

- **Query parameters (?user=Alice&year=2008)**: provides additional parameters
- **Fragment (#p2)**: Have browser scroll page to fragment (html: p2 is anchor tag), Used on the browser only; not sent to the server.

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

Examples: Internet Explorer, Netscape Navigator, Opera, Firefox-which was developed from Mozilla (the open source version of Netscape), Chrome

Search Engine

A search engine is a software program or script available through the Internet that searches documents and files for keywords and returns the results of any files containing those keywords.

Today, there are many different search engines available on the Internet, each with their own abilities and features.

The first search engine ever developed is considered Archie, which was used to search for FTP files and the first text-based search engine is considered Veronica.

Today, the most popular and well-known search engine is Google. Other popular search engines include AOL, Ask.com, Baidu, Bing, and Yahoo.

Search engines contain millions and sometimes billions of pages, many search engines not only just search the pages but also display the results depending on their importance. This importance is commonly determined by using various algorithms.

The source of all search engine data is a spider or crawler, which automatically visits pages and indexes their contents. Once a page has been crawled, the data contained in the page is processed and indexed.

Web servers

A Web server is a program that uses HTTP (Hypertext Transfer Protocol) to serve the files that form Web pages to users, in response to their requests, which are forwarded by their computers' HTTP clients. Dedicated computers and appliances may be referred to as Web servers as well.

The process is an example of the client/server model. All computers that host Web sites must have Web server programs.

Leading Web servers include Apache (the most widely-installed Web server), Microsoft's Internet Information Server (IIS) and nginx (pronounced engine X) from NGNIX. Other Web servers include Novell's NetWare server, Google Web Server (GWS) and IBM's family of Domino servers.

Web servers often come as part of a larger package of Internet- and intranet-related programs for serving email, downloading requests for File Transfer Protocol (FTP) files, and building and publishing Web pages.

Considerations in choosing a Web server include how well it works with the operating system and other servers, its ability to handle server-side programming, security characteristics, and the particular publishing, search engine and site building tools that come with it.

- Apache 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.

  The software offers an extensible and secure web server with services in sync with modern HTTP standards. HTTP Server is compatible with most UNIX-based operating systems (such as Mac OS, Linux, Solaris, Digital UNIX, and AIX), on other UNIX/POSIX-derived systems and on Microsoft Windows.

  Apache HTTP Server was the most popular webserver from 1996 until June of 2016.While Apache still remains one of the world's most heavily-used webservers it lost market share to NGINX, Microsoft and others since 2016.

- IIS

  Internet Information Services (IIS) 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.

- Proxy Server

  A proxy server is a dedicated computer or a software system running on a computer that acts as an intermediary between an endpoint device, such as a computer, and another server from

which a user or client is requesting a service. The proxy server may exist in the same machine as a firewall server or it may be on a separate server, which forwards requests through the firewall.

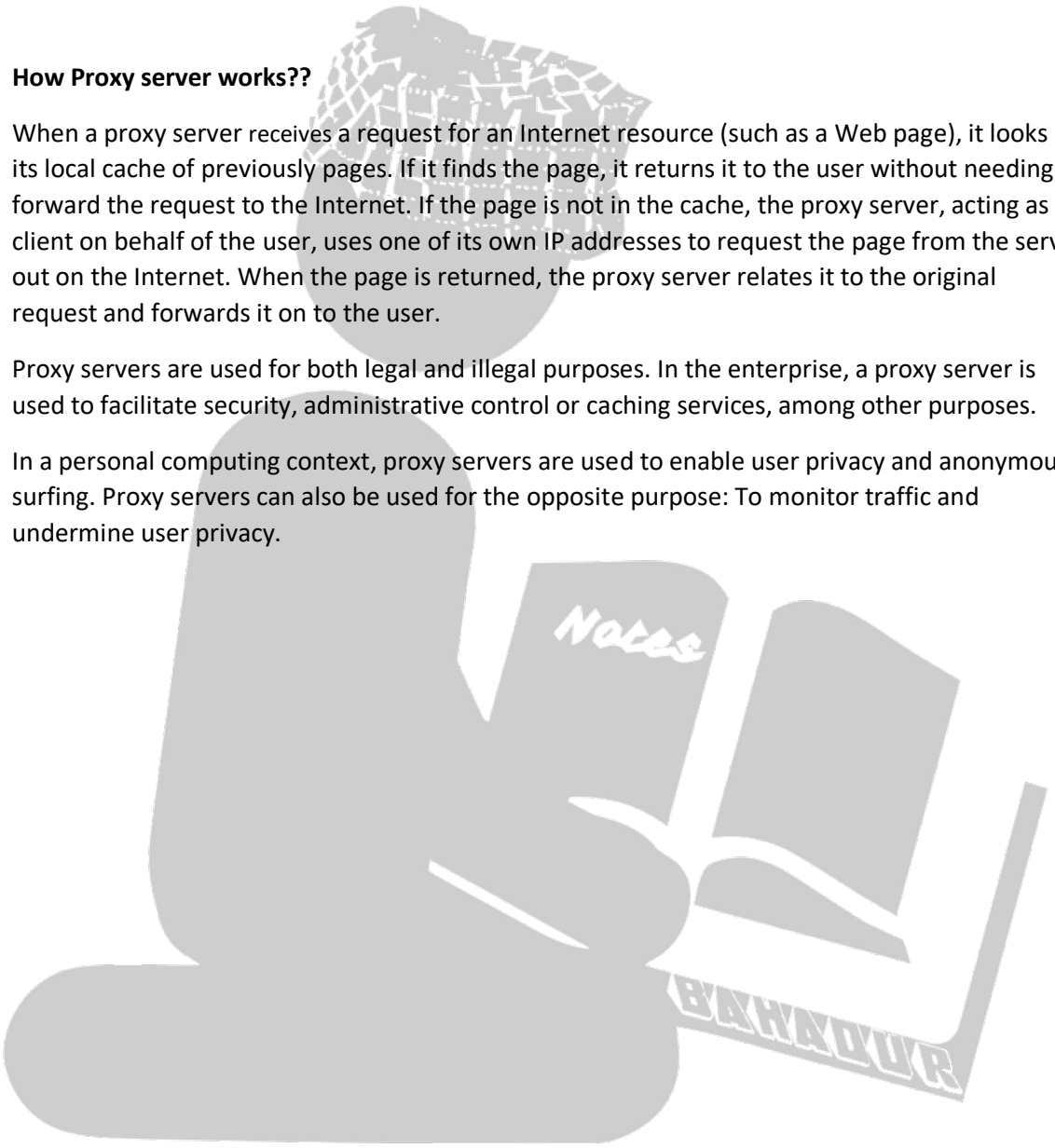
An advantage of a proxy server is that its cache can serve all users. If one or more Internet sites are frequently requested, these are likely to be in the proxy's cache, which will improve user response time. A proxy can also log its interactions, which can be helpful for troubleshooting.

How Proxy server works??

When a proxy server receives a request for an Internet resource (such as a Web page), it looks in its local cache of previously pages. If it finds the page, it returns it to the user without needing to forward the request to the Internet. If the page is not in the cache, the proxy server, acting as a client on behalf of the user, uses one of its own IP addresses to request the page from the server out on the Internet. When the page is returned, the proxy server relates it to the original request and forwards it on to the user.

Proxy servers are used for both legal and illegal purposes. In the enterprise, a proxy server is used to facilitate security, administrative control or caching services, among other purposes.

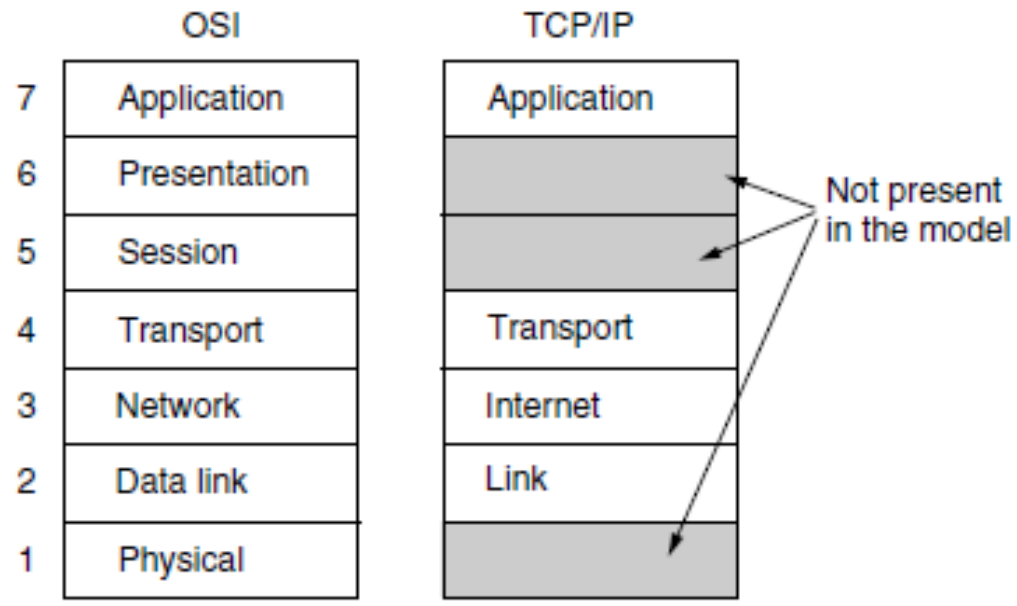
In a personal computing context, proxy servers are used to enable user privacy and anonymous surfing. Proxy servers can also be used for the opposite purpose: To monitor traffic and undermine user privacy.



TCP/IP protocol

- TCP/IP Reference Model is a four-layered suite of communication protocols. It was developed by the DoD (Department of Defense) in the 1960s.
- It is named after the two main protocols that are used in the model, namely, TCP and IP. TCP stands for Transmission Control Protocol and IP stands for Internet Protocol.

The four layers in the TCP/IP protocol suite are:



Link Layer

- The lowest layer in the model, the link layer describes what links such as serial lines and classic Ethernet must do to meet the needs of this connectionless internet layer.
- It is not really a layer at all, in the normal sense of the term, but rather an interface between hosts and transmission links.

Internet Layer

- The internet layer is the linchpin that holds the whole architecture together.
- Its job is to permit hosts to inject packets into any network and have them travel independently to the destination (potentially on a different network).
- They may even arrive in a completely different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired.
- The internet layer defines an official packet format and protocol called IP (Internet Protocol), plus a companion protocol called ICMP (Internet Control Message Protocol) that helps it

function. The job of the internet layer is to deliver IP packets where they are supposed to go. Packet routing is clearly a major issue here, as is congestion.

Transport Layer

- It is designed to allow peer entities on the source and destination hosts to carry on a conversation, just as in the OSI transport layer. Two end-to-end transport protocols have been defined here are UCP and UDP
- TCP (Transmission Control Protocol), is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet. It segments the incoming byte stream into discrete messages and passes each one on to the internet layer.
- At the destination, the receiving TCP process reassembles the received messages into the output stream. TCP also handles flow control to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle.
- UDP (User Datagram Protocol), is an unreliable, connectionless protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own.
- It is also widely used for one-shot, client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video.

Application Layer

- On top of the transport layer is the application layer. It contains all the higher- level protocols. The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP). Many other protocols have been added to these over the years.