CHAPTER-3: TELECOMMUNICATIONS & NETWORK

NETWORKING AN ENTERPRISE

❖ By using search networks, companies can perform more effectively as they can
  ▪ collaborate more creatively
  ▪ manage their business operations & organisational resources more effectively, &
  ▪ complete successfully in today's fast changing global economy

TRENDS IN TELECOMMUNICATION-

INDUSTRY TRENDS-

❖ Telecommunications networks & 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

TECHNOLOGY TRENDS-

❖ open systems with unrestricted connectivity, using Internet networking technologies
❖ increased industry & technical moves towards building client/server networks based on open
  system architecture
❖ change from analog to digital network technologies
❖ change in communications media from copper wire-based media & land-based microwave relay
  systems to fibre-optic lines & communications satellite transmissions
❖ fibre optic transmission has following advantages-
  ▪ reduced size and installation effort
  ▪ greater communication capacity
  ▪ faster transmission speeds, &
  ▪ freedom from electrical interference

BUSINESS APPLICATION TRENDS-

❖ Telecommunications networks are playing a vital and pervasive role in electronic commerce,
  enterprise collaboration & internal business applications
❖ 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 a workgroups,
  ▪ share resources,
  ▪ cut costs, and
  ▪ develop online operational processes
BUSINESS VALUE OF TELECOMMUNICATIONS-

❖ the widely-used information systems in enterprises are highly facilitated to telecommunication systems that help in increase in productivity and performance of an organisation
❖ its strategic capabilities include following-
  ▪ **overcoming geographic barriers** by capturing information about business transactions from remote locations
  ▪ **overcoming time barriers** by providing information to remote locations immediately after it is requested
  ▪ **overcoming cost barriers** by reducing the cost of more traditional means of communication
  ▪ **overcoming structural barriers** by supporting linkages for competitive advantage.

TELECOMMUNICATIONS NETWORK-

1. NEED & SCOPE OF NETWORKS-

❖ org. can improve efficiency by sharing information, such as, common files, databases & business application software over a telecommunication network
❖ advantages of a computer network are-
  ▪ **file sharing**- sharing of data files over the network
  ▪ **resource sharing**- sharing of computer resources, eg, hard disk, by multiple users simultaneously to reduce cost of installing & maintaining multiple resources in an org.
  ▪ **remote access**- remotely access data & information from org’s network via Internet in cost effective manner
  ▪ **shared databases**- simultaneous access to the shared databases to multiple users at the same time by ensuring the integrity of the database

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
❖ its components are-
  ▪ **terminals**-
    ▪ these are the starting and stopping points in any telecommunication network environment
    ▪ any input or output device that is used to transmit and receive data can be classified as a terminal component
    ▪ it includes video terminals, microcomputers, & telephones
  ▪ **telecommunications processors**-
    ▪ these support data transmission and reception between terminals and computers by providing a variety of control and support functions
    ▪ It includes following-
      ▪ **network interface card** is a computer hardware component that connects a computer to a computer network & has additional memory for buffering incoming & outgoing data packets, thus, improving the network throughput
      ▪ **modem** is a device that converts digital computer signal into analog telephone signal (called modulation) and do vice-versa as well (called demodulation) in a data communication system. These are required to send computer data with ordinary telephone lines because computer data is in digital form but telephone lines are analog.
- **Multiplexer** is a communication processor that allows a single communication channel to carry simultaneous data transmission from many terminals. It typically merges the transmission of several terminals at one end of a communication channel, while a similar unit separates the individual transmissions at the receiving end.

- **Internetwork processors** are special purpose communication processors. Its examples are:-
  - **Switch** makes connections between telecommunications circuits in a network so that a telecommunications message can reach its intended destination.
  - **Router** interconnects networks based on different rules or protocols, so that a telecommunications message can be routed to its destination.
  - **Hub** allows for the sharing of the network resources, eg, servers, printers etc.
  - **Bridge** connects numerous Local Area Networks (LAN) & magnifies the data transmission signal while passing data from one LAN to another.
  - **Repeater** boosts or amplifies the signal before passing it to the next section of a cable in a network.
  - **Gateway** connects networks that use different communication architectures.

- **Telecommunication media/channels**-
  - These are the part of a telecommunications network that connects the message source with the message receiver, & are used by channels, over which data are transmitted & received.
  - It is grouped into guided media and unguided media.
  - **Guided/Bound media** uses a “cabling system” that guides the data signals along a specific path. The data signals are “bound” or “guided” by the cabling system. Its examples are:-
    - **Twisted pair wire**
      - It is ordinary telephone wire, consisting of copper wire twisted into prayers and is most widely used media for both voice and data transmissions.
    - **Disadvantages**-
      - It is susceptible to various types of electrical interference, which limits the practical distances that data can be transmitted without being garbled.
      - Signals must be refreshed every 1 to 2 miles by repeaters which are very expensive and does not offer security.
    - **Coaxial cables**
      - It can carry a large volume of data and allows high speed data transmission used in high-service metropolitan areas for cable TV system, & for short distance connection of computers and peripheral devices.
      - These cables can be bundled together into a much larger cable for easy installation and can be placed underground and laid on the floors of lakes and oceans.
      - It’s only **disadvantage** is that it is more expensive than twisted pair.
    - **Fibre optics**
      - Signals are converted to light form and fired by laser in bursts.
      - Optical fibres can carry digital as well as analog signals & provides increased speed & greater carrying capacity than coaxial cables & twisted pair lines.
    - **Advantages**-
      - It is neither affected by electromagnetic radiation nor susceptible to electronic noise.
      - It is easy to install as it is smaller & more flexible.
      - It can be used under sea for transatlantic use.
    - **Disadvantage**- it can be difficult to install & costly to purchase.
**Unbounded media** consists of a means for the data signals to travel, but nothing to guide them along a specific path. Its examples include:

- **Terrestrial microwave**
  - It uses atmosphere as a medium to transmit signals
  - It is used for high-volume & long-distance communication of both data and voice in the form of electromagnetic waves
  - **Disadvantage:** it cannot bend around the curvature of the earth.
- **Radio waves** are an invisible form of electromagnetic radiation that varies in wavelength, making it one of the widest ranges in the electromagnetic spectrum.
- **Micro waves** are radio waves used for communication, radar systems, radio astronomy, navigation, etc.
- **Infrared waves** are used in industrial, scientific & medical applications. Night vision devices using it, allows the observer to detect people/animals, without being known
- **Communication satellites**
  - It uses the atmosphere as the medium through which to transmit signals
  - It is used for high volume as well as long distance communication of data and voice
  - It is a cost effective method for moving large quantities of data over long distances
  - **Disadvantages:**
    - signals weaken over long distances
    - weather conditions & solar activity can cause noise interference
    - sensitive data must be sent in a secret encrypted form, as anyone can listen on these

- **Computers** of all sizes & types are connected through media to perform communication assignment
- **Telecommunication control software** consists of program that control telecommunication activities & manage the functions of telecommunications network
- **Network Management**-
  - telecommunication software packages provide a variety of communication support services
  - Examples of network management functions are:
    - **traffic management:** manages network resources & traffic to avoid congestion & optimize telecommunications service levels to users
    - **security:** provides authentication, encryption, auditing function, & enforces security policies
    - **network monitoring:** troubleshoot & watch over network, informing network administrators of potential problems before they occur
    - **capacity planning:** determines how best to accommodate needs of the network as it grows & changes

**CLASSIFICATION OF TELECOMMUNICATION NETWORKS**

1. **LAN**-
   - it is a group of computers & network devices connected together, usually within the same building, spanned over limited distance & provides high speed data transfer and is relatively inexpensive.
   - **Advantages of LAN**-
     - **Security** for programs & data can be achieved using servers that are locked through both software and by physical means
     - **expanded PC usage through inexpensive workstation** as once LAN has been set up, existing PCS can be easily converted into nodes by adding network interface cards at less cost
organizational benefits by reducing costs in computer hardware, software & peripherals, and a drastic reduction in time & cost of training/re-training manpower to use system

data management benefits as it is easier to manage, access & back up data, because data is located centrally on the server

software cost & upgradation- network version can save money as there would be no need to buy multiple copies of the same software for every machine of org.. Also, software upgrade are much easier as any given packages is stored centrally on the server

2. MAN- 
❖ it is a larger network that usually spans in the same city or town 
❖ it sometimes refers to networks which connect systems or LANs within a metropolitan area 
❖ it can support both data & voice. 
❖ eg- cable network 

3. WAN- 
❖ It is a telecommunication network that cover large geographical areas, such as, large city, whole country or many countries. 
❖ These are high speed & relatively expensive. 
❖ Eg- telephone service, satellite transmission, airline reservation, interstate banking, etc. 

4. CLIENT-SERVER (C/S) NETWORKING 
❖ C/S network is a computer network in which one centralized powerful computer (called server) is connected to many less powerful PCs/workstations (called clients) 
❖ The clients run programs and access data that are stored on a server 
❖ Client is a single-user workstation & can be classified as follows- 
  - Fat/Thick client do not rely on a central processing server because processing is done locally on the user system, & the server is accessed primarily for storage purposes 
  - thin client use the resources of the host computer, & the machine is going to communicate with the central processing server 
  - hybrid client is a mixture of the above two client models. Like fat client, it processes locally, but relies on the server for storing persistent data 
❖ Server is one or more multi-user processors with shared memory providing computing, connectivity and the database services. 
❖ Characteristics of C/S Network- 
  - Service- The server process is a provider of services & the client is a consumer of services 
  - Shared Resources- It can service many clients at the same time and regulate the access to the shared resources 
  - Mix-&-Match- It is independent of hardware or operating system software platforms 
  - Scalability- client workstations can either be added or removed and also the server load can be distributed across multiple servers 
  - Integrity- the server code & server data is centrally managed, which results in cheaper maintenance and the guarding of shared data integrity 
❖ Issues in C/S Network- 
❖ When server goes down(crashes), all computers connected to it become unavailable to use 
❖ simultaneous access to data & services by user takes little more time for server to process the task
**5. PEER-TO-PEER NETWORKING (P2P)-**

- It is a type of decentralized & distributed network architecture in which individual nodes in the network, called peers, act as both suppliers & consumers of resources.
- It is created with two or more PCs connected together and share resources without going through a separate server computer.
- Example: Napster, Freenet, etc.
- Its prime objective is that many computers come together and pool their resources to form a content distribution system.
- Computers are called ‘peers’, as each one can alternately act as a client to another peer fetching its content, and as a server, providing content to other peers.
- It handles high volume of file sharing traffic by distributing load across many computers on Internet.
- It allows sharing of files, printers and, other resources, across all devices.
- It both scale better & more resilient than C/S network in case of failure or traffic bottlenecks.
- **Advantages-**
  - It is easy & simple to setup, & only require a Hub/Switch to connect all computers together.
  - It is very simple & cost effective.
  - If one computer fails to work, all other computers connected to it continue to work.
- **Disadvantages-**
  - There can be problem in accessing files, if computers are not connected properly.
  - Do not support connections with too many computers as the performance gets degraded in case of high network size.
  - Data security is very poor.

**6. MULTI-TIER ARCHITECTURE-**

- **SINGLE TIER SYSTEMS/ONE-TIER ARCHITECTURE-**
  - It means a single computer that contains a database & a front-end (GUI) to access the database.
  - There is one computer with stores all of the company’s data on a single database.
- **Advantages-**
  - It requires only one stand-alone computer.
  - It requires only one installation of proprietary software which makes it most cost-effective system available.
- **Disadvantage-** It can be used by only one user at a time.

- **TWO TIER SYSTEMS/ TWO-TIER ARCHITECTURE-**
  - It consists of a client and server, where the client is on the presentation tier and server is on the database tier of the architecture.
  - Database is stored on the server, & interface used to access the database is installed on the client.
- **Advantages-**
  - System performance is higher because business logic and database are physically close.
  - Processing is shared between the client & server, more users could interact with the system.
  - It has simple structure, & hence, it is easy to setup & maintain entire system smoothly.
- **Disadvantage-** Performance deteriorates if number of users increases.

- **THREE-TIER/n-TIER ARCHITECTURE-**
  - Its three tiers are the presentation tier, application tier, and data tier.
It is used when an effective distributed C/S design is needed that provides (when compared to two-tier) increased performance, flexibility, maintainability, reusability, & scalability, while holding the complexity of distributed processing from the user.

The three tiers are as follows-
- presentation tier communicates with other tiers, & occupies the top level and displays information related to services available on a website.
- application/middle/logic tier controls application functionality by performing detailed processing.
- Database tier-it houses the database servers where information is stored & retrieved.

General considerations-
- the database server is always layered on database tier and clients are always a part of presentation layer of the architecture.
- as tier increases from two-tier to n-tier, additional tiers are added in between these two tiers- database tier and presentation tier.
- database tier & presentation tier always lie on the extremes of the architecture.

Advantages of three-tier architecture-
- clear separation of user interface control and data presentation from application logic, allows more clients to have access to a wide variety of server applications.
- 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 & faster to exchange a component on the server than to furnish numerous PCs with new program versions.

Disadvantages of three-tier architecture -
- Creates increased need of network traffic management, server load balancing & fault tolerance.
- current tools are relatively immature and more complex.
- maintenance tools are currently inadequate for maintaining server libraries.

7. PUBLIC DATA NETWORK-
- It is defined as a network shared & accessed by users not belonging to a single organisation.
- it is a network established for the specific purpose of providing data transmission services for public.
- Eg- Internet.

8. PRIVATE DATA NETWORK-
- It provides dedicated network to businesses, govt. agencies, & orgs. of all sizes, so as to receive & transmit data continuously which critical to both daily operations & mission critical needs of an org.
- these are safe & secure, but too expensive.

9. VIRTUAL PRIVATE NETWORKS (VPN)-
- It is a private network that uses a public network (usually Internet) to connect remote sites or users together.
- It uses virtual connections routed through Internet from business’s private network to remote site or employee.
- it is a secure network but relies on the firewalls & other security features of Internet & Intranet connections and those of participating orgs.

Twitter- @tweetopians
**NOTE** - LAN/MAN/WAN are classified on basis of area; C-S/P2P/Multi-tier are classified on basis of functions & Public/Private/VPN network are classified on basis of ownership.

**NETWORK COMPUTING** -

- In it, network computers & other thin clients provide browser-based user interface for processing small application programs, called applets
- Network computers are designed as low-cost networking computing devices
- Application and database servers provide the operating system, application software, applets, databases and database management software needed by the end users in the network
- Two basic models of computing are:
  - **CENTRALIZED COMPUTING** -
    - It is computing done at a central location, using terminals that are attached to a central computer
    - The computer itself may control all peripherals directly or they may be attached via a terminal server
    - It offers great security as all the processing is controlled in a central location
    - Moreover, if one terminal breaks down the user can simply go to another terminal
    - **Disadvantages** -
      - It relies totally on the central computer. Should the central computer crash, the entire system will go down.
      - Should the central computer be inadequately supported by any means, then your usage will suffer greatly.
  - **DECENTRALIZED COMPUTING** -
    - It is the allocation of resources, both hardware & software, to each individual workstation, or office location
    - Collection of decentralized computer systems are components of largest computer network
    - These systems are capable of running independently of each other
    - It enables file sharing & all computers can share peripherals (eg- printer, scanner, modem), allowing all the computers in the network to connect to the Internet
    - However, all computers have to be updated individually, in case of upgradation.

**NETWORK TOPOLOGY** -

- The term topology defines physical/logical arrangement of links in a network. Basic topologies are-
  - **STAR TOPOLOGY** -
    - It involves a central unit that has a number of terminals tied into it.
    - **Characteristics** -
      - It ties end user computers to a central computer
      - The central computer is usually a mainframe (host), which acts as the file server
      - Well suited to orgs. with one large data processing facility shared by a number of smaller department
    - **Advantages** -
      - It can be used by several users at same time
      - It is easy to add new modes & 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** -
  - the whole network is affected if main 'unit goes' down & all communication stop
  - it is considered less reliable than ring network & is heavily dependent on the central host computer. If it fails, there is no backup processing & communications capability & local computers will be cut off from the corporate headquarters & from each other
  - its cost is very high

**BUS NETWORK/BUS TOPOLOGY** -
- In it, a single length of wire, cable or optical fibre connects a number of computers
- **Features** -
  - all communications travel along this cable, which is called the bus
  - it has a decentralized approach
- **Advantages** -
  - if one microcomputer fails, it will not affect the entire network
  - it requires least amount of cable to connect & is less expensive than other cabling arrangements
  - it is easy to extend
  - a repeater can also be used to extend a bus configuration
- **Disadvantages** -
  - heavy network traffic can slow a bus considerably
  - each connection between two cables weakens the electrical signal
  - It is difficult to troubleshoot. A cable break/malfunctioning computer can be difficult to find and can cause the whole network to stop functioning

**RING NETWORK** -
- In it, the length of wire, cable, optical fibre connects to form a loop
- **Characteristics** -
  - each device is being connected to two other devices
  - it follows a decentralized approach
  - when one computer needs data from another computer, data is passed along ring
  - it is considered more reliable & less costly than star network because if one computer fails, the other computers in the ring can continue to process their own work and communicate with each other
- **Advantages** -
  - It doesn’t 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 a network by using the common communication channel
  - it is not as susceptible to break down as a star network, because when one computer in the rings fails, it doesn’t necessarily affect the processing or communication capabilities of the other computers in the ring
  - it offers high performance for a small number of workstation
  - it can span longer distances and is easily extendable
- **Disadvantages** -
  - it is relatively expensive and difficult to install
  - failure of one computer can affect the whole network
  - it is difficult to troubleshoot
  - adding or removing computers can disturb the network
**MESH NETWORK**-
- In it, there is random connection of nodes using communication links
- it may be fully connected or connected with only partial links
- each node is connected by a dedicated point to point link to every node
- it is very reliable as alternate parts are always available, if direct link between two nodes is down or dysfunctional
- it has high cost
- only military installations, which need high degree of redundancy, may have this network, that too with a small number of nodes

**Advantages**-
- it yields greatest amount of redundancy in the event that if one of the node fails, the network traffic can be redirected to another node
- the network problems are easy to diagnose

**Disadvantage** - it is costly to install and maintain

❖ **DIGITAL DATA TRANSMISSION**-
❖ The binary data is to be transmitted on a communication channel. It can be transmitted by either parallel mode or serial mode.

<table>
<thead>
<tr>
<th>Serial Transmission</th>
<th>Parallel Transmission</th>
</tr>
</thead>
<tbody>
<tr>
<td>In it, data bits are transmitted serially one after another</td>
<td>in it, data bits are transmitted simultaneously</td>
</tr>
<tr>
<td>data is transmitted over a single wire</td>
<td>data is transmitted over 8 different wires</td>
</tr>
<tr>
<td>it is a cheaper mode of transferring data</td>
<td>it is relatively expensive mode of transferring data</td>
</tr>
<tr>
<td>is useful for long distance data transmission</td>
<td>not practical for long distance communications, as it uses parallel paths, so cross talk may occur</td>
</tr>
<tr>
<td>it is relatively slower</td>
<td>it is relatively faster</td>
</tr>
</tbody>
</table>

Further, there is only one way to send parallel data, but two ways to send data under serial transmission- asynchronous & synchronous.

<table>
<thead>
<tr>
<th>Asynchronous Transmission</th>
<th>Synchronous Transmission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Each data word is accompanied by start and stop bits (start bit-0, stop bit-1)</td>
<td>the characters are allowed to be sent down the line without Start-Stop bits</td>
</tr>
<tr>
<td>extra start and stop bits slow down the transmission process relatively</td>
<td>it makes transmission faster as in absence of start and stop bits, many data words can be transmitted per second</td>
</tr>
<tr>
<td>it is relatively cheaper as it requires less hardware</td>
<td>Its device is more expensive to build, as it must be smart enough to differentiate between actual data &amp; special synchronous characters</td>
</tr>
<tr>
<td>more reliable as start and stop bits ensure that the sender and the receiver remain in step with one another</td>
<td>there are relatively higher chances of data loss</td>
</tr>
<tr>
<td>it is less efficient, as it is relatively more complex</td>
<td>it is more efficient and has greater throughput</td>
</tr>
</tbody>
</table>
TRANSMISSION MODE-
The transmission mode is used to define the direction of signal flow between two linked devices

SIMPLEX MODE-
- In it, the data flows only in one direction from the transmitter to the receiver
- It is useful if the data do not need to flow in both directions
- Eg- keyboards, printers

HALF-DUPLEX-
- It is sometimes, called as alternating connection or semi replace
- In it, data flow in one direction or the other, but not both at the same time
- It makes bidirectional communication possible, by using the full capacity of the line
- Eg- walkie talkie

FULL DUALPLEX-
- In it, 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
- Eg- mobile phones

TRANSMISSION TECHNIQUES-
It can be categorized into- Broadcast & Switched Networks

BROADCAST NETWORK-
- In it, data transmitted by one node is received by many, sometimes all, of the other nodes
- It refers to the method of transferring a message to all recipients simultaneously
- Eg- Live television or recorded content such as, movies, newscast, etc.

SWITCHED NETWORKS-
- in it, data transferred from source to destination is routed through the switch nodes
- Three common switching techniques are-
  - CIRCUIT SWITCHING-
    - It is one that establishes a fixed bandwidth circuit or channel between nodes and terminals before the users may communicate
    - the route is dedicated, exclusive & released only when communication session terminates
    - Eg- home phones
    - it goes through 3 phases- establish a circuit, transfer of data & disconnect the circuit
  - PACKET SWITCHING-
    - It 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
  - MESSAGE SWITCHING-
    - In it, end-users communicate by sending each other a message, which contains the entire data being delivered from the source to destination node
    - Each intermediate switch within the network stores the entire message, before retransmitting them one at a time as proper resources become available
    - The above characteristic is often referred to as “store-and-forward”
    - Eg- email and voicemail
Network Architectures & Protocol:

Network architecture refers to the layout of the network consisting of the hardware, software, connectivity, communication protocols & mode of transmission, such as wired or wireless.

Protocols:

- It is a set of rules for inter-computer communication that have been agreed upon & implemented to ensure information being exchanged between the two parties is received and interpreted correctly. Ideally, it allows heterogeneous computers to talk to each other.
  - Protocol defines following 3 aspects of digital communication:
    - Syntax is the format of data being exchanged, character set used, type of error correction used & type of encoding scheme used
    - Semantics is the type and order of messages used
    - Timing defines data rate selection & correct timing for various events during data transfer
  - It is embedded/built either in a computer's memory or memory of transmission.

The “OSI” Model:

Layer 7: Application Layer

- It is closest to the end user, which means that both the OSI application layer and the user interact directly with the software application and provide user services by file transfer, file sharing, etc.

Layer 6: Presentation Layer

- Also known as syntax layer, it converts incoming & outgoing data from one presentation format to another & further, controls on-screen display of data.
  - Encryption, data compression, can also be undertaken at this layer level

Layer 5: Session Layer

- This layer sets up, coordinates, & terminates conversations, provides for full-duplex, half-duplex, or simplex-operation.
  - It is responsible for a ‘graceful close’ of sessions also

Layer 4: Transport Layer

- It ensures reliable & transparent transfer of data between user processes, assembles & disassemble message packets and provides error recovery and flow control.

Layer 3: Network Layer

- It makes a choice of the physical route of transmission, creates a virtual circuit for upper layers to make them independent of data transmission & switching, establishes, maintains, terminates connections between the nodes & ensure proper routing of data.

Layer 2: Data Link Layer

- It is the protocol layer which transfers data & ensures reliable transfer of data through the transmission medium.
  - It detects & possibly correct errors that may occur in the physical layer.

Layer 1: Physical Layer

- It is a hardware layer, which performs following major functions and services -
  - establishment & termination of a connection to a communication medium
  - participation in the process whereby the communication resources are effectively shared among multiple users.

Internet's TCP/IP:

- It has five layers:
  - Application/Process Layer = Application + Presentation + Session Layer of OSI Model
- Host-to-Host Transport Layer = Transport Layer of OSI Model
- Internet Protocol = Network Layer of OSI Model
- Network Interface = Data Link Layer of OSI Model
- Physical Layer = Physical Layer of OSI Model

The above points also show the relationship between TCP/IP & OSI Model

**NETWORK RISKS, CONTROLS & SECURITY** -

- There are two types of system security -
  - **physical security** is to protect the physical systems assets of the organisation
  - **logical security** protects data/information and software by having controls over
    - malicious/non-malicious threats to physical security, and,
    - malicious threats to logical security itself

**THREATS & VULNERABILITIES** -

- **Threats** -
  - It is a possible danger that can disrupt the operation, functioning, integrity or availability of a network or a system
  - It is categorized into 4 types -
    - **Unstructured threats** originate mostly from inexperienced individuals using easily available hacking tools from the Internet & are done more out of curiosity than with malicious intent
    - **Structured threats** originate from individuals who are highly motivated, technically competent & usually understand network systems design and their vulnerabilities. These are, usually, hired by industry competitors
    - **External threats** originate from individuals/organisations working outside an org, which does not have authorised access to org's computer systems or network
    - **Internal threats** typically originate from individuals who have authorised access to the network & may come from a discontented former or current employee. It has been seen that majority of security incidents originate from internal threats.

- **Vulnerability** -
  - It is an inherent weakness in the design, configuration, or implementation, of a network or system that renders it susceptible to a threat
  - Reasons behind occurrence of vulnerabilities are -
    - **Software Bugs** are so common that users have developed techniques to work around the consequences, and bugs that makes saving work necessary every hour or crash computer every so often are considered as normal part of computing (eg- access validation error)
    - **Timing Windows** may occur when a temporary file is exploited by intruder to gain access of same, overwrite important data & use file as a gateway for advancing further into system
    - **Insecure default configurations** occur when vendors use known default passwords to make it as easy as possible for consumers to set up new systems. Sadly, most intruders know this passwords & can access systems effortlessly (eg- 1234)
    - **Trusting untrustworthy information** as bogus routers can gain access to systems and do damage, when routers are not programmed to verify that they are receiving information from a unique host
    - **End users** are, generally, not professionals and are not always security conscious.
LEVELS OF SECURITY-
It means periodic review of control exercised & involves following 8 steps-

- **Preparing project plan for enforcing security** which includes outlining objectives of the review, determining scope of review & tasks to be accomplished, organizing task, assigning tasks to project team, preparing resources budget & fixing schedule for completion
- **Identifying assets** that need to be safeguarded & subdividing them into personnel, hardware, facilities, documentation, supplies, data, application software & system software
- **Valuation of assets** is to be done, which is considered as apart from valuation of logical asset. However, it is difficult step as it depends on who is doing valuation & method adopted
- **Identifying threats**, whose source can be internal/external & differs in nature as well (can write a little about types of threats done above)
- **Assessment of probability of occurrence of threats** over a given time period, & can be done either by statistical data or from associated stakeholders (end-users, management, etc)
- **Do exposure analysis** by identifying controls in place, assessing reliability of existing controls, evaluating probability of threat to be successful & resulting loss if threat is successful
- **Do controls adjustment**, which means whether over some time any control can be designed, implemented & operated, so that controlling cost is lower than reduction in expected losses, which is a difference between existing & improved set of controls
- **Report generation**, documenting the findings of review & recommending new assets safeguarding techniques to be implemented & existing techniques to be eliminated/rectified, recommending assignment of levels of security for end-users & systems.

NETWORK SECURITY-
It involves four aspects-

- **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 unintelligible to unauthorised users
  - **Cryptography** is constructing & analysing protocol to overcome the influence of adversaries & which are related to various aspects in information security, eg, data confidentiality, etc
  - **encryption** is the process of encoding messages in such way that hackers cannot read it but only authorised parties can. **Decryption** is recovery of original message from encrypted data
    - **plain text** is the message that is to be encrypted
    - **cipher text** is the output of the encryption process that is transmitted
    - **encryption model**- sometimes intruder injects his own message, or modify legitimate messages before they get to receiver. **Cryptanalysis** is art of breaking cipher & **cryptography** is art of devising them. **Cryptology**= cryptanalysis + cryptography.
  - Two categories of encryption/decryption(e/d) method-
    - in **secret key e/d method**, same key is used by both sender & receiver
    - in **public key encryption**, there are two keys: a private key and public key. The private key is kept by the receiver & the public is announced to the public
  - Two basic approaches to encryption-
    - **hardware encryption devices** are available at a reasonable cost & support high-speed traffic. Use of such devices can ensure that all traffic between these offices is secure.
    - **software encryption** is typically employed in conjunction with specific applications, eg, electronic mail packages

Twitter- @tweetopians
- **authentication** means that the receiver is sure of the sender’s identity and that an imposter has not sent the message
- **integrity** means that data must arrive at the receiver exactly as it was sent, without any changes during the transmission—either accidentally or malicious
- **non-repudiation** means that receiver must be able to prove that a received message came from a specific sender, to which the sender must not be able to deny
- All these can be achieved by using digital signature, where private key is used for encryption and the public key is used for decryption

**NETWORK SECURITY PROTOCOLS**-

- **SSH-SECURE SHELL (SSH)**
  - A program to log into another computer over network, to execute commands in a remote machine
  - it provides strong authentication and secure communications over insecure channels
  - during login, the entire login session, including transmission of password, is encrypted, therefore, it is almost impossible for an outsider to collect passwords
- **SFTP (SSH FILE TRANSFER PROTOCOL)/ Secure FTP**-
  - It encrypts commands and data both, preventing passwords and sensitive information from being transmitted in the clear over a network
- **HTTPS (HYPERTEXT TRANSFER PROTOCOL SECURE)**-
  - it is a communications protocol for secure communication over a computer network
  - Security of HTTPS encrypt the data flow between client and server
- **SSL (SECURE SOCKET LAYER)**-
  - It is typically used when a web browser needs to securely connect to a web server over the inherently insecure Internet
  - it is used to secure online credit card transactions, systems login, etc.

**NETWORK SECURITY TECHNIQUES**-

- Several tools/technologies are now available to protect information & systems against compromise, intrusion, or misuse. Some of them are-
  - **Intrusion detection system (IDS)** is a device to monitor network assets, so as to detect anomalous behaviour and misuse. Its types are-
    - network intrusion detection (NID) device intercept packets travelling along various communication mediums & protocols, in search of unwanted/malicious events. It detects outsider misuse
    - host based intrusion detection (HID) is concerned with what occurs on the host themselves. It is best suited to combat internal threats because of its ability to monitor & respond to specific user actions & file accesses on the host. It detects insider misuse.
  - **Firewall** is a device that forms a barrier between a secure and an open environment. It acts as a system or combination of systems that enforces a boundary between more than one networks.
  - **Network Access Control** handle access authentication & authorisation function, & can even control the data that specific users’ access, based on their ability to recognize users, their devices & their network roles.
  - **Anti-Malware** network tools help administrators identify block & remove malware. Best practices call for a multipronged defense, that also includes IP blacklisting, anti-virus, anti-spyware, etc.
Malware is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems & includes viruses, worms, trojan horses, etc.

- Site Blocking prohibits access to certain websites that are deemed inappropriate by management. Org can also log activities & determine the sites visited & amount of time spent on the Internet

**NETWORK ADMINISTRATION & MANAGEMENT:**

- Network management refers to the tools that pertain to operation, administration, maintenance, & provisioning of networked systems.
  - **Operation** deals with keeping the network (& services it provides) up & running smoothly & includes monitoring network to spot problem sooner, ideally before users are affected
  - **Administration** deals with keeping track of resources in network & how they are assigned & includes all housekeeping necessary to keep network under control
  - **Maintenance** deals with performing repairs & upgrades, and also includes corrective & preventive measures to make managed network run “better”.
  - **Provisioning** deals with configuring resources in network to support given service

- Common way of characterizing network management functions is FCAPS which is explained below-

  - **Fault Management**
    - Fault is an event that has negative significance
    - Fault management aims to recognize, isolate, correct & log faults that occur in network
    - It identifies & isolates network issues, proposes problem resolution, & logs the issues & associated resolutions

  - **Configuration Management**
    - It monitors network & system configuration information to track & manage the impact of network operations
    - Network changes, addition, deletions, need to be coordinated with network management personnel

  - **Accounting Management**
    - It is concerned with tracking network utilization information so that customers can be appropriately billed & charged for accounting purpose
    - For non-billed networks, it means administration, whose aim is to administer authorized users & administering the operations of the equipment

  - **Performance Management**
    - It measures & makes network performance data available, to maintain performance
    - It enables manager to prepare network for future, & to determine efficiency of current network
    - It addresses the throughput, network response time, packet loss rates, error rates, etc

  - **Security Management**
    - It controls access to network resources as established by organisational security guidelines
    - Its functions include managing network authentication, authorization, & auditing so that the users have access to appropriate network resources, configuration, IDS, etc

**THE INTERNET REVOLUTION:**

- The Internet does not have a central computer system or telecommunication centre. Instead, each message sent on 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 for governing body

Twitter- @tweetopians
- **Business value of applications of telecommunications networks on e-business**:  
  - overcome geographic barriers by capturing information about business transactions from remote location  
  - overcome time barriers by providing information to remote locations immediately after it is requested  
  - overcome cost barriers by reducing the cost of more traditional means of communication  
  - overcome structural barriers by supporting linkages for competitive advantage

- **NETWORKS AND THE INTERNET**:  
  - The **Internet** is the global computer network, or “information super-high way”. It is the network that serves as a backbone for the world-wide web  
  - **Intranet** is a company’s private network accessible only to the employees of that company, to distribute data/information to employees, to make shared data/files available and to manage projects within the company via chat rooms, video conference, etc  
  - **Extranet** is similar to an Intranet except that it offers access to selected outsiders. It allows business partners to exchange information, who may be given limited access to company servers & access only to the data necessary to conduct supply chain exchanges with the company

- **INTERNET ARCHITECTURE**:  
  - **Digital subscriber line (DSL)**:  
    - It reuses the telephone line that connects to our house for digital data transmission  
    - computer is connected to a device, called a DSL modem, that converts between digital packets and analog signals  
    - It is called dial-up  
    - at the other end, device called DSLAM (DSL Access Multiplexer) converts between signals & packets  
  - Another method is to send signals over cable TV system. The device at home-end is called cable modem & the device at cable head-end is called the CMTS (Cable Modem Termination System)  
  - **Wireless** is used for Internet access for 3G mobile phone networks. We call the location at which customer packets enter the ISP network for service the ISP’s POP (Point of Presence)

- **INTERNET APPLICATIONS**:  
  - **E-mail, browsing the sites**  
  - electronic Commerce transactions  
  - electronic discussion forums  
  - downloading software & information files and accessing databases  
  - holding real-time conversations

- **BUSINESS USE OF INTERNET**:  
  - strategic business alliances  
  - collaboration among business partners  
  - buying and selling products and services  
  - marketing, sales, and customer service applications  
  - enterprise communications and collaboration  
  - attracting new customers with innovative marketing and products  
  - retaining present customers with improved customer service and support  
  - Electronic Commerce

- **INTRANET**:  
  - An intranet is protected by security measures such as passwords, encryption & firewalls and thus, can be accessed by authorised users to the Internet

Twitter- @tweetopians
- **Business Value of Intranet** is that it supports communications & collaboration, business operations and management, web publishing.

- **Communications & Collaboration**-
  - it allows us to send and receive e-mail, voicemail, paging and fax
  - to collaborate better using services, eg, discussion groups, chat rooms, video conferencing

- **Web Publishing**: the comparative ease, attractiveness and lower cost of publishing & accessing multimedia business information such as company’s newsletters, technical drawings, product catalogs.

- **Business Operations & Management**: for developing and deploying critical business applications to support business operations and managerial decision making

❖ **EXTRANETS**-
   - Definition already done
   - **Business Value of Extranets**-
     - Makes customer and supplier access of intranet resources a lot easier and faster than previous business methods
     - It offers new kinds of services to their business partners
     - It enables & improve collaboration by business with its customer & other business partners
     - It facilitates an online, interactive product development, marketing.
   - It requires security & privacy that require firewall server management, user authentication, encryption of messages & use of VPN
   - It is used by companies to do following tasks-
     - share product catalogue
     - collaborate with other companies
     - develop and use training programs
     - provide or access services provided by one company to a group of other companies
     - share news of common interest
   - Telecommunications provide value by increasing efficiency of operations, improving effectiveness of management, & innovations in marketplace, which are provided by following impacts-
     - **time compression** by transmitting raw data & information quickly and accurately between remote sites.
     - **overcoming geographical dispersion** by enabling geographically remote sites to function, as though these sites were a single unit
     - **restructuring business relationship** by restructuring the interactions of people within a firm as well as a firm’s relationships with its customers by eliminating intermediaries.

❖ **ELECTRONIC COMMERCE**-
   - It 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.
   - **BENEFITS OF E-COMMERCE APPLICATION & IMPLEMENTATION**-
     - creation of new markets through the ability to easily and cheaply reach potential customers
     - easier entry into markets, especially geographically remote markets
     - better quality of goods as specifications are standardized and competition is increased
     - reduction in advertising costs

Twitter: @tweetopians
• reduction in overhead costs through uniformity, automation and large-scale integration of management processes.
• reduction in time to complete business transactions
• reduction in errors, time, and overhead costs and information processing, and,
• reduction in cost to buyers

RISKS INVOLVED IN e-COMMERCE-
• Problem of anonymity-
  ▪ Identify and authenticate users in the virtual global market where anyone can sell or buy from anyone, anything from anywhere
• Repudiation of contract-
  ▪ There is a possibility that the electronic transaction may be denied
• Lack of authenticity of transactions-
  ▪ the electronic documents that are produced may not be authentic and reliable
• 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
• Non-recognition of electronic transactions-
  ▪ e-Commerce transactions, as electronic records may not be recognised as evidence in court of law
• Lack of audit trail-
  ▪ audit trails in e-Commerce system may be lacking
• Payment Risk-
  ▪ Pre-payment also posses risk in e-commerce.

TYPES OF e-COMMERCE-
BUSINESS-TO-BUSINESS (B2B) e-COMMERCE
• It refers to the exchange of services, information &/or products from one business to another and IT is performed in much higher volume

BUSINESS-TO-CONSUMER (B2C) e-COMMERCE
• it means exchange of services, information &/or products from a business to a consumer
• it saves time and money, but customers must be provided with safe, secure, convenient and easy-to-use options when it comes to paying for merchandise
• ADVANTAGES-
  • Shopping can be faster & convenient
  • Offers & prices can change instantaneously
  • Call centers can be integrated with websites
  • Broadband telecommunications will enhance buying experience

CONSUMER-TO-BUSINESS (C2B) e-COMMERCE
• in it, consumers directly contact with business vendors by posting their project work online so that the needy companies review it & contact the customer directly (eg- freelancer.com)

CONSUMER-TO-CONSUMER (C2C) e-COMMERCE
• It provides a virtual environment in which consumers can sell to one another through a third party intermediary. (eg-OLX)

BUSINESS-TO-GOVERNMENT (B2G) e-COMMERCE
• it refers to the use of information & communication technologies to build & strengthen relationships between Government & employees, citizens, businesses.
**BUSINESS-TO-EMPLOYEE (B2E) e-COMMERCE**
- it has provided a means for business to offer online products & services to its employees

**KEY ASPECTS TO BE CONSIDERED IN IMPLEMENTING e-COMMERCE**
- Implement appropriate policies, standards and guidelines
- Perform cost benefit analysis and risk assessment
- Implement right level of security across all layers & processes
- Establish & implement best practice controls, and,
- Provide adequate user training

**MOBILE COMMERCE**
- It is the buying and selling of goods and services through wireless handheld devices
- it enables users to access the Internet without needing to find a place to plug in
- it is faster, more secure and scalable
- **Industries affected by mobile commerce are**-
  - financial services industry, which includes mobile banking also
  - telecommunications industry, in which service changes, bill payment, & account reviews can be conducted from the same handheld device
  - service/retail industry as consumers are given the ability to place and pay for orders
  - information services industry, which includes delivery of financial news, sports figures & traffic updates

**ELECTRONIC FUND TRANSFER (EFT)**
- It represents the way the business can receive direct deposit of all payments from the financial institution to the company bank account
- it is paperless, fast, safe, & means that money will be confirmed in user’s bank account quicker than if he had to wait for the mail, deposit cheque, and wait for the funds to become available
- **Examples of EFT are**-
  - Automated Teller Machines (ATMs)-
    - consumers can do their banking without the assistance of a teller electronically. These machines are used with a debit card & a PIN
  - Point-of-Sale (PoS) Transactions-
    - It 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. Money is taken out of the consumer’s account and put into the merchant’s account electronically
  - Preauthorized Transfers-
    - It 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 to do so. Eg-insurance, mortgage, other bills, etc
  - Telephone Transfers-
    - Consumer can transfer funds from one account to another through telephone instructions