3

Telecommunication and Networks

Learning Objectives

- To identify major developments and trends in the industries, technologies and business applications relating to telecommunications and Internet technologies;
- To identify the basic components, functions, and types of telecommunications networks used in enterprises;
- To explain the functions of major types of telecommunications network, hardware, software, media, and services;
- To understand various topologies and architectures that a computer network might use;
- To identify the risks involved in using a computer network and the control mechanisms to curb those risks;
- To name specific types of wired and wireless transmission media and explain how they transmit data;
- To understand some of the transmission protocols used in exchanging information over the network; and
- To have an overview of e-Commerce and m-Commerce.

Task Statements

- To review and evaluate developments and trends of telecommunication and Internet technologies;
- To make use Internet, Intranet, and Extranet applications in businesses;
- To identify the suitability of components, functions, and types of telecommunications networks;
- To do the classification and application of various topologies and architectures of a computer network;
- To secure communication over a network, to some extent;
- To explain and name specific types of wired and wireless transmission media; and
- To use e-Commerce and m-Commerce in various functions of an enterprise.

Knowledge Statements

- To know the basic components, functions, and types of telecommunications networks used in business;
- To know the risks and related controls of a telecommunications network;
- To know various network topologies and applications;
- To know the specific types of wired and wireless transmission media; and
- To know various transmission protocols used to exchange information over the network.

3.1 Introduction

Organizations are becoming internetworked enterprises that use the Internet, intranets, and other telecommunications networks to support e-business operations and collaboration within the enterprise, and with their customers, suppliers, and other business partners. Telecommunications has entered a deregulated and fiercely competitive environment with many vendors, carriers, and services. Telecommunications technology is moving toward open, internetworked digital networks for voice, data, video, and multimedia. A major trend is the pervasive use of the Internet and its technologies to build interconnected enterprises and global networks, like intranets and extranets, to support enterprise collaboration, electronic commerce, and other e-business applications.

The explosive growth of the Internet and the use of its enabling technologies have revolutionized computing and telecommunications. The Internet has become the key platform for a rapidly expanding list of information and entertainment services and business applications, including enterprise collaboration and electronic commerce systems. Open systems with unrestricted connectivity using Internet technologies are the primary telecommunications technology drivers in e-business systems. Their primary goal is to promote easy and secure access by business professionals and consumers to the resources of the Internet, enterprise intranets, and inter-organizational extranets.

Companies are deriving strategic business value from the In ternet, which enables them to disseminate information globally, communicate and trade interactively with customized information and services for individual customers, and foster collaboration of people and integration of business processes within the enterprise and with business partners. These capabilities allow them to generate cost savings from using Internet technologies, revenue increases from electronic commerce, and better customer service and relationships through interactive marketing and customer relationship management.

Businesses are installing and extending intranets throughout their organizations to improve communications and collaboration among individuals and teams within the enterprise; to publish and share valuable business information easily, inexpensively, and effectively via enterprise information portals and intranet websites and other intranet services; and to develop and deploy critical applications to support business operations and decision making.

The primary role of extranets is to link the intranet resources of a company to the intranets of its customers, suppliers, and other business partners. Extranets can also provide access to operational company databases and legacy systems to business partners. Thus, extranets provide significant business value by facilitating and strengthening the business relationships of a company with customers and suppliers, improving collaboration with its business partners, and enabling the development of new kinds of W eb-based services for its customers, suppliers, and others.

The major generic components of any telecommunications network are terminals, telecommunications processors, communication channels, computers, and telecommunications software. There are several basic types of telecommunications networks, including wide area networks (WANs) and local area networks (LANs). Most WANs and LANs are interconnected using client/server, network computing, peer-to-peer, and Internet networking technologies.

Telecommunications processors include modems, multiplexers, internetworked processors, and various devices to help interconnect and enhance the capacity and efficiency of telecommunications channels. Telecommunications networks use such media as twisted-pair wiring, coaxial cables, fiber-optic cables, terrestrial microwave, communications satellites, cellular and PCS systems, wireless LANs, and other wireless technologies. Telecommunications software, such as network operating systems and telecommunications monitors, controls and manages the communications activity in a telecommunications network.

3.2 Networking an Enterprise

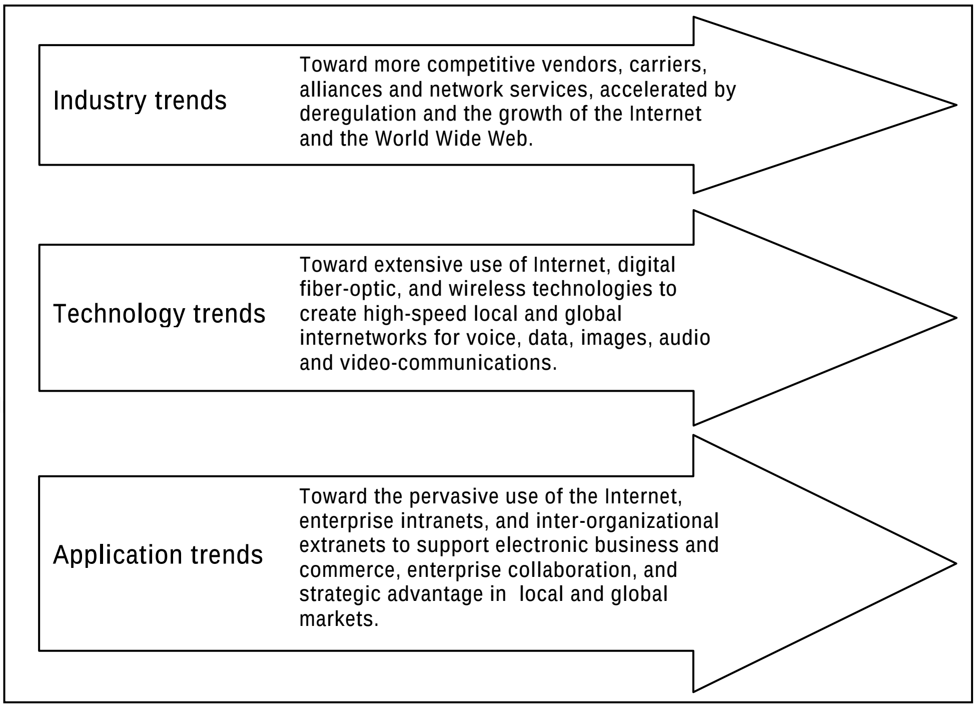
In today's world, most businesses are expected to be networked enterprises to be able to sustain and grow. The Internet and Internet-like networks inside the enterprise are called Intranets, between an enterprise and its trading partners are called Extranets. These and other types of n etworks serve as the primary information technology infrastructure for many enterprises. Managers, teams, end users, and workgroups use telecommunications networks to electronically exchange data and information anywhere in the world with other end users, customers, suppliers, and business partners. By using such networks, companies can perform more effectively as they can:

- Collaborate more creatively;
- Manage their business operations and organizational resources more effectively; and
- Compete successfully in today's fast changing global economy.

Now-a-days, survival of many organizations is not feasible without a variety of interconnected computer networks to service their various information processing and communications needs.

3.3 Trends in Telecommunication

Major trends are occurring in the field of telecommunications and these have a significant impact on management decisions. Therefore, it is necessary for managers, end users and other stakeholders to be aware of m ajor trends in telecommunications industries, technologies, and applications that significantly increase the decision alternatives confronting their organizations. A pictorial representation of major telecommunications trend is shown in the Fig. 3.3.1.



Industry trends

Toward more competitive vendors, carriers, alliances and network services, accelerated by deregulation and the growth of the Internet and the World Wide Web.

Technology trends

Toward extensive use of Internet, digital fiber-optic, and wireless technologies to create high-speed local and global internetworks for voice, data, images, audio and video-communications.

Application trends

Toward the pervasive use of the Internet, enterprise intranets, and inter-organizational extranets to support electronic business and commerce, enterprise collaboration, and strategic advantage in local and global markets.

Fig. 3.3.1: Trends in Telecommunication[*]

Let us discuss these aforementioned trends in detail.

3.3.1 Industry Trends

Some of the major industry trends are:

- Telecommunications networks and services are available from numerous large and small telecommunications companies.
- Explosive growth of the Internet and the World Wide Web has created a host of new telecommunications products, services and providers.
- Business firms have dramatically increased their use of the Internet and the Web for electronic commerce and collaboration.

[*] "Introduction to Information Systems" by James O'Brien, George M. Marakas, 11th edition, McGraw Hill, Page 221

3.3.2 Technology Trends

Now-a-days, technology is moving towards:

- Open systems with unrestricted connectivity, using Internet networking technologies as their technology platform, are becoming the primary telecommunications technology drivers.
- Increased industry and technical moves towards building client/server networks based on open system architecture. Open systems are information systems that use common standards for hardware, software, applications, and networking. Any open system provides greater connectivity, that is, the ability of network computers and other devices to easily access and communicate with each other and share information. Open systems architecture also provides a high degree of network interoperability. That is, open systems enable many different applications of end users to be accomplished using the different varieties of computer systems, software packages, and databases provided by a variety of interconnected networks.
- Change from analog to digital network technologies. Local and global telecommunications networks are rapidly converting to digital transmission technologies that transmit information in the form of discrete pulses, rather than waves. Digital transmission offers higher transmission speeds (transmits with pulses),movement of greater amounts of information, greater economy, much lower error rates than analog systems, and telecommunications networks to carry multiple types of communications (data, voice, and video) on the same circuits. (Integrated Services Digital Network (ISDN) technology)
- Change in communications media. Many telecommunications networks are changing from copper wire-based media and land-based microwave relay systems to fiber-optic lines and communications satellite transmissions. Fiber-optic transmission, which uses pulses of a laser-generated light, offer significant advantages in terms of:
  - Reduced size and installation effort
  - Greater communication capacity,
  - Faster transmission speeds, and
  - Freedom from electrical interference.

3.3.3 Business Application Trends

Some of the today's application trends are:

- The trend toward more vendors, services, Internet technologies, and open systems, and the rapid growth of the Internet, the World Wide Web, and corporate intranets and extranets, dramatically increases the number of feasible telecommunications applications.

- Telecommunications networks are playing a v ital and pervasive role in electronic commerce, enterprise collaboration, and internal business applications that support the operations, management, and strategic objectives of both large and small companies.
- Telecommunications functions have become an integral part of local and global computer networks that are used to dramatically:
  - Lock in customers and suppliers,
  - Shorten business lead times and response times,
  - Support electronic commerce,
  - Improve the collaboration of workgroups,
  - Develop new products and services,
  - Share resources,
  - Cut costs, and
  - Develop online operational processes.

3.4 The Business Value of Telecommunications

Information technology, especially in telecommunications-based business applications, helps company overcome barriers to business success. The widely used information systems in enterprises are highly facilitated through telecommunication systems that help in increase in productivity and performance of an o rganization. The strategic capabilities of telecommunications and other information technologies include:

- Overcome geographic barriers: capture information about business transactions from remote locations.
- Overcome time barriers: Provide information to remote locations immediately after it is requested.
- Overcome cost barriers: Reduce the cost of more traditional means of communication.
- Overcome structural barriers: Support linkages for competitive advantage.

Organizations, therefore, in a telecommunication network can improve communication, reduce costs, improve efficiency, reduce errors and improve consistency under the light of the aforementioned capabilities of computer network.

3.5 Telecommunications Network

Telecommunications is a highly technical, rapidly changing field of information systems technology. Most end users do not need a detailed knowledge of its technical characteristics. However, they need a basic understanding and appreciation for some of the important characteristics of the basic components of telecommunications networks.

3.5.1 Need and Scope of Networks

As the business grows, good communication between employees is needed. The organizations can improve efficiency by sharing information such as common files, databases and business application software over a telecommunication network. With improvements in network capacity and the ability to work wirelessly or remotely, successful businesses should regularly re-evaluate their needs and their IT infrastructure. Here are some of the advantages of a computer network in an organization:

(i) **File Sharing -** It provides sharing and grouping of data files over the network.

(ii) **Resource Sharing -** It provides sharing of c omputer resources such as hard disk, printers etc. by multiple users simultaneously to reduce the cost of installing and maintaining multiple resources in the organization.

(iii) **Remote Access -** Network allows users to remotely access the data and information from organization's network via Internet in cost effective manner.

(iv) **Shared Databases -**Network facilitates simultaneous access to the shared databases to multiple users at the same time by ensuring the integrity of the database.

(v) **Fault Tolerance -** By using network, fault tolerance can be implemented as a defense against accidental data loss. Usually, primary and secondary line of defense backups the data in case of system failure. Additional measures can also be taken by attaching a server with un-interruptible power supply in case of power failure or blackouts.

(vi) **Internet Access and Security -** It provides access to the Internet for transferring the document and to access the resources available on World Wide Web by maintaining data security through firewall system in the organization's network.

3.5.2 Telecommunication Network Model

Generally, a communication network is any arrangement where a sender transmits a message to a receiver over a channel consisting of some type of medium.

Fig. 3.5.1 illustrates a simple conceptual model of a telecommunications network, which shows that it consists of five basic categories of components: **Terminals, Telecommunications Processors, Telecommunications Media/Channels, Computers and Telecommunications Control Software.**

A. Terminals: Terminals are the starting and stopping points in any telecommunication network environment. Any input or output device that is used to transmit or receive data can be classified as a te rminal component. These include Video Terminals, Microcomputers, Telephones, Office Equipment, Telephone and Transaction Terminals.

B. Telecommunications Processors: Telecommunications Processors support data transmission and reception between terminals and computers by providing a variety of control and support functions. They include Network Interface Card, Modem, Multiplexer and Internetworked Processors.

- Network Interface Card (NIC): Network Interface Card (NIC) is a computer hardware component that connects a computer to a computer network. It has additional memory for buffering incoming and outgoing data packets, thus improving the network throughput.
- Modems: A MODEM is a device that converts a digital computer signal into an analog telephone signal (i.e. it modulates the signal) and converts an analog telephone signal into a digital computer signal (i.e. it demodulates the signal) in a data communication system. The word "modem" is a contraction of modulate and demodulate. Modems are required to send computer data with ordinary telephone lines because computer data is in digital form but telephone lines are analog.
- Multiplexers: A multiplexer is a communications processor that allows a single communications channel to carry simultaneous data transmissions from many terminals. Typically, a multiplexer merges the transmissions of several terminals at one end of a communications channel, while a similar unit separates the individual transmissions at the receiving end.
- Internetwork Processors: Telecommunications networks are interconnected by special-purpose communications processors called internetwork processors such as switches, routers, hubs, bridges, repeaters and gateways.
  - Switch - Switch is a communications processor that makes connections between telecommunications circuits in a network so that a telecommunications message can reach its intended destination.
  - Router – Router is a communications processor that interconnects networks based on different rules or *protocols*, so that a telecommunications message can be routed to its destination.
  - Hub – Hub is a port-switching communications processor. This allows for the sharing of the network resources such as servers, LAN workstations, printers, etc.
  - Bridge – Bridge is a communications processor that connects numerous Local Area Networks (LANs). It magnifies the data transmission signal while passing data from one LAN to another.
  - Repeater – Repeater is a communications processor that boosts or amplifies the signal before passing it to the next section of cable in a network.
  - Gateway – Gateway is a communications processor that connects networks that use different communication architectures.

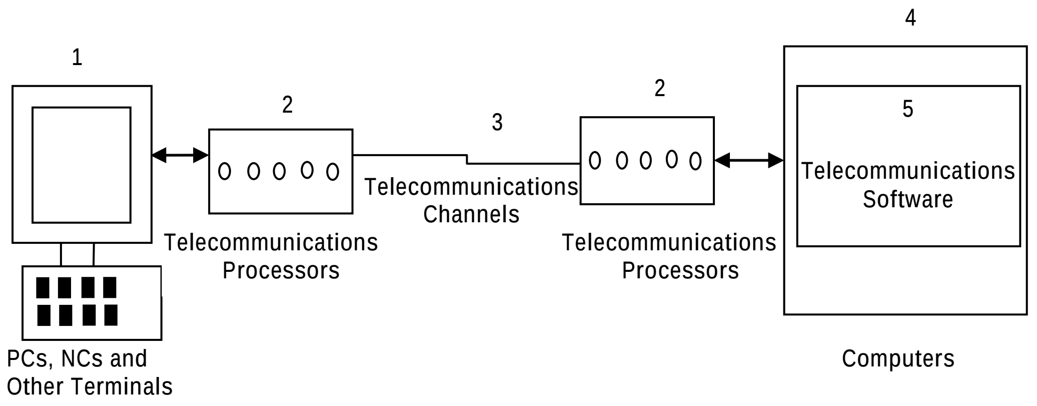

1
2
3
2
4
5
0 0 0 0 0
Telecommunications Channels
0 0 0 0 0
Telecommunications Software
Telecommunications Processors
Telecommunications Processors
PCs, NCs and Other Terminals
Computers

Fig. 3.5.1: Telecommunications Network Model[*]

C. Telecommunications Media/Channels: Telecommunications channels are the part of a telecommunications network that connects the message source with the message receiver. Data are transmitted and received over channels, which use a variety of telecommunications media. Telecommunications media are grouped into Guided Media and Unguided Media.

♦ Guided Media/Bound Media: Guided Transmission Media uses a "cabling" system that guides the data signals along a specific path. The data signals are bound by the "cabling" system. Some of the common examples of guided media are Twisted Pair, Coaxial cable and Fiber optics.

- Twisted-Pair Wire: Twisted-pair is ordinary telephone wire, consisting of copper wire twisted into pairs as shown in the Fig. 3.5.2. It is the most widely used media for telecommunications and is used for both voice and data transmissions. It is used extensively in home and office telephone systems and many LANs and WANs. However, there are few disadvantages of the same. Twisted Pair Wire is susceptible to various types of electrical interference (noise), which limits the practical distances that data can be transmitted without being garbled. Signals must be “refreshed” every one to two miles through the use of repeaters, which are very expensive and does not offer security.

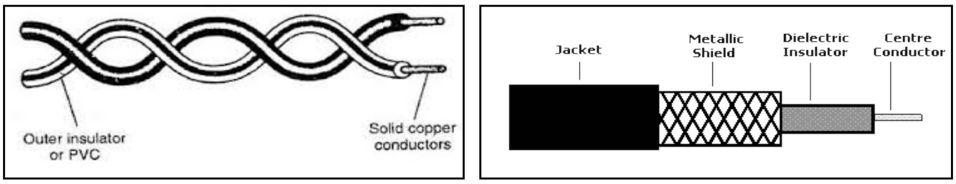


Fig. 3.5.2: Twisted Pair and Coaxial Cable respectively

[*] “Introduction to Information Systems” by James O’Brien, George M. Marakas, 11th edition, McGraw Hill, Page No. 238

- **Coaxial Cable:** This telecommunications media consists of copper or aluminum wire wrapped with spacers to insulate and protect it (as shown in the Fig. 3.5.2). Insulation minimizes interference and distortion of the signals the cable carries. Coaxial cables can carry a large volume of data and allows high-speed data transmission used in high-service metropolitan areas for cable TV systems, and for short-distance connection of computers and peripheral devices. These cables can be bundled together into a much larger cable for ease of installation and can be placed underground and laid on the floors of lakes and oceans. It is used extensively in office buildings and other work sites for local area networks. The only disadvantage of coaxial cable is that it is more expensive than twisted pair.

- **Fiber Optics:** This media consists of one or more hair-thin filaments of glass fiber wrapped in a protective jacket as shown in the Fig. 3.5.3. Signals are converted to light form and fired by laser in bursts. Optical fibers can carry digital as well as analog signals and provides increased speed and greater carrying capacity than coaxial cable and twisted-pair lines. It is not affected by electromagnetic radiation and not susceptible to electronic noise and so it has much lower error rates than twisted-pair and coaxial cable. Fiber optic cables are easy to install since they are smaller and more flexible and can be used undersea for transatlantic use. Speed of communications is 10,000 times faster than that of microwave and satellite systems.

  Biggest disadvantages of using fiber optic cable are that installation can be difficult and costly to purchase.

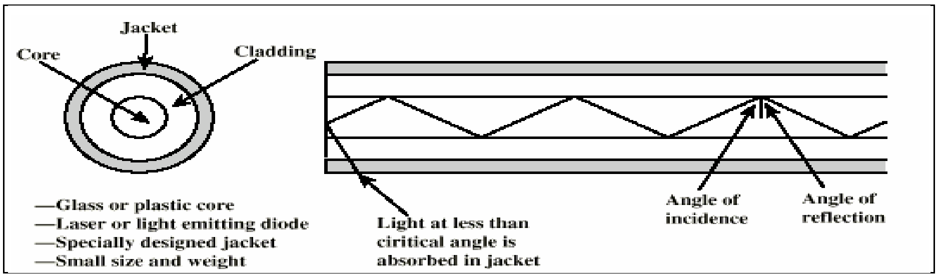

Jacket
Core
Cladding
—Glass or plastic core
—Laser or light emitting diode
—Specially designed jacket
—Small size and weight
Light at less than ciritical angle is absorbed in jacket
Angle of incidence
Angle of reflection

Fig. 3.5.3: Optical Fiber

♦ **Unguided Media/Unbound Media:** Unguided Transmission Media consists of a means for the data signals to travel but nothing to guide them along a specific path. The data signals are not bound to a cabling media. Some of the common examples of unguided media are **Terrestrial Microwave, Radio waves, Micro Waves, Infrared Waves** and **Communications Satellites**.

- **Terrestrial Microwave: Terrestrial microwave** involves earthbound microwave systems, which transmit high-speed radio signals in a line-of-sight path between relay stations spaced approximately 30 miles apart. Terrestrial microwave media uses the atmosphere as the medium through which to transmit signals, and is used extensively for high-volume as well as long-distance communication of both data and voice in the form of electromagnetic waves. However major disadvantage of terrestrial microwave is that it cannot bend around the curvature of the earth.

- Radio Waves: Wireless networks do not require any physical media or cables for data transmission. Radio waves are an invisible form of electromagnetic radiation that varies in wavelength from around a millimeter to 100,000 km, making it one of the widest ranges in the electromagnetic spectrum. Radio waves are most commonly used transmission media in the wireless Local Area Networks.

- Micro Waves: Microwaves are radio waves with wavelengths ranging from as long as one meter to as short as one millimeter, or equivalently, with frequencies between 300 MHz (0.3 GHz) and 300 GHz. These are used for communication, radar systems, radio astronomy, navigation and spectroscopy.

- Infrared Waves: Infrared light is used in industrial, scientific, and medical applications. Night-vision devices using infrared illumination allow people or animals to be observed without the observer being detected. Infrared tracking, also known as infrared homing, refers to a passive missile guidance system which uses the emission from a target of electromagnetic radiation in the infrared part of the spectrum to track it.

- Communication Satellites: Communication satellites use the atmosphere (microwave radio waves) as the medium through which to transmit signals. A satellite is some solar-powered electronic device that receives, amplifies, and retransmits signals; the satellite acts as a relay station between satellite transmissions stations on the ground (earth stations). They are used extensively for high-volume as well as long-distance communication of both data and voice. It is cost-effective method for moving large quantities of data over long distances. However, satellites are very expensive to develop and place in orbit and have an age limit of 7-10 years. Signals weaken over long distances; weather conditions and solar activity can also cause noise interference. Anyone can listen in on satellite signals, so sensitive data must be sent in a secret, or encrypted, form.

D. Computers: In a telecommunications networks, computers of all sizes and types are connected through media to perform their communication assignments. They include Host Computers (mainframes), Front-End Processors (minicomputers) and Network Servers (microcomputers).

E. Telecommunications Control Software: This consists of programs that control telecommunications activities and manage the functions of telecommunications networks. They include Telecommunication Monitors (mainframe host computers), Network Operating Systems (microcomputer network servers) for network servers, Network Management Components and Communication Packages (Microcomputer Web browsers). This software can reside on al most any component of th e network and can provide such features as performance monitoring, activity monitoring, priority assigning, transmission error correction and network problem mitigation.

- ♦ **Network Management:** Telecommunications software packages provide a variety of communication support services. For example, they work with a communications processor to connect and disconnect communications links and establish communications parameters such as transmission speed, mode, and direction. Examples of major network management functions include:
  - **Traffic management**– manages network resources and traffic to avoid congestion and optimize telecommunications service levels to users.
  - **Security**– provides authentication, encryption, and auditing functions, and enforces security policies.
  - **Network monitoring**– troubleshoot and watch over the network, informing network administrators of potential problems before they occur.
  - **Capacity planning**– surveys network resources and traffic patterns and users' needs to determine how best to accommodate the needs of the network as it grows and changes.

  Note: Detail of Network Management Function is provided in the later section (3.9: Network Administration and Management) of the Chapter.

3.6 Classification of Telecommunication Networks

There are many different types of telecommunications networks which can be classified on the basis of different factors like: **Area Coverage Based, Functional Based and Ownership-based** etc. as briefed in the Table 3.6.1.

Table 3.6.1: Computer Networks Classification

1	Class I	Area Coverage Based Classification
	LAN	A Local Area Network (LAN) is a group of computers and network devices connected together, usually within the same building, campus or spanned over limited distance. It provides high speed data transfer and is relatively inexpensive.
	MAN	A Metropolitan Area Network (MAN) is a larger network that usually spans in the same city or town. Cable network is an example of a MAN.
	WAN	A Wide Area Network (WAN) is not restricted to a geographical location, although it might be confined within the bounds of a state or country. The technology is high speed and relatively expensive. The Internet is an example of a world-wide public WAN.
2	Class II	Functional Based Classification
	Client-Server	This partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients.

	Peer-to-Peer	It is a type of decentralized and distributed network architecture in which individual nodes in the network (called "peers") act as both suppliers and consumers of resources
	Multi-Tier	It provides a model by which developers can create flexible and re-usable applications.
3	Class III	Ownership-based Classification
	Public Network	Network established for all users across the world is known as public network. Internet is an example of public network.
	Private Network	Private Network is used by particular organization, particular campus or particular enterprise only. This is a network that is not available to the outside world. Intranet is an example of it.
	Virtual Private Network (VPN)	A Virtual Private Network (VPN) is a network that uses a public network, such as the Internet, to provide secure access to organization's private network. A key feature of a VPN is its ability to work over both private networks as well as public networks like the Internet. Using a method called tunneling, a VPN uses the same hardware infrastructure as existing Internet or Intranet links.

A detailed discussion on the aforementioned networks is as follows:

3.6.1 Area Coverage Based Classification

A. Local Area Network: The Local Area Networks (LAN) are telecommunications networks that connect information-processing devices within a limited physical area. These networks cover areas such as Offices, Classrooms, Buildings, Manufacturing plant etc. Some of the characteristics of LANs include the following:

- LANs use a variety of telecommunications media, such as ordinary telephone wiring, coaxial cable, or wireless radio systems to interconnect microcomputer workstations and computer peripherals.
- To communicate over the network, a PC usually has a circuit board called a network interface card.
- Most LANs use a powerful microcomputer with a large disk capacity as a file server or network server that contains a network operating system (e.g., Novell NetWare) that controls telecommunications and the use of network resources.
- LANs allow end users in a workgroup to communicate electronically; share hardware, software, and data resources; and pool their efforts when working on group projects.

LANs on a distributed environment allow having our own independent processing stations while sharing expensive computer resources like disk files, printers and plotters. Further LAN provides:

(i) Security - Security for programs and data can be achieved using servers that are locked through both software and by physical means. Diskless nodes also offer security by not allowing users to download important data on floppies/CDs or upload unwanted software or virus.

(ii) Expanded PC usage through inexpensive workstation - Once a LAN has been set up, it actually costs less to automate additional employees through diskless PCs. Existing PCs can be easily converted into nodes by adding network interface cards.

(iii) Distributed processing - Many organizations operate as if they had distributed system in place. If numerous PCs are installed around the office, these machines represent the basic platform for a LAN with inter-user communication and information exchange.

(iv) Electronic mail and Message Broadcasting - Electronic mail allows users to communicate more easily among them. Messages to other users can be dropped into the recipient's mail-box and read by them when they log into the network.

(v) Organizational Benefits - LANs provide numerous benefits that include reduced costs in computer hardware, software and peripherals, and a drastic reduction in the time and cost of training or re-training manpower to use the systems.

(vi) Data management benefits - Since data is located centrally on the server, it becomes much easier to manage it, access it, as well as back it up.

(vii) Software cost and up-gradation - If the organization is concerned about using licensed software purchasing, a network version can save a lot of money since there would be no need to buy multiple copies of the same software for every machine in the organization. Therefore, software upgrades are much easier as any given package is stored centrally on the server.

B. Metropolitan Area Network (MAN): A Metropolitan Area Network (MAN) is somewhere between a LAN and a WAN. The term MAN is sometimes used to refer to networks which connect systems or local area networks within a metropolitan area (roughly 40 km in length from one point to another). A MAN interconnects computer resources in a geographic area or region larger than that covered by a large LAN but smaller than the area covered by a WAN.

A MAN can support both data and voice. Cable television networks are examples of MANs that distribute television signals. A MAN just has one or two cables and does not contain switching elements.

C. **Wide Area Network (WAN): Wide Area Networks** are telecommunications networks that cover large geographic areas with various communication facilities such as long distance telephone service, satellite transmission, and under-sea cables. These networks cover areas such as:

- Large city or metropolitan area
- Whole country
- Many countries and continents

Examples of WANs are interstate banking networks and airline reservation systems.

3.6.2 Functional Based Classification

A. **Client-Server Networking**

Client/Server (C/S) Networks: Client/server networks have become predominate information architecture of enterprise computing. Computing power has rapidly become distributed and interconnected throughout many organizations by networked computer systems that take the form of client/server networks. The Client/Server computing is an environment that satisfies the business need buy appropriate allocating the application processing between the client and the server processors.

Client/Server network is a computer network in which one centralized powerful computer (called Server) is connected to many less powerful PCs or workstations (called Clients). The clients run programs and access data that are stored on the server. Example – WWW/E-Mail.

- **Client:** A client is a single-user workstation that provides a presentation services and the appropriate computing, connectivity and the database services relevant to the business need. Client computers can be classified as **Fat Client, Thin Client or Hybrid Client.**
  - **Fat / Thick Client:** A **fat client** or **thick client** is a client that performs the bulk of any data processing operations itself, and does not necessarily rely on the server. Unlike thin clients, thick clients do not rely on a central processing server because the processing is done locally on the user system, and the server is accessed primarily for storage purposes. For that reason, thick clients often are not well-suited for public environments. To maintain a thick client, IT needs to maintain all systems for software deployment and upgrades, rather than just maintaining the applications on the server. For example – Personal Computer.
  - **Thin Client: Thin clients** use the resources of the host computer. A thin client generally only presents processed data provided by an application server, which performs the bulk of any required data processing. A thin client machine is going to communicate with a central processing server, meaning there is

little hardware and software installed on the user's machine. A device using web application (such as Office Web Apps) is a thin client.

- **Hybrid Client:** A **Hybrid Client** is a mixture of the above two client models. Similar to a fat client, it processes locally, but relies on the server for storing persistent data. This approach offers features from both the fat client (multimedia support, high performance) and the thin client (high manageability, flexibility). Hybrid clients are well suited for video gaming.

- **Server:** A **server** is one or more multi-user processors with shared memory providing computing, connectivity and the database services and the interfaces relevant to the business need.

Working of a Client/Server Network: A typical Client/Server architecture has been shown in the Fig. 3.6.1.

- Servers are typically powerful computers running advanced network operating systems. Servers can host e-mail; store common data files and serve powerful network applications such as Microsoft's SQL Server. As a centerpiece of the network, the server validates login to the network and can deny access to both networking resources as well as client software.
- End user Personal Computer or Network Computer workstations are the Clients.
- Clients are interconnected by local area networks and share application processing with network servers, which also manage the networks. Client and Server can operate on separate computer platforms.
- Either the client platform or the server platform can be upgraded without having to upgrade the other platform.
- The server is able to service multiple clients concurrently; in some client/server systems, clients can access multiple servers.
- Action is usually initiated at the client end, not the server end.
- The network system implemented within the client/server technology is commonly called by the computer industry as **Middleware**. Middleware is all the distributed software needed to allow clients and servers to interact. General Middleware allows for communication, directory services, queuing, distributed file sharing, and printing.

A typical Client/Server architecture looks like Fig. 3.6.1.

Some of the prominent characteristics of C/S architecture are as follows:

- **Service:** C/S provides a clean separation of function based on the idea of service. The server process is a provider of services and the client is a consumer of services.

- Shared Resources: A server can service many clients at the same time and regulate their access to the shared resources.
- Transparency of Location: C/S software usually masks the location of the server from the clients by redirecting the service calls when needed.
- Mix-and-Match: The ideal C/S software is independent of hardware or Operating System software platforms.
- Scalability: In a C/S environment, client workstations can either be added or removed and also the server load can be distributed across multiple servers.
- Integrity: The server code and server data is centrally managed, which results in cheaper maintenance and the guarding of shared data integrity. At the same time, the clients remain personal and independent.

Issues in Client/Server Network

(i) When the server goes down or crashes, all the computers connected to it become unavailable to use.

(ii) Simultaneous access to data and services by the user takes little more time for server to process the task.

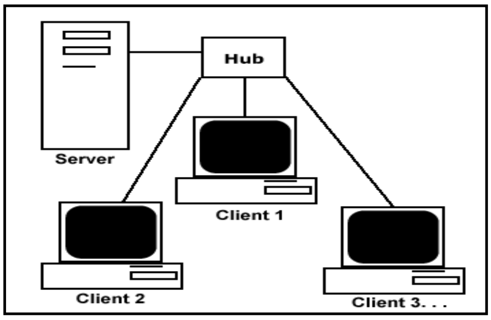


Fig. 3.6.1: Client/Server Components

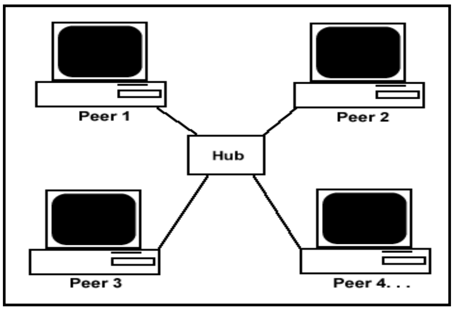


Fig. 3.6.2: Peer-to-Peer Architecture

B. Peer-to-Peer Networking (P2P)

Peer-to-Peer Network: A Peer-to-Peer (P2P) network is created with two or more PCs connected together and share resources without going through a separate server computer. A P2P network can be an ad hoc connection - a couple of computers connected via a universal serial bus to transfer files. A P2P network also can be a permanent infrastructure that links half-dozen computers in a small office over copper wires. Example – Napster, Freenet etc. Refer to the Fig. 3.6.2.

The prime objective goal of a P2P (Peer-to-Peer) file-sharing network is that many computers come together and pool their resources to form a content distribution system. The computers are often simply home computers. They do not need to be machines in

Internet data centers. The computers are called peers because each one can alternately act as a client to another peer, fetching its content, and as a server, providing content to other peers. Though there is no dedicated infrastructure, P2P networks handle a very high volume of file sharing traffic by distributing the load across many computers on the Internet. Everyone participates in the task of distributing content, and there is often no central point of control.

Configured computers in P2P workgroups allow sharing of files, printers and other resources across all of the devices. Peer networks allow data to be shared easily in both directions, whether for downloads to the computer or uploads from the computer. Because they do not rely exclusively on central servers, P2P networks both scale better and are more resilient than client-server networks in case of failures or traffic bottlenecks. A P2P network can be a network on a much grander scale in which special protocols and applications set up direct relationships among users over the Internet.

Advantages

Following are the major advantages of Peer-to-Peer networks:

(i) Peer-to-Peer Networks are easy and simple to set up and only require a Hub or a Switch to connect all the computers together.

(ii) It is very simple and cost effective.

(iii) If one computer fails to work, all other computers connected to it continue to work.

Disadvantages

The major disadvantages of peer-to-peer networks are as below:

(i) There can be problem in accessing files if computers are not connected properly.

(ii) It does not support connections with too many computers as the performance gets degraded in case of high network size.

(iii) The data security is very poor in this architecture.

C. Multi-Tier Architecture

A tier is a distinct part of hardware or software.

a. Single Tier Systems/ One-Tier Architecture

A single computer that contains a database and a front-end (GUI) to access the database is known as Single Tier System. Generally, this type of system is used in small businesses. Fig. 3.6.3 shows single tier architecture.

One-tier architecture involves putting all of the required components for a software application or technology on a single server or platform. This kind of architecture is often contrasted with multi-tiered architecture or the three-tier architecture that's used for some

Web applications and other technologies where various presentation, business and data access layers are housed separately. There is one computer which stores all of the company's data on a single database. The interface used to interact with the database may be part of the database or another program which ties into the database itself.

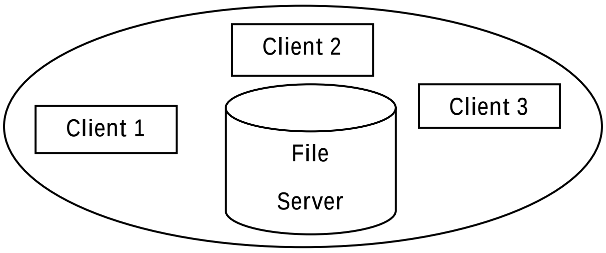


Fig. 3.6.3: Single Tier Architecture

Advantages: A single-tier system requires only one stand-alone computer. It a lso requires only one installation of pr oprietary software which makes it the most cost-effective system available.

Disadvantages: It can be used by only one user at a ti me. A single tier system is impractical for an or ganization which requires two or more users to interact with the organizational data stores at the same time.

b. Two Tier Systems/ Two Tier Architecture

A two-tier system consists of a client and a server. A two-tier architecture is a software architecture in which a presentation layer or interface runs on a client, and a data layer or data structure gets stored on a server. In other words, the database is stored on the server, and the interface used to access the database is installed on the client.

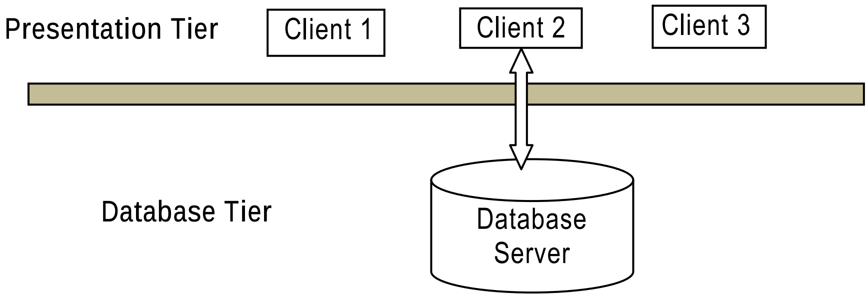


Fig. 3.6.4: Two Tier Architecture

Separating these two components into different locations represents two-tier architecture, as opposed to single-tier architecture. Other kinds of m ulti-tier architectures add additional layers in distributed software design. The user system interface is usually located in the user's desktop environment and the database management services are usually in a server that is more powerful machine that services many clients. Refer Fig. 3.6.4.

The advantages of Two-Tier systems are as follows:

- The system performance is higher because business logic and database are physically close.
- Since processing is shared between the client and server, more users could interact with system.
- By having simple structure, it is easy to setup and maintain entire system smoothly.

The disadvantages of Two-Tier systems are as follows:

- Performance deteriorates if number of users increases.
- There is restricted flexibility and choice of DBMS, since data language used in server is proprietary to each vendor.

c. n-Tier Architecture

n-Tier Architecture is a client–server architecture in which presentation, application processing, and data management functions are logically separated. By segregating an application into tiers, developers acquire the option of modifying or adding a specific layer, instead of reworking the entire application. For example, an application that uses middleware to service data requests between a user and a database employs multi-tier architecture. The most widespread use of multi-tier architecture is the Three-tier architecture.

Three Tier Architecture

Three-tier architecture is a client-server architecture in which the functional process logic, data access, computer data storage and user interface are developed and maintained as independent modules on separate platforms. Three-tier architecture is a software design pattern and well-established software architecture. Its three tiers are the presentation tier, application tier and data tier. The three tier architecture is used when an effective distributed client/server design is needed that provides (when compared to the two-tier) increased performance, flexibility, maintainability, reusability and scalability, while holding the complexity of distributed processing from the user.

As shown in the Fig. 3.6.5, the three tiers in three-tier architecture are as follows:

i. Presentation Tier: Occupies the top level and displays information related to services available on a website. This tier communicates with other tiers by sending results to the browser and other tiers in the network.

ii. Application Tier: Also called the middle tier, logic tier, business logic or logic tier, this tier is pulled from the presentation tier. It controls application functionality by performing detailed processing.

iii. Database Tier: This tier houses the database servers where information is stored and retrieved. Data in this tier is kept independent of application servers or business logic.

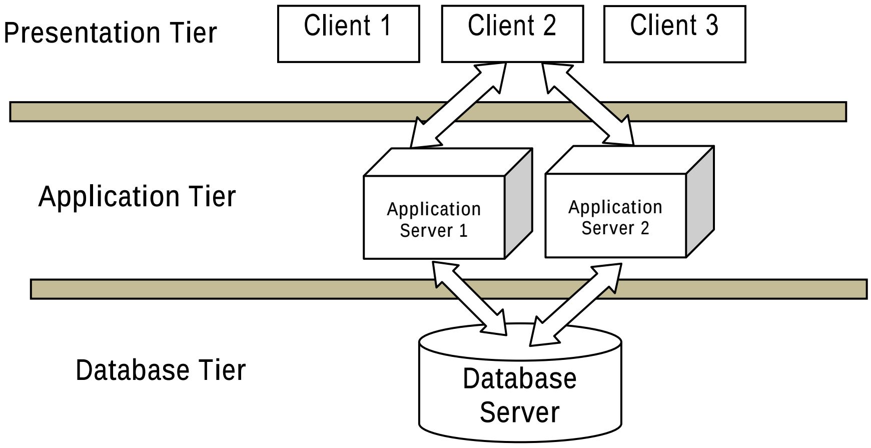


Fig. 3.6.5: Three-Tier Architecture

The following are the advantages of Three-Tier systems:

- Clear separation of user-interface-control and data presentation from application-logic: Through this separation more clients are able to have access to a wide variety of server applications. The two main advantages for client-applications are quicker development through the reuse of pre-built business-logic components and a shorter test phase.
- Dynamic load balancing: If bottlenecks in terms of performance occur, the server process can be moved to other servers at runtime.
- Change management: It is easy and faster to exchange a component on the server than to furnish numerous PCs with new program versions.

The disadvantages of Three-Tier systems are as below:

- It creates an increased need for network traffic management, server load balancing, and fault tolerance.
- Current tools are relatively immature and are more complex.
- Maintenance tools are currently inadequate for maintaining server libraries. This is a potential obstacle for simplifying maintenance and promoting code reuse throughout the organization.

3.6.3 Ownership Based Classification

A. Public Data Network: A Public Data Network is defined as a network shared and accessed by users not belonging to a single organization. It is a network established and operated by a telecommunications administration, or a recognized private operating agency, for the specific purpose of providing data transmission services for the public. The Internet is an example of a Public Data Network.

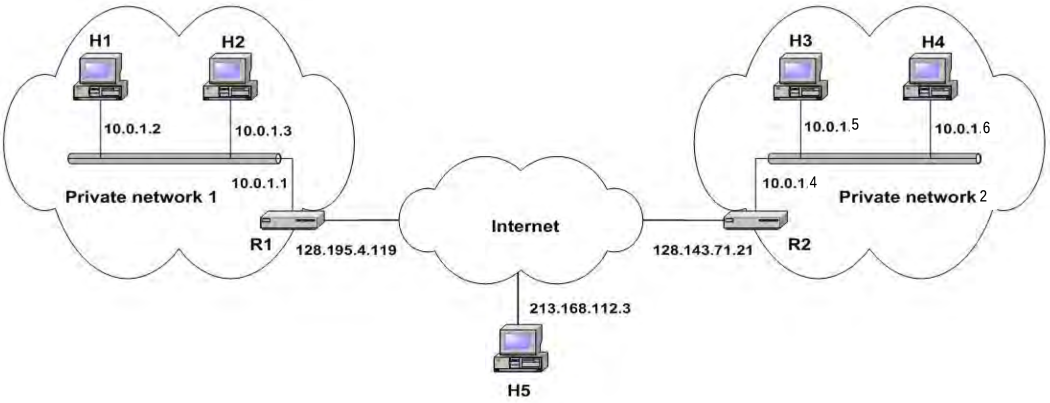


Fig. 3.6.6: Public vs. Private Network

B. Private Data Network: Private Data Networks provide businesses, government agencies and organizations of all sizes as a dedicated network to continuously receive and transmit data critical to both the daily operations and mission critical needs of an organization.

Fig. 3.6.6 displays the difference between Private and Public Data Networks.

C. Virtual Private Networks (VPN): Many companies have offices and plants scattered over many cities, sometimes over multiple countries. In the olden days, before public data networks, it was common for such companies to lease lines from the telephone company between some or all pairs of locations. Private networks work fine and are very secure. If the only lines available are the leased lines, no traffic can leak out of company locations and intruders have to physically wiretap the lines to break in, which is not easy to do. The problem with private networks is that leasing a dedicated line between two is too expensive.

This demand soon led to the innovation of VPNs (Virtual Private Networks), which are overlay networks on top of public networks but with most of the properties of private networks. They are called ''virtual'' because they are merely an illusion, just as virtual.

Many organizations use Virtual Private Networks (VPNs) to establish secure intranets and extranets. A VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. The VPN uses "virtual" connections routed through the In ternet from the business's private network to the remote site or employee. By using a VPN, businesses ensure security - anyone intercepting the encrypted data can't read it.

VPN is a secure network that uses the Internet as its main backbone network, but relies on the firewalls and other security features of the Internet and Intranet connections and those of participating organizations.

3.7 Network Computing

The growing reliance on the computer hardware, software, and data resources of the Internet, Intranets, extranets, and other networks has emphasized that for many users "the network is the computer". Fig. 3.7.1 depicts network computing model. This network computing, or network-centric, concept views networks as the central computing resource of any computing environment. Features of network computing include the following:

- In Network Computing, network computers and other thin clients provide a browser-based user interface for processing small application programs called applets. Thin clients include network computers, Net PCs, and other low-cost network devices or information appliances.

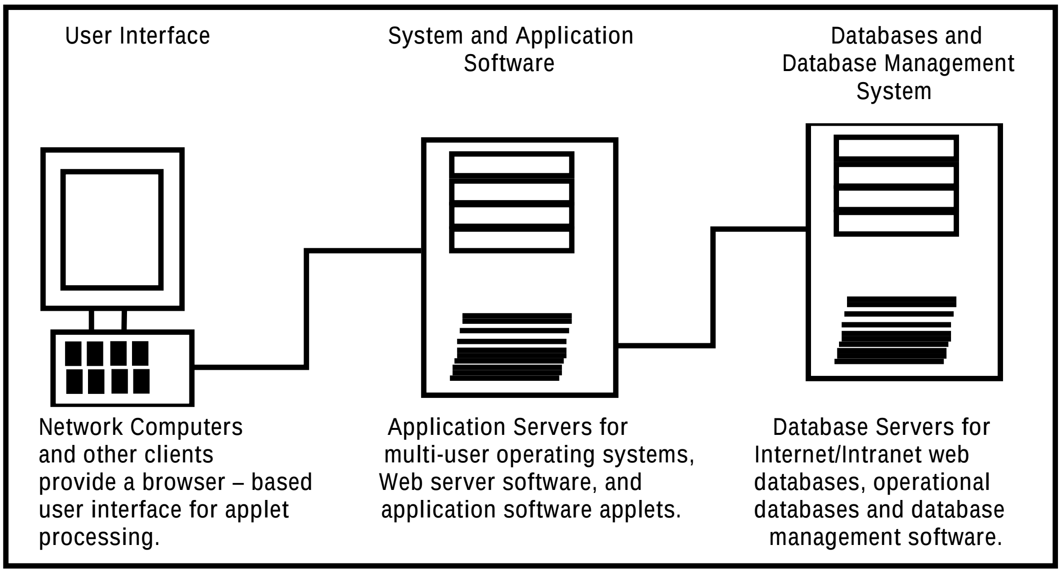

User Interface
System and Application Software
Databases and Database Management System
Network Computers and other clients provide a browser – based user interface for applet processing.
Application Servers for multi-user operating systems, Web server software, and application software applets.
Database Servers for Internet/Intranet web databases, operational databases and database management software.

Fig. 3.7.1: Network Computing Model*

- Network computers are microcomputers without floppy or hard disk drives that are designed as low-cost networking computing devices.

* "Introduction to Information Systems" by James O'Brien, George M. Marakas, 11th edition, McGraw Hill, Page No. 242

- Application and database servers provide the operating system, application software, applets, databases, and database management software needed by the end users in the network.

  After we have all the necessary pre-requisites for network communication, a structure must be put in place that organizes the way communication and sharing occurs on the basis of which many models are recognized. The two basic models of computing are discussed as below:

  - Centralized Computing: Centralized computing is computing done at a central location, using terminals that are attached to a central computer. The computer itself may control all the peripherals directly (if they are physically connected to the central computer), or they may be attached via a terminal server. It offers greater security over decentralized systems because all of the processing is controlled in a central location. In addition, if one terminal breaks down, the user can simply go to another terminal and log in again, and all of their files will still be accessible. Depending on the system, they may even be able to resume their session from the point they were at before, as if nothing had happened.

    This type of arrangement does have some disadvantages.

    - The central computer performs the computing functions and controls the remote terminals. This type of system relies totally on the central computer. Should the central computer crash, the entire system will "go down" (i.e. will be unavailable).

    - Central computing relies heavily on the quality of administration and resources provided to its users. Should the central computer be inadequately supported by any means (e.g. size of home directories, problems regarding administration), then your usage will suffer greatly.

    The reverse situation, however, (i.e., a system supported better than your needs) is one of the key advantages to centralized computing.

  - Decentralized Computing: Decentralized computing is the allocation of resources, both hardware and software, to each individual workstation, or office location. In contrast, centralized computing exists when the majority of functions are carried out, or obtained from a remote centralized location. A collection of decentralized computers systems are components of a larger computer network, held together by local stations of equal importance and capability. These systems are capable of running independently of each other. Decentralized systems enable file sharing and all computers can share peripherals such as printers and scanners as well as modems, allowing all the computers in the network to connect to the internet.

However, in case of up-gradation, all computers have to be updated individually with new software, unlike a centralized computer system.

3.7.1 Network Topology

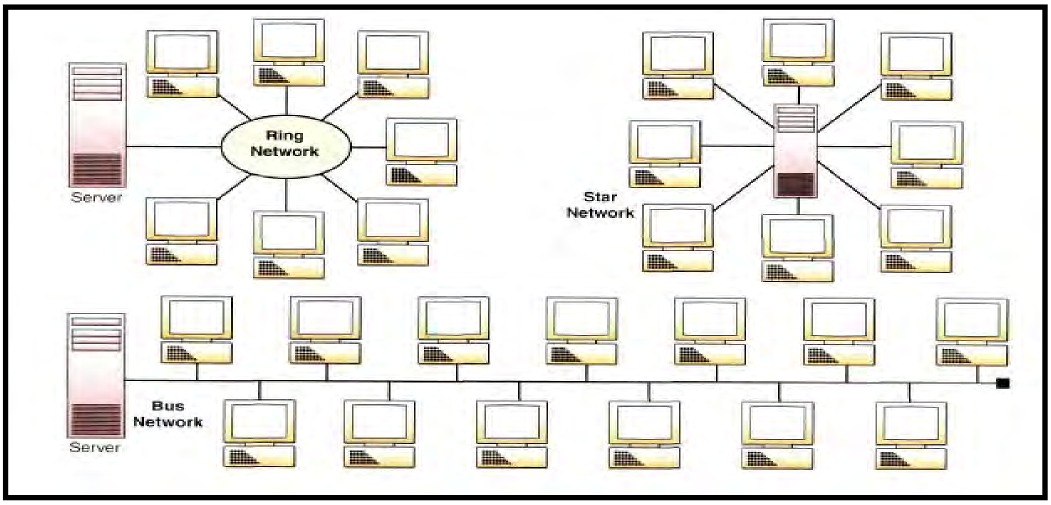


Fig. 3.7.2: Ring, Star and Bus Topologies*

The term 'Topology' defines the physical or logical arrangement of links in a network. It is the geometric representation of the relationship of all the links and linking devices (usually called Nodes) to each other. There are several basic types of network topologies, or structures, in telecommunications networks as shown in the Fig. 3.7.2. Four basic topologies used in wide area and local area telecommunications networks are as follows:

- Star network
- Ring network
- Bus network
- Mesh Network

A. Star Network: The star network, a popular network configuration, involves a central unit that has a number of terminals tied into it. The characteristics of a star network are:

- It ties end user computers to a central computer.
- The central unit in the star network acts as the traffic controller among all the other computers tied to it. The central computer is usually a mainframe (host), which acts as the file server.
- A star network is well suited to companies with one large data processing facility shared by a number of smaller departments. Many star networks take the form of hierarchical networks with a centralized approach.

* "Introduction to Information Systems" by James O'Brien, George M. Marakas, 11th edition, McGraw Hill, Page No.254

Advantages of the star network include the following:

- Several users can use the central unit at the same time.
- It is easy to add new nodes and remove existing nodes.
- A node failure does not bring down the entire network.
- It is easier to diagnose network problems through a central hub.

Disadvantages of the star network are as follows:

- The whole network is affected if the main unit "goes down," and all communications stop.
- Considered less reliable than a ring network, since the other computers in the star are heavily dependent on the central host computer. If it fails, there is no backup processing and communications capability and the local computers will be cut off from the corporate headquarters and from each other.
- Cost of cabling the central system and the points of the star network together are very high.

B. Bus Network: In a bus network, a single length of wire, cable, or optical fiber connects a number of computers. The features of a bus network are as follows:

- All communications travel along this cable, which is called a bus.
- Bus networks have a decentralized approach.

Advantages of bus network include the following:

- There is no host computer or file server, which makes bus network reliable as well as easy to use and understand.
- If one of the microcomputers fails, it will not affect the entire network.
- Requires the least amount of cable to connect the computers together and therefore is less expensive than other cabling arrangements.
- Is easy to extend. Two cables can be easily joined with a connector, making a longer cable for more computers to join the network.
- A repeater can also be used to extend a bus configuration.

Disadvantages of bus network include the following:

- Heavy network traffic can slow a bus considerably since any computer can transmit at any time. But networks do not coordinate when information is sent. Computers interrupting each other can use a lot of bandwidth.
- Each connection between two cables weakens the electrical signal.
- The bus configuration can be difficult to troubleshoot. A cable break or malfunctioning computer can be difficult to find and can cause the whole network to stop functioning.

C. Ring Network: A ring network is much like a bus network, except the length of wire, cable, or optical fiber connects to form a loop. The characteristics of a ring network are:

- Local computer processors are tied together sequentially in a ring with each device being connected to two other devices.
- A ring network has a decentralized approach.
- When one computer needs data from another computer, the data is passed along the ring.
- Considered more reliable and less costly than star networks because if one computer fails, the other computers in the ring can continue to process their own work and communicate with each other.

Advantages of ring network include the following:

- Ring networks do not require a central computer to control activity nor does it need a file server.
- Each computer connected to the network can communicate directly with the other computers in the network by using the common communication channel, and each computer does its own independent applications processing.
- The ring network is not as susceptible to breakdowns as the star network, because when one computer in the ring fails, it does not necessarily affect the processing or communications capabilities of the other computers in the ring.
- Ring networks offer high performance for a small number of workstations or for larger networks where each station has a similar workload.
- Ring networks can span longer distances than other types of networks.
- Ring networks are easily extendable.

Disadvantages of ring network are as follows:

- Relatively expensive and difficult to install.
- Failure of one computer on the network can affect the whole network.
- It is difficult to troubleshoot a ring network.
- Adding or removing computers can disrupt the network.

D. Mesh Network: In this structure, there is random connection of nodes using communication links. A mesh network may be fully connected (as shown in Fig 3.7.3) or connected with only partial links. In fully interconnected topology, each node is connected by a dedicated point to point link to every node. The reliability is very high as there are always alternate paths available if direct link between two nodes is down or dysfunctional. Fully connected networks are not very common because of the high cost. Only military installations, which need high degree of redundancy, may have such networks, that too with a small number of nodes.

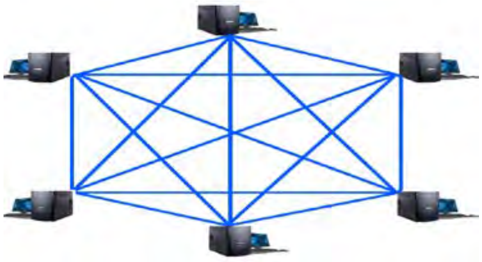


Fig. 3.7.3: Mesh Network

Advantages of mesh network are as under:

- Yields the greatest amount of redundancy in the event that if one of the nodes fails, the network traffic can be redirected to another node.
- Network problems are easier to diagnose.

Disadvantage of mesh network is its high cost of installation and maintenance (more cable is required than any other configuration).

3.7.2 Digital Data Transmission

Binary data, consisting of 1s and 0s, may be organized into groups of n bits each. Computers produce and consume data in groups of bits such as we conceive of and use spoken language in the form of words rather than letters. A given transmission on a communication channel between two machines can be accomplished either in **Parallel mode** or **Serial mode**. Further, while there is only one way to send parallel data, there are two subclasses of serial transmission: **Asynchronous** and **Synchronous**. (As listed in Fig. 3.7.4)

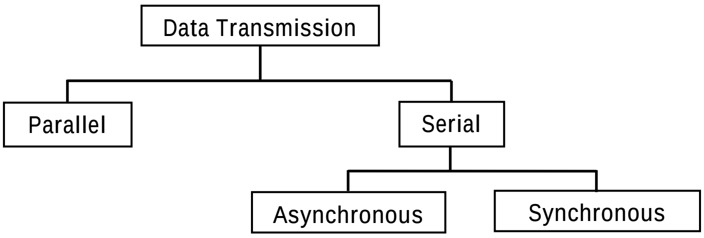


Fig. 3.7.4: Data Transmission

A. **Serial versus Parallel Transmission:** The transmission of binary data across a link can be accomplished either in **Serial Mode** or **Parallel Mode**.

- **Parallel Transmission:** In Parallel transmission, there are separate parallel paths corresponding to each bit of the byte so that all character bits are transmitted simultaneously as shown in Fig 3.7.5. Centronic port is the example of parallel port used for printer.

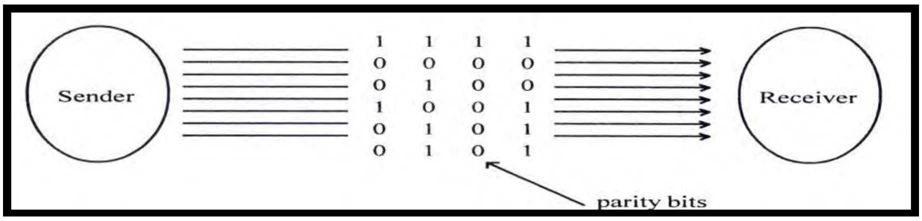


Fig. 3.7.5: Parallel Transmission

- Serial Transmission: In serial transmission, the bits of each byte are sent along a single path one after another as illustrated in Fig 3.7.6. As one bit follows another, so only one communication channel is required between two communicating devices. RS-232 is an example of serial port used for the mouse or MODEM.

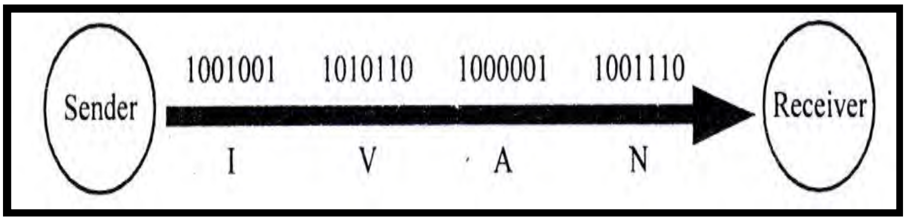


Fig. 3.7.6: Serial Transmission

Table 3.7.1 highlights major differences between Serial Transmission and Parallel Transmission.

Table 3.7.1: Serial Transmission versus Parallel Transmission

S.No	Serial Transmission	Parallel Transmission
1	In this, the data bits are transmitted serially one after another.	In this, the data bits are transmitted simultaneously.
2	Data is transmitted over a single wire.	Data is transmitted over 8 different wires.
3	It is a cheaper mode of transferring data.	It is relatively expensive mode of transferring data.
4	It is useful for long distance data transmissions.	Not practical for long distance communications as it uses parallel paths, so cross talk may occur.
5	It is relatively slower.	It is relatively faster.

As in serial connections, wherein a single wire transports the data, the problem is how to synchronize the transmitter and receiver, in other words, the receiver can not necessarily distinguish the characters (or more generally the bit sequences) because the bits are sent one after the other. When a computer sends the data bits and parity bit down the same communication channel, the data are grouped together in predetermined bit patterns for the receiving devices to recognize when each byte (character) has been transmitted. There are two basic ways of transmitting serial binary data that addresses the problem of sequencing and re-arranging of data at receiver end: Asynchronous and Synchronous. There are two types of transmission that address this problem:

- Asynchronous Transmission: In this, each character is sent at irregular intervals in time as in the case of characters entered at the keyboard in real time. So, the sender provides a synchronization signal to the receiver before starting the transfer of each message. For example, imagine that a single byte is transmitted during a long period of silence... the receiver will not be able to know if this is 00010000, 10000000 or 00000100. To correct this problem, each character is preceded by some information indicating the start of character transmission by start-of-transmission information (called a START bit usually 0) and ends by sending end-of-transmission information (called STOP bit usually 1), as shown in Fig 3.7.7.

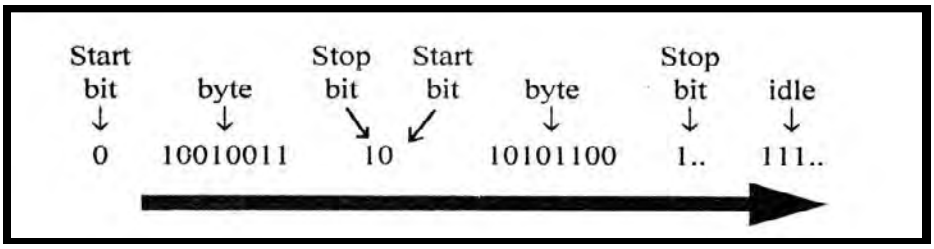


Fig. 3.7.7: Asynchronous Transmission

- Synchronous Transmission: In this, the transmitter and receiver are paced by the same clock. The receiver continuously receives (even when no bits are transmitted) the information at the same rate the transmitter sends it. This is why the transmitter and receiver are paced at the same speed. In addition, supplementary information is inserted to guarantee that there are no errors during transmission, as shown in Fig 3.7.8.

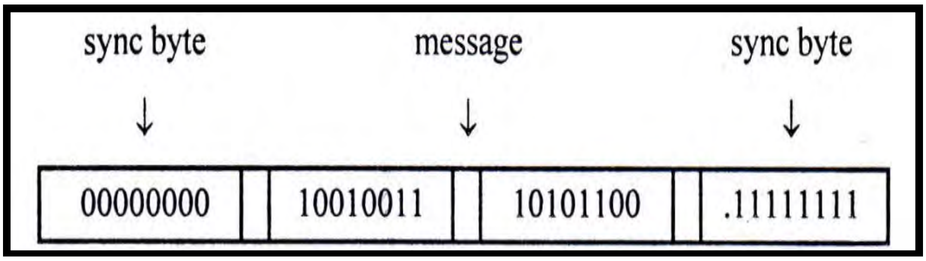


Fig. 3.7.8: Synchronous Transmission

A group of synchronization bits must be placed at the beginning and ending of each block to maintain synchronization.

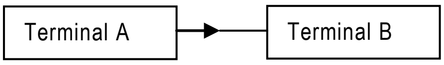
Table 3.7.2 lists the differences between Asynchronous and Synchronous Transmission.

Table 3.7.2: Asynchronous vs Synchronous Transmission

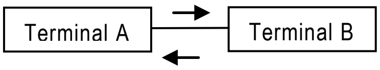
S.No.	ASYNCHRONOUS TRANSMISSION	SYNCHRONOUS TRANSMISSION
1	Each data word is accompanied by Start and Stop bits.	Allows characters to be sent down the line without Start-Stop bits.
2	Extra Start and Stop bits slow down the transmission process relatively.	Transmission is faster as in absence of Start and Stop bits, many data words can be transmitted per second.
3	It is relatively cheaper as it requires less hardware.	The synchronous device is more expensive to build as it must be smart enough to differentiate between the actual data and the special synchronous characters.
4	More reliable as the Start and Stop bits ensure that the sender and the receiver remain in step with one another.	Chances of data loss are relatively higher.
5	It is less efficient as it is relatively more complex.	It is more efficient and has greater throughput.

B. Transmission Mode: The Transmission Mode is used to define the direction of signal flow between two linked devices. There are three types of transmission modes characterized according to the direction of the exchanges: Simplex, Half-Duplex and Duplex.

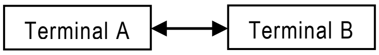
- Simplex: In Simplex mode, the data flows in only one direction (ie.. unidirectional) from the transmitter to the receiver. This type of connection is useful if the data do not need to flow in both directions. For example, Keyboards can only introduce input and printer can only receive the data.



- Half-Duplex: In Half-Duplex mode, (sometimes called an alternating connection or semi-duplex) the data flows in one direction or the other, but not both at the same time. This type of connection makes it possible to have bidirectional communications using the full capacity of the line. For example: Walkie Talkie. In this, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.



- Full-Duplex: In Full-Duplex mode, the data flows in both directions simultaneously. Each end of the line can thus transmit and receive at the same time, which means that the bandwidth is divided in two for each direction of data transmission if the same transmission medium is used for both directions of transmission. For example: Mobile Phones. In this, signals going in either direction share the capacity of the link wither by containing two separate physical links (one for sending and the other for receiving) or by dividing the capacity of the channel between signals travelling in opposite direction.



C. Transmission Techniques: A communication network consists of a collection of devices (or nodes) that wish to communicate and interconnect together. The primary objective in any communication network is simply moving information from one source to one or more destination nodes. Based on the techniques used to transfer data, communication networks can be categorized into Broadcast and Switched networks.

- Broadcast Networks - In Broadcast networks, data transmitted by one node is received by many, sometimes all, of the other nodes as shown in the Fig. 3.7.9. This refers to a method of transferring a message to all recipients simultaneously. For example – a corporation or other voluntary association, that provides live television or recorded content such as movies, newscasts, sports, public affairs programming, and other television programs for broadcast over a group of radio stations or television stations.

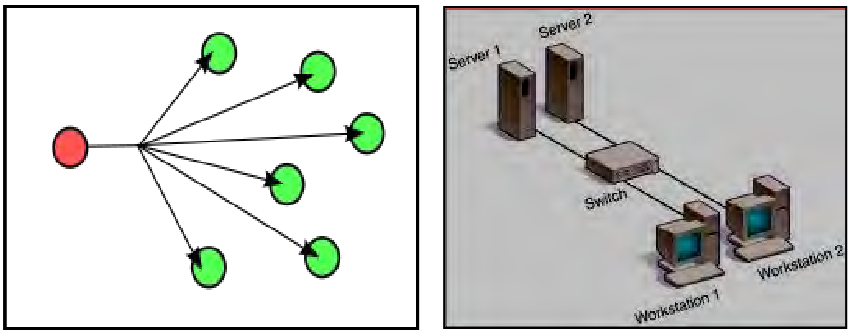


Fig. 3.7.9: Broadcast and Switched networks respectively

- Switched Networks - In switched-communication networks, the data transferred from source to destination is routed through the switch nodes as shown in the Fig. 3.7.9. The way in which the nodes switch data from one link to another, as it is transmitted from source to destination node, is referred to as a switching technique. Three common switching techniques are Circuit Switching, Packet Switching, and Message Switching.

  (i) Circuit Switching: A Circuit Switching network is one that establishes a fixed bandwidth circuit (or channel) between nodes and terminals before the users may communicate, as if the nodes were physically connected with an electrical circuit. The route is dedicated and exclusive, and released only when the communication session terminates. Circuit switching is what most of us encounter on our home phones. A single circuit is used for the entire duration of the call. Applications which use circuit switching go through three phases: Establish a Circuit, Transfer of data and Disconnect the Circuit.

(ii) Packet Switching: It is a sophisticated means of maximizing transmission capacity of networks. Packet switching refers to protocols in which messages are broken up into small transmission units called packets, before they are sent. Each packet is transmitted individually across the net. The packets may even follow different routes to the destination. Since there is no fixed path, different packets can follow different path and thus they may reach to destination out of order.

(iii) Message Switching: In message switching, end-users communicate by sending each other a message, which contains the entire data being delivered from the source to destination node. As a message is routed from its source to its destination, each intermediate switch within the network stores the entire message, providing a very reliable service. The intermediary nodes (switches) have the responsibility of conveying the received message from one node to another in the network. Therefore, each intermediary node within the network must store all messages before retransmitting them one at a time as proper resources become available. This characteristic is often referred to as Store-and-Forward. Electronic mail (e-mail) and voice mail are examples of message switching systems.

3.7.3 Network Architectures and Protocols

Network Architecture: Network Architecture refers to the layout of the network consisting of the hardware, software, connectivity, communication protocols and mode of transmission, such as wired or wireless. The diagram of the network architecture provides a full picture of the established network with detailed view of all the resources accessible.

In other words, Network Architecture includes hardware components used for communication, cabling and device types, network layout and topologies, physical and wireless connections, implemented areas and future plans. In addition, the software rules and protocols also constitute to the network architecture. This architecture is always designed by a network manager/administrator with coordination of network engineers and other design engineers.

The goal of network architecture is to promote an open, simple, flexible, and efficient telecommunications environment. This is accomplished by the use of Standard protocols; Standard communications hardware and software interfaces; and standard multilevel interface between end users and computer systems.

The network architecture of the Internet is predominantly expressed by its use of the Internet Protocol Suite, rather than a specific model for interconnecting networks or nodes in the network, or the usage of specific types of hardware links.

Protocols: **Protocols** are software that performs a variety of actions necessary for data transmission between computers. Stated more precisely, protocols are a set of rules for inter-computer communication that have been agreed upon and implemented by many vendors, users and standards bodies to ensure that the information being exchanged between the two parties is received and interpreted correctly. Ideally, a protocols standard allows heterogeneous computers to talk to each other.

At the most basic level, protocols define the physical aspects of communication, such as how the system components will be interfaced and at what voltage levels will be transmitted.

At higher levels, protocols define the way that data will be transferred, such as the establishment and termination of "sessions" between computers and the synchronization of those transmissions. At still higher levels, protocols can standardize the way data itself is encoded and compressed for transmission. Thus we can say that, Network protocols which are essentially software are sets of rules for-

- ♦ Communicating timings, sequencing, formatting, and error checking for data transmission.
- ♦ Providing standards for data communication.

A **protocol** defines the following three aspects of digital communication.

(a) **Syntax:** The format of data being exchanged, character set used, type of error correction used, type of encoding scheme (e.g., signal levels) being used.

(b) **Semantics:** Type and order of messages used to ensure reliable and error free information transfer.

(c) **Timing:** Defines data rate selection and correct timing for various events during data transfer.

As stated earlier, communication protocols are rules established to govern the way the data are transmitted in a computer network. These rules are embedded or built into the software which resides either in – Computer's memory or Memory of transmission device. Different protocols cannot talk to each other hence standard protocols have been structured to resolve the problem. The entire operation of data transmission over a network is broken down into discrete systematic steps. Each step has its own rules or protocol. Steps must be carried out in consistent order for every computer in the network, either receiving or sending data.

At the sending computer, protocols –

(i) Break data down into packets;

(ii) Add destination address to the packet; and

(iii) Prepares data for transmission through Network Interface Card (NIC)

At the receiving computer, protocols –

(i) Take data packets off the cable;

(ii) Bring packets into computer through Network Interface Card (NIC;

(iii) Strip the packets off any transmitting information;

(iv) Copy data from packet to a buffer for reassembly; and

(v) Pass the reassembled data to the application.

A. The OSI Model

The International Standards Organization (ISO) developed a seven-layer Open Systems Interconnection (OSI) model to serve as a standard model for network architectures. Dividing data communications functions into seven distinct layers promotes the development of modular network architectures, which assists the development, operation, and maintenance of complex telecommunications networks. Seven layers of OSI include the following:

♦ Layer 7 or Application Layer: The application layer of OSI layer architecture is closest to the end user, which means that both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications and provides user services by file transfer, file sharing, etc. Database concurrency and deadlock situation controls are undertaken at this layer level. This is the layer at which communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified.

♦ Layer 6 or Presentation Layer: This layer at times referred as Syntax Layer also, is usually a part of an operating system, that converts incoming and outgoing data from one presentation format to another (for example, from a text stream into a popup window with the newly arrived text). The presentation service data units are then encapsulated into Session Protocol Data Units, and moved down the stack. It further controls on screen display of data, transforms data to a standard application interface. Encryption, data compression can also be undertaken at this layer level.

♦ Layer 5 or Session Layer: This layer sets up, coordinates, and terminates conversations, exchanges, and dialogs between the applications at each end. It deals with session and connection coordination. It provides for full-duplex, half-duplex, or simplex operation, and establishes check pointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for "graceful close" of sessions also.

♦ Layer 4 or Transport Layer: This layer ensures reliable and transparent transfer of data between user processes, assembles and disassembles message packets, and provides error recovery and flow control. Multiplexing and encryption are undertaken at this layer level. This means that the Transport Layer can keep track of the segments and retransmit those that fail.

♦ Layer 3 or Network Layer: The Network Layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks, while maintaining the quality of service requested by the Transport Layer. The Network Layer makes a c hoice of the physical route of transmission, creates a virtual circuit for upper layers to make them independent of data transmission and switching, establishes, maintains, terminates connections between the nodes and ensure proper routing of data.

- Layer 2 or Data Link Layer: The Data Link Layer responds to service requests from the Network Layer and issues service requests to the Physical Layer. The Data Link Layer is the protocol layer which transfers data between adjacent network nodes in a wide area network or between nodes on the same local area network segment. This layer is also a hardware layer which specifies channel access control method and ensures reliable transfer of data through the transmission medium. It provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical Layer.
- Layer 1 or Physical Layer: The Physical Layer is a hardware layer which specifies mechanical features as well as electromagnetic features of the connection between the devices and the transmission. In particular, it defines the relationship between a device and a physical medium. This includes the layout of pins, voltages, cable specifications, Hubs, repeaters, network adapters, Host Bus Adapters (HBAs used in Storage Area Networks) and more. The major functions and services performed by the Physical Layer are as follows:
  - Establishment and termination of a connection to a communications medium.
  - Participation in the process whereby the communication resources are effectively shared among multiple users. For example, contention resolution and flow control.
  - Modulation or conversion between the representation of d igital data in user equipment and the corresponding signals transmitted over a communications channel. These are signals operating over the physical cabling (such as copper and optical fiber) or over a radio link.

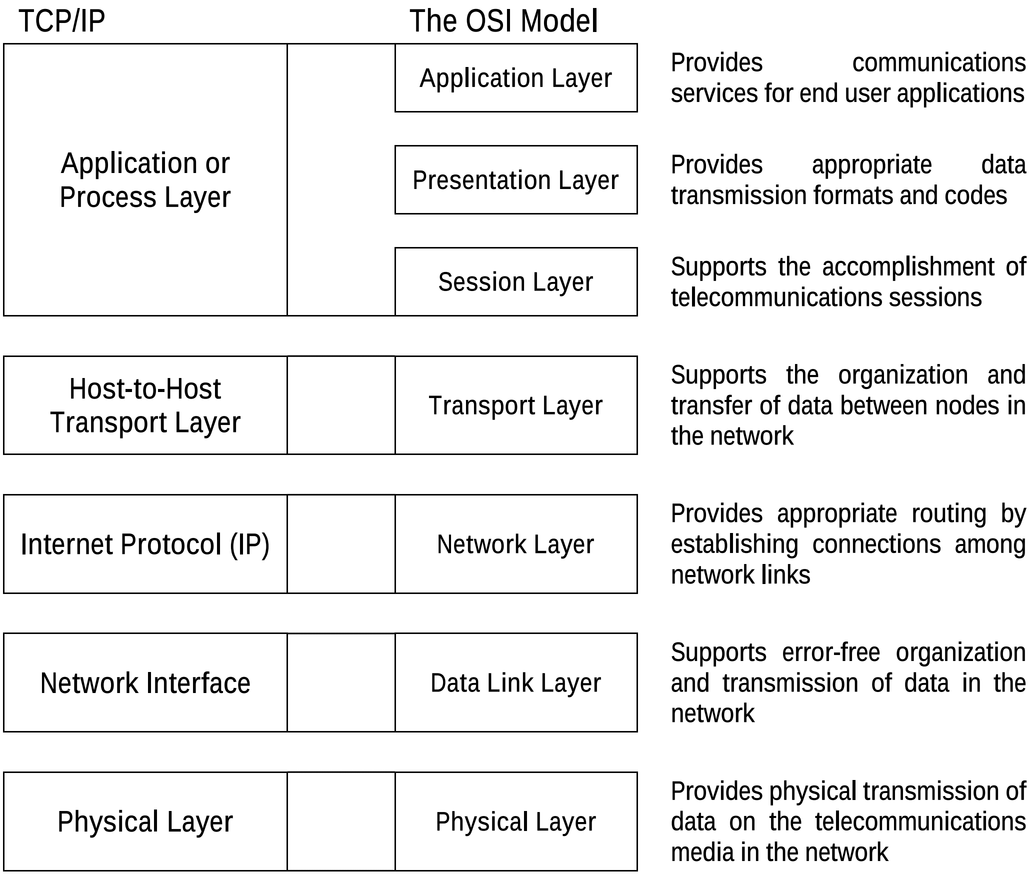
B. Internet's TCP/IP

The Internet uses a system of telecommunications protocols that has become so widely used that it is equivalent to network architecture. The Internet's protocol suite is called Transmission Control Protocol /Internet Protocol and is known as TCP/IP. TCP/IP consists of five levels of protocols that can be related to the seven layers of the OSI architecture. TCP/IP is used by the Internet and by all Intranets and extranets. Many companies and other organizations are also converting their client/server networks to TCP/IP.

Five levels of TCP/IP include as shown in the Fig. 3.7.10 are as follows:

- Application or process layer
- Host-to-Host Transport layer
- Internet Protocol (IP)
- Network Interface

- Physical layer



TCP/IP	The OSI Model	
Application or Process Layer	Application Layer	Provides communications services for end user applications
	Presentation Layer	Provides appropriate data transmission formats and codes
	Session Layer	Supports the accomplishment of telecommunications sessions
Host-to-Host Transport Layer	Transport Layer	Supports the organization and transfer of data between nodes in the network
Internet Protocol (IP)	Network Layer	Provides appropriate routing by establishing connections among network links
Network Interface	Data Link Layer	Supports error-free organization and transmission of data in the network
Physical Layer	Physical Layer	Provides physical transmission of data on the telecommunications media in the network

Fig. 3.7.10: Relationship between layers of TCP/IP and OSI Model*

3.8 Network Risks, Controls and Security

The basic objective for providing network security is two-fold. It is:

(i) to safeguard assets, and

(ii) to ensure and maintain the data integrity.

The boundary subsystem is an interface between the potential users of a system and the system itself. Controls in the boundary subsystem have the following purposes like it is used:

* "Introduction to Information Systems" by James O'Brien, George M. Marakas, 11th edition, McGraw Hill

(i) to establish the system resources that the users desire to employ and

(ii) to restrict the actions undertaken by the users who obtain the system resource to an authorized set.

There are two types of Systems Security.

- Physical Security: A Physical security is implemented to protect the physical systems assets of an organization like the personnel, hardware, facilities, supplies and documentation.
- Logical Security: A Logical security is intended protect data/information and software. Security administrators tend to have responsibility for controls over

  (i) malicious and non-malicious threats to physical security, and

  (ii) malicious threats to logical security itself.

3.8.1 Threats and Vulnerabilities

Threat: A Threat is a possible danger that can disrupt the operation, functioning, integrity, or availability of a network or system. Network security threats can be categorized into four broad themes:

- ♦ Unstructured Threats - These originate mostly from inexperienced individuals using easily available hacking tools from the Internet. Many tools available to anyone on the Internet can be used to discover weaknesses in a company's network. These include port-scanning tools, address-sweeping tools, and many others. Most of these kinds of probes are done more out of curiosity than with a malicious intent in mind.

  For example, if a company's external web site is hacked; the company's integrity is damaged. Even if the external web site is separate from the internal information that sits behind a protective firewall, the public does not know that. All they know is that if the company's web site is hacked, then it is an unsafe place to conduct business.
- ♦ Structured Threats - These originate from individuals who are highly motivated and technically competent and usually understand network systems design and the vulnerabilities of those systems. They can understand as well as create hacking scripts to penetrate those network systems. An individual who presents a structured threat typically targets a specific destination or group. Usually, these hackers are hired by industry competitors, or state-sponsored intelligence organizations.
- ♦ External Threats - These originate from individuals or organizations working outside an organization, which does not have authorized access to organization's computer systems or network. They usually work their way into a network from the Internet or dialup access servers.
- ♦ Internal Threats - Typically, these threats originate from individuals who have authorized access to the network. These users either have an account on a server or physical access to the network. An internal threat may come from a discontented former or current

employee or contractor. It has been seen that majority of security incidents originate from internal threats.

Vulnerability: Vulnerability is an inherent weakness in the design, configuration, or implementation of a network or system that renders it susceptible to a threat.

The following facts are responsible for occurrence of vulnerabilities in the software:

- Software Bugs - Software bugs are so common that users have developed techniques to work around the consequences, and bugs that make saving work necessary every half an hour or crash the computer every so often are considered to be a normal part of computing. For example - buffer overflow, failure to handle exceptional conditions, access validation error, input validation errors are some of the common software flaws.
- Timing Windows - This problem may occur when a temporary file is exploited by an intruder to gain access to the file, overwrite important data, and use the file as a gateway for advancing further into the system.
- Insecure default configurations - Insecure default configurations occur when vendors use known default passwords to make it as easy as possible for consumers to set up new systems. Unfortunately, most intruders know these passwords and can access systems effortlessly.
- Trusting Untrustworthy information - This is usually a problem that affects routers, or those computers that connect one network to another. When routers are not programmed to verify that they are receiving information from a unique host, bogus routers can gain access to systems and do damage.
- End users - Generally, users of computer systems are not professionals and are not always security conscious. For example, when the number of passwords of an user increases, user may start writing them down, in the worst case to places from where they are easy to find. In addition to this kind of negligence towards security procedures users do human errors, for example save confidential files to places where they are not properly protected.

3.8.2 Level of Security

The task of a Security Administration in an organization is to conduct a security program which is a series of ongoing, regular and periodic review of controls exercised to ensure safeguarding of assets and maintenance of data integrity. Security programs involve the following eight steps –

(i) Preparing project plan for enforcing security: The project plan components are at first outlining the objectives of the review followed by in sequence determining the scope of the review and tasks to be accomplished, assigning tasks to the project team after organizing it, preparing resources budget which will be determined by the volume and complexity of the review and fixing a target / schedule for task completion.

(ii) Asset identification: Assets which need to be safeguarded can be identified and subdivided into Personnel, Hardware, Facilities, Documentation, Supplies, Data, Application Software and System Software.

(iii) Asset valuation: This step of valuation of assets can pose a difficulty. The process of valuation can differ depending on who is asked to render the valuation, the way in which the asset can be lost and the period for which it is lost and how old is the asset.

Valuation of physical assets cannot be considered apart from the valuation of the logical assets. For example, the replacement value of the contents in a micro computer's hard disk may be several times more than the replacement value of the disk itself.

(iv) Threat identification: The source of a threat can be external or internal and the nature of a threat can be accidental / non-deliberate or deliberate. The example of a non-deliberate external threat is an act of God, non-deliberate internal threat is pollution, deliberate external threat is hackers, and deliberate internal threat is employees.

(v) Threats probability of occurrence assessment: This step is an assessment of the probability of occurrence of threats over a given time period. This exercise is not so difficult if prior period statistical data is available. If however, prior period data is not available, it has to be elicited from the associated stakeholders like end users (furnishing the data aspect) and the management (furnishing the control aspect).

(vi) Exposure analysis: This step is the Exposures Analysis by first identifying the controls in the place, secondly assessing the reliability of the existing controls, thirdly evaluating the probability that a threat can be successful and lastly assessing the resulting loss if the threat is successful. For each asset and each threat the expected loss can be estimated as the product of the probability of threat occurrence, probability of control failure and the resulting loss if the threat is successful.

(vii) Controls adjustment: The involves the adjustment of controls which means whether over some time period any control can be designed, implemented and operated such that the cost of control is lower than the reduction in the expected losses. The reduction in the expected losses is the difference between expected losses with the (i) existing set of controls and (ii) improved set of controls.

(viii) Report generation outlining the levels of security to be provided for individual systems, end user, etc.: This is the last step that involves report generation documenting, the findings of the review and specially recommending new assets safeguarding techniques that should be implemented and existing assets safeguarding mechanisms that should be eliminated / rectified, and also recommending the assignment of the levels of security to be pervaded for individual end users and systems.

3.8.3 Network Security

Network security is becoming more and more crucial as the volume of data being exchanged on the Internet increases. Based on the increasing demand and expectations, the security involves four aspects: **Privacy (Confidentiality)**, **Message Authentication**, **Message Integrity** and **Non-repudiation.** Network Security Protocols are primarily designed to prevent any unauthorized user, application, service or device from accessing network data. This applies to virtually all data types regardless of the network medium used. Network security protocols generally implement digital signatures, cryptography and encryption techniques.

(a) **Privacy:** This means that the sender and the receiver expect confidentiality. The transmitted message should make sense to only the intended receiver and the message should be un intelligible to un authorized users. This is achieved by cryptography and encryption techniques so that the data is secured and can only be decrypted with a special algorithm, logical key, mathematical formula and/or a combination of all of them.

- ➢ **Cryptography:** Cryptography is the practice and study of t echniques for secure communication in the presence of third parties (called Adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, integrity, authentication, and non-repudiation.

- ➢ **Encryption:** In Cryptography, encryption is the process of encoding messages (or information) in such a w ay that eavesdroppers or hackers cannot read it, but only authorized parties can. Decryption is defined as the recovery of the original message from the encrypted data.

    - **Plaintext -** It is the message that is to be encrypted. It is transformed by a function that is parameterized by a key.

    - **CipherText -** It is the output of the encryption process that is transmitted often by a messenger or radio.

    - **Encryption Model -** The intruder may hear and accurately copies down the complete ciphertext. However, unlike the intended recipient, he does not know what the decryption key is and so cannot decrypt the ciphertext easily. Sometimes the intruder can not only listen to the communication channel (passive intruder) but can also record messages and play them back later, inject his own messages, or modify legitimate messages before they get to the receiver (active intruder). The art of breaking ciphers is known as **Cryptanalysis** and the art of devising them is known as **Cryptography**. Both Cryptanalysis and Cryptography are collectively known as **Cryptology**. Refer to the Fig. 3.8.1.

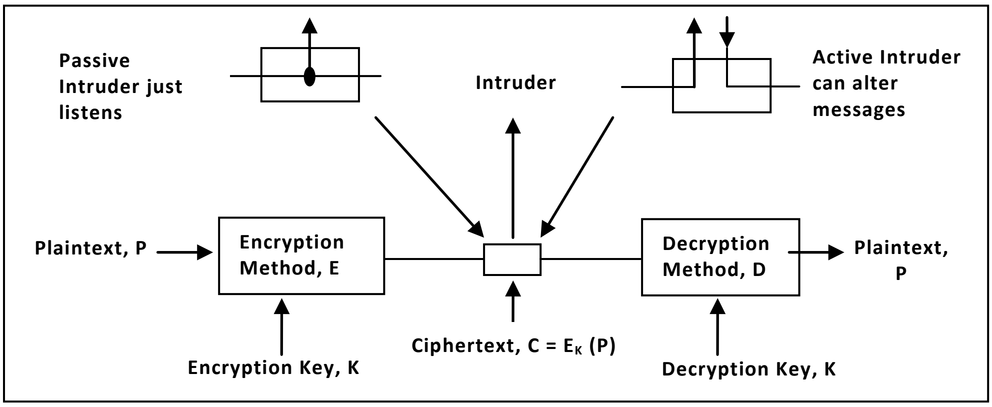


Fig. 3.8.1: Encryption Model

- There are two categories of encryption/decryption methods: the Secret Key Method and the Public Key Method.
  - In Secret key encryption/decryption method, the same key is used by both sender and the receiver. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to d ecrypt the data. In t his, the algorithm used for decryption is the inverse of the algorithm used for encryption.
  - In Public key encryption, there are two keys: a private key and a public key. The private key is kept by the receiver and the public key is announced to the public.
- There are two basic approaches to encryption:
  - Hardware encryption devices are available at a reasonable cost, and can support high- speed traffic. If th e Internet is being used to e xchange information among branch offices or development collaborators, for instance, use of such devices can ensure that all traffic between these offices is secure.
  - Software encryption is typically employed in conjunction with specific applications. Certain electronic mail packages, for example, provide encryption and decryption for message security.

(b) Authentication: This means that the receiver is sure of the sender's identity and that an imposter has not sent the message.

(c) Integrity: This means that the data must arrive at the receiver exactly as it was sent. There must not be any changes during the transmission – either accidental or malicious.

(d) Non-Repudiation: This means that a receiver must be able to prove that a received message came from a specific sender and the sender must not be able to deny sending it.

These can be achieved using Digital Signatures. Public key encryption can be used to sign a document. However, the roles of the public and private key are different. The sender uses her private key to encrypt (sign) the message just as a person uses her signature (which is private in the sense that it is difficult to forge) to sign a paper document, The receiver, on the other hand, uses the public key of the sender to decrypt the message just as a person verifies from memory another person's signature. In digital signature, the private key is used for encryption and the public key for decryption.

3.8.4 Network Security Protocols

Some of the popular network security protocols include Secure Shell (SSH), Secure File Transfer Protocol (SFTP), Secure Hypertext Transfer Protocol (HTTPS) and Secure Socket Layer (SSL) etc.

- SSH - Secure Shell (SSH) is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. SSH protects a network from attacks such as IP spoofing, IP source routing, and DNS spoofing. An attacker cannot play back the traffic or hijack the connection when encryption is enabled. During ssh login, the entire login session, including transmission of password, is encrypted; therefore it is almost impossible for an outsider to collect passwords.
- SFTP – The SSH File Transfer Protocol (also known as Secure FTP or SFTP) is a computing network protocol for accessing and managing files on remote file systems. Unlike standard File Transfer Protocol (FTP), SFTP encrypts commands and data both, preventing passwords and sensitive information from being transmitted in the clear over a network.
- HTTPS – HyperText Transfer Protocol Secure (HTTPS) is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. The security of HTTPS uses long term public and secret keys to exchange a short term session key to encrypt the data flow between client and server.
- SSL – Secure Socket Layer (SSL) is essentially a protocol that provides a secure channel between two machines operating over the Internet or an internal network. In today's Internet focused world, the SSL protocol is typically used when a web browser needs to securely connect to a web server over the inherently insecure Internet. In practice, SSL is used to secure online credit card transactions, system logins and any sensitive information exchanged online, to secure webmail and applications like Outlook Web Access, Exchange and Office Communications Server, to secure the connection

between an email client such as Microsoft Outlook and an email server such as Microsoft Exchange, to secure intranet based traffic such as internal networks, file sharing, extranets, and database connections etc.

3.8.5 Network Security Techniques

As data is shared and organizations become connected to the outside world, the possibility of data exposure to vendors, service providers, and trading partners is significantly increased. In spite of the varied concerns, corporations understand that the Internet is clearly the most promising infrastructure for “anywhere, anytime” electronic communication between businesses, customers, and suppliers; and progress is being made as companies further realize and respond to these concerns. Several tools/technologies are now available to protect information and systems against compromise, intrusion, or misuse. Some of them are as follows:

1. **Intrusion Detection System (IDS):** An **Intrusion Detection System** is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station. The goal of intrusion detection is to monitor network assets to detect anomalous behavior and misuse. IDS are primarily of two types:

   (i) **Network Intrusion Detection (NID):** Network Intrusion Detection System is placed on a network to analyze traffic in search of unwanted or malicious events on the wire between hosts. Typically referred to as "packet-sniffers", network intrusion detection devices intercept packets traveling along various communication mediums and protocols, usually TCP/IP. NNID is a type of NID. The advantage of NNID is its ability to defend specific hosts against packet-based attacks in these complex environments where conventional NID is ineffective.

   (ii) **Host-based Intrusion Detection (HID):** Host-based Intrusion Detection systems are designed to monitor, detect, and respond to user and system activity and attacks on a given host. The difference between host-based and network-based intrusion detection is that NID deals with data transmitted from host to host while HID is concerned with what occurs on the hosts themselves. Host-based intrusion detection is best suited to combat internal threats because of its ability to monitor and respond to specific user actions and file accesses on the host. In other words, HID detects insider misuse while NID detects outsider misuse.

   (iii) **Hybrid Intrusion Detection:** Hybrid Intrusion Detection systems offer management of and alert notification from both network and host-based intrusion detection devices. Hybrid solutions provide the logical complement to NID and HID - central intrusion detection management.

2. **Firewall:** Firewall is a device that forms a barrier between a secure and an open environment when the latter environment is usually considered hostile, for example, the Internet. It acts as a system or combination of systems that enforces a boundary between

more than one networks. Access controls are common form of controls encountered in the boundary subsystem by restricting the use of system resources to authorized users, limiting the actions authorized users can take with these resources and ensuring that the users obtain only authentic system resources.

3. **Network Access Control:** Network Access Control (NAC) products enforce security policy by granting only security policy–compliant devices access to network assets. They handle access authentication and authorization functions and can even control the data that specific users' access, based on their ability to recognize users, their devices and their network roles.
4. **Anti – Malware:** Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses etc. and other malicious programs. Anti-malware network tools help administrators identify block and remove malware. They enable the IT department to tailor its anti-malware policies to identify known and unknown malware sources. Malware is always on the lookout for network vulnerabilities - in security defenses, operating systems, browsers, applications and popular targets such as Adobe Flash, Acrobat and Reader - that they can exploit to fully access a victim's network. Best practices call for a multipronged defense that might also include IP blacklisting, data loss prevention (DLP) tools, anti-virus and anti-spyware software, web browsing policies, egress filtering, and outbound-traffic proxies.
5. **Site Blocking:** It is a software-based approach that prohibits access to certain Web sites that are deemed inappropriate by management. For example, sites that contain explicit objectionable material can be blocked to prevent employee's from accessing these sites from company Internet servers. In addition to blocking sites, companies can also log activities and determine the amount of time spent on the Internet and identify the sites visited.

3.9 Network Administration and Management

In computer networks, **Network Management** refers to the activities, methods, procedures, and tools that pertain to the **Operation**, **Administration**, **Maintenance**, and **Provisioning** of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.

- **Operation** deals with keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot problems as soon as possible, ideally before users are affected.
- **Administration** deals with keeping track of resources in the network and how they are assigned. It includes all the "housekeeping" that is necessary to keep the network under control.

- Maintenance is concerned with performing repairs and upgrades—for example, when equipment must be replaced, when a router needs a pat ch for an op erating system image, when a new switch is added to a network. Maintenance also involves corrective and preventive measures to make the managed network run "better", such as adjusting device configuration parameters.

- Provisioning is concerned with configuring resources in the network to support a given service. For example, this might include setting up the network so that a new customer can receive voice service.

A common way of characterizing network management functions is FCAPS - Fault, Configuration, Accounting, Performance and Security. FCAPS is the ISO Telecommunications Management Network model and framework for network management.

(i) Fault Management - A fault is an event that has a negative significance. The goal of fault management is to recognize, isolate, correct and log faults that occur in the network. Most fault management systems poll the managed objects for error conditions and present this information to the n etwork manager. Fault management identifies and isolates network issues, proposes problem resolution, and subsequently logs the issues and associated resolutions.

(ii) Configuration Management - Monitors network and system configuration information so that the impact on network operations (hardware and software elements) can be tracked and managed. Network changes, additions, and deletions need to be coordinated with the network management personnel.

(iii) Accounting Management - Accounting management is concerned with tracking network utilization information, such that individual users, departments, or business units can be appropriately billed or charged for accounting purposes. For non-billed networks, accounting refers to administration whose primary goal is to administer the set of authorized users by establishing users, passwords, and permissions and to a dminister the operations of the equipment such as by performing software backup and synchronization.

(iv) Performance Management - Measures and makes network performance data available so that performance can be maintained and acceptable thresholds. It enables the manager to prepare the network for the future, as well as to determine the efficiency of the current network. The network performance addresses the throughput, network response times, packet loss rates, link utilization, percentage utilization, error rates and so forth.

(v) Security Management - Controls access to network resources as established by organizational security guidelines. Most network management systems address security regarding network hardware, such as someone logging into a router. Security management functions include managing network authentication, authorization, and auditing, such that both internal and external users only have access to appropriate network resources, configuration and management of network firewalls, intrusion detection systems, and security policies (such as access lists).

Functions that are performed as part of network management accordingly include controlling, planning, allocating, deploying, coordinating, and monitoring the resources of a network, network planning, frequency allocation, predetermined traffic routing to support balancing, cryptographic distribution authorization, configuration management, fault management, security management, management, bandwidth management, Route analytics and accounting management.

3.10 The Internet Revolution

The Internet is the largest ''network of networks'' today, and the closest model we have to the information superhighway of tomorrow. Some distinguishing features of the Internet include:

- The Internet does not have a central computer system or telecommunications center. Instead, each message sent on the Internet has a unique address code so any Internet server in the network can forward it to its destination.
- The Internet does not have a headquarters or governing body.
- The Internet is growing rapidly.

Table 3.10.1 shows the strategic capabilities of Internet along with their business applications.

Table 3.10.1: Examples of the business value of e-Business Applications of Telecommunications Networks

Strategic Capabilities	e-Business Examples	Business Value
Overcome geographic barriers: Capture information about business transactions from remote locations.	Use the Internet and extranets to transmit customer orders from travelling salespeople to a corporate data centre for order processing and inventory control.	Provides better customer service by reducing delay in filling orders and improves cash flow by speeding up the billing of customers.
Overcome time barriers: Provide information to remote locations immediately after it is requested.	Credit authorization at the point of sale using online POS networks.	Credit inquiries can be made and answered in seconds.
Overcome cost barriers: Reduce the cost of more traditional means of communication.	Desktop videoconferencing between a company and its business partners using the Internet, Intranets, and Extranets.	Reduces expensive business trips; allows customers, suppliers, and employees to collaborate, thus improving the quality of decisions reached.
Overcome structural barriers: Support	Business-to-business electronic commerce websites for	Fast, convenient services lock in customers and

linkages for competitive advantage.	transactions with suppliers and customers using the Internet and Extranets.	suppliers.

3.10.1 Networks and the Internet

A Computer Network is two or more computers linked together to share information and/or resources. There are several types of computers networks, but the types most important are Local Area Network (LAN), the Internet, Extranet, and Intranet.

The Internet is the global computer network, or “information super-high way”. The Internet developed from a variety of university and government–sponsored computer networks that have evolved and are not made up of millions and millions of computers and sub networks throughout the world. The Internet is the network that serves as the backbone for the World Wide Web (WWW).

An Intranet is a company’s private network accessible only to the employees of that company. The intranet uses the common standards and protocols of the Internet. The purpose of an intranet is to distribute data or information to employees, to make shared data or files available, and to manage projects within the company.

An Extranet is similar to an Intranet except that it offers access to selected outsiders, such as buyers to an intranet except, and wholesalers in the supply chain. Extranets allow business partners to exchange information. These business partners may be given limited access to company serves and access only to the data necessary to conduct supply chain exchanges with the company.

3.10.2 Internet Architecture

The architecture of the Internet has also changed a great deal as it has grown explosively. Fig. 3.10.1 gives an overview of Internet architecture. We shall examine this figure piece by piece, starting with a computer at home (at the edges of the figure).

(a) To join the Internet, the computer is connected to an Internet Service Provider, or simply ISP, from whom the user purchases Internet access or connectivity. This lets the computer exchange packets with all of the other accessible hosts on the Internet. There are many kinds of Internet access, and they are usually distinguished by how much bandwidth they provide and how much they cost, but the most important attribute is connectivity.

(b) A common way to connect to an ISP is to use the phone line to our house, in which case our phone company is our ISP. ISP networks may be regional, national, or international in scope. However, there are several other popular ways to connect to an ISP.

- DSL (Digital Subscriber Line) reuses the telephone line that connects to our house for digital data transmission. The computer is connected to a device called a DSL modem that converts between digital packets and analog signals that can pass unhindered over the telephone line. DSL is a higher-bandwidth way to use the local telephone line than to send bits over a traditional telephone call instead of a voice conversation. That is called dial-up and done with a different kind of modem at both ends. The word modem is short for ''modulator demodulator'' and refers to any device that converts between digital bits and analog signals. At the other end, a device called a DSLAM (Digital Subscriber Line Access Multiplexer) converts between signals and packets.

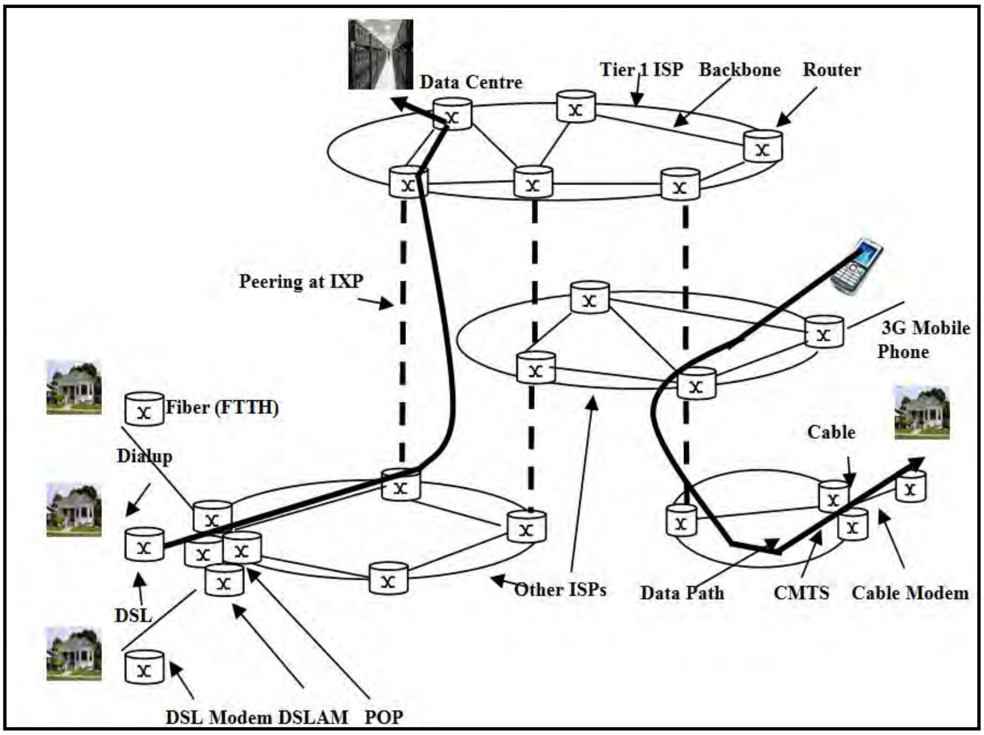


Fig. 3.10.1: Overview of the Internet Architecture*

- Another method is to send signals over the cable TV system. Like DSL, this is a way to reuse existing infrastructure, in this case otherwise unused cable TV channels. The device at the home end is called a cable modem and the device at the cable head-end is called the CMTS (Cable Modem Termination System).
- Wireless is used for Internet access for 3G mobile phone networks. They can provide data delivery at r ates of 1 Mbps or higher to mobile phones and fixed

* Tanenbaum and Wetherall, 'Computer Networks', Fifth Edition, Prentice Hall, 2001, Page No. 62

subscribers in the coverage area. We call the location at which customer packets enter the ISP network for service the ISP's POP (Point of Presence). Packets are moved between the POPs of different ISPs. From this point on, the system is fullydigital and packet switched.

(c) Internet Service Provider's architecture is made up of long-distance transmission lines that interconnect routers at POPs in the different cities that the ISPs serve. This equipment is called the backbone of the ISP. If a packet is destined for a host served directly by the ISP, that packet is routed over the backbone and delivered to the host. Otherwise, it must be handed over to another ISP.

(d) ISPs connect their networks to exchange traffic at IXPs (Internet eXchange Points). The connected ISPs are said to peer with each other. There are many IXPs in cities around the world. They are drawn vertically in the figure because ISP networks overlap geographically. Basically, an IXP is a room full of routers, at least one per ISP. A LAN in the room connects all the routers, so packets can be forwarded from any ISP backbone to any other ISP backbone. IXPs can be large and independently owned facilities.

(e) The peering that happens at IXPs depends on the business relationships between ISPs. There are many possible relationships. For example, a small ISP might pay a larger ISP for Internet connectivity to reach distant hosts, much as a customer purchases service from an Internet provider.

(f) The path a packet takes through the Internet depends on the peering choices of the ISPs. If the ISP delivering a packet peers with the destination ISP, it might deliver the packet directly to its peer. Otherwise, it might route the packet to the nearest place at which it connects to a paid transit provider so that provider can deliver the packet. Two example paths across ISPs are drawn in the figure.

(g) Often, the path a packet takes will not be the shortest path through the Internet. At the top of the food chain are a small handful of companies that operate large international backbone networks with thousands of routers connected by high-bandwidth fiber optic links. These ISPs do not pay for transit. They are usually called tier 1 ISPs and are said to form the backbone of the Internet, since everyone else must connect to them to be able to reach the entire Internet.

Companies that provide lots of content, such as Google and Yahoo!, locate their computers in data centers that are well connected to the rest of the Internet. These data centers are so large (tens or hundreds of thousands of machines) that electricity is a major cost, so data centers are sometimes built in areas where electricity is cheap.

3.10.3 Internet Applications

Internet can be used as a very effective media for various applications such as:

- E-mail, browsing the sites on the World Wide Web, and participating in special interest newsgroups are the most popular Internet applications.

- Electronic commerce transactions between businesses and their suppliers and customers can also performed with online web applications.
- The Internet provides electronic discussion forums and bulletin board systems formed and managed by thousands of special-interest newsgroups.
- Other applications include downloading software and information files and accessing databases provided by thousands of businesses, governments, and other organizations.
- The Internet allows holding real-time conversations with other Internet users.
- The Internet allows gathering information through online services using web browsers and search engines.
- Internet browser software enables millions of users to surf the World Wide Web by clicking their way to the multimedia information resources stored on the hyperlinked pages of businesses, government, and other websites.

3.10.4 Business Use of the Internet

Business uses of the Internet include the following:

- Strategic business alliances
- Providing customer and vendor support
- Collaboration among business partners
- Buying and selling products and services
- Marketing, sales, and customer service applications
- Growth of cross-functional business applications
- Emergence of a pplications in engineering, manufacturing, human resources and accounting.
- Enterprise communications and collaboration
- Attracting new customers with innovative marketing and products.
- Retaining present customers with improved customer service and support.
- Developing new web-based markets and distribution channels for existing products.
- Developing new information-based products accessible on the Web.
- Generating revenue through electronic commerce applications is a g rowing source of business value.
- Electronic commerce

3.10.5 Intranet

An **Intranet** is a network inside an organization that uses Internet technologies such as web browsers and servers, TCP/IP network protocols, HTML hypermedia document publishing and databases, and so on, to provide an Internet-like environment within the enterprise for information sharing, communications, collaboration, and the support of business processes.

An Intranet is protected by security measures such as passwords, encryption, and firewalls, and thus can be accessed by authorized users through the Internet. A Company's Intranet can also be accessed through the Intranets of customers, suppliers, and other business partners via extranet links. Refer to the Fig. 3.10.2.

- **The Business Value of Intranets:** Intranet applications support communications and collaboration, business operations and management, web publishing, and Intranet management. These applications can be integrated with existing IS resources and Applications, and extended to customers, suppliers, and business partners.
- **Communications and Collaboration:** Intranets can significantly improve communications and collaboration within an enterprise. Examples include:
  - Using an Intranet browser and workstation to send and receive e-mail, voicemail, paging, and fax to communicate with others within the organization, and externally through the Internet and extranets.
  - Using Intranet groupware features to improve team and project collaboration with services such as discussion groups, chat rooms, and audio and videoconferencing.

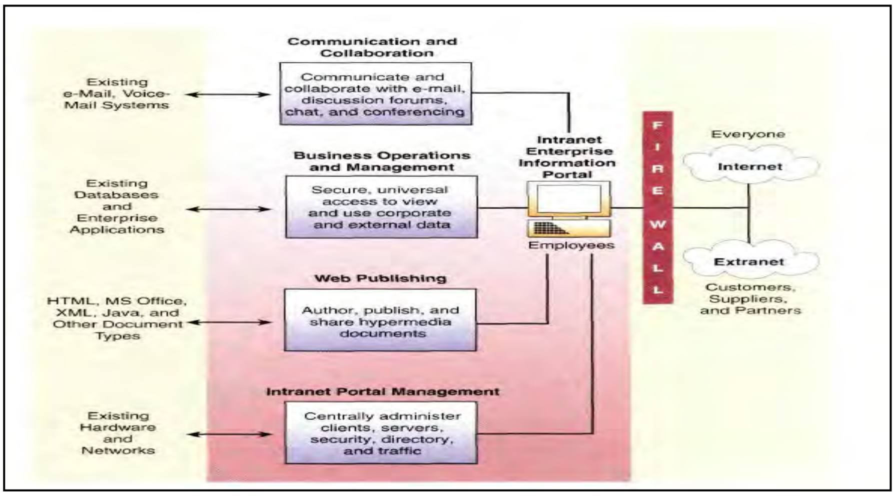

Communication and Collaboration
Existing e-Mail, Voice-Mail Systems
Communicate and collaborate with e-mail, discussion forums, chat, and conferencing
Business Operations and Management
Existing Databases and Enterprise Applications
Secure, universal access to view and use corporate and external data
Web Publishing
HTML, MS Office, XML, Java, and Other Document Types
Author, publish, and share hypermedia documents
Intranet Portal Management
Existing Hardware and Networks
Centrally administer clients, servers, security, directory, and traffic
Intranet Enterprise Information Portal
Employees
FIREWALL
Everyone
Internet
Extranet
Customers, Suppliers, and Partners

Fig. 3.10.2: Role of Intranet in any organization[*]

[*] “Introduction to Information Systems” by James O'Brien, George M. Marakas, 11th edition, McGraw Hill

- Web Publishing: The advantages of developing and publishing hyperlinked multimedia documents to hypermedia databases accessible on World Wide Web servers has moved to corporate intranets. The comparative ease, attractiveness, and lower cost of publishing and accessing multimedia business information internally via intranet web sites have been one of the primary reasons for the explosive growth of the use of intranets in business. Publishing of various information products such as company's newsletters, technical drawings, product catalogs in variety of ways including hypermedia, web pages, e-mail and net broadcasting etc.
- Business Operations and Management: Intranets are being used as the platform for developing and deploying critical business applications to support business operations and managerial decision making across the internetworked enterprise. Examples include:
    - Many companies are developing customer applications like order processing, inventory control, sales management, and executive information systems that can be implemented on intranets, extranets, and the Internet.
    - Many applications are designed to interface with, and access, existing company databases and legacy systems. The software for such business uses, is then installed on Intranet web servers.
    - Employees within a c ompany, or external business partners, can access and run applications using web browsers from anywhere on the network whenever needed.
    - Company newsletters, technical drawings, and product catalogs can be published in a variety of ways including hypermedia and web pages, e-mail, net broadcasting, and as part of in-house business applications.
    - Intranet software browsers, servers, and search engines can help to easily navigate and locate the business information.

3.10.6 Extranets

Extranets are network links that use Internet technologies to interconnect the Intranet of a business with the Intranets of its customers, suppliers, or other business partners. Companies can use Extranets to perform following functions:

- Establish direct private network links between themselves, or create private secure Internet links between them called virtual private networks.
- Use the unsecured Internet as the extranet link between its intranet and consumers and others, but rely on encryption of sensitive data and its own firewall systems to provide adequate security.

Business Value of Extranets

The business value of extranets is derived from several factors:

- The web browser technology of extranets makes customer and supplier access of intranet resources a lot easier and faster than previous business methods.

- Extranets enable a company to offer new kinds of interactive Web-enabled services to their business partners. Thus, extranets are another way that a business can build and strengthen strategic relationships with its customers and suppliers.
- Extranets enable and improve collaboration by a business with its customers and other business partners.
- Extranets facilitate an online, interactive product development, marketing, and customer-focused process that can bring better designed products to market faster.

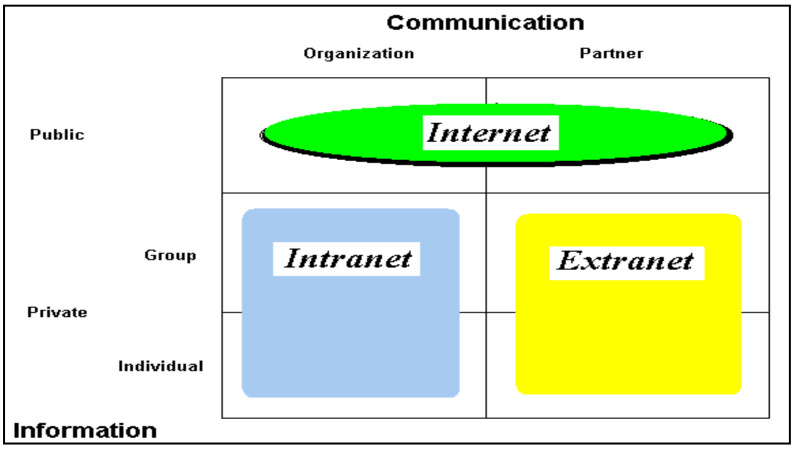


Fig. 3.10.3: Relationship between the Internet, Intranet and Extranet

An organization uses the Internet to communicate public information about itself to members of the organization and to others outside the organization. Referring to t he Fig. 3.10.3, Intranets and Extranets are private versions of the Internet. An organization uses an intranet to share information between the members of the organization. Organizations use extranets to exchange information with and provide services to their business partners (customers, suppliers, etc.)

An extranet requires security and privacy that require firewall server management, the issuance and use of digital certificates or similar means of user authentication, encryption of messages, and the use of Virtual Private Networks (VPN) that tunnel through the public network.

Companies can use an extranet to do the following tasks:

- Share product catalogs exclusively with wholesalers or those "in the trade";
- Collaborate with other companies on joint development efforts;
- Jointly develop and use training programs with other companies;
- Provide or access services provided by one company to a group of other companies; and
- Share news of common interest exclusively with partner companies.

With competitive advantage as the ultimate prize, two fundamental drivers are propelling large enterprises to the extranet: market consolidation and service externalization. Markets are consolidating as the pace of m erger, investment, and acquisition intensifies. Yet within companies, core services are also increasingly being externalized, delivered by a ne twork of external parties that includes outsourcers, demand and supply chain partners, consultants, and contractors. This dynamic environment presents clear business needs, which can be summarized as the Five Rules of the Extranet which are as follows:

- Be as flexible as the business: An extranet must be d riven by the demands of the market, not the limitations of technology. It must be extremely flexible and allow companies to immediately deploy extranet services that best fit the business need, be it intimate supply chain partners using a wide range of applications or mass e-commerce extranets driven by Web-based applications.
- Deploy in "Internet time": To deploy an extranet, companies shouldn't have to roll out a new infrastructure or go through a major re-architecting of their applications. To remain market-driven, enterprises must be able to deploy their extranet quickly, and leverage their existing infrastructure to do so.
- Protect the interests of the data owner: Extranet services need to be deployed in a fast and flexible way, but with the complete assurance that only the correct users can access the right services. An extranet must ensure that what's supposed to be private stays private.
- Serve the partner as a customer: An extranet presents a very important and delicate balance: providing customer service to key partners (who might also be customers) in a competitive environment with mission-critical resources at risk. The final solution must be an extranet without compromise. Partners should never be required to change their security policies, networks, applications, and firewalls for the "good" of the extranet community.
- Drive information to the decision-maker: An extranet must provide a central means to measure progress, performance, and popularity. Business units deploying applications need to understand which extranet content and applications are most successful.

3.10.7 Information Systems and Telecommunication

Telecommunications give an organization the capability to move information rapidly between distant locations and to provide the ability for the employees, customers, and suppliers to collaborate from anywhere, combined with the capability to bring processing power to the point of the application. All of this offers firm important opportunities to restructure its business processes and to c apture high competitive ground in the marketplace. Through telecommunications, this value may be:

(i) An increase in the efficiency of operations;

(ii) Improvements in the effectiveness of management; and

(iii) Innovations in the marketplace.

Telecommunications may provide these values through the following impacts:

(a) Time compression - Telecommunications enable a firm to transmit raw data and information quickly and accurately between remote sites.

(b) Overcoming geographical dispersion - Telecommunications enable an organization with geographically remote sites to function, to a degree, as though these sites were a single unit. The firm can then reap benefits of scale and scope which would otherwise be unobtainable.

(c) Restructuring business relationships - Telecommunications make it possible to create systems which restructure the interactions of people within a firm as well as a firm's relationships with its customers. Operational efficiency may be raised by eliminating intermediaries from various business processes.

3.11 Electronic Commerce

Electronic Commerce (e-Commerce) and its related technologies are unquestionably the current leading-edge business and finance delivery systems for the 21st Century. The explosion in the application of technologies and the delivery of these technologies into the hands of consumers has made the vision, the dream, the fantasy, of conducting business electronically, anywhere in the global community, a reality. Electronic Commerce (EC) is no longer just a concept; it is a market force to be reckoned with. As more and more organizations launch Internet/World Wide Web (WWW) home pages and intranets to disseminate company/product information, and expand their customer base, countless yet unnamed companies are just beginning to investigate this alternative. These companies are realizing that business via the Internet is inevitable that they will not be able to ignore. The lure of reaching additional customers, expanding market shares, providing value-added services, advancing technological presence, and increasing corporate profits is just too valuable to disregard, and will eventually attract companies to electronic commerce like moths to a flame.

Electronic Commerce is the process of doing business electronically. It refers to the use of technology to enhance the processing of commercial transactions between a company, its customers and its business partners. It involves the automation of a variety of business-to-business and business-to-consumer transactions through reliable and secure connections.

E-Commerce is a sophisticated combination of technologies and consumer-based services integrated to form a new paradigm in business transaction processing. The future of e-Commerce is bright and viable—the application, however, has not yet reached full integration into the business mainstream. Several significant hurdles remain, which must be cleared before electronic commerce will become a mainstay business strategy.

3.11.1 Benefits of e-Commerce Application and Implementation

E-Commerce presents immense benefits to individual organizations, consumers, and society as a whole.

- Reduction in costs to buyers from increased competition in procurement as more suppliers are able to compete in an electronically open marketplace.
- Reduction in errors, time, and overhead costs in information processing by eliminating requirements for re-entering data.
- Reduction in costs to suppliers by electronically accessing on-line databases of bid opportunities, on-line abilities to submit bids, and on-line review of rewards.
- Reduction in time to complete business transactions, particularly from delivery to payment.
- Creation of new markets through the ability to easily and cheaply reach potential customers.
- Easier entry into new markets, especially geographically remote markets, for enterprises regardless of size and location.
- Better quality of goods as specifications are standardized and competition is increased and improved variety of goods through expanded markets and the ability to produce customized goods.
- Faster time to m arket as business processes are linked, thus enabling seamless processing and eliminating time delays.
- Optimization of resource selection as businesses form cooperative teams to increase the chances of economic successes, and to provide the customer products and capabilities more exactly meeting the requirements.
- Reduction in inventories and reduction of risk of obsolete inventories as the demand for goods and services is electronically linked through just-in-time inventory and integrated manufacturing techniques.
- Reduction in overhead costs through uniformity, automation, and large-scale integration of management processes.
- Reduction in use of ecologically damaging materials through electronic coordination of activities and the movement of information rather than physical objects).
- Reduction in advertising costs.

Clearly, the benefits of corporate-wide implementation of e-Commerce are many, and this list is by no means complete. With the benefits, however, also come the risks. An organization should be c autious not to leap blindly into e-Commerce, but rather first develop an e-Commerce strategy, and then organize a corporate-wide team to implement that strategy.

3.11.2 Risks involved in e-Commerce

The risks associated with e-Commerce are multi-faceted. Given below is a sample listing of risks of e-Commerce:

- Problem of anonymity: There is need to identify and authenticate users in the virtual global market where anyone can sell to or buy from anyone, anything from anywhere.
- Repudiation of contract: There is possibility that the electronic transaction in the form of contract, sale order or purchase by the trading partner or customer may be denied.
- Lack of authenticity of transactions: The electronic documents that are produced in the course of an e-Commerce transaction may not be authentic and reliable.
- Data Loss or theft or duplication: The data transmitted over the Internet may be lost, duplicated, tampered with or replayed.
- Attack from hackers: Web servers used for e-Commerce may be vulnerable to hackers.
- Denial of Service: Service to customers may be denied due to non-availability of system as it may be affected by viruses, e-mail bombs and floods.
- Non-recognition of electronic transactions: e-Commerce transactions, as electronic records and digital signatures may not be recognized as evidence in courts of law.
- Lack of audit trails: Audit trails in e-Commerce system may be lacking and the logs may be incomplete, too voluminous or easily tampered with
- Problem of piracy: Intellectual property may not be adequately protected when such property is transacted through e-Commerce

3.11.3 Types of e-Commerce

There are four general classes of e-Commerce applications:

(a) Business-to-Business (B2B) e-Commerce

(b) Business-to-Consumer (B2C) e-Commerce

(c) Consumer-to-Business (C2B) e-Commerce

(d) Consumer-to-Consumer (C2C) e-Commerce

(e) Business-to-Government (B2G) e-Commerce

(f) Business-to-Employee (B2E) e-Commerce

A. Business-to-Business (B2B) e-Commerce

B2B refers to the exchange of services, information and/or products from one business to another. B2B electronic commerce typically takes the form of automated processes between trading partners and is performed in much higher volumes than Business-to-Consumer (B2C) applications. B2B can also encompass marketing activities between businesses, and not just the final transactions that result from marketing.

B. Business-to-Consumer (B2C) e-Commerce

It is defined as the exchange of services, information and/or products from a business to a consumer, as opposed to between one business and another. Typically, a B2C e-Commerce business has a virtual store front for consumers to purchase goods and services eliminating the need to physically view or pick up the merchandise.

The Business-to-Consumer (B2C) model can save time and money by doing business electronically but customers must be provided with safe and secure as well as easy-to-use and convenient options when it comes to paying for merchandise. This minimizes internal costs created by inefficient and ineffective supply chains and creates reduces end prices for the customers. This could be beneficial especially if we are in the business of commodity-like products where we must be innovative and accommodating to gain and retain customers.

Advantages of B2C E-Commerce include:

(i) Shopping can be faster and more convenient.

(ii) Offerings and prices can change instantaneously.

(iii) Call centers can be integrated with the website.

(iv) Broadband telecommunications will enhance the buying experience.

C. Consumer-to-Business (C2B) e-Commerce

In C2B e-Commerce model, consumers directly contact with business vendors by posting their project work online so that the needy companies review it and contact the consumer directly with bid. The consumer reviews all the bids and selects the company for further processing. Some examples are guru.com, rentacoder.com, getacoder.com, freelancer.com.

D. Consumer-to-Consumer (C2C) e-Commerce

C2C e-Commerce is an Internet-facilitated form of commerce that has existed for the span of history in the form of barter, flea markets, swap meets, yard sales and the like. C2C e-Commerce sites provide a virtual environment in which consumers can sell to one another through a third-party intermediary.

E. Business-to-Government (B2G) e-Commerce

B2G e-Commerce, also known as e-Government, refers to the use of information and communication technologies to build and strengthen relationships between government and employees, citizens, businesses, non-profit organizations, and other government agencies.

F. Business-to-Employee (B2E) e-Commerce

B2E e-Commerce, from an intra-organizational perspective, has provided the means for a business to offer online products and services to its employees.

3.11.4 Key aspects to be considered in implementing e-Commerce

Successful implementation of e -Commerce requires involvement of key stakeholders and should ideally include representatives from: accounting/ finance, internal audit, IT security, telecommunications, end users, system analysts, and legal. Further, key trading partners, external auditors, and representatives from other institutions such as banks, trading houses, brokers, and other third-party services should also be involved to obtain valuable insight into the design and deployment of the e-Commerce solution. Other key aspects to be considered are as follows:

- Implementing appropriate policies, standards and guidelines
- Performing cost benefit analysis and risk assessment to ensure value delivery
- Implementing the right level of security across all layers and processes
- Establishing and implementing the right level of baseline (best practice) controls
- Integration of e-Commerce with the business process and the physical delivery channels
- Providing adequate user training
- Performing post implementation review to ensure controls are working as envisaged.

3.12 Mobile Commerce

Mobile Commerce or m-Commerce, is about the explosion of applications and services that are becoming accessible from Internet-enabled mobile devices. It involves new technologies, services and business models. It is quite different from traditional e-Commerce. Mobile phones or PDAs impose very different constraints than desktop computers. But they also open the door to a slew of new applications and services.

M-commerce (mobile commerce) is the buying and selling of goods and services through wireless handheld devices such as cellular telephone and personal digital assistants (PDAs) Known as next-generation e-commerce, m-commerce enables users to access the Internet without needing to find a place to plug in. The emerging technology behind m-commerce, which is based on the Wireless Application Protocol (WAP), has made strides in countries, where mobile devices equipped with Web-ready micro-browsers are much more common.

As content delivery over wireless devices becomes faster, more secure, and scalable, there is wide speculation that m-commerce will surpass wire-line e-commerce as the method of choice for digital commerce transactions. The industries affected by m-commerce include:

- Financial services, which includes mobile banking (when customers use their handheld devices to access their accounts and pay their bills) as well as brokerage services, in which stock quotes can be displayed and trading conducted from the same handheld device.
- Telecommunications, in which service changes, bill payment and account reviews can all be conducted from the same handheld device.

- Service/retail, as consumers are given the ability to place and pay for orders on-the-fly.
- Information services, which include the delivery of financial news, sports figures and traffic updates to a single mobile device.

3.13 Electronic Fund Transfer

Electronic Funds Transfer (EFT) represents the way the business can receive direct deposit of all payments from the financial institution to the company bank account. Once the user Signs Up, Money Comes to him directly and sooner than ever before. EFT is fast, safe, and means that the money will be confirmed in user's bank account quicker than if he had to wait for the mail, deposit the cheque, and wait for the funds to become available.

The payment mechanism moves money between accounts in a fast, paperless way. These are some examples of EFT systems in operation:

- Automated Teller Machines (ATMs): Consumers can do their banking without the assistance of a teller, or to make deposits, pay bills, or transfer funds from one account to another electronically. These machines are used with a debit or EFT card and a code, which is often called a personal identification number or "PIN."
- Point-of-Sale (PoS) Transactions: Some debit or EFT cards (sometimes referred to as check cards) can be used when shopping to allow the transfer of funds from the consumer's account to the merchant's. To pay for a purchase, the consumer presents an EFT card instead of a cheque or cash. Money is taken out of the consumer's account and put into the merchant's account electronically.
- Preauthorized Transfers: This is a method of automatically depositing to or withdrawing funds from an individual's account, when the account holder authorizes the bank or a third party (such as an employer) to do so. For example, consumers can authorize direct electronic deposit of wages, social security, or dividend payments to their accounts. Or they can authorize financial institutions to make regular, ongoing payments of insurance, mortgage, utility, or other bills.
- Telephone Transfers: Consumers can transfer funds from one account to another through telephone instructions rather than traditional written authorization or instrument. The accounts being debited can be checking or savings, for example—or can order payment of specific bills by phone.

3.14 Summary

Before wires and virtual networks transmitted communications, there were smoke signals, drums and carrier pigeons. Fortunately, technology has come a long way since then to the point where it's impossible to overemphasize the significance of telecommunications technology to any business, especially as it relates to growing the capacity of small businesses. From telephones, facsimile, television, Internet and the vast array of private networks, telecommunications technology has become firm's central nervous system. Without it, a small business couldn't compete or survive in the nation's information service-dependent economy, making it one of the most important investments we will make as we build our business.

Telecommunication is an important tool for businesses. It enables companies to communicate effectively with customers and deliver high standards of customer service. Telecommunication is also a key element in teamwork, allowing employees to collaborate easily from wherever they are located. Mobile telecommunication gives companies the opportunity to introduce more flexible working by allowing employees to work efficiently from home. The introduction of Internet gives employees new levels of productivity and capability on the move.