

Unit-II

INTERNET-INTRANET-EXTRANET

The Internet, intranet, and extranet are the most popular platforms for e-commerce. In Internet is the most common platform for B2C e-commerce; the intranet is most the common for platform for corporate internal management; and the extranet is the most common platform for B2B e-commerce.

Network Type	Typical Users	Access	Type of information
The Internet	Any individual with dial-up access or LAN	Unlimited public; no restrictions	General public, and advertorial
Intranet	Authorized employees only	Private and restricted	Specific, corporate, and proprietary
Extranet	Authorized groups from collaborating companies	Private and authorized outside partners	Shared in authorized collaborating groups

The Internet

1. The Internet is a public and global communication network that provides direct connectivity to anyone over a local area network (LAN) or **Internet Service Provider (ISP)**.
2. The Internet is a public network that is connected and routed over gateways. End users are connected to local access providers (LANs or ISPs), who are connected to the Internet access providers, to network access providers, and eventually to the Internet backbone.
3. Since access to the Internet is open to all, there is a lack of control that may result in an unruly proliferation of information.

The Intranet:

1. An intranet is a corporate LAN or wide area network (WAN) that uses Internet technology and is secured behind company's firewalls (see security and protection).
2. The intranet links various servers, clients, databases, and application programs like Enterprise Resource Planning (ERP). Although intranets are developed on the same TCP/IP protocol as the Internet, they operate as a private network with limited access.
3. Only authorized employees are able to use it. Intranets are limited to information pertinent to the company and contain exclusive and often proprietary and sensitive information.

4. The firewalls protect the intranets from unauthorized outside access; the intranet can be used to enhance the communications and collaboration among authorized employees, customers, suppliers, and other business partners.
5. Since the intranet allows access through the Internet, it does not require any additional implementation of leased networks. This open and flexible connectivity is a major capability and advantage of intranet. Intranets provide the infrastructure for many **intra-business commerce** applications.

The Extranet

1. An extranet, or “extended intranet”, uses the TCP/IP protocol network of the Internet, to link intranets in different locations.
2. Extranet transmission is usually conducted over the Internet, which offers little privacy or transmission security.
3. Therefore, when using an extranet, it is necessary to improve the security of connecting portions of the Internet. This can be done by creating tunnels (see paragraph on security and protection) of secured data flows, using cryptography and authorization algorithm.
4. The Internet with tunneling technology is known as a **virtually private network (VPN)**.
5. Extranets provide secured connectivity between corporation’s intranets and the intranets of its business partners, material suppliers, financial services, government, and customers.
6. Access to intranets is usually limited by agreements of the collaborating parties, is strictly controlled, and is only available to authorized personnel.
7. The protected environment of the extranet allows groups to collaborate, sharing information exclusively, and exchanging it securely.
8. Since an extranet allows connectivity between businesses through the Internet, it is an open and flexible platform suitable for supply chain management.
9. To increase security, many companies replicate the database they are willing to share with their business partners and separate them physically from their regular intranets.

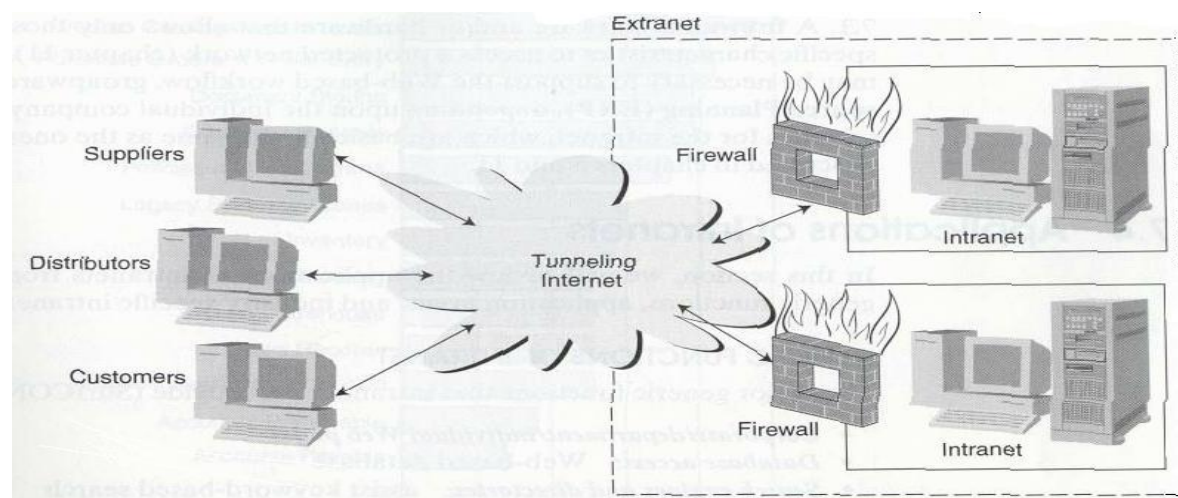


Figure Diagrammatic Contrast of the Internet, Intranet, and Extranet

Q. Compare internet, intranet and extranet? Or different between internet, intranet, and extranet?

Internet	Intranet	Extranet
It is a global system of interconnected computer networks.	It is a private network specific to an organization.	It is a private network that uses public network to information with suppliers vendors
Not regulated by any one	It is regulated by an organization	It is regulated by multiple organizations.
Thus content in the network is accessible to every one connected.	Thus content in the network is accessible only to members of organization.	The content in the network is accessible to members of organization and external members with access to network.
It is largest in terms of number of connected device.	It is small network with minimal number of connected device.	The number of devices connected is comparable with intranet.
It is owned by no one.	It is owned by single organization	It is owned by single/multiple organization.
It is means of sharing information through out the world.	It is means of sharing sensitive information through out organization	It is means of sharing information between members and external members.
Security is depending of the user of device connected to network.	Security is enforced via a firewall.	Security is enforced via a firewall that separates internet and extranet.
Users can access internet anonymously.	Users should have valid username/password to access intranet.	Users should have valid username/password to access extranet.

Explain about Firewalls?

Fire walls:

A firewalls is a system that prevents un-authorized access to or from a private network. T examines each message entering and leaving the network, and allows only those authorized message to pass through. It can be implemented in hardware and software or both. A firewall helps to keep your computer more secure. It restricts information that comes to your computer from other computers, giving you more control over the data on your computer and providing a line of defense against people or programs.

Importance:

1. It allows only authorized access to inside network.
2. It prevent insider stacks on critical systems.
3. A firewall as a barrier, check information coming from the internet or a network and allow it to pass through to your computer, depending on your firewall settings.
4. It provides the ability to control access to site system. It can greatly improve network security and reduce risk to hosts on the subnet by filtering inherently insecure services.

Benefits or advantages of firewalls:

1. Internet firewalls allow the network administrator to define a centralized 'choke point' that keeps unauthorized users such as hackers, crackers, vandals and spies and providing protection from various types of routing attacks.
2. Firewalls offer a convenient point where internet security can be monitored and alarms generated.
3. An internet firewall is a logical place to deploy a network address translator (NAT) that can help alleviate the address space shortage and eliminate the need to re-number when an organization changes its ISP's.
4. An internet firewall is the perfect point to audit or log internet usage.
5. An internet firewall can also offer a central point of contract for information delivery service to customers.

Types of firewalls:

1. **Application Gateways:** the first firewalls were application gateways, and are sometimes known as proxy gateways. These are sun with special software to act as a proxy server.
2. **Packet filtering:** packet filtering is a techniques where by routers have ACLs(Access Control Lists) turned on. By default, a router will pass all traffic sent it, and will do so without any sort of restrictions.
3. **Hybrid Systems:** in an attempt to marry the security of the application layer gateways with the flexibility and speed of packet filtering, some vendors have created systems that use the principles of both.

Explain about Protocol?

Protocol:

In information technology, a protocol is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols specify interactions between the communicating entities.

Protocols exist at several levels in a telecommunication connection. For example, there are protocols for the data interchange at the hardware device level and protocols for data interchange at the application program level. In the standard model known as Open Systems Interconnection (OSI), there are one or more protocols at each layer in the telecommunication exchange that both ends of the exchange must recognize and observe. Protocols are often described in an industry or international standard.

The TCP/IP Internet protocols, a common example, consist of:

- Transmission Control Protocol (TCP), which uses a set of rules to exchange messages with other Internet points at the information packet level

- Internet Protocol (IP), which uses a set of rules to send and receive messages at the Internet address level
- Additional protocols that include the Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP), each with defined sets of rules to use with corresponding programs elsewhere on the Internet.

TCP/IP Addresses

- Addressing in TCP/IP is specified by the Internet Protocol (IP)
- Each host is assigned a 32-bit number
 - Called the IP address or Internet address
 - Unique across entire Internet
- Each IP address is divided into a prefix and a suffix
 - Prefix identifies network to which computer is attached
 - No two networks can be assigned the same network number
 - Suffix identifies computer within that network
 - No two computers on the same network can have the same suffix, but computers on different networks can have the same suffix
 - Address format makes routing efficient

Properties of IP Addresses

- Network numbers (prefix) are unique
 - Assignment of network numbers must be coordinated globally to ensure uniqueness
 - Assigned by ICANN (formerly InterNIC/Network Solutions)
- Host addresses (suffix) may be reused on different networks
 - combination of network number prefix and host address suffix will be unique
 - assignment of host addresses can be managed locally
- E.g. your ISP can set the host addresses and names within the purview of their assigned network by ICANN

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

- Transmission Control Protocol TCP corresponds to the Transport Layer of OSI Model.
- TCP is a reliable and connection oriented protocol.
- TCP offers:
 - Stream Data Transfer.
 - Reliability.

- Efficient Flow Control Full-duplex operation.
- Multiplexing.
- TCP offers connection oriented end-to-end packet delivery.
- TCP ensures reliability by sequencing bytes with a forwarding acknowledgement number that indicates to the destination the next byte the source expect to receive.
- It retransmits the bytes not acknowledged with in specified time period.

TCP Services: TCP offers following services to the processes at the application layer:

1. Stream Delivery Service
2. Sending and Receiving Buffers
3. Bytes and Segments
4. Full Duplex Service
5. Connection Oriented Service
6. Reliable Service

Stream Deliver Service: TCP protocol is stream oriented because it allows the sending process to send data as stream of bytes and the receiving process to obtain data as stream of bytes.

Sending and Receiving Buffers: It may not be possible for sending and receiving process to produce and obtain data at same speed, therefore, TCP needs buffers for storage at sending and receiving ends.

Bytes and Segments: The Transmission Control Protocol TCP, at transport layer groups the bytes into a packet. This packet is called segment. Before transmission of these packets, these segments are encapsulated into an IP datagram.

Full Duplex Service : Transmitting the data in duplex mode means flow of data in both the directions at the same time.

Connection Oriented Service :

TCP offers connection oriented service in the following manner:

1. TCP of process-1 informs TCP of process – 2 and gets its approval.
2. TCP of process – 1 and TCP of process – 2 and exchange data in both the two directions.
3. After completing the data exchange, when buffers on both sides are empty, the two TCP's destroy their buffers.

Q. Explain about HTTP, SMTP and FTP Protocol?

1. HTTP (Hyper Text Transfer Protocol):

The Hypertext Transfer Protocol (HTTP) is an application-level protocol with the lightness and speed necessary for distributed, collaborative, hypermedia information systems. HTTP has been in use by the World-Wide Web global information initiative since 1990.

HTTP allows an open-ended set of methods to be used to indicate the purpose of a request. It builds on the discipline of reference provided by the Uniform Resource Identifier (URI). Messages are passed in a format similar to that used by Internet Mail and the Multipurpose Internet Mail Extensions (MIME).

The HTTP protocol is a request/response protocol. A client sends a request to the server in the form of a request method, URI, and protocol version, followed by a MIME-like message containing request modifiers, client information, and possible body content over a connection with a server.

Protocol Structure HTTP messages consist of requests from client to server and responses from server to client.

The request message has the following format:

Request Line	General Header	Request header	Entity header	Message Body
--------------	----------------	----------------	---------------	--------------

The Request-Line begins with a method token, followed by the Request-URI and the protocol version, and ends with CRLF. The elements are separated by SP characters. No CR or LF is allowed except in the final CRLF sequence. The details of the general header, request header and entity header can be found in the reference documents.

The response message has the following format:

Status Line	General header	Response header	Entity header	Message Body
-------------	----------------	-----------------	---------------	--------------

The Status-Code element is a 3-digit integer result code of the attempt to understand and satisfy the request. The Reason-Phrase is intended to give a short textual description of the Status-Code. The Status-Code is intended for use by automata and the Reason-Phrase is intended for the human user. The client is not required to examine or display the Reason-Phrase. The details of the general header, response header and entity header could be found in the reference documents.

2. SMTP (Simple Mail Transfer Protocol):

Simple Mail Transfer Protocol (SMTP) is a protocol designed to transfer electronic mail reliably and efficiently. SMTP is a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and provides notification regarding incoming mail. SMTP is independent of the particular transmission subsystem and requires only a reliable ordered data stream channel.

An important feature of SMTP is its capability to transport mail across networks, usually referred to as "SMTP mail relaying". A network consists of the mutually-TCP-accessible hosts on the public Internet, the mutually-TCP-accessible hosts on a firewall-isolated TCP/IP Intranet, or hosts in some other LAN or WAN environment utilizing a non-TCP transport-level protocol.

Using SMTP, a process can transfer mail to another process on the same network or to some other network via a relay or gateway process accessible to both networks. In this way, a mail message may pass through a number of intermediate relay or gateway hosts on its path from sender to ultimate recipient.

3.FTP(File Transfer Protocol):

1. File Transfer Protocol (FTP) enables file sharing between hosts.
2. FTP uses TCP to create a virtual connection for control information and then creates a separate TCP connection for data transfers.
3. The control connection uses an image of the TELNET protocol to exchange commands and messages between hosts. The key functions of FTP are:

- 1) to promote sharing of files (computer programs and/or data);
- 2) to encourage indirect or implicit (via programs) use of remote computers;
- 3) to shield a user from variations in file storage systems among hosts; and
- 4) to transfer data reliably and efficiently.

FTP, though usable directly by a user at a terminal, is designed mainly for use by programs. FTP control frames are TELNET exchanges and can contain TELNET commands and option negotiation. However, most FTP control frames are simple ASCII text and can be classified as FTP commands or FTP messages. FTP messages are responses to FTP commands and consist of a response code followed by explanatory text.

Q. **Explain about Utility program?**

1. **Ping:**

Ping is a network debugging tool used to determine whether a specific IP address is accessible. It is implemented using the ICMP Echo and and ICMP Echo Reply messages. This is documented in RFC 792. In an IP network, 'ping' sends an ICMP Echo message (in a single packet) to the destination IP address and listens for a single packet in reply (the ICMP Echo Reply).

What ping can tell you: Determine if packets have been dropped, duplicated or reordered. Recall that an ICMP Echo/Echo Reply messages can support 'sequence numbers'. Ping uses these sequence numbers to facilitate this. Detect some forms of damaged packets by using the 'checksum' field in the ICMP Echo/Echo Reply messages. Compute the Round Trip Time (RTT) by placing a timestamp in each packet, which is echoed back. Can report other ICMP messages, such as if a router is declaring the target host unreachable.

What ping can't tell you: May not always be able to tell the reason for unanswered packets. The reason could be due to routers silently discarding undeliverable packets or a destination host chooses not to reply as in the case of Microsoft at www.microsoft.com) Can't tell the reason for a damaged, delayed or duplicated packet nor where it occurred although a logical deduction can usually be made with respect to this. Can't provide a detailed description of every host/router that handled the packet and everything that happened every step of the way.

2. **Tracer:**

1. Tracer is a network debugging tool that is used to trace a packet from the source host to a destination host.
2. It attempts to trace the route the packet takes, i.e., it shows how many hops the packet requires in order to reach the destination host, and how long each hop takes.
3. Trace route works because it DEPENDS on the common router practice of sending an ICMP Time Exceeded message (defined in RFC 792).

4. Recall the TTL (Time to Live) IP header field in an IP packet. The TTL is designed to prevent packets from running in loops in an internet.

3. Finger:

1. The Finger user information protocol provides an interface to a remote user information program (RUIP). Finger, based on the Transmission Control Protocol, is a protocol for the exchange of user information using TCP port 79.
2. The local host opens a TCP connection to a remote host on the Finger port. An RUIP becomes available on the remote end of the connection to process the request.
3. The local host sends the RUIP a one line query based upon the Finger query specification and waits for the RUIP to respond. The local host receives the answer and the close signal and then proceeds to close its end of the connection.
4. Finger discloses information about users; moreover, such information may be considered sensitive.
5. Security administrators should make explicit decisions about whether to run Finger and what information should be provided in responses. This makes it possible to track conversations in progress and see where someone's attention was focused. Sites that are information-security conscious should not run Finger without an explicit understanding of how much information it is giving away.
6. Like Telnet, FTP and SMTP, Finger is one of the protocols at the security perimeter of a host. Accordingly, the soundness of the implementation is paramount. The implementation should receive just as much security scrutiny during design, implementation, and testing as Telnet, FTP, or SMTP.

The Finger query specification is defined:

$\{Q1\} ::= [\{W\} | \{W\}\{S\}\{U\}]\{C\}$

$\{Q2\} ::= [\{W\}\{S\}][\{U\}]\{H\}\{C\}$

$\{U\} ::= \text{username}$

$\{H\} ::= @\text{hostname} | @\text{hostname}\{H\}$

$\{W\} ::= /W$

$\{W\} ::= /W$

$\{S\} ::= | \{S\}$

4. Telnet:

1. TELNET is the terminal emulation protocol in a TCP/IP environment.
2. TELNET uses the TCP as the transport protocol to establish connection between server and client.

3. After connecting, TELNET server and client enter a phase of option negotiation that determines the options that each side can support for the connection.
4. Each connected system can negotiate new options or renegotiate old options at any time. In general, each end of the TELNET connection attempts to implement all options that maximize performance for the systems involved.

When a TELNET connection is first established, each end is assumed to originate and terminate at a "Network Virtual Terminal", or NVT. An NVT is an imaginary device which provides a standard, network-wide, intermediate representation of a canonical terminal. This eliminates the need for "server" and "user" hosts to keep information about the characteristics of each other's terminals and terminal handling conventions.

Modern Telnet is a versatile terminal emulation due to the many options that have evolved over the past twenty years. Options give TELNET the ability to transfer binary data, support byte macros, emulate graphics terminals, and convey information to support centralized terminal management.

Q. Explain about World Wide Web (WWW)?

1. The WWW is such an immensely popular Internet facility that for many users, it has become synonymous with the Internet.
2. Developed in 1992 at the European Laboratory for Particle Physics at Cern, Switzerland, the WWW links users to Internet sites.
3. The basic unit of WWW communication is the page, similar to this printed page. Within a Web page are "links" on which users can click and be automatically connected to related pages at the same or other Internet Websites.
4. With its ease of use and its multimedia ability to transmit text, graphics, audio, and video and to retrieve detailed information from anywhere in the world in seconds, the WWW has quickly become the interface of choice for Internet users.

COMPONENTS OF THE WWW

Key to the success of the WWW is its powerful system of links, allowing users to explore related sets of data stored in different computers on the Internet. This system of embedding links in the text of a Web page, called "hypertext," allows any sort of data to be accessed from a Web page by clicking on highlighted and/or underlined links that point to other pages.

Users are automatically routed to the selected Web page even if it resides in a distant computer. This web of interconnected pages gives the WWW its name. Every Web page has its own unique title, known as the Uniform Resource Locator (URL). A URL contains both the Internet address of the computer on which a Web page is stored and the name of the computer file that actually contains the page. More than 1/2 million WWW sites exist on the Internet, and each may contain numerous URLs.

The result is tens of millions of Web pages! So that users may view and retrieve Web pages without having to know and type the URL each time, a special type of program, known as a "browser," was developed. A browser program operates on a personal computer, interfacing it with the Internet and allowing users to "surf the WWW. Browsers are inexpensive and typically available without cost to educators.

All browsers allow Internet users to

- (1) retrieve Web pages from other computers;

(2) display these pages on the user's screen, using formatting commands that were specified by the author of the page; and

(3) make the Web pages active, progressing to the referenced file or URL by pointing and clicking on a hypertext link embedded in a page. Browsers are very easy to use, and even a computer novice can become accustomed to navigating the Internet within minutes.

The new user will soon realize, however, that navigating effectively through millions of Web pages requires skill in searching. To deal with this abundance of information, Internet users take advantage of WWW software tools known as "search engines."

A Web site is a collection of related Web pages and associated items, such as documents and pictures, stored on a Web server. A Web server is a computer that delivers requested Web pages to your computer. The same Web server can store multiple Web sites.

Q. Internet Features and services?

1. The Internet is a public and global communication network that provides direct connectivity to anyone over a local area network (LAN) or **Internet Service Provider (ISP)**.
2. The Internet is a public network that is connected and routed over gateways. End users are connected to local access providers (LANs or ISPs), who are connected to the Internet access providers, to network access providers, and eventually to the Internet backbone.
3. Since access to the Internet is open to all, there is a lack of control that may result in an unruly proliferation of information.

Major Features of Internet:

1. The World Wide Web.
2. E-Mail.
3. News
4. Telnet.
5. File Transfer Protocol(FTP).
6. Internet Relay Chat(IRC).

1. The World Wide Web:

- The World Wide Web is a part of the internet, which supports hypertext documents, allowing users to view and navigate different types of data.
- A web page is a document encoded with hypertext markup language (HTML) tags.
- HTML allows designers to link content together via hyperlinks.
- Every web page has an address , a uniform resource locator(URL).

2. E-Mail:

- Electronic mail(E-Mail) is the most popular reason people use the internet.
- To create, send, and receive e-mail messages you need an e-mail program and an account on an internet mail server with a domain name.
- To use e-mail, a user must have an e-mail address, which you create by adding your user name to the e-mail create by adding your user name to the e-mail server's domain name, as in jusmith@gmail.com.

3. News:

- One internet based service called news, includes tens of thousands of newsgroups.

- Each newsgroup hosts discussion on a specific topic. A newsgroups a some indicated its users special topic of interest, such as alt.food.cake.
- To participate in a newsgroup, you need a news-reader program hat.left you read articles that have been posted on a news server. You can post articles for others to read and respond to.

4. Telnet:

- telnet is a specialized service that lets you use one computer to access the contents of another computer a telnet host.
- A telnet program creates a “Window” into the host so you can access files, issue commands, and exchange data.
- Telnet is widely used by libraries to allow visitors to look up information find articles and so on.

5. File Transfer Protocol:

- File Transfer Protocol(FTP) is the internet tool used to copy files from one computer to another.
- Using a special FTP program or a web browser, you can log into an ETP host computer over the internet and copy files on to your computer.
- FTP is handy for finding and copying software files, articles and other types of data.

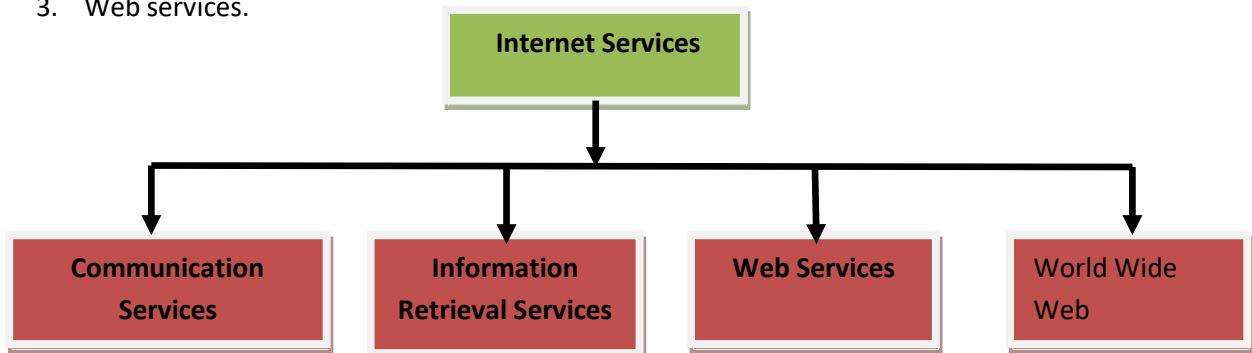
6. Internet Relay Chat(IRC):

- Internet Relay Chat is a service that allows users to communicate in real time by typing text in a special window.
- Like news, there are hundreds of IRC “Channels” each devoted to a subject or user group.
- You can use a special IRC program to participate in chat room discussion but many chat rooms are set up in web sites, ending visitors to chat directly in their window.

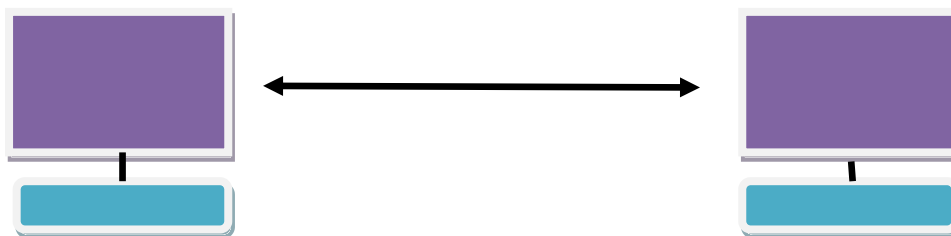
Q. Explain about Internet services?

Internet services allow us to access huge amount of information such as text, graphics, sound and software over the internet. Following are the internet services.

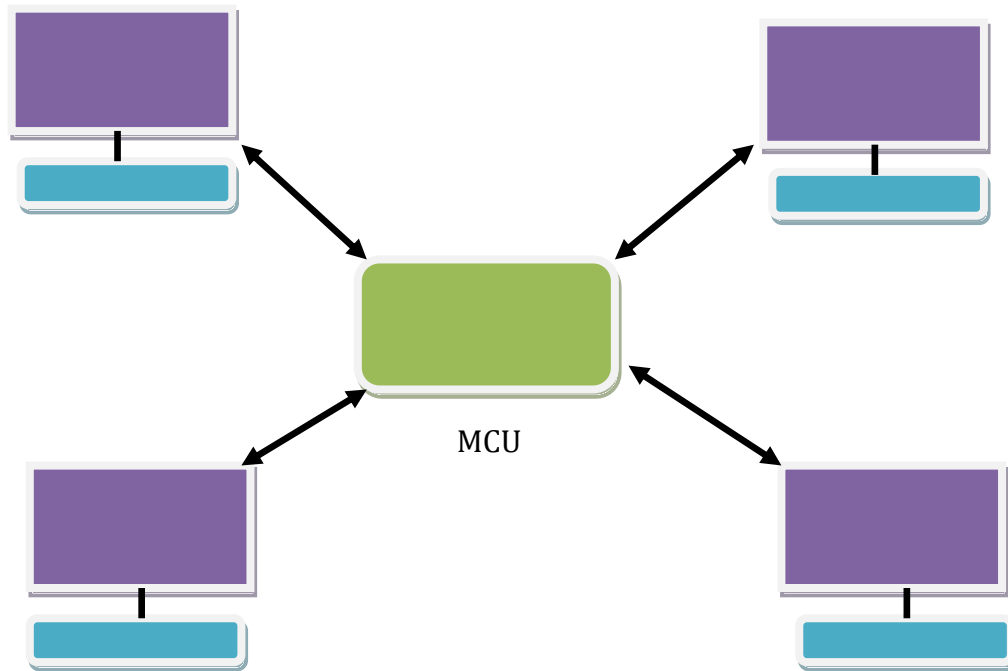
1. Communication Services.
2. Information Retrieval Services.
3. Web services.



1. **Communication Services:** There are various Communication Services available that offer exchange of information with individuals or groups. The following are the communication services.
 - a. **E-Mail:** Electronic Mail used to send electronic messages over the internet.
 - b. **Telnet:** Telnet is used to log on to a remote computer that is attached to internet.
 - c. **Newsgroups:** Offers a forum for people to discuss topics of common interests.
 - d. **IRC:** Allows the people from all over the world to communicate in real time.
 - e. **Mailing List:** Used to organize group of internet users to share common information through e-mail.
 - f. **Internet Telephony (VoIP):** Allows the internet users to talk across internet to any PC equipped to receive the call.
 - g. **Instant Messaging:** Offers real time chat between individuals and group of people. Eg: yahoo messenger, MNS messenger.
2. **Information Retrieval Services:** There exist several information retrieval services offering easy access to information present on the internet. The following are the information retrieval services.
 - a. **File Transfer Protocol:** enable the users to transfer files.
 - b. **Archie:** It's updated database of public FTP sites and their content. It helps to search a file by its name.
 - c. **Gopher:** Used to search, retrieve and display documents on remote sites.
 - d. **Very Easy Rodent Oriented Net wide Index to computer Achieved (VERONICAA):** is gopher based resource. It allows access to the information resource stored on gopher's servers.
3. **Web Services:** Web services allow exchange of information between application the web using web services, applications can easily interact with each other.
The web services are offered using concept of Utility Computing.
 - a. **WWW:** is also known as W3. It offers a way to access documents spread over the several servers over the internet. These documents may contain text, graphics, audio, video, hyperlinks. The hyperlinks allow the users to navigate between the documents.
 - b. **Video conferencing:** Video conferencing or video teleconferencing is a method of communicating by two-way video and audio transmission with help of telecommunication technologies.
 - c. **Modes of Video Conferencing:**
 - i) **Point-to point:** this mode of conferencing connects two locations only.



- ii) **Multi-point:** this mode of conferencing connects more than two locations through multi-point Control Unit.



Q. Explain about portal vs. website vs. communities?

Sometimes the terms “website” and “portal “ are used interchangeably and this usage isn’t entirely inaccurate but do you really know the difference between website vs portal?

- By definition, a website is a location on the internet that is unique and which is accessed via a web browser using a specific URL.
- Portals are also accessed via a web browser and specific URL, but content is login protected and user-specific.
- A resident portal is a web site, but a website is not necessarily a portal; it’s like the rhombus vs. square argument.

Website: A location on the internet, publicly accessible with a unique URL(web address).

- ❖ No login required.
- ❖ Anyone can see contents.
- ❖ Content does not change for different individuals.
- ❖ Can have interactive features, but does not reference personalized database.
- ❖ “Front-facing”, corporate site for marketing and web presence.

Portal: A private location on the internet, accessible with a unique URL(web address) and unique username and password.

- ❖ Personal login is required.
- ❖ Only portal members can see content.
- ❖ Content is unique to user based on linked account information and group members setting/permissions.
- ❖ Secure access point for personalized information.
- ❖ Communication features with other portal members or groups.
- ❖ Interactive functionality for portal site members.
- ❖ “back-end” site for designated set of users.
- ❖ Educate portal site members about association information and provide association content, such as governing documents in a self-serve environment.

Online Community vs. Portal:

- ❖ In many ways, portals were early aversions of online communities-just with more limitations.
- ❖ For instance, a traditional business portal is generally “one-size-fits-all” while an online communities has the ability to create a more personalized experience for members.
- ❖ Portals are also designed to have a top-down communication structure with most of the knowledge exchange coming from communication teams and formal experts.
- ❖ In contrast, online communities bring together many different voices including customers, experts, and advocates.
- ❖ Portals are still evolving and new “community portals or “community engagement portals” fix many of these communication limitations.
- ❖ These new options blur distinction between portals and online communities, so when yours comparing choices, focus on the capabilities of each platform, rather than getting caught up in terminology.