# Unit-III

Internet

Internet is defined as an Information super Highway, to access information over the web. However, It can be defined in many ways as follows:

- Internet is a world-wide global system of interconnected computer networks.

- Internet uses the standard Internet Protocol (TCP/IP).

- Every computer in internet is identified by a unique IP address.

- IP Address is a unique set of numbers (such as 110.22.33.114) which identifies a computer location.

- A special computer DNS (Domain Name Server) is used to give name to the IP Address so that user can locate a computer by a name.

- For example, a DNS server will resolve a name **http://www.Allenhouse** **colleges.com** to a particular IP address to uniquely identify the computer on which this website is hosted.

- Internet is accessible to every user all over the world.
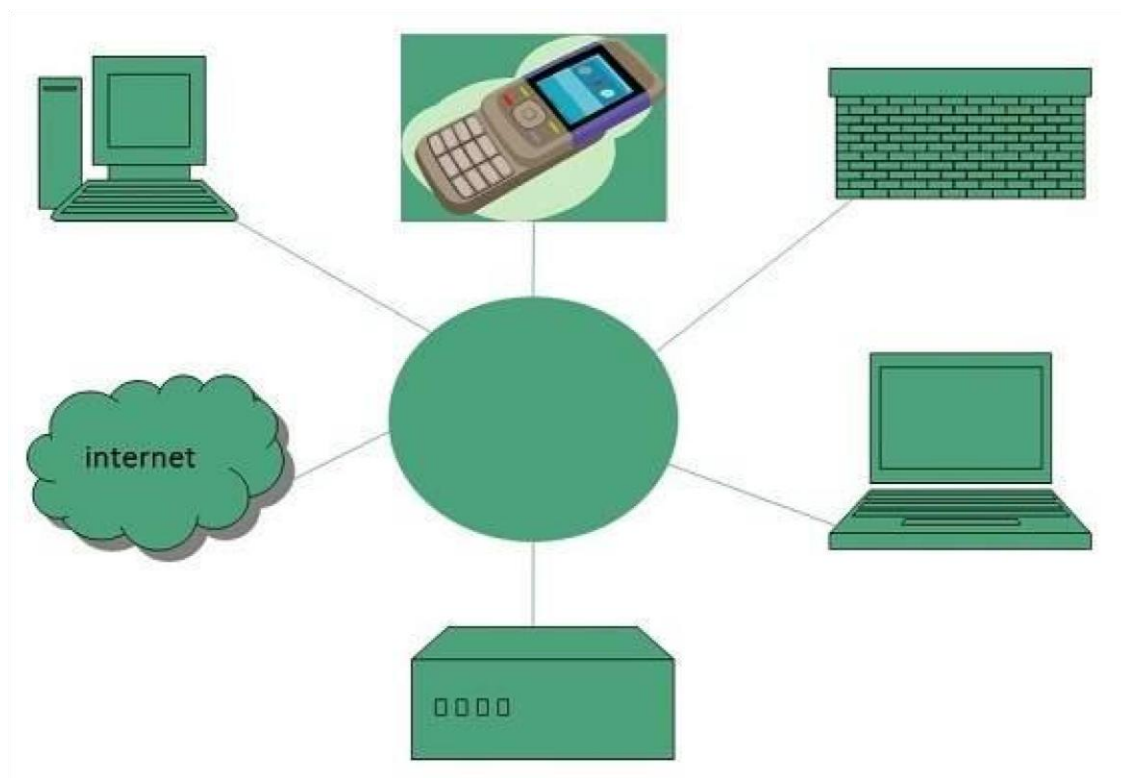
Evolution

The concept of Internet was originated in 1969 and has undergone several technological & Infrastructural changes as discussed below:

- The origin of Internet devised from the concept of **Advanced Research Project Agency Network (ARPANET).**
- **ARPANET** was developed by United States Department of Defense.
- Initially, there were only four nodes, formally called **Hosts.**
- In 1972, the **ARPANET** spread over the globe with 23 nodes located at different countries and thus became known as **Internet.**
- By the time, with invention of new technologies such as TCP/IP protocols, DNS, WWW, browsers, scripting languages etc.,Internet provided a medium to publish and access information over the web.

Advantages

Internet covers almost every aspect of life, one can think of. Here, we will discuss some of the advantages of Internet:
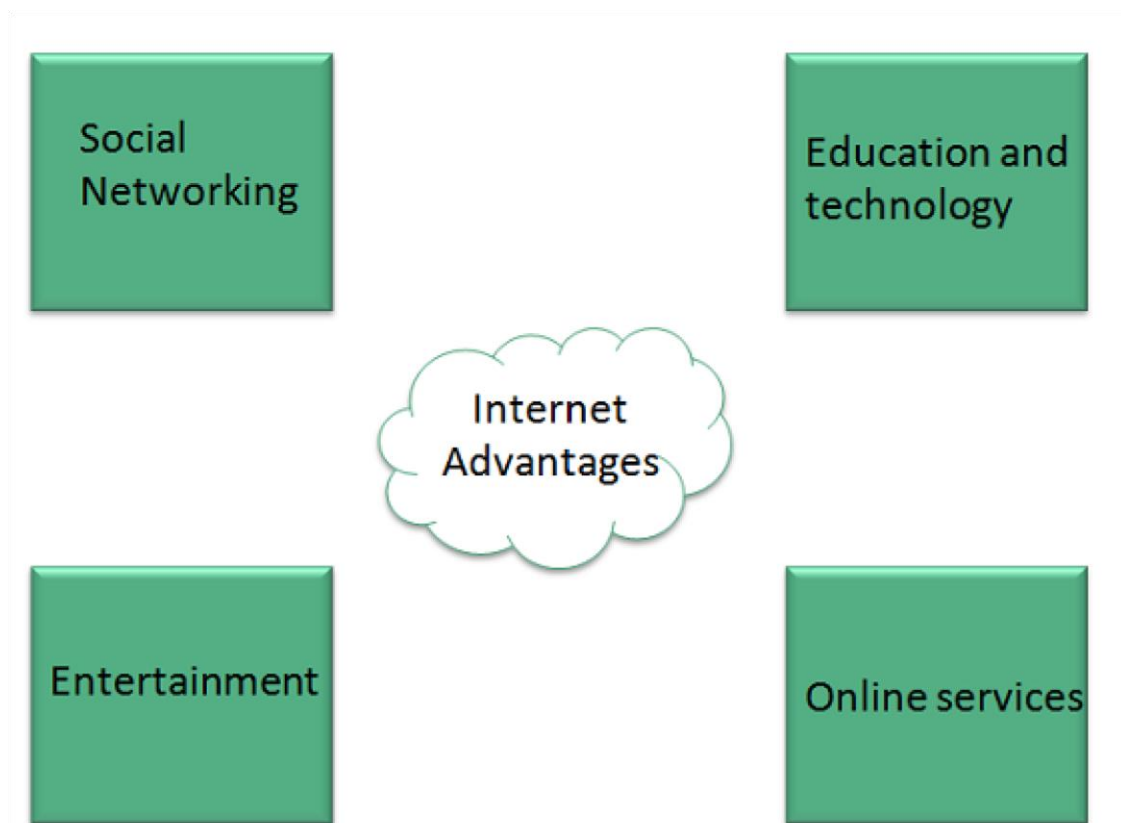

- Internet allows us to communicate with the people sitting at remote locations. There are various apps available on the wed that uses Internet as a medium for communication. One can find various social networking sites such as:

    o Facebook o Twitter o

    Yahoo o Google+ o Flickr

    o Orkut

- One can surf for any kind of information over the internet. Information regarding various topics such as Technology, Health & Science, Social Studies, Geographical Information, Information Technology, Products etc can be surfed with help of a search engine.

- Apart from communication and source of information, internet also serves a medium for entertainment. Following are the various modes for entertainment over internet.

  - Online Television o
  Online Games o Songs o
  Videos   o   Social
  Networking Apps

- Internet allows us to use many services like:

  - Internet   Banking   o
  Matrimonial   Services   o
  Online Shopping o Online
  Ticket Booking o Online
  Bill   Payment   o   Data
  Sharing o E-mail

- Internet provides concept of **electronic commerce**, that allows the business deals to be conducted on electronic systems

Disadvantages

However, Internet has prooved to be a powerful source of information in almost every field, yet there exists many disadvanatges discussed below:
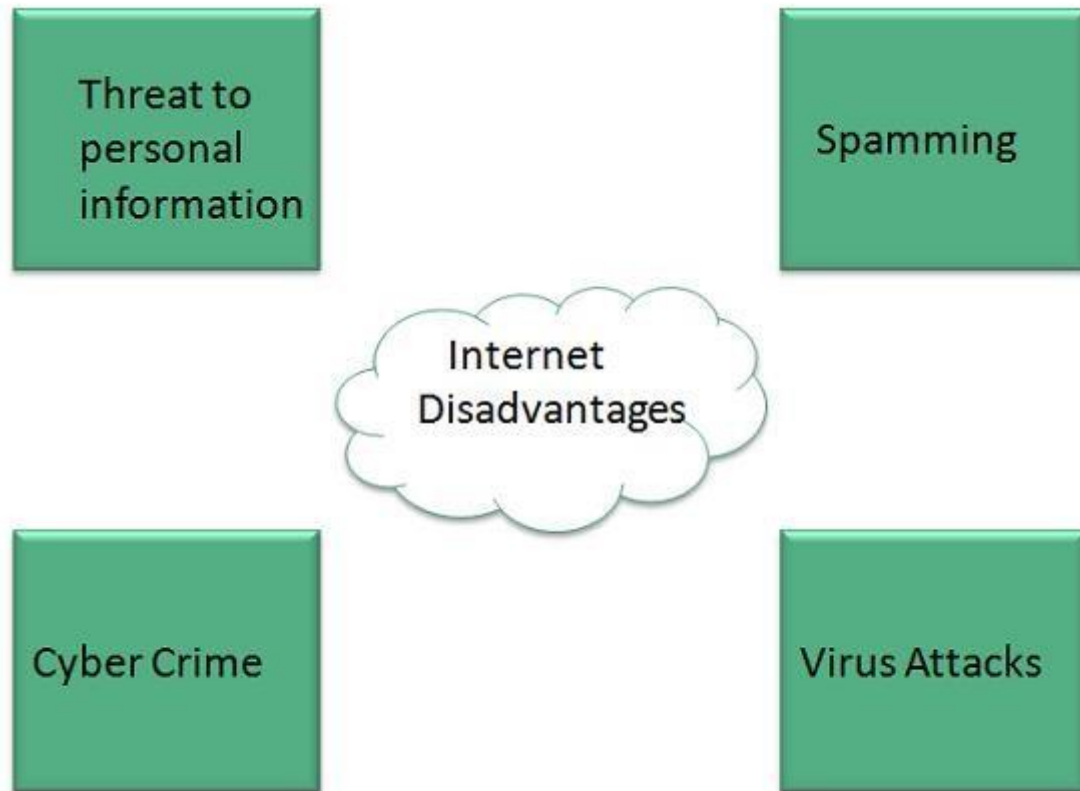
- There are always chances to loose personal information such as name, address, credit card number. Therefore, one should be very careful while sharing such information. One should use credit cards only through authenticated sites.

- Another disadvantage is the Spamming.Spamming corresponds to the unwanted e-mails in bulk. These e-mails serve no purpose and lead to obstruction of entire system.

- Virus can easily be spread to the computers connected to internet. Such virus attacks may cause your system to crash or your important data may get deleted.

- There are various websites that do not provide the authenticated information. This leads to misconception among many people.

Intranet

Intranet is defined as private network of computers within an organization with its own server and firewall. Moreover we can define Intranet as:

- Intranet is system in which multiple PCs are networked to be connected to each other. PCs in intranet are not available to the world outside of the intranet.

- Usually each company or organization has their own Intranet network and members/employees of that company can access the computers in their intranet.

- Every computer in internet is identified by a unique IP address.

- Each computer in Intranet is also identified by a IP Address, which is unique among the computers in that Intranet.
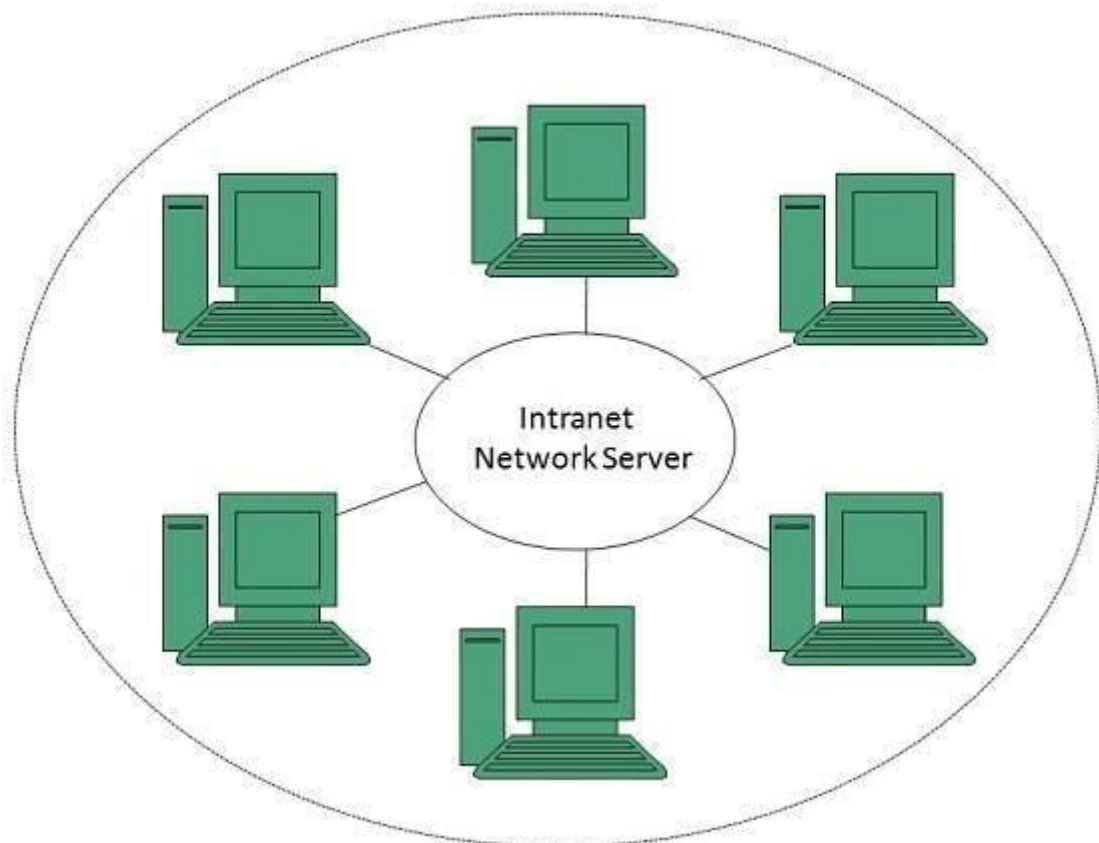
<mark>Benefits</mark>

Intranet is very efficient and reliable network system for any organization. It is beneficial in every aspect such as collaboration, cost-effectiveness, security, productivity and much more.

Intranet Advantages
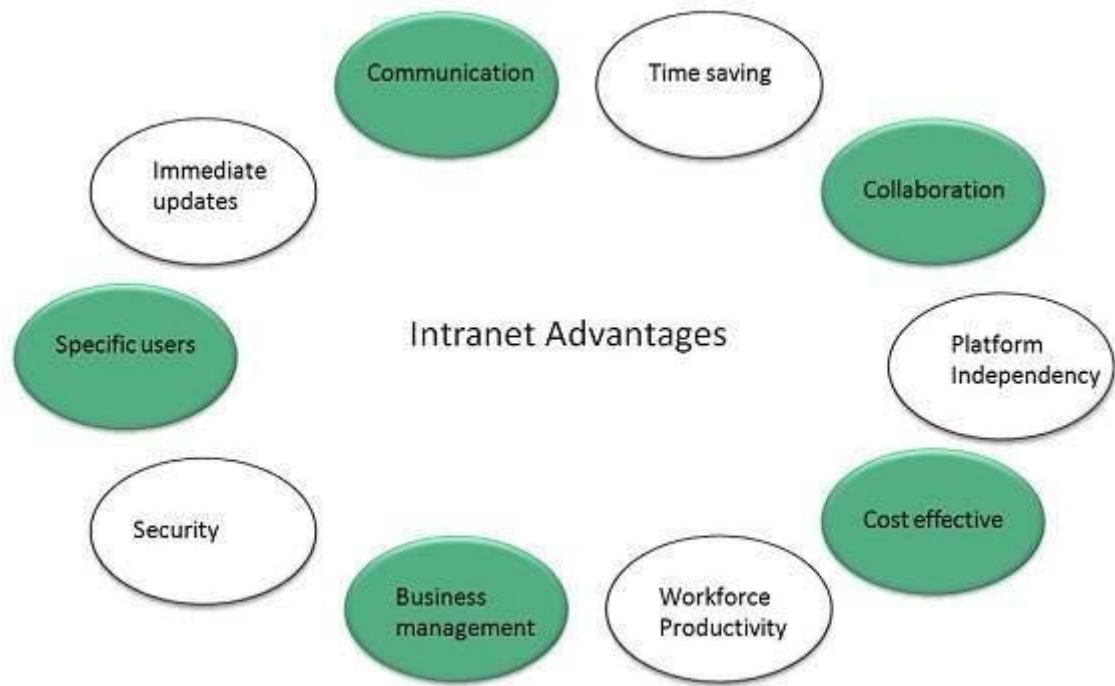
Communication

Intranet offers easy and cheap communication within an organization. Employees can communicate using chat, e-mail or blogs.

Time Saving

Information on Intranet is shared in real time.

Collaboration

Information is distributed among the employees as according to requirement and it can be accessed by the authorized users, resulting in enhanced teamwork.

Platform Independency

Intranet can connect computers and other devices with different architecture.

Cost Effective

Employees can see the data and other documents using browser rather than printing them and distributing duplicate copies among the employees, which certainly decreases the cost.

Workforce Productivity

Data is available at every time and can be accessed using company workstation. This helps the employees work faster.

Business Management

It is also possible to deploy applications that support business operations.

Security

Since information shared on intranet can only be accessed within an organization, therefore there is almost no chance of being theft.
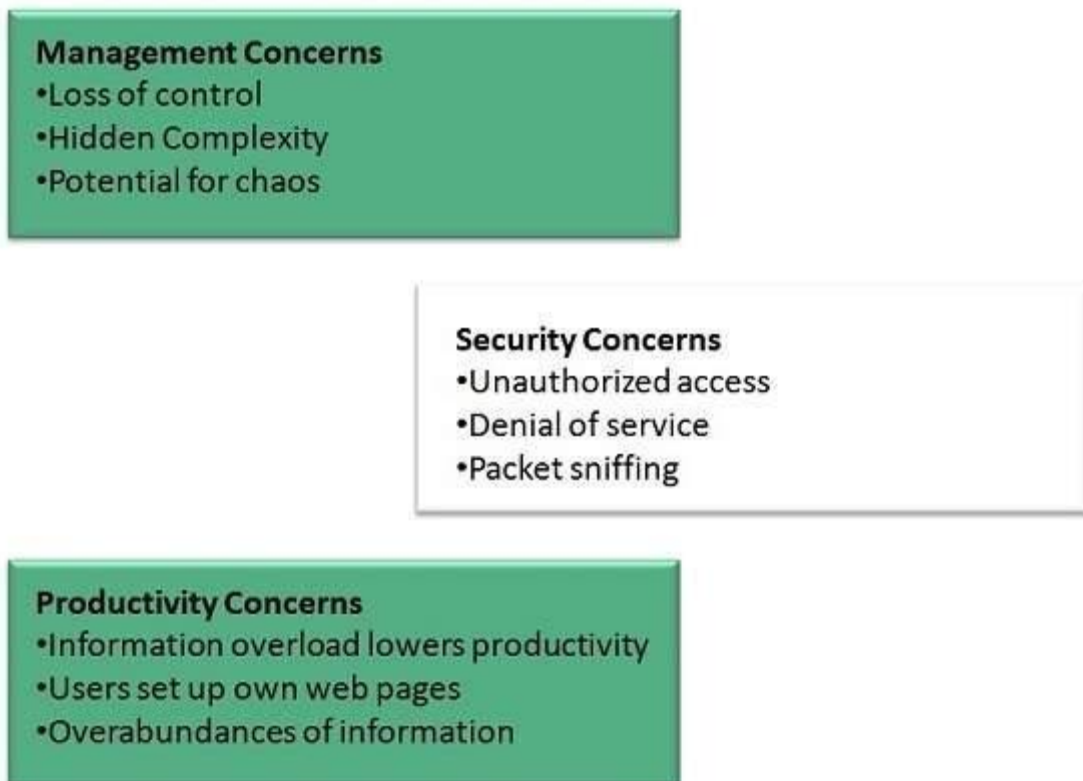
Specific Users

Intranet targets only specific users within an organization therefore, once can exactly know whom he is interacting.

Immediate Updates

Any changes made to information are reflected immediately to all the users.

Issues

Apart from several benefits of Intranet, there also exist some issues.. These issues are shown in the following diagram:

Management Concerns
- Loss of control
- Hidden Complexity
- Potential for chaos

Security Concerns
- Unauthorized access
- Denial of service
- Packet sniffing

Productivity Concerns
- Information overload lowers productivity
- Users set up own web pages
- Overabundances of information

Applications

Intranet applications are same as that of Internet applications. Intranet applications are also accessed through a web browser. The only difference is that, Intranet applications reside on local server while Internet applications reside on remote server. Here, we've discussed some of these applications:
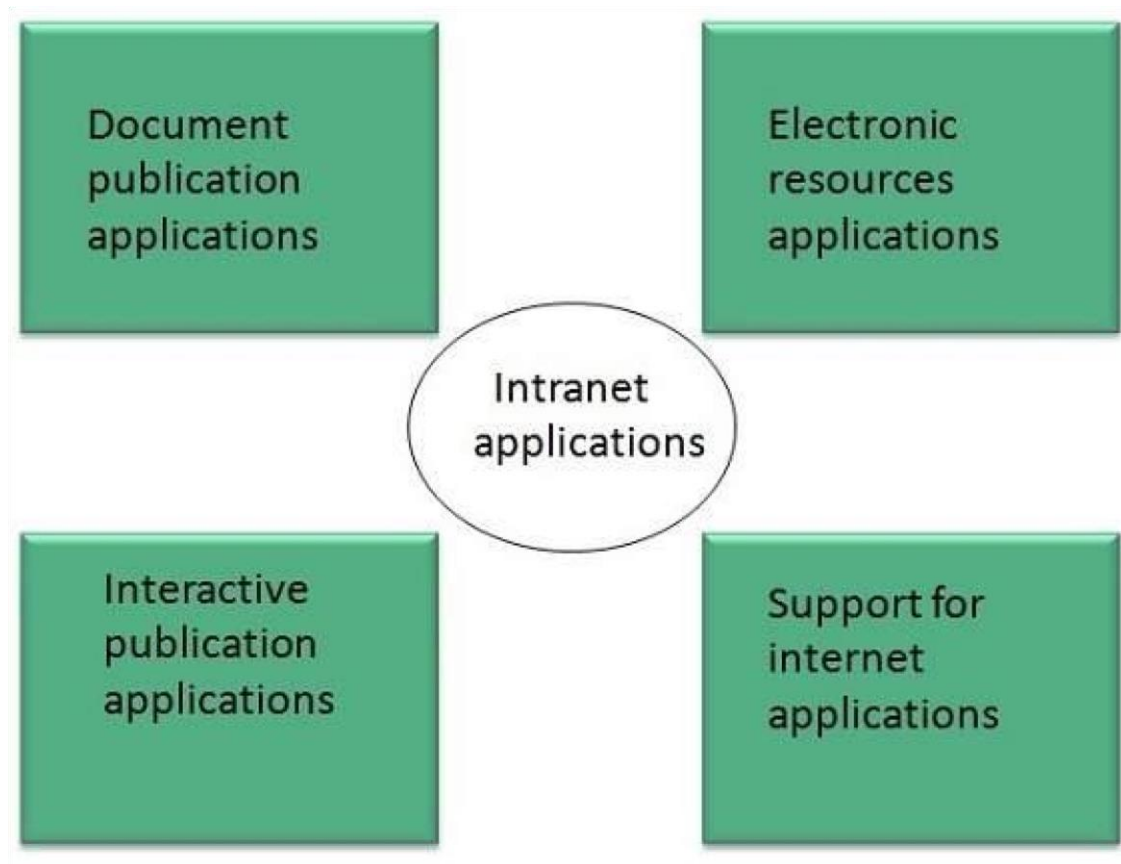
Document publication applications

Document publication applications allow publishing documents such as manuals, software guide, employee profits etc without use of paper.

Electronic resources applications

It offers electronic resources such as software applications, templates and tools, to be shared across the network.

Interactive Communication applications

Like on internet, we have e-mail and chat like applications for Intranet, hence offering an interactive communication among employees.

Support for Internet Applications

Intranet offers an environment to deploy and test applications before placing them on Internet.

Extranet

Extranet refers to network within an organization, using internet to connect to the outsiders in controlled manner. It helps to connect businesses with their customers and suppliers and therefore allows working in a collaborative manner.
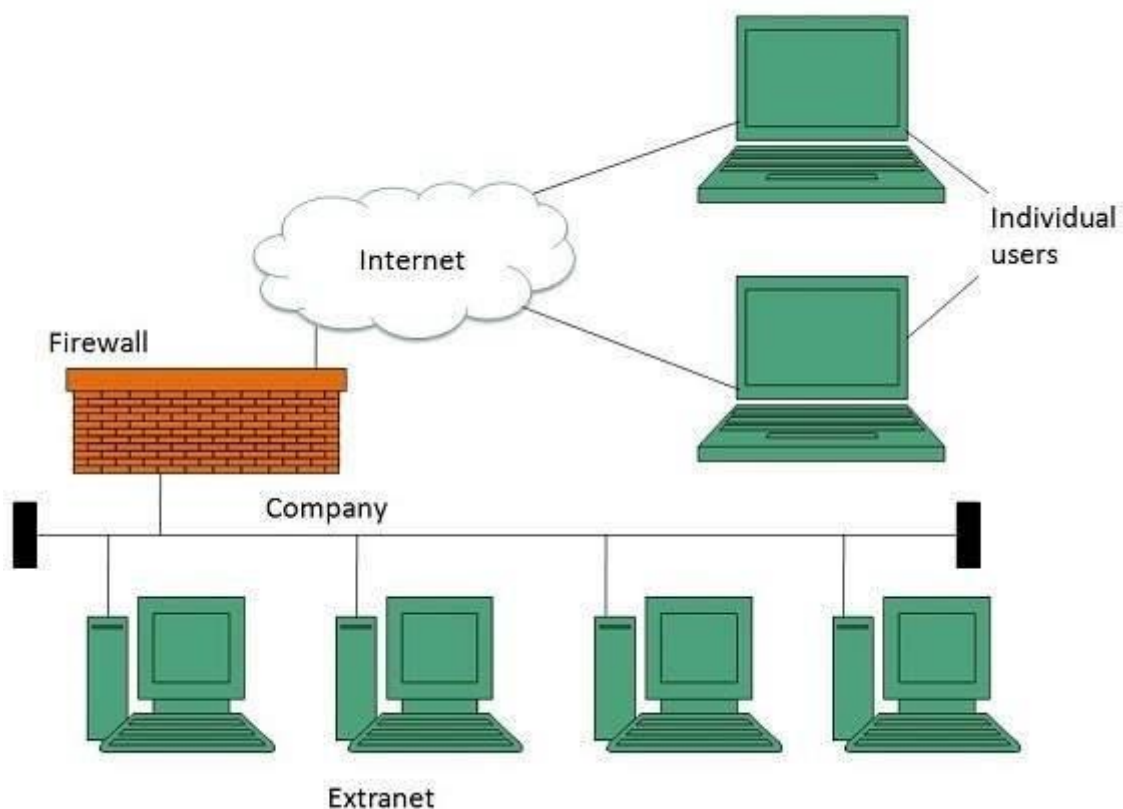
Implementation

Extranet is implemented as a Virtual Private Networks (VPN) because it uses internet to connect to corporate organization and there is always a threat to information security. VPN offers a secure network in public infrastructure (Internet).

A VPN Implementation
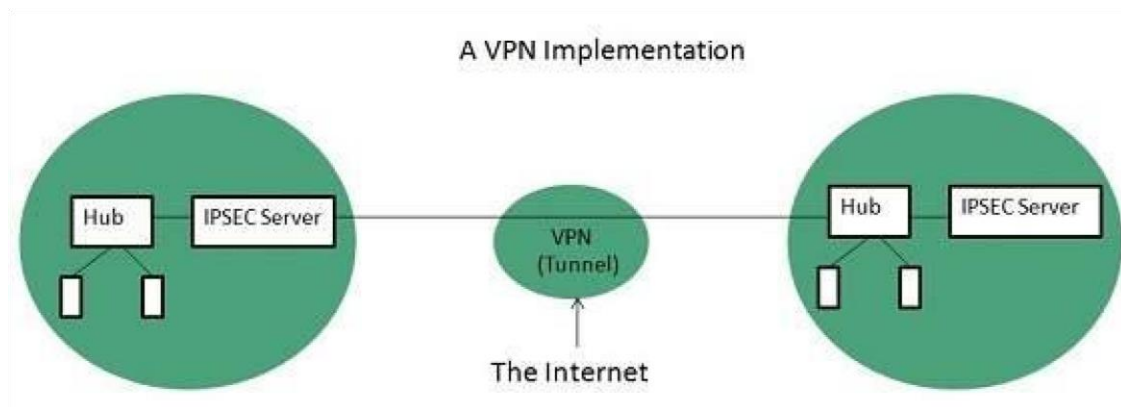
Key Points

- The packet is encapsulated at boundary of networks in IPSEC complaint routers.

- It uses an encryption key to encapsulate packets and IP addresses as well.

- The packet is decoded only by the IPSEC complaint routers or servers.

- The message is sent over VPN via VPN Tunnel and this process is known as tunneling.

VPN uses **Internet Protocol Security Architecture (IPSEC)** Protocol to provide secure transactions by adding an additional security layer to TCP/IP protocol. This layer is created by encapsulating the IP packet to a new IP packet as shown in the following diagram:
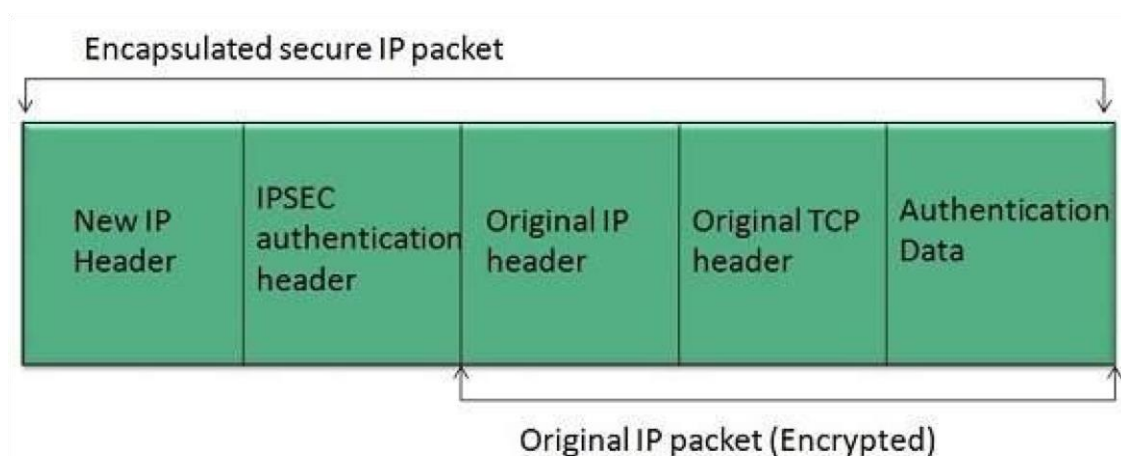
Benefits

Extranet proves to be a successful model for all kind of businesses whether small or big. Here are some of the advantages of extranet for employees, suppliers, business partners, and customers:

Issues

Apart for advantages there are also some issues associated with extranet. These issues are discussed below: ==Hosting==
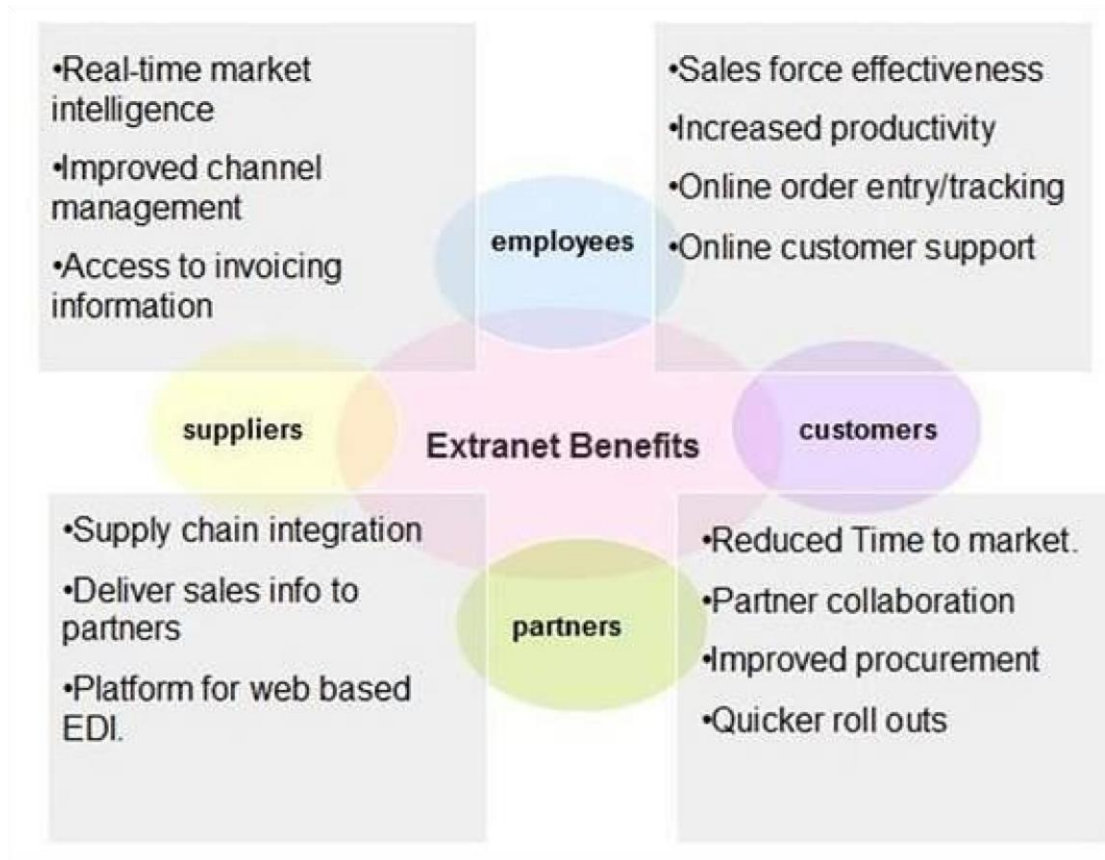
Where the extranet pages will be held i.e. who will host the extranet pages. In this context there are two choices:

- Host it on your own server.
- Host it with an Internet Service Provider (ISP) in the same way as web pages.

But hosting extranet pages on your own server requires high bandwidth internet connection which is very costly. Security

Additional firewall security is required if you host extranet pages on your own server which result in a complex security mechanism and increase work load.

Accessing Issues

Information can not be accessed without internet connection. However, information can be accessed in Intranet without internet connection. Decreased Interaction

It decreases the face to face interaction in the business which results in lack of communication among customers, business partners and suppliers.

Extranet vs. Intranet

The following table shows differences between Extranet and Intranet:

Extranet	Intranet
Internal network that can be accessed externally.	Internal network that cannot be accessed externally.
Extranet is extension of company's Intranet.	Only limited users of a company.
For limited external communication between customers, suppliers and business partners.	Only for communication within a company.

Reference Model

Reference Model offers a means of standardization which is acceptable worldwide. Since people using the computer network are located over a wide physical range and their network devices might have heterogeneous architecture. In order to provide communication among heterogeneous devices, we need a standardized model i.e. a reference model, which would provide us way how these devices can communicate regardless their architecture.

We have two reference models such as **OSI** model and **TCP/IP** reference model, however, the OSI model is a hypothetical one but the TCP/IP is absolutely practical model.

OSI Model

OSI is acronym of Open System Interface. This model is developed by the International organization of Standardization (ISO) and therefore also referred as ISO-OSI Model.

The OSI model consists of seven layers as shown in the following diagram. Each layer has a specific function, however each layer provide services to the layer above.
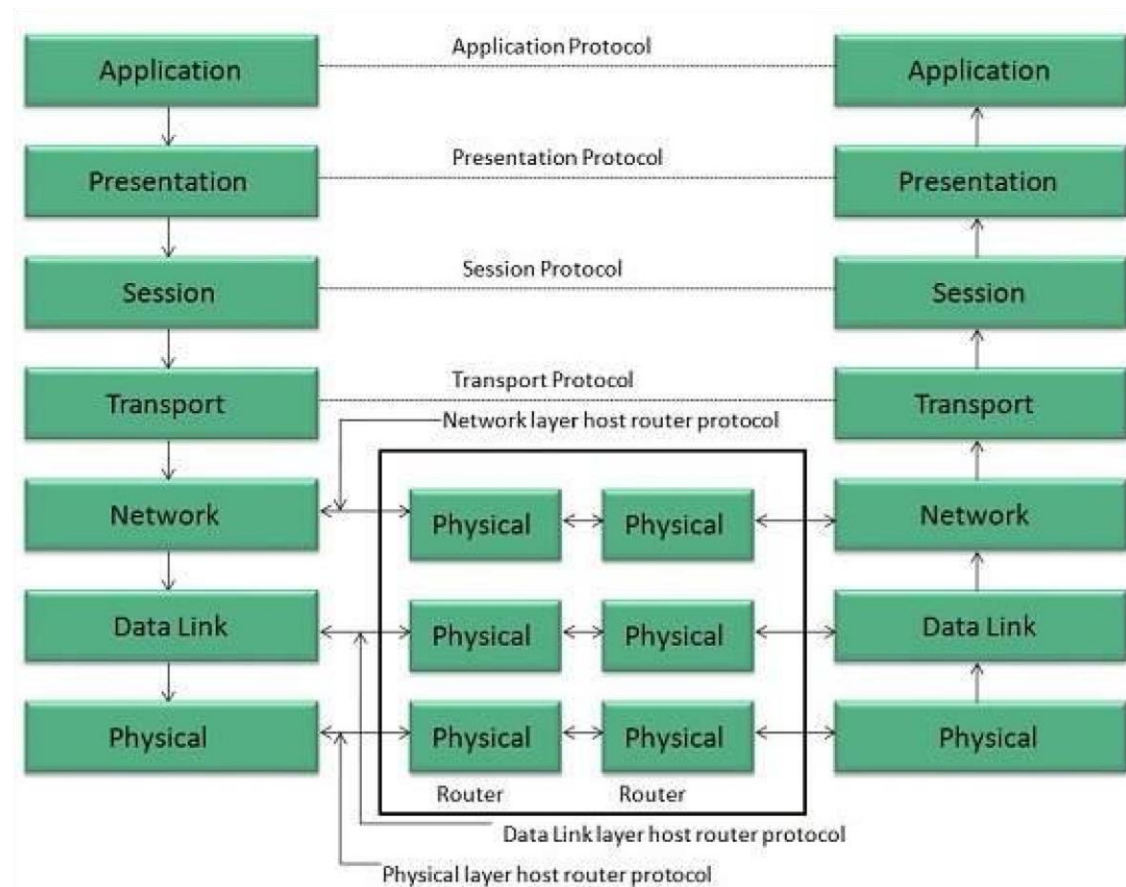
Physical Layer

The Physical layer is responsible for the following activities:

- Activating, maintaining and deactivating the physical connection.
- Defining voltages and data rates needed for transmission.
- Converting digital bits into electrical signal.
- Deciding whether the connection is simplex, half duplex or full duplex.

Data Link Layer

The data link layer performs the following functions:

- Performs synchronization and error control for the information which is to be transmitted over the physical link.
- Enables error detection, and adds error detection bits to the data which are to be transmitted.

Network Layer

Following are the functions of Network Layer:

- To route the signals through various channels to the other end.
- To act as the network controller by deciding which route data should take.
- To divide the outgoing messages into packets and to assemble incoming packets into messages for higher levels.

Transport Layer

The Transport layer performs the following functions:

- It decides if the data transmission should take place on parallel paths or single path.

- It performs multiplexing, splitting on the data.

- It breaks the data groups into smaller units so that they are handled more efficiently by the network layer.

The Transport Layer guarantees transmission of data from one end to other end.

Session Layer

The Session layer performs the following functions:

- Manages the messages and synchronizes conversations between two different applications.

- It controls logging on and off, user identification, billing and session management.

Presentation Layer

The Presentation layer performs the following functions:

- This layer makes it sure that the information is delivered in such a form that the receiving system will understand and use it.

Application Layer

The Application layer performs the following functions:

- It provides different services such as manipulation of information in several ways, retransferring the files of information, distributing the results etc.

- The functions such as LOGIN or password checking are also performed by the application layer.

TCP/IP Model

TCP/IP model is practical model and is used in the Internet. TCP/IP is acronym of Transmission Control Protocol and Internet Protocol.

The **TCP/IP** model combines the two layers (Physical and Data link layer) into one layer i.e. **Host-to-Network** layer. The following diagram shows the various layers of TCP/IP model:

TCP/IP Model

Application
Transport
Internet
Host to network

Application Layer

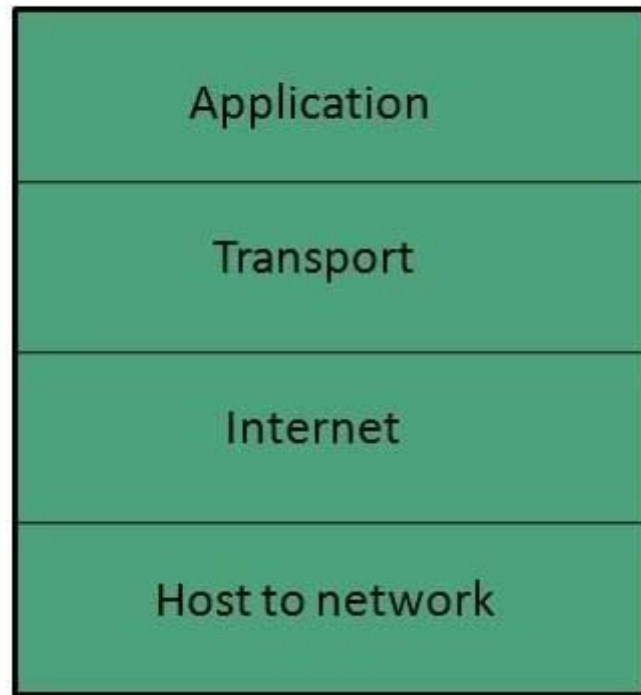This layer is same as that of the OSI model and performs the following functions:

- It provides different services such as manipulation of information in several ways, retransferring the files of information, distributing the results etc.

- The functions such as LOGIN or password checking are also performed by the application layer.

Protocols used: TELNET, FTP, SMTP, DN, HTTP, NNTP are the protocols employed in this layer.

Transport Layer

It does the same functions as that of transport layer in OSI model. Here are the key points regarding transport layer:

- It uses **TCP** and **UDP** protocol for end to end transmission.

- TCP is reliable and **connection oriented protocol.**

- TCP also handles flow control.

- The UDP is not reliable and a **connection less protocol** also does not perform flow control.

Protocols used: TCP/IP and **UDP** protocols are employed in this layer.

Internet Layer

The function of this layer is to allow the host to insert packets into network and then make them travel independently to the destination. However, the order of receiving the packet can be different from the sequence they were sent.

Protocols used: Internet Protocol (IP) is employed in Internet layer.

Host-to-Network Layer

This is the lowest layer in TCP/IP model. The host has to connect to network using some protocol, so that it can send IP packets over it. This protocol varies from host to host and network to network.

Protocols used: ARPANET, SATNET, LAN, packet radio are the protocols which are used in this layer.

Internet Service Providers (ISP)

Internet Service Provider (ISP) is a company offering access to internet. They offer various services:

- Internet Access
- Domain name registration
- Dial-up access
- Leased line access

ISP Types

ISPs can broadly be classified into six categories as shown in the following diagram:
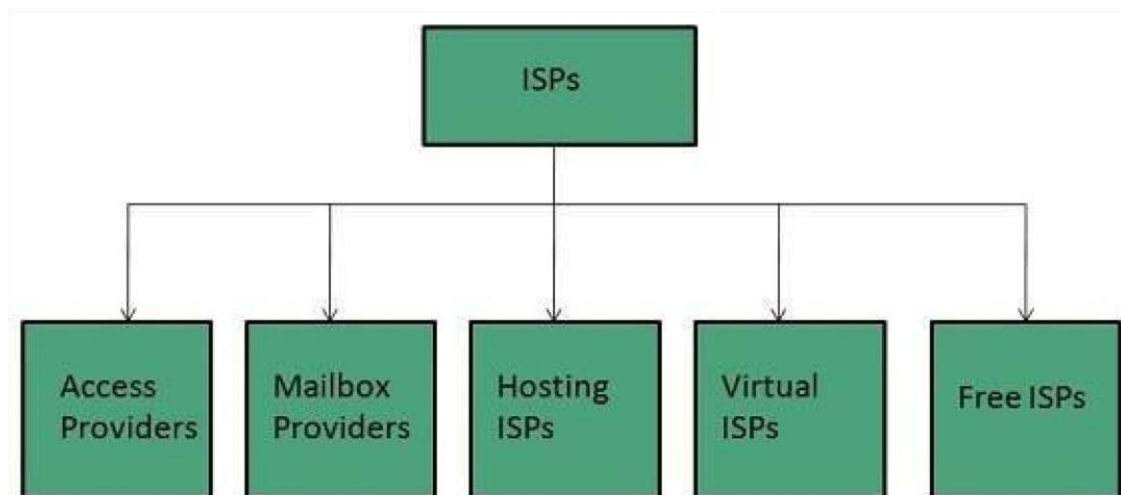
Access providers

They provide access to internet through telephone lines, cable wi-fi or fiber optics.

Mailbox Provider

Such providers offer mailbox hosting services.

Hosting ISPs

Hosting ISPs offers e-mail, and other web hosting services such as virtual machines, clouds etc.

Virtual ISPs

Such ISPs offer internet access via other ISP services.

Free ISPs

Free ISPs do not charge for internet services.

Connection Types

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

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:
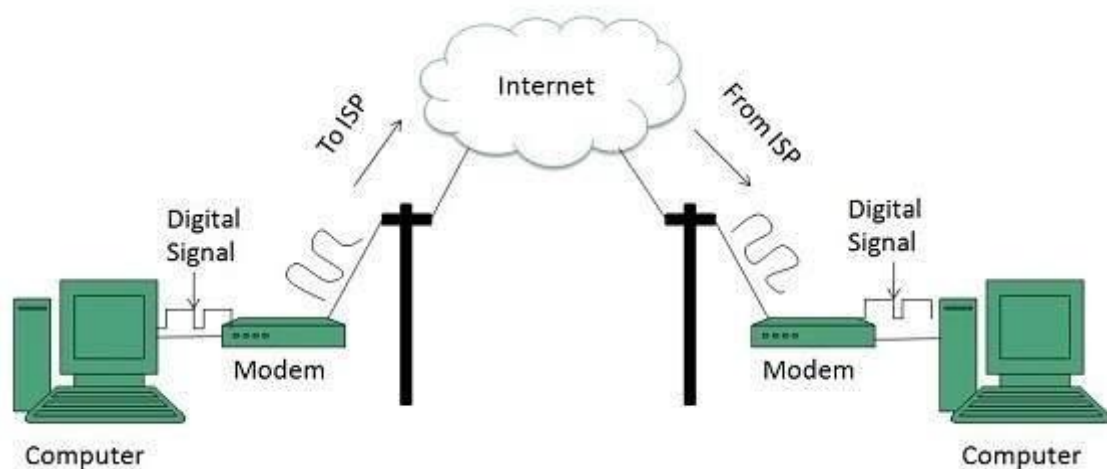
ISDN

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:
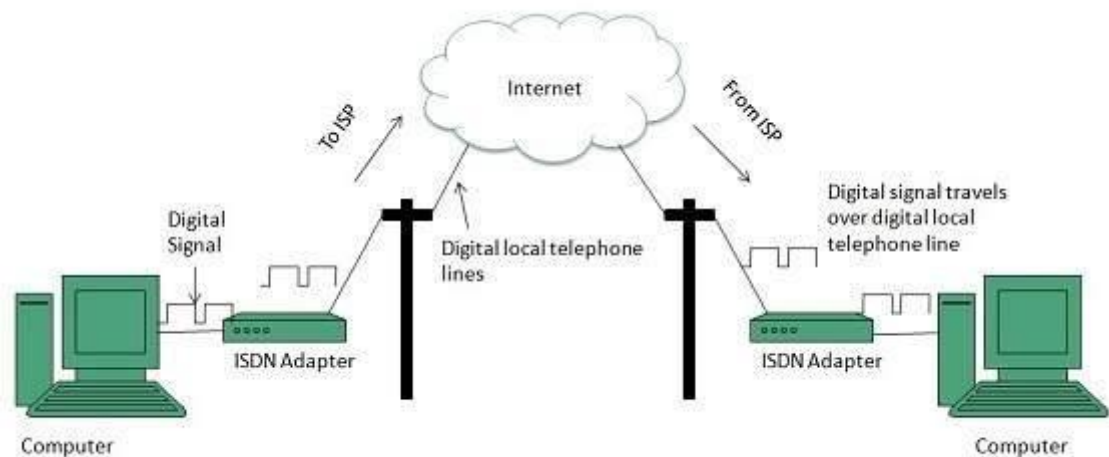
DSL

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.

18

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

Internet Access Using DSL Modem
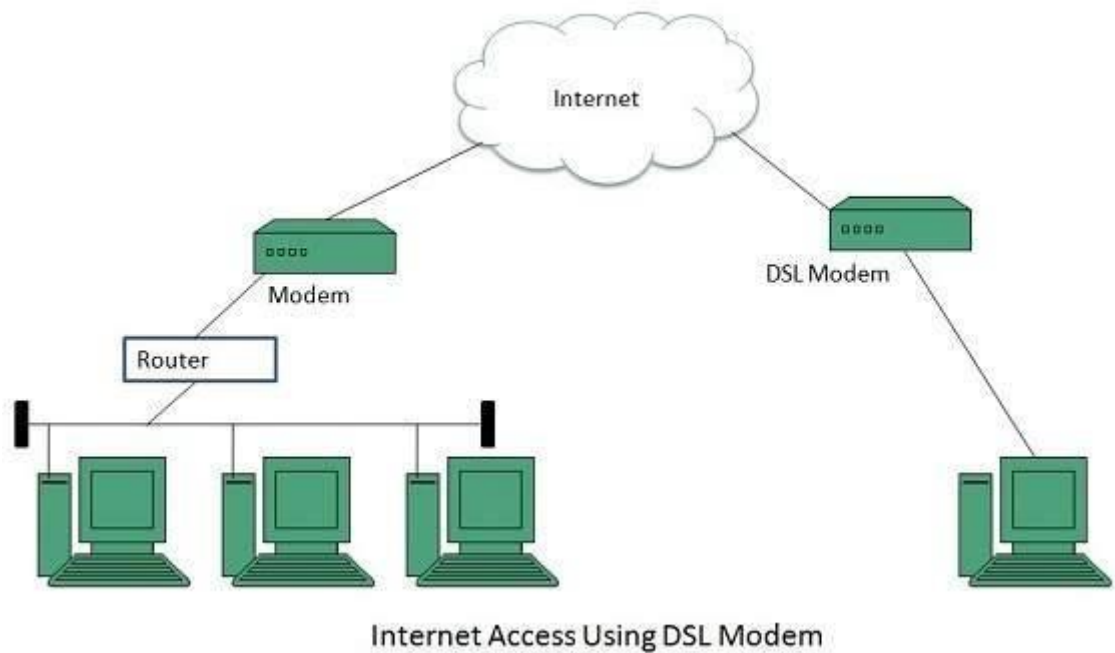
Cable TV Internet Connection

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:
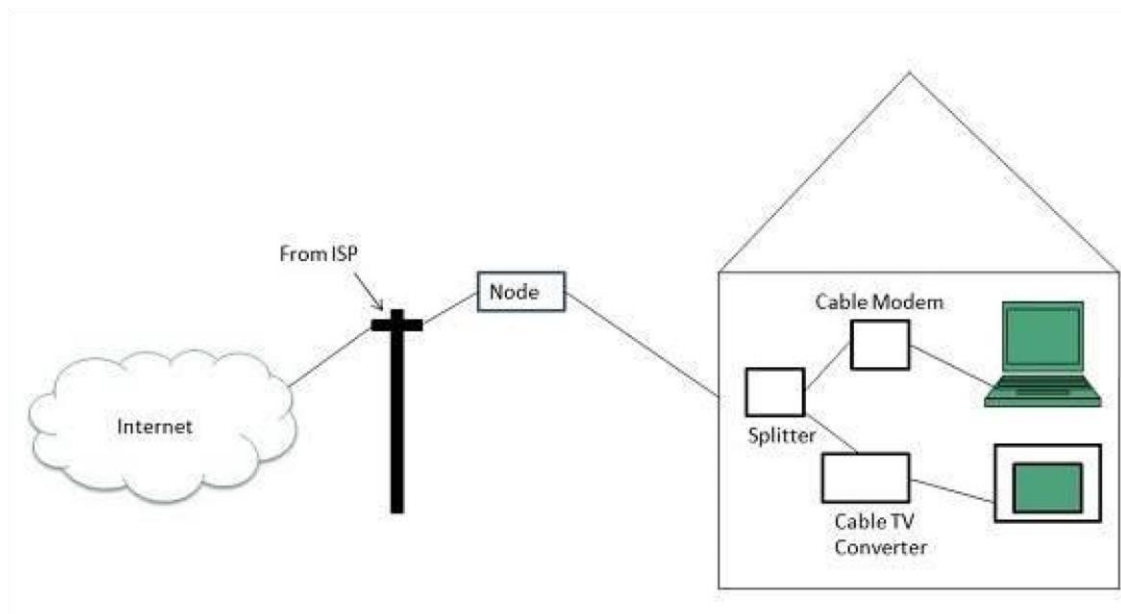
Satellite Internet Connection

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:
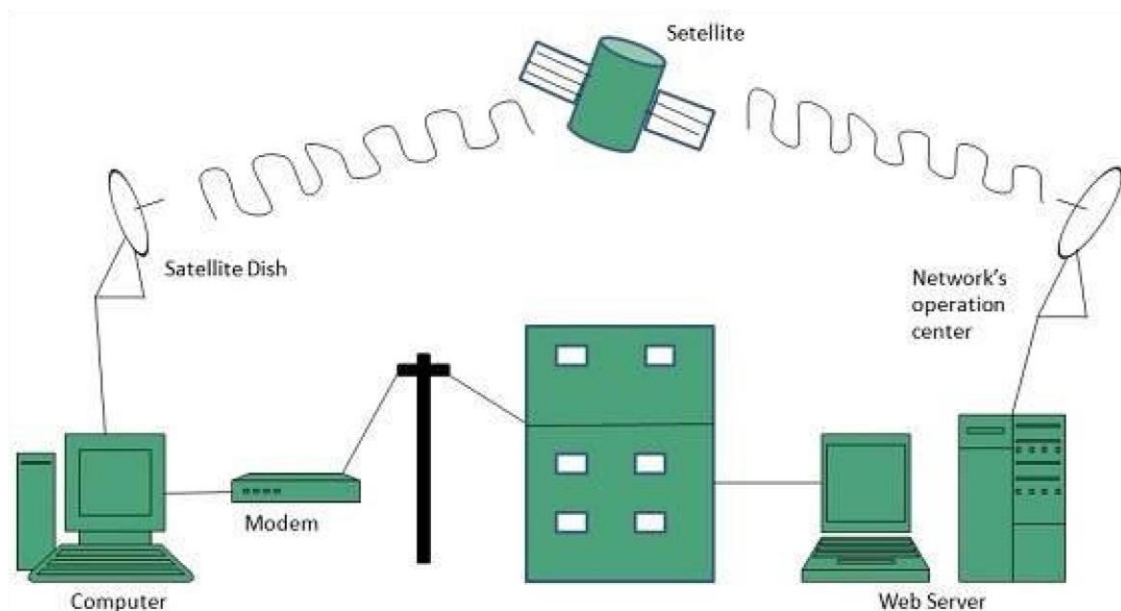
Wireless Internet Connection

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.

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:

  - o Stream Data Transfer. o

    Reliability.

  - o Efficient Flow Control o

    Full-duplex operation.

  - o 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:

- Stream Delivery Service

- Sending and Receiving Buffers

- Bytes and Segments

- Full Duplex Service

- Connection Oriented Service

- 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.

Reliable Service

For sake of reliability, TCP uses acknowledgement mechanism.

Internet Protocol (IP)

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

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

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

4	8		16	32 bits

VER	HLEN	D.S. type of service	Total length of 16 bits	
Identification of 16 bits			Flags 3 bits	Fragmentation Offset (13 bits)
Time to live		Protocol	Header checksum (16 bits)	
Source IP address				
Destination IP address				
Option + Padding				
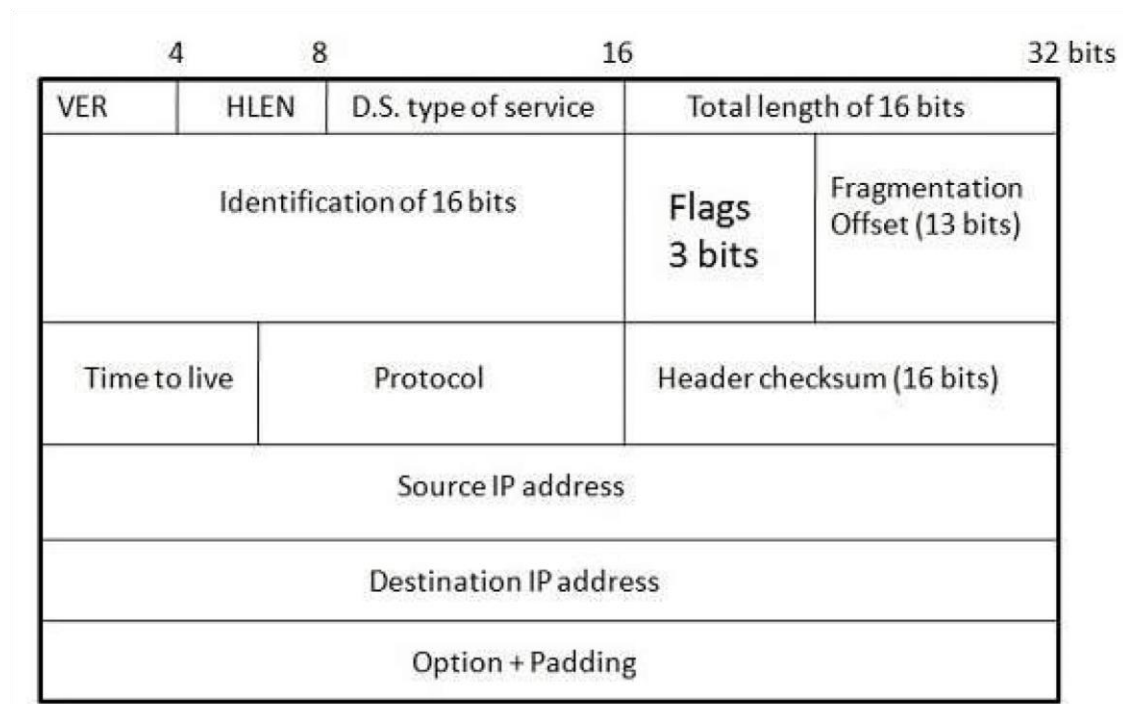
Points to remember:

- The length of datagram is variable.
- The Datagram is divided into two parts: **header** and **data.**
- The length of header is 20 to 60 bytes.
- The header contains information for routing and delivery of the packet.

User Datagram Protocol (UDP)

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

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

Source Port	Destination Port
Length	UDP checksum
Data	
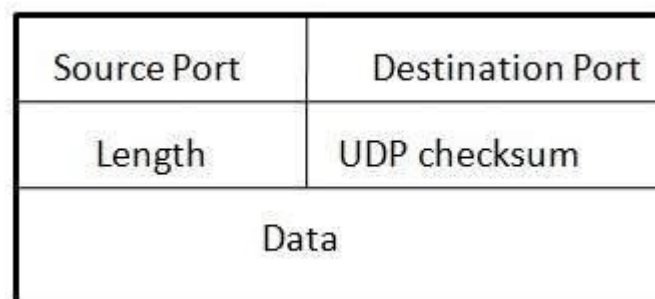
Points to remember:

- UDP is used by the application that typically transmit small amount of data at one time.

- UDP provides protocol port used i.e. UDP message contains both source and destination port number, that makes it possible for UDP software at the destination to deliver the message to correct application program.

File Transfer Protocol (FTP)

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

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

- FTP establishes two different connections: one is for data transfer and other is for control information.

- **Control connection** is made between **control processes** while **Data Connection** is made between<="" b="">

- FTP uses **port 21** for the control connection and **Port 20** for the data connection.
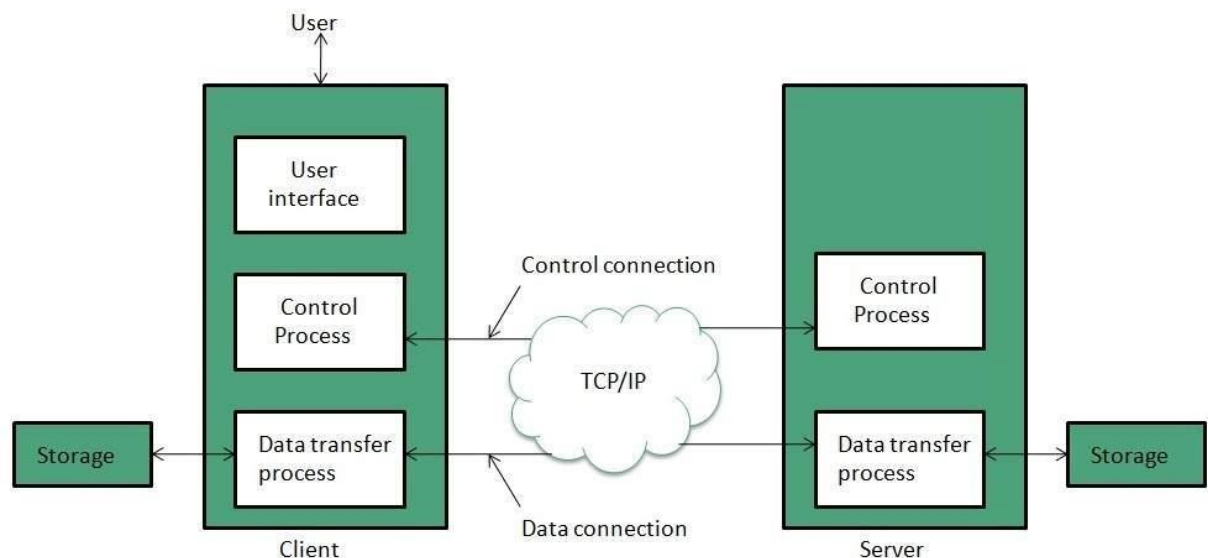
Trivial File Transfer Protocol (TFTP)

Trivial File Transfer Protocol is also used to transfer the files but it transfers the files without authentication. Unlike FTP, TFTP does not separate control and data information. Since there is no authentication exists, TFTP lacks in security features therefore it is not recommended to use TFTP.

Key points

- TFTP makes use of UDP for data transport. Each TFTP message is carried in separate UDP datagram.

- The first two bytes of a TFTP message specify the type of message.

- The TFTP session is initiated when a TFTP client sends a request to upload or download a file.

- The request is sent from an ephemeral UDP port to the **UDP port 69** of an TFTP server.

Difference between FTP and TFTP

S.N.	Parameter	FTP	TFTP
1	Operation	Transferring Files	Transferring Files
2	Authentication	Yes	No
3	Protocol	TCP	UDP
4	Ports	21 – Control, 20 – Data	Port 3214, 69, 4012
5	Control and Data	Separated	Separated
6	Data Transfer	Reliable	Unreliable

Telnet

Telnet is a protocol used to log in to remote computer on the internet. There are a number of Telnet clients having user friendly user interface. The following diagram shows a person is logged in to computer A, and from there, he remote logged into computer B.
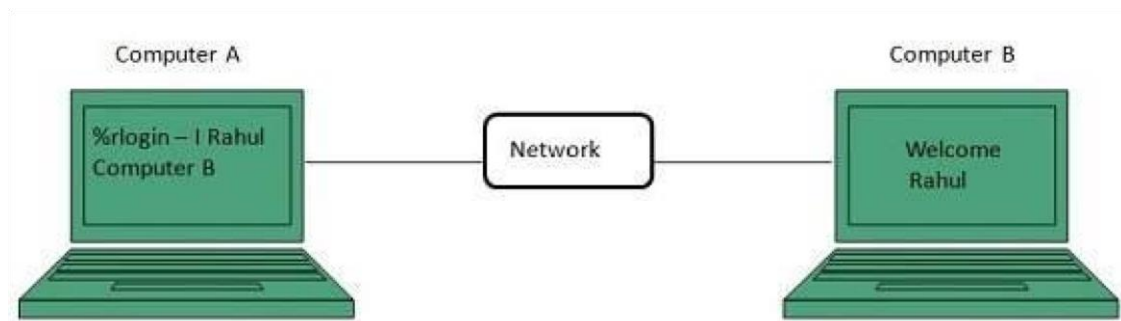
Hyper Text Transfer Protocol (HTTP)

HTTP is a communication protocol. It defines mechanism for communication between browser and the web server. It is also called request and response protocol because the communication between browser and server takes place in request and response pairs.

HTTP Request

HTTP request comprises of lines which contains:

- Request line

- Header Fields

- Message body

Key Points

- The first line i.e. the **Request line** specifies the request method i.e. **Get** or **Post.**

- The second line specifies the header which indicates the domain name of the server from where index.htm is retrieved.

HTTP Response

Like HTTP request, HTTP response also has certain structure. HTTP response contains:

- Status line

- Headers

- Message body

Email

Email is a service which allows us to send the message in electronic mode over the internet. It offers an efficient, inexpensive and real time mean of distributing information among people.

E-Mail Address

Each user of email is assigned a unique name for his email account. This name is known as E-mail address. Different users can send and receive messages according to the e-mail address.

E-mail is generally of the form username@domainname. For example, webmaster@tutorialspoint.com is an e-mail address where webmaster is username and tutorialspoint.com is domain name.

- The username and the domain name are separated by @ **(at)** symbol.

- E-mail addresses are not case sensitive.

- Spaces are not allowed in e-mail address.

E-mail Message Components

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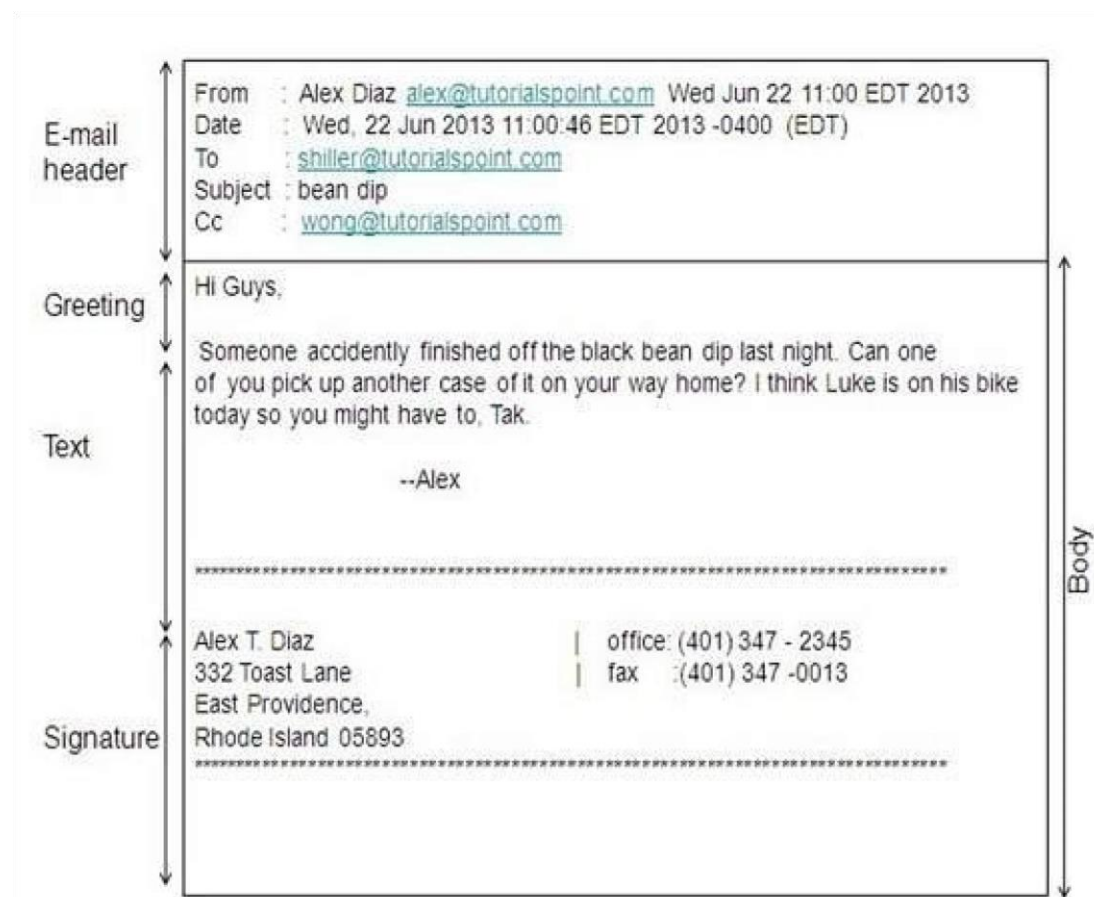
E-mail Header

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

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.

27

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.

Greet*ing*

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

Reliable

Many of the mail systems notify the sender if e-mail message was undeliverable.

Convenience

There is no requirement of stationary and stamps. One does not have to go to post office. But all these things are not required for sending or receiving an mail.

Speed

E-mail is very fast. However, the speed also depends upon the underlying network.

Inexpensive

The cost of sending e-mail is very low. Printable

It is easy to obtain a hardcopy of an e-mail. Also an electronic copy of an e-mail can also be saved for records.

Global

E-mail can be sent and received by a person sitting across the globe.

Generality

It is also possible to send graphics, programs and sounds with an e-mail.

Disadvantages

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

- Forgery
- Overload
- Misdirection
- Junk
- No response

Forgery

E-mail doesn't prevent from forgery, that is, someone impersonating the sender, since sender is usually not authenticated in any way.

Overload

Convenience of E-mail may result in a flood of mail. Misdirection

It is possible that you may send e-mail to an unintended recipient.

Junk

Junk emails are undesirable and inappropriate emails. Junk emails are sometimes referred to as spam.

E-mail Protocols are set of rules that help the client to properly transmit the information to or from the mail server. Here in this tutorial, we will discuss various protocols such as **SMTP, POP,** and **IMAP.**

SMPTP

SMTP stands for **Simple Mail Transfer Protocol**. It was first proposed in 1982. It is a standard protocol used for sending e-mail efficiently and reliably over the internet.

Key Points:

- SMTP is application level protocol.
- SMTP is connection oriented protocol.

- SMTP is text based protocol.

- It handles exchange of messages between e-mail servers over TCP/IP network.

- Apart from transferring e-mail, SMPT also provides notification regarding incoming mail.

- When you send e-mail, your e-mail client sends it to your e-mail server which further contacts the recipient mail server using SMTP client.

- These SMTP commands specify the sender's and receiver's e-mail address, along with the message to be send.

- The exchange of commands between servers is carried out without intervention of any user.

- In case, message cannot be delivered, an error report is sent to the sender which makes SMTP a reliable protocol.

SMTP Commands

The following table describes some of the SMTP commands:

S.N.	Command Description
1	**HELLO** This command initiates the SMTP conversation.
2	**EHELLO** This is an alternative command to initiate the conversation. ESMTP indicates that the sender server wants to use extended SMTP protocol.
3	**MAIL FROM** This indicates the sender's address.
4	**RCPT TO** It identifies the recipient of the mail. In order to deliver similar message to multiple users this command can be repeated multiple times.
5	**SIZE** This command let the server know the size of attached message in bytes.

6	**DATA** The **DATA** command signifies that a stream of data will follow. Here stream of data refers to the body of the message.
7	**QUIT** This commands is used to terminate the SMTP connection.
8	**VERFY** This command is used by the receiving server in order to verify whether the given username is valid or not.
9	**EXPN** It is same as VRFY, except it will list all the users name when it used with a distribution list.

IMAP

IMAP stands for **Internet Mail Access Protocol.** It was first proposed in 1986. There exist five versions of IMAP as follows:

1. Original IMAP
2. IMAP2
3. IMAP3
4. IMAP2bis
5. *IMAP4 Key*

Points:

- IMAP allows the client program to manipulate the e-mail message on the server without downloading them on the local computer.
- The e-mail is hold and maintained by the remote server.
- It enables us to take any action such as downloading, delete the mail without reading the mail.It enables us to create, manipulate and delete remote message folders called mail boxes.
- IMAP enables the users to search the e-mails.
- It allows concurrent access to multiple mailboxes on multiple mail servers.

IMAP Commands

The following table describes some of the IMAP commands:

S.N.	Command Description	32
1	**IMAP_LOGIN** This command opens the connection.	
2	**CAPABILITY** This command requests for listing the capabilities that the server supports.	
3	**NOOP** This command is used as a periodic poll for new messages or message status updates during a period of inactivity.	
4	**SELECT** This command helps to select a mailbox to access the messages.	
5	**EXAMINE** It is same as SELECT command except no change to the mailbox is permitted.	
6	**CREATE** It is used to create mailbox with a specified name.	
7	**DELETE** It is used to permanently delete a mailbox with a given name.	
8	**RENAME** It is used to change the name of a mailbox.	
9	**LOGOUT** This command informs the server that client is done with the session. The server must send BYE untagged response before the OK response and then close the network connection.	

POP

POP stands for Post Office Protocol. It is generally used to support a single client. There are several versions of POP but the POP 3 is the current standard.

Key Points

- *POP is an application layer internet standard protocol.*
- *Since POP supports offline access to the messages, thus requires less internet usage time.*
- *POP does not allow search facility.*
- *In order to access the messaged, it is necessary to download them.*
- *It allows only one mailbox to be created on server.*
- *It is not suitable for accessing non mail data.*
- *POP commands are generally abbreviated into codes of three or four letters. Eg. STAT.*

POP Commands

The following table describes some of the POP commands:

S.N.	Command Description
1	**LOGIN** This command opens the connection.
2	**STAT** It is used to display number of messages currently in the mailbox.
3	**LIST** It is used to get the summary of messages where each message summary is shown.
4	**RETR** This command helps to select a mailbox to access the messages.

5	**DELE** It is used to delete a message.	34
6	**RSET** It is used to reset the session to its initial state.	
7	**QUIT** It is used to log off the session.	

Comparison between POP and IMAP

S.N.	POP	IMAP
	ABS, KANPUR	35
1	Generally used to support single client.	Designed to handle multiple clients.
2	Messages are accessed offline.	Messages are accessed online although it also supports offline mode.
3	POP does not allow search facility.	It offers ability to search emails.
4	All the messages have to be downloaded.	It allows selective transfer of messages to the client.
5	Only one mailbox can be created on the server.	Multiple mailboxes can be created on the server.
6	Not suitable for accessing non-mail data.	Suitable for accessing non-mail data i.e. attachment.
7	POP commands are generally abbreviated into codes of three or four letters. Eg. STAT.	IMAP commands are not abbreviated, they are full. Eg. STATUS.
8	It requires minimum use of server resources.	Clients are totally dependent on server.
9	Mails once downloaded cannot be accessed from some other location.	Allows mails to be accessed from multiple locations.

10	The e-mails are not downloaded automatically.	Users can view the headings and sender of emails and then decide to download.
10	POP requires less internet usage time.	IMAP requires more internet usage time.

WWW

WWW stands for **World Wide Web.** A technical definition of the World Wide Web is : all the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP).

A broader definition comes from the organization that Web inventor **Tim Berners-Lee** helped found, the **World Wide Web Consortium (W3C).**

The World Wide Web is the universe of network-accessible information, an embodiment of human knowledge.

In simple terms, The World Wide Web is a way of exchanging information between computers on the Internet, tying them together into a vast collection of interactive multimedia resources.

Internet and **Web** is not the same thing: Web uses internet to pass over the information.
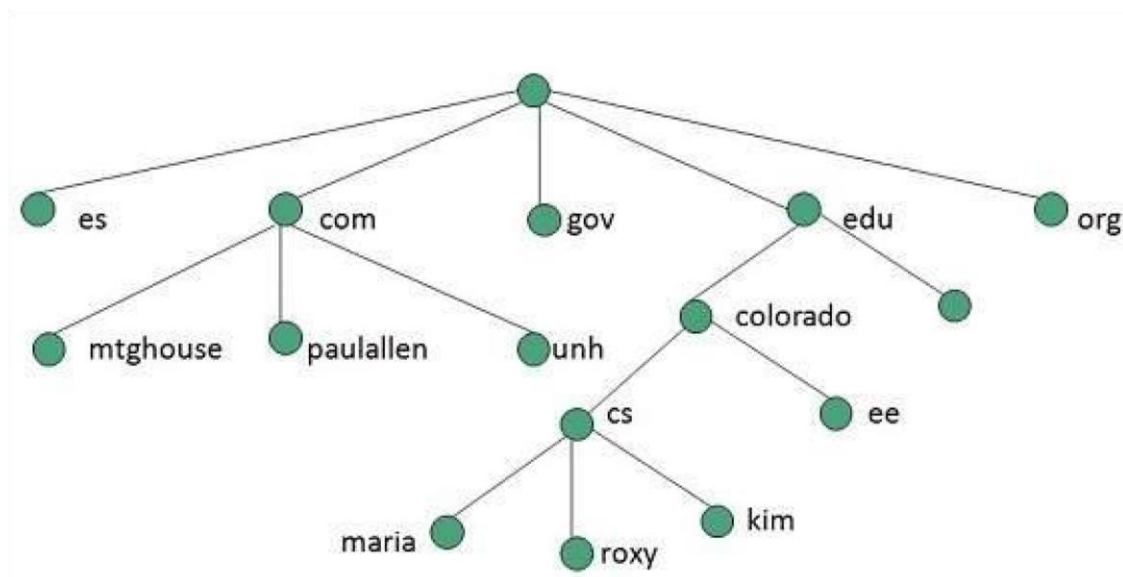
Evolution

World Wide Web was created by **Timothy Berners Lee** in 1989 at **CERN** in **Geneva.** World Wide Web came into existence as a proposal by him, to allow researchers to work together effectively and efficiently at **CERN.** Eventually it became **World Wide Web.**

The following diagram briefly defines evolution of World Wide Web:

Web 1.0
•Static web pages
•Brochure ware
•Mostly publishing
•No Communities

Web 2.0
•Social Media
•Keyword search
•Rich user experience
•Tagging

Web 3.0
•Highly Mobile
•OpenID
•Semantic search
•Micro Blogging
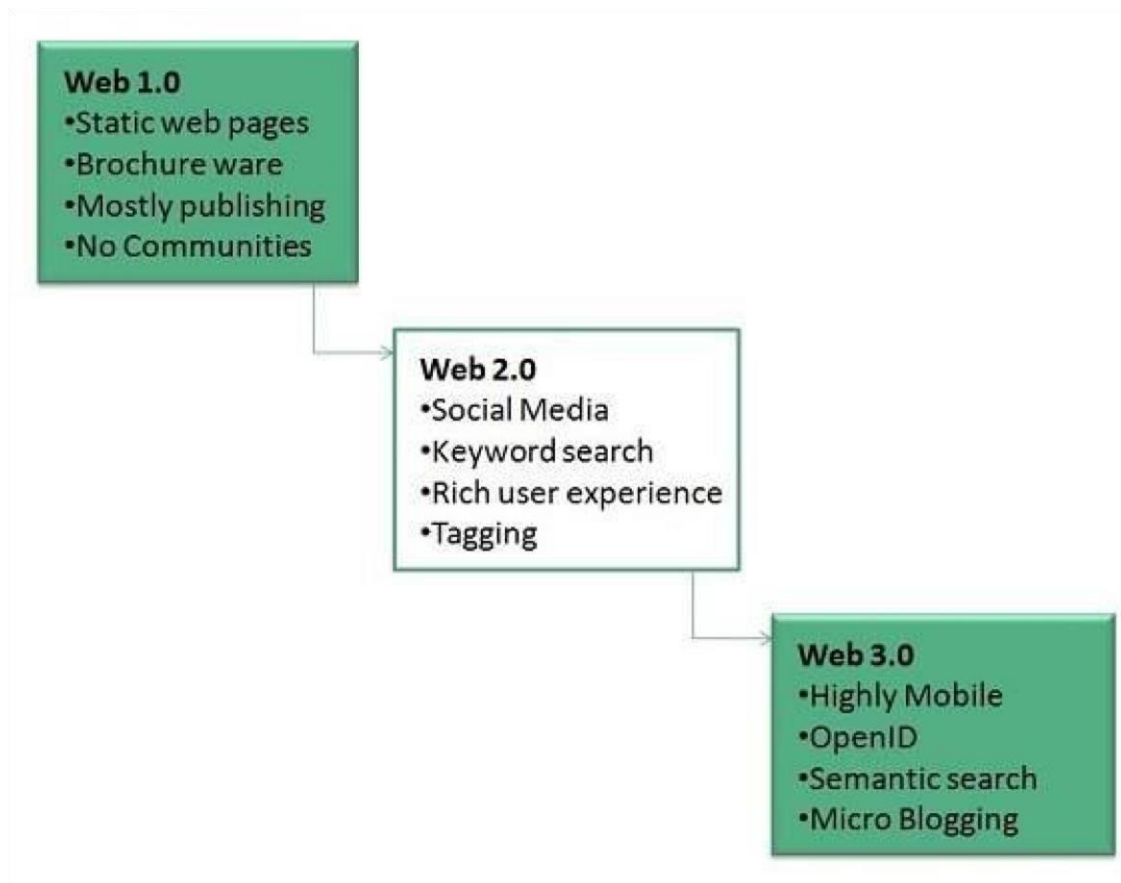
WWW Architecture

WWW architecture is divided into several layers as shown in the following diagram:
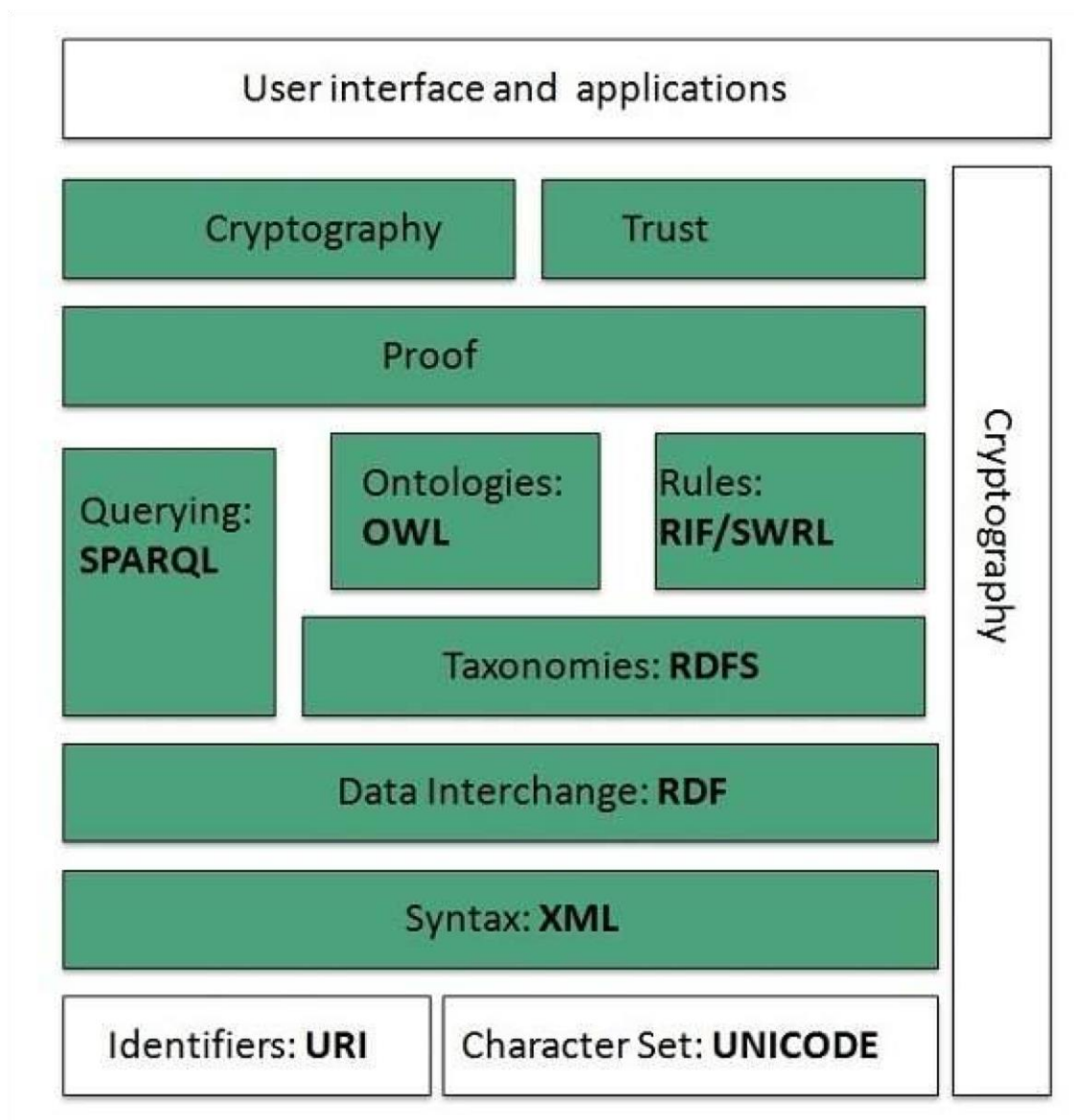
Identifiers and Character Set

Uniform Resource Identifier (URI) is used to uniquely identify resources on the web and **UNICODE** makes it possible to built web pages that can be read and write in human languages.

Syntax

XML (Extensible Markup Language) helps to define common syntax in semantic web.

Data Interchange

Resource Description Framework (RDF) framework helps in defining core representation of data for web. RDF represents data about resource in graph form.

Taxonomies

RDF Schema (RDFS) allows more standardized description of **taxonomies** and other **ontological** constructs.

Ontologies

Web Ontology Language (OWL) offers more constructs over RDFS. It comes in following three versions:

- OWL Lite for taxonomies and simple constraints.

- OWL DL for full description logic support.

- OWL for more syntactic freedom of RDF

Rules

RIF and **SWRL** offers rules beyond the constructs that are available from **RDFs** and **OWL.** Simple Protocol and **RDF Query Language (SPARQL)** is SQL like language used for querying RDF data and OWL Ontologies. Proof

All semantic and rules that are executed at layers below Proof and their result will be used to prove deductions.

Cryptography

Cryptography means such as digital signature for verification of the origin of sources is used.

User Interface and Applications

On the top of layer **User interface and Applications** layer is built for user interaction.

WWW Operation

WWW works on client- server approach. Following steps explains how the web works:

1. User enters the URL (say, **http://www.tutorialspoint.com**) of the web page in the address bar of web browser.

2. Then browser requests the Domain Name Server for the IP address corresponding to www.tutorialspoint.com.

3. After receiving IP address, browser sends the request for web page to the web server using HTTP protocol which specifies the way the browser and web server communicates.

4. Then web server receives request using HTTP protocol and checks its search for the requested web page. If found it returns it back to the web browser and close the HTTP connection.

5. Now the web browser receives the web page, It interprets it and display the contents of web page in web browser's window.
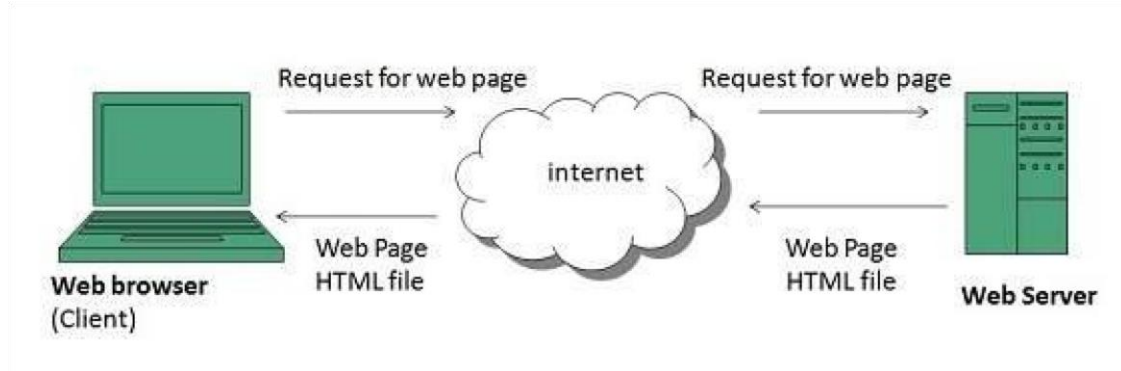
Future

There had been a rapid development in field of web. It has its impact in almost every area such as education, research, technology, commerce, marketing etc. So the future of web is almost unpredictable.

Apart from huge development in field of WWW, there are also some technical issues that W3 consortium has to cope up with. User Interface

Work on higher quality presentation of 3-D information is under deveopment. The W3 Consortium is also looking forward to enhance the web to full fill requirements of global communities which would include all regional languages and writing systems.

Technology

Work on privacy and security is under way. This would include hiding information, accounting, access control, integrity and risk management. Architecture

There has been huge growth in field of web which may lead to overload the internet and degrade its performance. Hence more better protocol are required to be developed.

Search Engine refers to a huge database of internet resources such as web pages, newsgroups, programs, images etc. It helps to locate information on World Wide Web.

User can search for any information by passing query in form of keywords or phrase. It then searches for relevant information in its database and return to the user.

Search Engine Components

Generally there are three basic components of a search engine as listed below:

1. Web Crawler
2. Database
3. Search Interfaces

Web crawler

It is also known as **spider** or **bots.** It is a software component that traverses the web to gather information.

Database

All the information on the web is stored in database. It consists of huge web resources.

Search Interfaces

This component is an interface between user and the database. It helps the user to search through the database.

Search Engine Working

Web crawler, database and the search interface are the major component of a search engine that actually makes search engine to work. Search engines make use of Boolean expression AND, OR, NOT to restrict and widen the results of a search. Following are the steps that are performed by the search engine:

- The search engine looks for the keyword in the index for predefined database instead of going directly to the web to search for the keyword.

- It then uses software to search for the information in the database. This software component is known as web crawler.

- Once web crawler finds the pages, the search engine then shows the relevant web pages as a result. These retrieved web pages generally include title of page, size of text portion, first several sentences etc.

These search criteria may vary from one search engine to the other. The retrieved information is ranked according to various factors such as frequency of keywords, relevancy of information, links etc.

- User can click on any of the search results to open it.

Architecture

The search engine architecture comprises of the three basic layers listed below:

- Content collection and refinement.

- Search core

- User and application interfaces
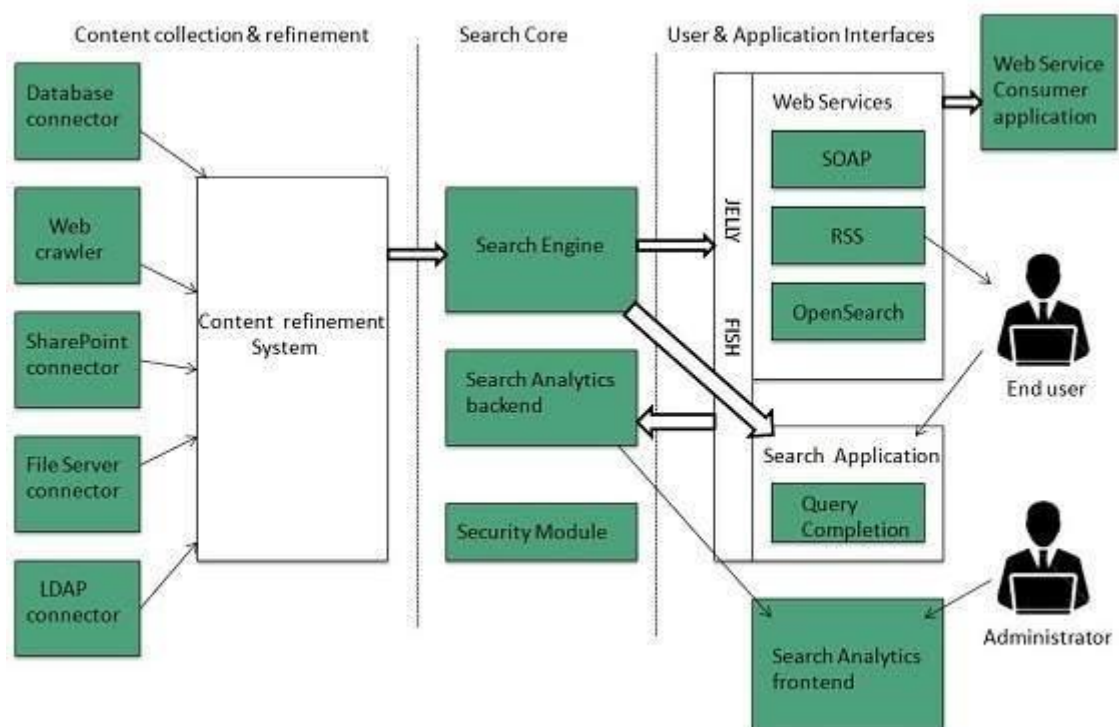
Search Engine Processing

Indexing Process

Indexing process comprises of the following three tasks:

- Text acquisition
- Text transformation
- Index creation

Text acquisition

It identifies and stores documents for indexing.

Text Transformation

It transforms document into index terms or features.

Index Creation

It takes index terms created by text transformations and create data structures to suport fast searching.

Query Process

Query process comprises of the following three tasks:

- User interaction
- Ranking
- Evaluation

User interaction

It supporst creation and refinement of user query and displays the results.

Ranking

It uses query and indexes to create ranked list of documents.

Evaluation

It monitors and measures the effectiveness and efficiency. It is done offline.

Examples

Following are the several search engines available today:

Search Engine	Description

Google	It was originally called **BackRub.** It is the most popular search engine globally.
Bing	It was launched in 2009 by **Microsoft.** It is the latest web-based search engine that also delivers Yahoo's results.
Ask	It was launched in 1996 and was originally known as **Ask Jeeves.** It includes support for match, dictionary, and conversation question.
AltaVista	It was launched by **Digital Equipment Corporation** in 1995. Since 2003, it is powered by Yahoo technology.
AOL.Search	It is powered by Google.
LYCOS	It is top 5 internet portal and 13th largest online property according to Media Matrix.
Alexa	It is subsidiary of Amazon and used for providing website traffic information.

E-Payment System:

 Electronic payment systems are central to on-line business process as companies look for ways to serve customers faster and at lower cost. Emerging innovations in the payment for goods and services in electronic commerce promise to offer a wide range of new business opportunities.

Electronic payment systems and e-commerce are highly linked given that on-line consumers must pay for products and services. Clearly, payment is an integral part of the mercantile

process and prompt payment is crucial. If the claims and debits of the various participants (consumers, companies and banks) are not balanced because of payment delay, then the entire business chain is disrupted. Hence an important aspect of e-commerce is prompt and secure payment, clearing, and settlement of credit or debit claims.

Electronic payment systems are becoming central to on-line business transactions nowadays as companies look for various methods to serve customers faster and more cost effectively. Electronic commerce brings a wide range of new worldwide business opportunities. There is no doubt that electronic payment systems are becoming more and more common and will play an important role in the business world. Electronic payment always involves a payer and a payee who exchange money for goods or services. At least one financial institution like a bank will act as the issuer (used by the payer) and the acquirer (used by the payee).

3.2   Types of Electronic Payment Systems:

Electronic payment systems are proliferating in banking, retail, health care, on-line markets, and even government—in fact, anywhere money needs to change hands.

- Organizations are motivated by the need to deliver products and services more cost effectively and to provide a higher quality of service to customers.
- The emerging electronic payment technology labeled electronic funds transfer (EFT).
- EFT is defined as ―any transfer of funds initiated through an electronic terminal telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution.

EFT can be segmented into three broad categories:

  ➢ **Banking and financial payments**
  - Large-scale or wholesale payments (e.g., bank-to-bank transfer)
  - Small-scale or retail payments (e.g., automated teller machines
  - Home banking (e.g., bill payment)
      ➢   **Retailing payments**
  - Credit Cards (e.g., VISA or MasterCard)
  - Private label credit/debit cards (e.g., J.C. Penney Card)
  - Charge Cards (e.g., American Express)
  ➢ **On-line electronic commerce payments ❖ Token-based payment systems**

     Electronic cash (e.g., DigiCash)

- Electronic checks (e.g., NetCheque)
- Smart cards or debit cards (e.g., Mondex Electronic Currency Card)
- ❖ **Credit card-based payments systems**

  Encrypted Credit Cards (e.g., World Wide Web form-based encryption)
- Third-party authorization numbers (e.g., First Virtual)

3.3 E-Cash:

- There are many ways that exist for implementing an e-cash system, all must incorporate a few common features.
- Electronic Cash is based on cryptographic systems called ―digital signatures‖.
- This method involves a pair of numeric keys: one for locking (encoding) and the other for unlocking (decoding).

E-cash must have the following four properties.

- ➢ Monetary value
- ➢ Interoperability
- ➢ Retrievability
- ➢ Security

- Electronic cash is a general term that describes the attempts of several companies to create value storage and exchange system that operates online in much the same way that government-issued currency operates in the physical world.

- Concerns about electronic payment methods include:

  – Privacy

  – Security

  – Independence

  – Portability

Electronic Cash Storage:

• Two methods

     – **On-line**

• Individual does not have possession personally of electronic cash

• Trusted third party, e.g. e-banking, bank holds customers' cash accounts

     – **Off-line**

• Customer holds cash on smart card or electronic wallet

• Fraud and double spending require tamper-proof encryption

The purchase of e-cash from an on-line currency server (or bank) involves two steps:

➢ Establishment of an account
➢ Maintaining enough money in the account to bank the purchase.

- Once the tokens are purchased, the e-cash software on the customer's PC stores digital money undersigned by a bank.

- The users can spend the digital money at any shop accepting e-cash, without having to open an account there or having to transmit credit card numbers.

- As soon as the customer wants to make a payment, the software collects the necessary amount from the stored tokens
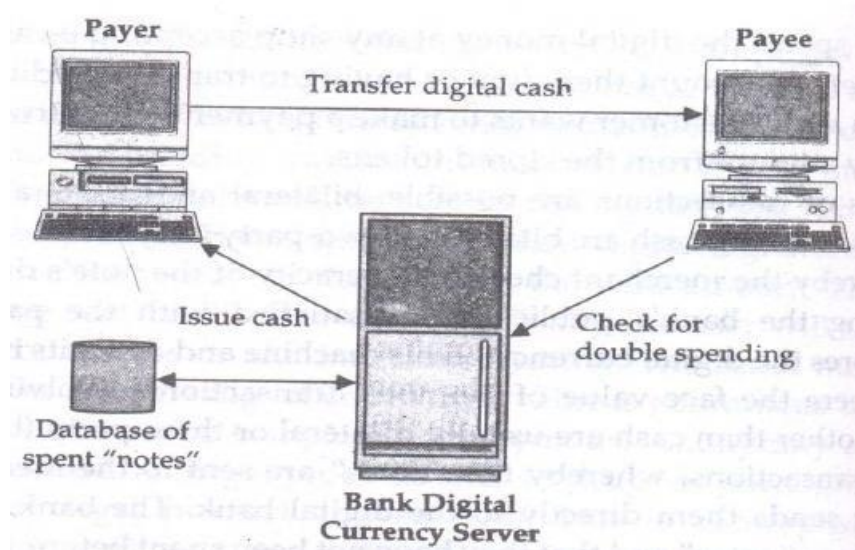
– Convenience

3.4 Electronic Checks:

- It is another form of electronic tokens.
- Buyers must register with third-party account server before they are able to write electronic checks.
- The account server acts as a billing service.
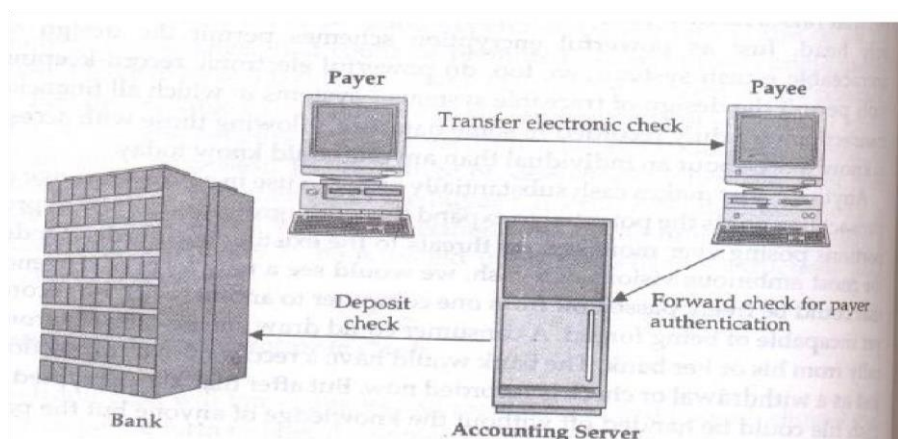
Advantages of Electronic Checks:

1. They work in the same way as traditional checks.

2. These are suited for clearing micropayments.

3. They create float & availability of float is an important for commerce.

4. Financial risk is assumed by the accounting server & may result in easier acceptance.

3.5 Smart Cards & Electronic Payment Systems:

- Smart cards have been in existence since the early 1980s and hold promise for secure transactions using existing infrastructure.

- Smart cards are credit and debit cards and other card products enhanced with microprocessors capable of holding more information than the traditional magnetic

- stripe. The smart card technology is widely used in countries such as France, Germany, Japan,   and Singapore to pay for public phone calls, transportation, and shopper loyalty programs.

Types of Smart Cards:

- Relationship-Based Smart Credit Cards
- Electronic Purses also known as debit cards

➢ **Relationship-Based Smart Credit Cards:**

- It is an enhancement of existing cards services &/ or the addition of new services that a   financial institution delivers to its customers via a chip-based card or other device.

- These services include access to multiple financial accounts, value-added marketing programs, or other information card holders may want to store on their card.

- It includes access to multiple accounts, such as debit, credit, cash access, bill payment & multiple access options at multiple locations.

➢ **Electronic Purses:**

To replace cash and place a financial instrument are racing to introduce electronic purses, wallet-sized smart cards embedded with programmable microchips that store sums of money for people to use instead of cash for everything.

The electronic purse works in the following manner:

- After purse is loaded with money at an ATM, it can be used to pay for candy in a vending machine with a card reader.

- It verifies card is authentic & it has enough money, the value is deducted from balance on the card & added to an e-cash & remaining balance is displayed by the vending machine.

Credit Card-Based Electronic Payment Systems:

Payment cards are all types of plastic cards that consumers use to make purchases:

– Credit cards

• Such as a Visa or a MasterCard, has a preset spending limit based

on the user's credit limit. – Debit cards

• Removes the amount of the charge from the cardholder's account

and transfers it to the seller's bank. – Charge cards

• Such as one from American Express, carries no preset spending

limit. **Advantages:**

– Payment cards provide fraud protection.

– They have worldwide acceptance.

– They are good for online transactions.

Disadvantages:

Payment card service companies charge merchants per-transaction fees and monthly processing fees.

3.6 Risks in Electronic Payment systems:

➢ Customer's risks

– Stolen credentials or password

– Dishonest merchant

– Disputes over transaction

– Inappropriate use of transaction details

➢ Merchant's risk

– Forged or copied instruments
– Disputed charges

– Insufficient funds in customer's account – Unauthorized redistribution of purchased items

3.7   Electronic payments Issues:

- Secure transfer across internet
- High reliability: no single failure point
- Atomic transactions
- Anonymity of buyer
- Economic and computational efficiency: allow micropayments
- Flexibility: across different methods
- Scalability in number of servers and users

Security Requirements In Electronic Payment Systems:

> **Integrity and authorization**

Apayment system with integrity allows no money to be taken from a user without explicit authorization by that user. It may also disallow the receipt of payment without explicit consent, to prevent occurrences of things like unsolicited bribery. Authorization constitutes the most important relationship in a payment system. Payment can be authorized in three ways: via out-band authorization, passwords, and signature.

> **Out-band authorization**

In this approach, the verifying party (typically a bank) notifies the authorizing party (the payer) of a transaction. The authorizing party is required to approve or deny the payment using a secure, out-band channel (such as via surface mail or the phone). This is the current approach for credit cards involving mail orders and telephone orders: Anyone who knows a user's credit card data can initiate transactions, and the legitimate user must check the statement and actively complain about unauthorized transactions. If the user does not complain within a certain time (usually 90 days), the transaction is considered ―approved‖ by default.

> **Password authorization**

Atransaction protected by a password requires that every message from the authorizing party include a cryptographic check value. The check value is computed using a secret known only to the authorizing and verifying parties. This secret can be a personal identification number, a password, or any form of shared secret. In addition, shared secrets that are short - like a six-digit PIN - are inherently susceptible to various kinds of attacks. They cannot by themselves provide a high degree of security. They should only

be used to control access to a physical token like a smart card (or a wallet) that performs the actual authorization using secure cryptographic mechanisms, such as digital signatures.

➢ **Signature authorization**

In this type of transaction, the verifying party requires a digital signature of the authorizing party. Digital signatures provide non repudiation of origin.

➢ **Confidentiality**

Some parties involved may wish confidentiality of transactions. Confidentiality in this context means the restriction of the knowledge about various pieces of information related to a transaction: the identity of payer/payee, purchase content, amount, and so on. Typically, the confidentiality requirement dictates that this information be restricted only to the participants involved. Where anonymity or un-traceability are desired, the requirement may be to limit this knowledge to certain subsets of the participants only, as described later.

➢ **Availability and reliability**

All parties require the ability to make or receive payments whenever necessary. Payment transactions must be atomic: They occur entirely or not at all, but they never hang in an unknown or inconsistent state. No payer would accept a loss of money (not a significant amount, in any case) due to a network or system crash. Availability and reliability presume that the underlying networking services and all software and hardware components are sufficiently dependable. Recovery from crash failures requires some sort of stable storage at all parties and specific resynchronization protocols. These fault tolerance issues are not discussed here, because most payment systems do not address them explicitly.

3.8 Electronic Data Interchange(EDI):

- Electronic Data Interchange (EDI) - interposes communication of business information in standardized electronic form.

- Prior to EDI, business depended on postal and phone systems that restricted communication to those few hours of the workday that overlap between time zones.

Why EDI?

• Reduction in transaction costs

• Foster closer relationships between trading partners **EDI & Electronic Commerce**

• Electronic commerce includes EDI & much more

• EDI forges boundary less relationships by improving interchange of information between trading partners, suppliers, & customers.

3.9 EDI layered architecture:

• Semantic (or application) layer

• Standards translation layer

• Packing (or transport) layer

• Physical network infrastructure layer

EDI semantic layer	Application level services	
EDI standard layer	EDIFACT business form standards	
	ANSI X12 business form standards	
EDI transport layer	Electronic mail	X.435, MIME
	Point to point	FTP, TELNET
	World Wide Web	HTTP
Physical layer	Dial-up lines, Internet, I-way	

EDI semantic layer:

• Describes the business application

• Procurement example

– Requests for quotes

– Price quotes

– Purchase orders

– Acknowledgments

– Invoices

• Specific to company & software used

Standards translation:

• Specifies business form structure so that information can be exchanged

• Two competing standards

– American National Standards Institute(ANSI)X12

– EDIFACT developed by UN/ECE, Working Party for the Facilitation of International Trade Procedures

EDI transport layer

• How the business form is sent, e.g. post, UPS, fax

• Increasingly, e-mail is the carrier

• Differentiating EDI from e-mail

– Emphasis on automation

– EDI has certain legal status

Physical network infrastructure layer
• Dial-up lines, Internet, value-added network, etc.

Information flow with EDI:
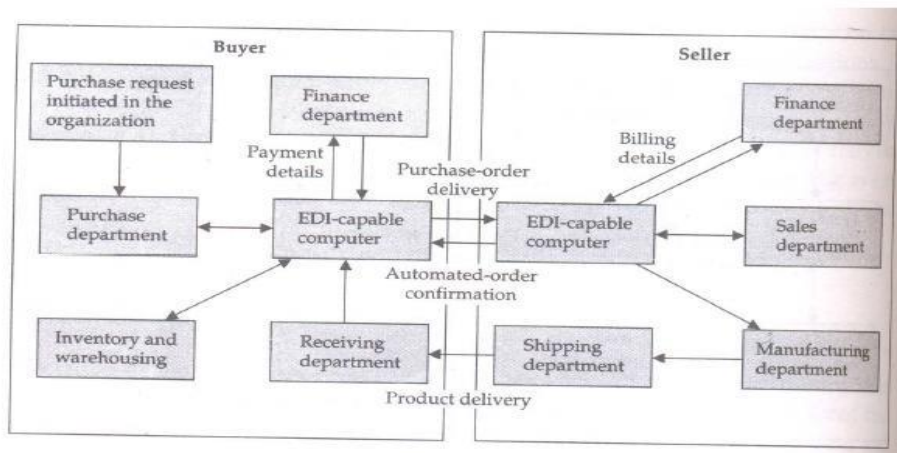
1. Buyer sends purchase order to seller computer

2. Seller sends purchase order confirmation to buyer

3. Seller sends booking request to transport company

4. Transport company sends booking confirmation to seller

5. Seller sends advance ship notice to buyer

6. Transport company sends status to seller

7. Buyer sends Receipt advice to seller
8. Seller sends invoice to buyer

9. Buyer sends payment to seller

3.10   Applications of EDI:

1. Role of EDI in international trade: Reduced transaction expenditures

- Quicker movement of imported & exported goods
- Improved customer service through —track & trace‖ programs
- Faster customs clearance & reduced opportunities for corruption, a huge problem in
- trade

2. Interbank Electronic Funds Transfer (EFT)

- EFTS is credit transfers between banks where funds flow directly from the payer's bank to the payee's bank.

- The two biggest funds transfer services in the United States are the Federal Reserve's system, Fed wire, & the Clearing House Interbank Payments System (CHIPS) of the New York clearing house

3. Health care EDI for insurance EDI

- Providing good & affordable health care is a universal problem
- EDI is becoming a permanent fixture in both insurance & health care industries as medical provider, patients, & payers

- Electronic claim processing is quick & reduces the administrative costs of health care.
- Using EDI software, service providers prepare the forms & submit claims via communication lines to the value-added network service provider

- The company then edits sorts & distributes forms to the payer. If necessary, the insurance company can electronically route transactions to a third-party for price evaluation

- Claims submission also receives reports regarding claim status & request for additional Information

4. Manufacturing & retail procurement using EDI

- These are heavy users of EDI
- In manufacturing, EDI is used to support just-in-time.
- In retailing, EDI is used to support quick response

3.11   EDI Protocols:

- ➢ ANSI X12
- ➢ EDIFACT

Comparison of EDIFACT & X.12 Standards:

- These are comprised of strings of data elements called segments.
- A transaction set is a set of segments ordered as specified by the standard.
- ANSI standards require each element to have a very specific name, such as order date or invoice date.
- EDIFACT segments, allow for multiuse elements, such as date.
- EDIFACT has fewer data elements & segments & only one beginning segment (header),but it has more composites.
- It is an ever-evolving platform.

3.12 E-Marketing:

- E-marketing is directly marketing a commercial message to a group of people using email. In its broadest sense, every email sent to a potential or current customer could be considered email marketing.

- It usually involves using email to send ads, request business, or solicit sales or donations, and is meant to build loyalty, trust, or brand awareness.

Email marketing can be done to either sold lists or a current customer database. Broadly, the term is usually used to refer to sending email messages with the purpose of enhancing the relationship of a merchant with its current or previous customers, to encourage customer loyalty and repeat business, acquiring new customers or convincing current customers to purchase something immediately, and adding advertisements to email messages sent by other companies to their customers.

Advantages:

- An exact return on investment can be tracked and has proven to be high when done properly. Email marketing is often reported as second only to search marketing as the most effective online marketing tactic.
-

- Email marketing is significantly cheaper and faster than traditional mail, mainly because of high cost and time required in a traditional mail campaign for producing the artwork, printing, addressing and mailing.

Advertisers can reach substantial numbers of email subscribers who have opted in (i.e., consented) to receive email communications on subjects of interest to them.

Almost half of American Internet users check or send email on a typical day with email blasts that are delivered between 1 am and 5 am local time outperforming those sent at other times in open and click rates.

- Email is popular with digital marketers, rising an estimated 15% in 2009 to £292 m in the UK.

- If compared to standard email, direct email marketing produces higher response rate and higher average order value for e-commerce businesses.

Disadvantages:

- A report issued by the email services company Return Path, as of mid-2008 email deliverability is still an issue for legitimate marketers. According to the report, legitimate email servers averaged a delivery rate of 56%; twenty percent of the messages were rejected, and eight percent were filtered.

- Companies considering the use of an email marketing program must make sure that their program does not violate spam laws such as the United States' Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM),the European Privacy and Electronic Communications Regulations 2003, or their Internet service provider's acceptable use policy.

3.13   Tele Marketing:

- Telemarketing is a method of direct marketing in which a salesperson solicits prospective customers to buy products or services, either over the phone or through a subsequent face to face or Web conferencing appointment scheduled during the call.

- Telemarketing can also include recorded sales pitches programmed to be played over the phone via automatic dialing.

- Telemarketing may be done from a company office, from a call center, or from home. It may involve a live operator voice broadcasting which is most frequently associated with political messages.

- An effective telemarketing process often involves two or more calls. The first call (or series of calls) determines the customer's needs. The final call (or series of calls) motivates the customer to make a purchase. Prospective customers are identified by various means, including past purchase history, previous requests for information, credit limit, competition entry forms, and application forms. Names may also be purchased from another company's consumer database or obtained from a telephone directory or another public list. The qualification process is intended to determine which customers are most likely to purchase the product or service.

- Charitable organizations, alumni associations, and political parties often use telemarketing to solicit donations. Marketing research companies use telemarketing techniques to survey the prospective or past customers of a client's business in order to assess market acceptance of or satisfaction with a particular product, service, brand, or company. Public opinion polls are conducted in a similar manner.

- Telemarketing techniques are also applied to other forms of electronic marketing using email or fax messages, in which case they are frequently considered spam by receivers.

Disadvantages:

- Telemarketing has been negatively associated with various scams and frauds, such as pyramid schemes, and with deceptively overpriced products and services

- Telemarketing is often criticized as an unethical business practice due to the perception of high-pressure sales techniques during unsolicited calls.

- Telemarketers marketing telephone companies may participate in telephone slamming, the practice of switching a customer's telephone service without their knowledge or authorization.

- Telemarketing calls are often considered an annoyance, especially when they occur during the dinner hour, early in the morning, or late in the evening.

3.14 Security Threats to E-commerce:

E-Commerce security requirements can be studied by examining the overall process, beginning with the consumer and ending with the commerce server. Considering each logical link in the commerce chain, the assets that must be protected to ensure secure e-commerce include client computers, the messages travelling on the communication channel, and the web and commerce servers – including any hardware attached to the servers. While telecommunications are certainly one of the major assets to be protected, the telecommunications links are not the only concern in computer and e-commerce security. For instance, if the telecommunications links were made secure but no security measures were implemented for either client computers or commerce and web-servers, then no communications security would exist at all.

Client threats

Until the introduction of executable web content, Web pages were mainly static. Coded in HTML, static pages could do little more than display content and provide links to related pages with additional information. However, the widespread use of active content has changed this perception.

Active content: Active content refers to programs that are embedded transparently in web pages and that cause action to occur. Active content can display moving graphics, download and play audio, or implement web-based spreadsheet programs. Active content is used in e-commerce to place items one wishes to purchase into a shopping cart and to compute the total invoice amount, including sales tax, handling, and shipping costs. The best known active content forms are Java applets, ActiveX controls, JavaScript, and VBScript.

Malicious codes: Computer viruses, worms and trojan horses are examples of malicious code. A trojan horse is a program which performs a useful function, but performs an unexpected action as well. Virus is a code segment which replicates by attaching copies to existing

executables. A worm is a program which replicates itself and causes execution of the new copy. These can create havoc on the client side.

Server-side masquerading*:* Masquerading lures a victim into believing that the entity with which it is communicating is a different entity. For example, if a user tries to log into a computer across the internet but instead reaches another computer that claims to be the desired one, the user has been spoofed. This may be a passive attack (in which the user does not attempt to authenticate the recipient, but merely accesses it), but it is usually an active attack.

Communication channel threats

The internet serves as the electronic chain linking a consumer (client) to an e-commerce resource. Messages on the internet travel a random path from a source node to a destination node. The message passes through a number of intermediate computers on the network before reaching the final destination. It is impossible to guarantee that every computer on the internet through which messages pass is safe, secure, and non-hostile.

Confidentiality threats: Confidentiality is the prevention of unauthorized information disclosure. Breaching confidentiality on the internet is not difficult. Suppose one logs onto a website – say www.anybiz.com – that contains a form with text boxes for name, address, and email address. When one fills out those text boxes and clicks the submit button, the information is sent to the web-server for processing. One popular method of transmitting data to a web-server is to collect the text box responses and place them at the end of the target server's URL. The captured data and the HTTP request to send the data to the server is then sent. Now, suppose the user changes his mind, decides not to wait for a response from the anybiz.com server, and jumps to another website instead – say www.somecompany.com. The server somecompany.com may choose to collect web demographics and log the URL from which the user just came (www.anybiz.com). By doing this, somecompany.com has breached confidentiality by recording the secret information the user has just entered.

Integrity threats: An integrity threat exists when an unauthorized party can alter a message stream of information. Unprotected banking transactions are subject to integrity violations. Cyber vandalism is an example of an integrity violation. Cyber vandalism is the electronic defacing of an existing website page. Masquerading or spoofing – pretending to be someone you are not or representing a website as an original when it really is a fake – is one means of creating havoc on websites. Using a security hole in a domain name server (DNS), perpetrators can substitute the address of their website in place of the real one to spoof website visitors.

Integrity threats can alter vital financial, medical, or military information. It can have very serious consequences for businesses and people.

Availability threats: The purpose of availability threats, also known as delay or denial threats, is to disrupt normal computer processing or to deny processing entirely. For example, if the processing speed of a single ATM machine transaction slows from one or two seconds to 30 seconds, users will abandon ATM machines entirely. Similarly, slowing any internet service will drive customers to competitors' web or commerce sites.

Server threats

The server is the third link in the client-internet-server trio embodying the e-commerce path between the user and a commerce server. Servers have vulnerabilities that can be exploited by anyone determined to cause destruction or to illegally acquire information.

Web-server threats: Web-server software is designed to deliver web pages by responding to HTTP requests. While web-server software is not inherently high-risk, it has been designed with web service and convenience as the main design goal. The more complex the software is, the higher the probability that it contains coding errors (bugs) and security holes – security weaknesses that provide openings through which evildoers can enter.

Commerce server threats: The commerce server, along with the web-server, responds to requests from web browsers through the HTTP protocol and CGI scripts. Several pieces of software comprise the commerce server software suite, including an FTP server, a mail server, a remote login server, and operating systems on host machines. Each of this software can have security holes and bugs.

Database threats: E-commerce systems store user data and retrieve product information from databases connected to the web-server. Besides product information, databases connected to the web contain valuable and private information that could irreparably damage a company if it were disclosed or altered. Some databases store username/password pairs in a non-secure way. If someone obtains user authentication information, then he or she can masquerade as a legitimate database user and reveal private and costly information.

Common gateway interface threats: A common gateway interface (CGI) implements the transfer of information from a web-server to another program, such as a database program. CGI and the programs to which they transfer data provide active content to web pages. Because CGIs are programs, they present a security threat if misused. Just like web-servers, CGI scripts can be set up to run with their privileges set to high – unconstrained. Defective or malicious

CGIs with free access to system resources are capable of disabling the system, calling privileged (and dangerous) base system programs that delete files, or viewing confidential customer information, including usernames and passwords.

Password hacking: The simplest attack against a password-based system is to guess passwords. Guessing of passwords requires that access to the complement, the complementation functions, and the authentication functions be obtained. If none of these have changed by the time the password is guessed, then the attacker can use the password to access the system.

3.15 Security Requirements For E-Commerce:

Authentication:

This is the ability to say that an electronic communication (whether via email or web) does genuinely come from who it purports to.Without face-to-face contact, passing oneself off as someone else is not difficult on the internet.

In online commerce the best defence against being misled by an imposter is provided by unforgeable digital certificates from a trusted authority (such as VeriSign). Although anyone can generate digital certificates for themselves, a trusted authority demands real-world proof of identity and checks its validity before issuing a digital certificate. Only certificates from trusted authorities will be automatically recognized and trusted by the major web browser and email client software.

Authentication can be provided in some situations by physical tokens (such as a drivers license), by a piece of information known only to the person involved (eg. a PIN), or by a physical property of a person (fingerprints or retina scans). Strong authentication requires at least two or more of these. A digital certificate provides strong authentication as it is a unique token and requires a password for its usage.

 Privacy:

In online commerce, privacy is the ability to ensure that information is accessed and changed only by authorized parties. Typically this is achieved via encryption. Sensitive data (such as credit card details, health records, sales figures etc.) are encrypted before being transmitted across the open internet – via email or the web. Data which has been protected with strong 128bit encryption may be intercepted by hackers, but cannot be decrypted by them within a short time. Again, digital certificates are used here to encrypt email or establish a secure

HTTPS connection with a web-server. For extra security, data can also be stored long-term in an encrypted format.

Authorization:

Authorization allows a person or computer system to determine if someone has the authority to request or approve an action or information. In the physical world, authentication is usually achieved by forms requiring signatures, or locks where only authorized individuals hold the keys.

Authorization is tied with *authentication*. If a system can securely verify that a request for information (such as a web page) or a service (such as a purchase requisition) has come from a known individual, the system can then check against its internal rules to see if that person has sufficient authority for the request to proceed.

In the online world, authorization can be achieved by a manager sending a digitally signed email. Such an email, once checked and verified by the recipient, is a legally binding request for a service. Similarly, if a web-server has a restricted access area, the server can request a digital certificate from the user's browser to identify the user and then determine if they should be given access to the information according to the server's permission rules.

Integrity:

Integrity of information means ensuring that a communication received has not been altered or tampered with. Traditionally, this problem has been dealt with by having tight control over access to paper documents and requiring authorized officers to initial all changes made – a system with obvious drawbacks and limitations. If someone is receiving sensitive information online, he not only wants to ensure that it is coming from who he expects it to (authentication), but also that it hasn't been intercepted by a hacker while in transit and its contents altered. The speed and distances involved in online communications requires a very different approach to this problem from traditional methods.

One solution is afforded by using digital certificates to digitally —sign‖ messages. A travelling employee can send production orders with integrity to the central office by using their digital certificate to sign their email. The signature includes a hash of the original message – a brief numerical representation of the message content. When the recipient opens the message, his email software will automatically create a new hash of the message and compare it against the

one included in the digital signature. If even a single character has been altered in the message, the two hashes will differ and the software will alert the recipient that the email has been tampered with during transit.

Non-repudiation:

Non-repudiation is the ability to guarantee that once someone has requested a service or approved an action. Non-repudiation allows one to legally prove that a person has sent a specific email or made a purchase approval from a website. Traditionally non-repudiation has been achieved by having parties sign contracts and then have the contracts notarized by trusted third parties. Sending documents involved the use of registered mail, and postmarks and signatures to date-stamp and record the process of transmission and acceptance. In the realm of e-commerce, non repudiation is achieved by using digital signatures. Digital signatures which have been issued by a trusted authority (such as VeriSign) cannot be forged and their validity can be checked with any major email or web browser software. A digital signature is only installed in the personal computer of its owner, who is usually required to provide a password to make use of the digital signature to encrypt or digitally sign their communications. If a company receives a purchase order via email which has been digitally signed, it has the same legal assurances as on receipt of a physical signed contract.

3.16 Security policy for E-commerce:

The security policy may cover issues like:

- What service types (e.g., web, FTP, SMTP) users may have access to?
- What classes of information exist within the organization and which should be encrypted before being transmitted?
- What client data does the organization hold. How sensitive is it? How is it to be protected?
- What class of employees may have remote access to the corporate network?
- Roles and responsibilities of managers and employees in implementing the security policy.
- How security breaches are to be responded to?

The security policy should also consider physical aspects of network security. For example,

- Who has access to the corporate server?

- Is it in a locked environment or kept in an open office?

- What is the procedure for determining who should be given access? The security policy regulates the activities of employees just as much as it defines how IT infrastructure will be configured. The policy should include details on how it is to be enforced • How individual responsibilities are determined?

For it to be effective, the policy needs regular testing and review to judge the security measures. The review process needs to take into account any changes in technology or business practices which may have an influence upon security. Lastly, the policy itself needs to be regarded as a living document which will be updated at set intervals to reflect the evolving ways in which the business, customers and technology interact. **Security Standards:**

There are various standards pertaining to the security aspects of enterprises. Some of them are

- ➢ ISO 17799 (Information technology – Code of practice for information security management).

- ➢ (ISO/IEC 2000).
- ➢ SSE-CMM (Systems security engineering – Capability maturity model).
- ➢ (SSE-CMM 2003).
- ➢ COBIT (Control objectives for information and related technology).
- ➢ (COBIT 2000).

ISO 17799 provides detailed guidelines on how a management framework for enterprise security should be implemented. It conceives ten security domains. Under each domain there are certain security objectives to be fulfilled. Each objective can be attained by a number of controls. The controls may prescribe management measures like guidelines and procedures, or some security infrastructure in the form of tools and techniques. It details various methods that can be followed by enterprises to meet security needs for e-commerce. It talks about the need for security policies, security infrastructure, and continuous testing in the same manner as has been detailed above.

The main objective of the COBIT is the development of clear policies and good practices for security and control in IT for worldwide endorsement by commercial, governmental and

professional organizations. The SSE-CMM is a process reference model. It is focused upon the requirements for implementing security in a system or series of related systems that are in the Information Technology Security domain.

3.17   Firewall:

A firewall is a network security system that controls the incoming and outgoing network traffic based on an applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is assumed not to be secure and trusted. Firewalls exist both as software to run on general purpose hardware and as a hardware appliance. Many hardware-based firewalls also offer other functionality to the internal network they protect, such as acting as a DHCP server for that network.

Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions.

Types of Firewall:

There are different types of firewalls depending on where the communication is taking place, where the communication is intercepted and the state that is being traced.

- Network layer Firewall
- Application layer firewall
- Proxy server
- Network address translation

➢ **Network layer Firewall:**
  Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. The firewall administrator may define the rules; or default rules may apply.
  Network layer firewalls generally fall into two sub-categories,
  - Stateful Firewalls
  - Stateless Firewalls

Stateful firewalls maintain context about active sessions, and use that "state information" to speed packet processing. Any existing network connection can be described by several properties, including source and destination IP address, UDP or TCP ports, and the current stage of the connection's lifetime (including session initiation, handshaking, data transfer, or completion connection). If a packet does not match an existing connection, it will be evaluated according to the rule set for new connections. If a packet matches an existing connection based on comparison with the firewall's state table, it will be allowed to pass without further processing.

Stateless firewalls require less memory, and can be faster for simple filters that require less time to filter than to look up a session. They may also be necessary for filtering stateless network protocols that have no concept of a session. However, they cannot make more complex decisions based on what stage communications between hosts have reached.

➢ Application Layer Firewall:

Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic), and may intercept all packets traveling to or from an application. They block other packets (usually dropping them without acknowledgment to the sender).

On inspecting all packets for improper content, firewalls can restrict or prevent outright the spread of networked computer worms and trojans. The additional inspection criteria can add extra latency to the forwarding of packets to their destination.

Application firewalls function by determining whether a process should accept any given connection. Application firewalls accomplish their function by hooking into socket calls to filter the connections between the application layer and the lower layers of the OSI model. Application firewalls that hook into socket calls are also referred to as socket filters. Application firewalls work much like a packet filter but application filters apply filtering rules (allow/block) on a per process basis instead of filtering connections on a per port basis. Generally, prompts are used to define rules for

processes that have not yet received a connection. It is rare to find application firewalls not combined or used in conjunction with a packet filter.

Also, application firewalls further filter connections by examining the process ID of data packets against a ruleset for the local process involved in the data transmission. The extent of the filtering that occurs is defined by the provided ruleset. Given the variety of software that exists, application firewalls only have more complex rulesets for the standard services, such as sharing services. These per process rulesets have limited efficacy in filtering every possible association that may occur with other processes.

- **Proxy server:**

A proxy server running either on dedicated hardware or as software on a general-purpose machine may act as a firewall by responding to input packets (connection requests, for example) in the manner of an application, while blocking other packets. A proxy server is a gateway from one network to another for a specific network application, in the sense that it functions as a proxy on behalf of the network user.

Proxies make tampering with an internal system from the external network more difficult and misuse of one internal system would not necessarily cause a security breach exploitable from outside the firewall. Conversely, intruders may hijack a publicly reachable system and use it as a proxy for their own purposes; the proxy then masquerades as that system to other internal machines. While use of internal address spaces enhances security, crackers may still employ methods such as IP spoofing to attempt to pass packets to a target network.

- **Network Address Translation:**

Firewalls often have network address translation (NAT) functionality, and the hosts protected behind a firewall commonly have addresses in the "private address range", as defined in RFC 1918.

Firewalls often have such functionality to hide the true address of protected hosts. Originally, the NAT function was developed to address the limited number of IPv4 routable addresses that could be used or assigned to companies or individuals as well as reduce both the amount and therefore cost of obtaining enough public addresses for every computer in an organization. Hiding the addresses of protected devices has become an increasingly important defense against network reconnaissance.

3.18 Digital Signatures:

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures. In some countries, including the United States, India, Brazil, and members of the European Union, electronic signatures have legal significance.

A digital signature scheme typically consists of three algorithms;
- A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.

- A signing algorithm that, given a message and a private key, produces a signature.
- A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

Applications of digital signatures:

Authentication:

Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

Integrity:

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it. (Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message after signature invalidates the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions (see collision resistance).

Non-repudiation:

Non-repudiation, or more specifically non-repudiation of origin, is an important aspect of digital signatures. By this property, an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

Some digital signature algorithms:

RSA-based signature schemes, such as RSA-PSS

DSA and its elliptic curve variant ECDSA

ElGamal signature scheme as the predecessor to DSA, and variants Schnorr signature and Pointcheval–Stern signature algorithm

- Rabin signature algorithm

- Pairing-based schemes such as BLS

- Undeniable signatures

  Aggregate signature - a signature scheme that supports aggregation: Given n signatures

- on n messages from n users, it is possible to aggregate all these signatures into a single

- signature whose size is constant in the number of users. This single signature will

- convince the verifier that the n users did indeed sign the n original messages.

- • Signatures with efficient protocols - are signature schemes that facilitate efficient cryptographic protocols such as zero-knowledge proofs or secure computation.

3.19   Digital Certificate:

- It is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner.

- The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply. An individual wishing to send an encrypted message applies for a digital certificate from a Certificate Authority (CA). The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through print publicity or perhaps on the Internet.

- The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply. • The most widely used standard for digital certificates is X.509.

Contents Of a Typical Digital Certificate:

- Serial Number: Used to uniquely identify the certificate.
- Subject: The person, or entity identified.
- Signature Algorithm: The algorithm used to create the signature.
- Signature: The actual signature to verify that it came from the issuer.
- Issuer: The entity that verified the information and issued the certificate.
- Valid-From: The date the certificate is first valid from.
- Valid-To: The expiration date.
- Key-Usage: Purpose of the public key (e.g. encipherment, signature, certificate signing...).
- Public Key: The public key.
- Thumbprint Algorithm: The algorithm used to hash the public key certificate.
- Thumbprint (also known as fingerprint): The hash itself, used as an abbreviated form of the public key certificate.

Payment in E-Commerce

Types of payment in e-commerce

Payment is a main part of commercial transaction against the goods supplied. In E-commerce four types of payment are made. They are as under -

1) Credit card payments

2) Electronic cheque payments

3) Payment for services such as internet, these payments is micro or small payment.

4) Electronic-cash payments

5) Digital cash (e-cash)

6) Online stored value system

7) Smart Cards

8) B2B payment system

Credit card payment - Online credit card is much similar to actual card being used no card impression is taken and no signature is available. For credit card payment there is a participation of four members. They are as follows:

• Customer and credit card of him

• Merchant who accept the credit card (such as VISA, MASTER CARD etc)

• issuing Bank of the credit card which collects payment from customers.

•In this process the bank or the financial institution sets up an account with a merchant and authenticates the card information which is send electronically by merchant and sanctions sales depending on the credit card status of the customer. Bank then accepts the credit cards. Credit cards may be of different credit card companies. Merchant gets the payment from the bank with guarantee. Bank issuing credit card returns financial information.

When customer wants to purchase he or she adds the item to the merchant's shopping cart When the customer wants for the payment a secure tunnel through the internet is created using SSL (Secure Socket Layer). Using encryption SSL secures the session during which the credit card information will be sent to the merchant and protects the information. Once the consumer credit card information is received the merchant software contacts a clearing house which authenticates credit card and verifies account balances. Clearing house contacts the issuing bank to verify the account information. Once verified the issuing bank credits the account of the merchant's bank. The debit to the consumer account is transmitted to the consumer [21].

Electronic Cheque Payment

A special hardware is required in order to sign the cheques which are used to do transactions which are attached to PC.A special hardware is used to do encryption of the signature. Public keys of the business partners are authenticated by certifying agencies.

Steps in transaction

1. Purchaser sends Purchase order and payment advice with his private key. He encrypts his Public key certificate using vendor's public key and sends it to vendor.

2. Vendor converts the message in the readable format using his private key checks certificate and cheque and then attaches deposit slip encrypts with

73

Figure 1.8: Electronic Cheque Payment
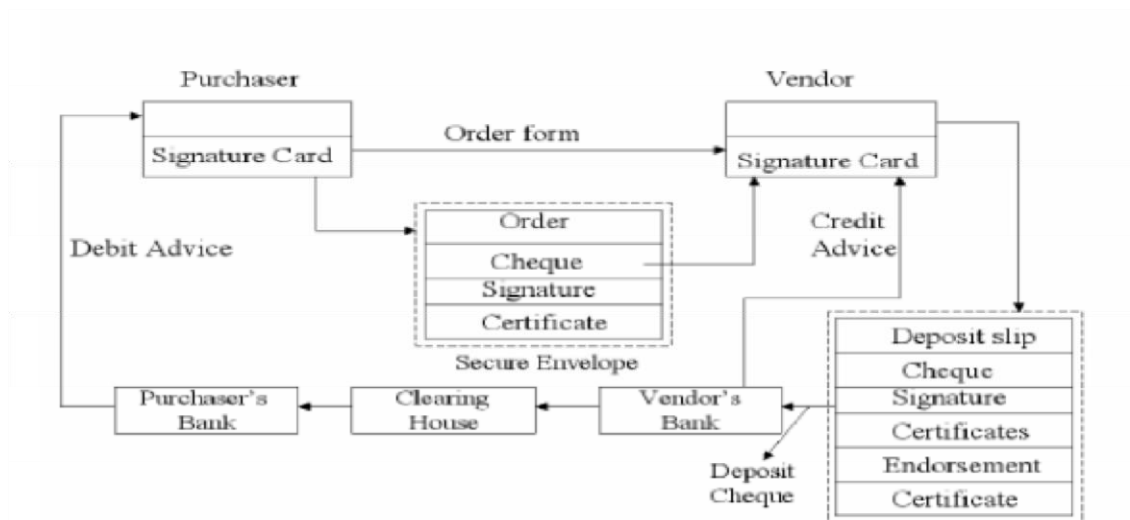
Payments of Small Amounts on Internet

bank's public key and sends it to bank.. Then he also sends public key certificate after encryption

3.   After checking the signatures and credits, bank clears cheque. Credit advice is given to vendor and combined debit advice is sent to purchaser from time to time. Payment for services such as internet, these payments is micro or small payment.

NETBILL'S PROPRIETARY SYSTEM

- Only after customer is charge, information delivered
- After information is delivered, vendor guaranteed payment
- Net bill is the intermediary
  MAJOR STEPS
- When customer asks for information, vendor sends encrypted information to the customer but without encryption to customer.

- Along with the information obtained, Payment order is sent to vendor
- Copy of purchase order and key for decryption is sent by Vendor to NET BILL.
- Credit of the customer is checked by NET BILL. If it is ok it sends key to customer.

- Vendor account is credited and customer account is debited and a key is send to the customer to debit customer account.

- Customer decrypts information

Figure 1.9: Paying for Small Internet Transactions
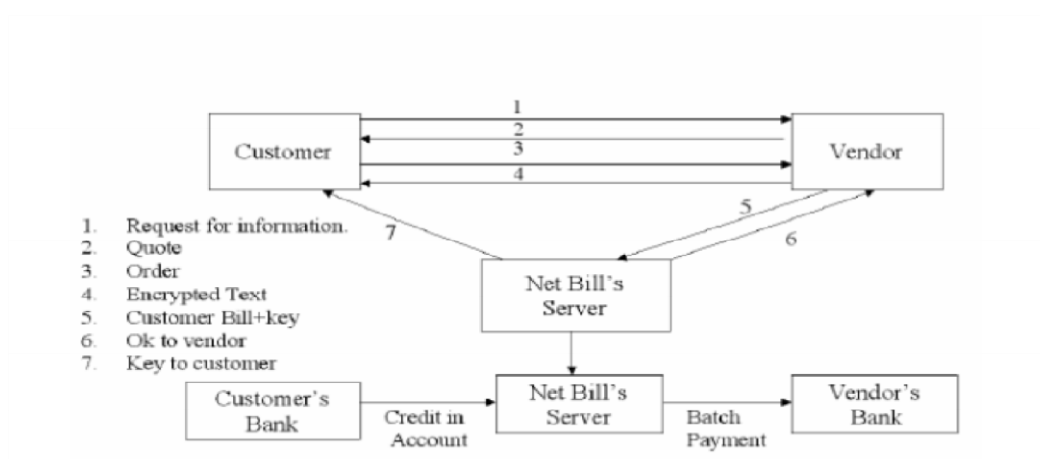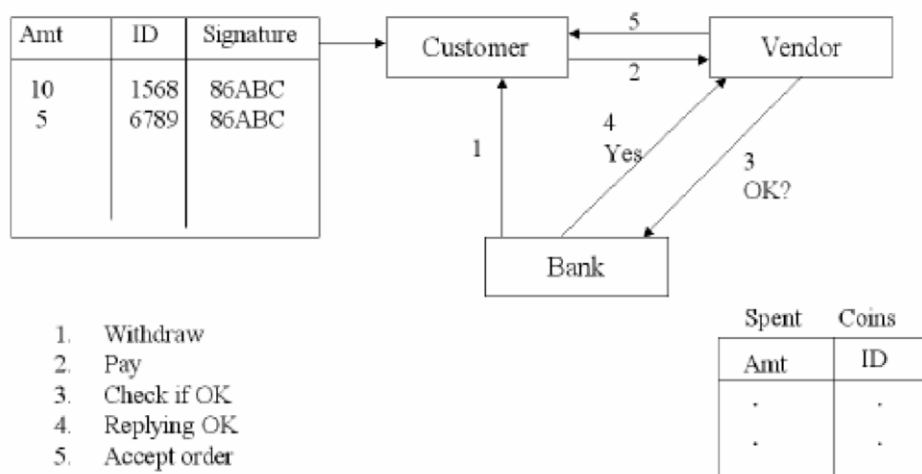

Electronic Cash (Digital Cash)

- For small payment Cash payment is done

- Cash preserves secrecy

- Cash should not be traceable

- It is cheaper than credit card transaction

- DES is normally used for these transactions as it is cheap and amount involved is small

Traceable cash payments

STEPS

1. Customer withdraws coins in various denominations signed by bank
   Structure of the file is as follows- serial no, denomination, signature of bank
   A copy of issued coins is stored by bank.

2. Using signed coins customer pays to vendor.

3. Bank checks for whether it is current or spent

4. If it is current, it authorizes dispatch of goods and credits vendor account with electronic coins

Figure 1.10: Electronic cash

Amt	ID	Signature
10	1568	86ABC
5	6789	86ABC

1. Withdraw
2. Pay
3. Check if OK
4. Replying OK
5. Accept order

Spent	Coins
Amt	ID
.	.
.	.

Digital cash was one of the first forms of alternative payment systems developed for e-commerce. The early generations of digital cash were quite complex and required the generation of entire new payment industry standards & practices. First generation digital cash worked as follows - To use e-cash customer had to first establish an account at bank that was using e-cash system. Once the account was established the customer then downloads digital wallet software on his computer. Then the customer could request a transfer of digital cash. Once the digital wallet had cash the consumer could spend that cash at merchants who were willing to accept it. The software would deduct the cash from the digital wallet and transfer to the merchants. The merchant could then transfer the cash back to the bank to confirm that it has not been double spent. The bank would then cancel the e-coins and credit the merchant's account at the bank. These early concepts were not market successes proving too complicated for both consumers and merchant. One variation on the digital cash concept is gifi cash which is a form of e-cash that is earned as a "points". Two of the best providers of gifi cash are Beenz.com (which issued points as a reward for purchase) and Flooz.com (which could be purchased as a form of gift certificate) both ceased operations in August 2001.Mypoints.com which issues points that can be redeemed for merchandise or gift certificates (but not cash) at partners sites in exchange for viewing ads or trying special offers is still in business as of August 2001. However mypoints.com can be considered a gift cash provider although the primary focus of its efforts is developing loyalty programs for clients rather than providing an online currency

[21]. The way of handling digital cash and its details are given in table no. 1.8[20] **Table No. 1.6 Types of Digital Cash and their Year Founded /description**

System	Year Founded /description
First Virtual	1994 – 1st secured stored value system based on credit card pre use deposits and pin numbers. Ceased operations in 1998.
Digital Cash (e–cash)	1996 Encryption based stored value system requiring digital wallet on hard drive to store e-coins. Ceased operations in 1998 returned as ecash
Millicent	1996 Digital equipment Corporation's entry into micro payment e-cash. Now a Compaq platform product with multiple options.
Peer to peer payment Systems	
Paypal	1999 free P2P micropayment system
Yahoo Paydirect	1999 . Free Yahoo P2P payment service
Money Zap	1999 Western Union fee-based money transfer system

Online Stored value system: Makes customer pay instantly to merchants and other individuals based on value stored in an online account. Some stored value systems require the user to download a digital wallet (for example Monetta's debit service and eCharge's prepaid service) where as others require to simply sign up and transfer money from their existing credit card accounts into an online stored value account. Online stored value systems rely on the value stored in a consumer's bank checking or credit card account. For example Ecount offers a prepaid debit account. To use Ecount a consumer first establishes an account with Ecount funded by a credit or debit card. Account information is transferred via the web using SSL. Once Ecount has verified the account and its balance with the consumer's card issuing bank. Consumers can shop on the web where Mastercard is accepted and email payments to individuals. Ecount debits the consumers account and transfers the funds to the merchant or individuals. At the end of the

month the consumer's card issuing bank sends a statement showing the debit to Ecount. Rocketcash is another company that offers online stored value system in this case aimed at teenagers [20]. Table no. 5 gives detail online stored value system and use of cards.

Table 1.7: Online Stored Value System

System	Year Founded /Description
Ecount	1998 Prepaid debit account
Monetta Prepaid	2000 Prepaid virtual card that allows consumers to make online payments without using a credit card or bank account digital wallet.
Monetta Debit	2000 Account that allows users to pay fro m existing checking savings online of credit accounts Digital Wallet
eCharge	1997 Prepaid account with digital wallet.
Millicent	1998 Prepaid cards purchased at convenience stores (Japan only)
Smart Cards	
Mondex	1994 smart card stored value system in which value is stored on a chip on a card.
American Express Blue	1999 bined credit and smart card

Smart Cards as Stored Value System - are another kind of stored value system based on credit cards that have embedded chips that store personal information. Where as credit cards store a single charge account number in the magnetic strip on the back smart cards can hold 100 times more data including multiple credit card numbers and information regarding health insurance transportation personal identification bank accounts and loyalty programs such as frequent flyer accounts. This capacity makes them an attractive alternative to carrying dozen or so credit and ID card in a physical wallet. Smart cards can also require a password unlike credit cards adding another layer of security. There are two types of smart cards – contact & contactless depending on the technology embedded. In order for contact cards to be read they must be physically placed into a card reader while contact less cards have an antenna built in that enables transmission of data without direct contact. A stored value smart card such as retail gift card purchased in a certain dollar value is an example of contact card because it must be swiped through a

smart card reader in order for payment to be processed. A highway toll payment system such as EZPass is an example of a contactless smart card because the EZPass device in the card is read by a remote sensor with the appropriate toll automatically deduced from the card at the end of the trip. The Mondex card is one of the original smart cards invented in 1990 by Natwest bank in England [21].   **B2B Payment Systems** - Most of the payment are

done physically by checks because of the complexity of the B2B business. There are two main types of B2B payment systems that have risen to the challenge. They are – 1) Systems that replace traditional banks 2) existing banking systems extending to the B2B marketplace. No system on the market today yet provides all of the features listed. Actrade is an example of an online B2B payment system that replaces the functionality provided traditionally by banks. Actrade serves as an international marketplace intermediary in the payment process by paying foreign sellers immediately and allowing domestic buyers a variable time a variable time period for repayment.