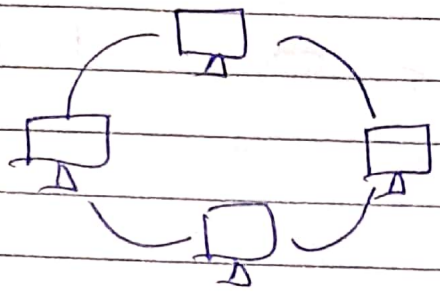
Unit=4

Computer Network :- A group of computers which are connected to each other for the purpose of sharing their resources is called computer network.



First Computer Network :- ARPANET

Advanced Research projects Agency Network

Characteristics of Computer Network :-

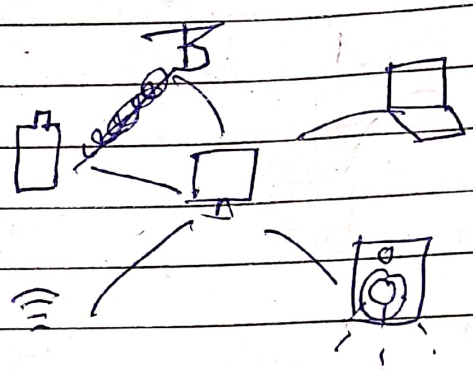
1. Resource sharing
2. Communication speed
3. Back up
4. Scalability
5. Reliability
6. S/w & H/w sharing
7. Security

Network Devices :-

HUB, Switch, BRIDGE, Gateway, modem, Router, Repeater etc....

Network types :-

① PAN :- Personal Area Network

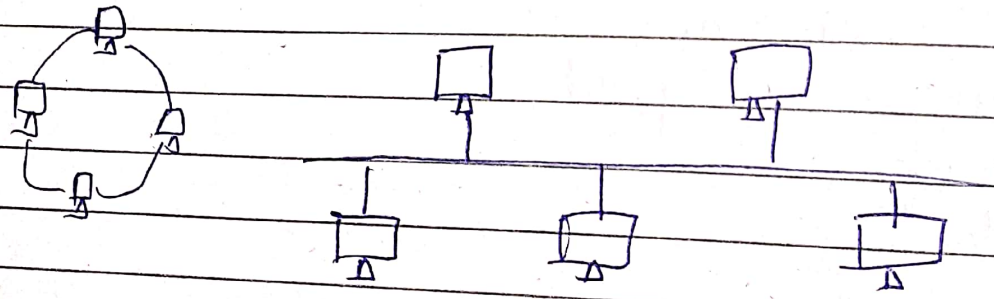


Range - (<10m)

Use :- Home (for personal use)

PAN is a small network. PAN can be wired or wireless, and are often used in homes and offices.

② LAN :- Local Area Network

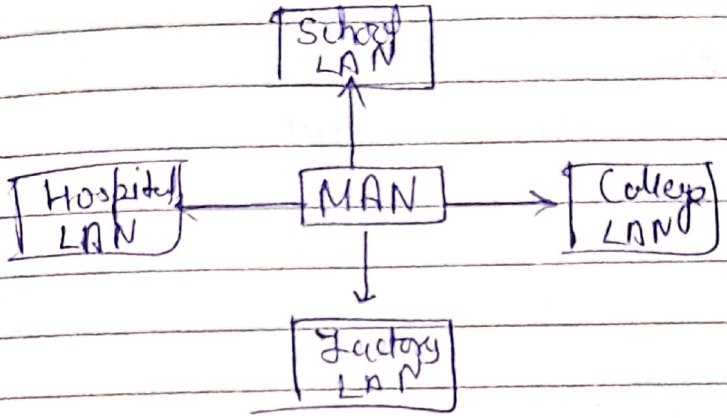


Range < 150 km

Use → office (Building

Media access control method in a LAN, the bus-based Ethernet and token ring.

③ MAN :- Metropolitan Area Network

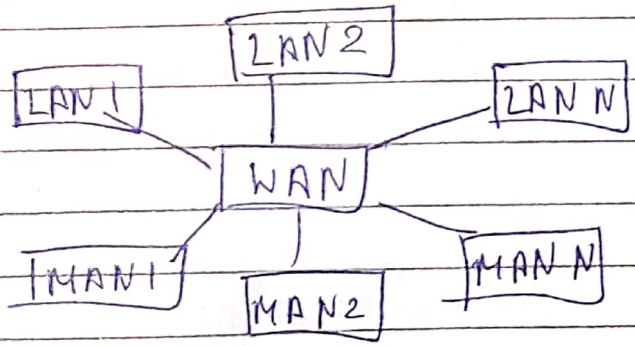


Range :- <50 KM

Use :- Within City.

It covers the towns and cities (50 KM). MAN is used by the communication medium for optical fiber cable, it also used for other media.

④ WAN :- Wide Area Network



Range :-
< Not Fixed >

Use :- All around world.

It's covers the large distance. Communication medium used are satellites, telephone which are connected by the routers.

Advantages :- ① open to everyone
② File sharing
③ Security
④ Easy to add new devices
⑤ Backup & storage

Disadvantages :- ① N/w devices required
② Virus attack
③ Required Handler
④ High speed Internet

Goals :- ① Resource sharing
② performance
③ Security
④ Reliability
⑤ Expanded storage capability
⑥ Secure remote access
⑦ Error minimization.

OSI / ISO - Reference Model

(Open system interconnection) / (International standard organization)

⇒ The OSI reference model has 7 layers.

⇒ Each layer should perform a well defined function.

DATE
PAGE

⇒ Big picture of communication over network is understandable.
⇒ We see how hardware and software work together.
⇒ We can understand new technologies as they are developed.

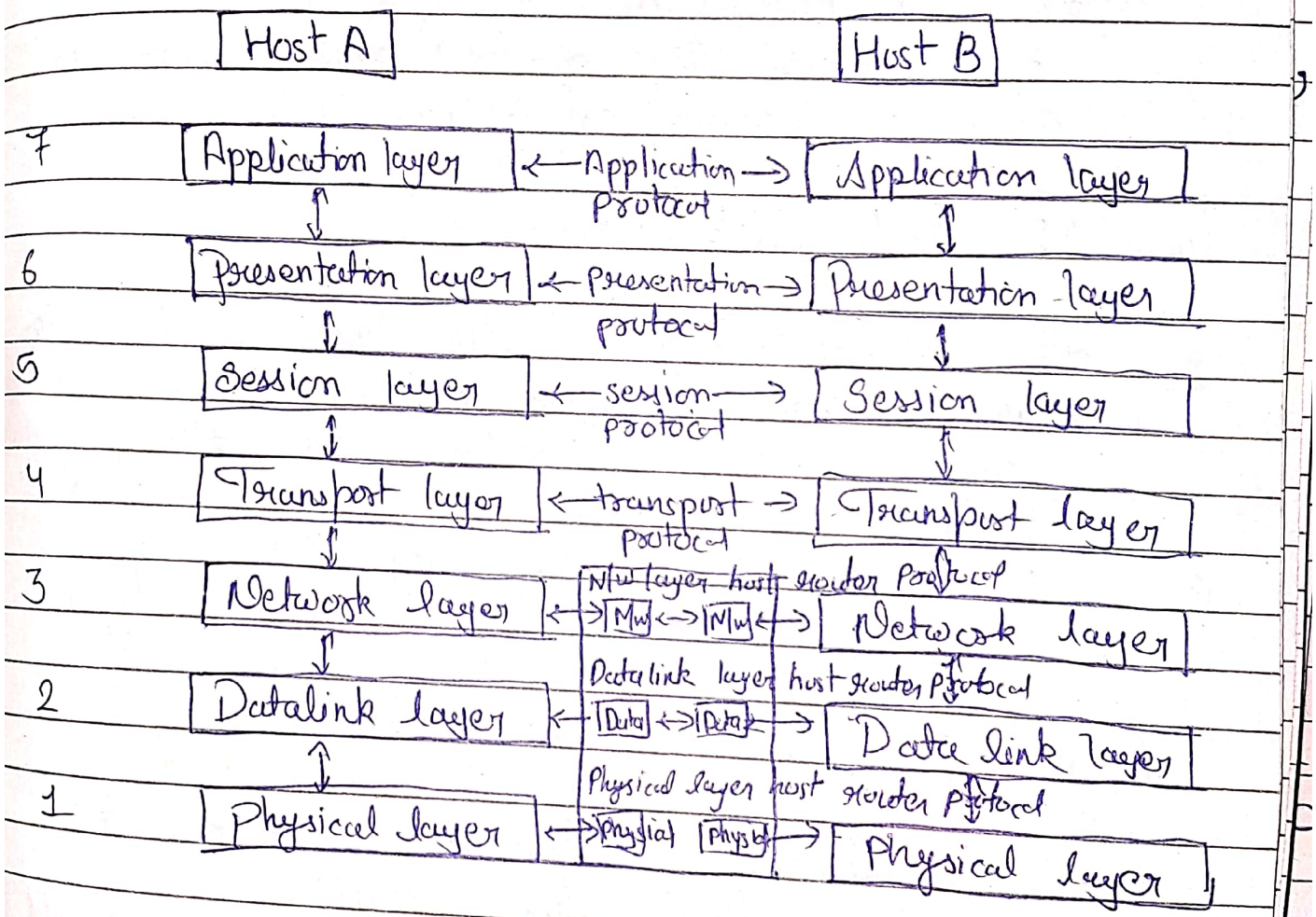


fig :- OSI Reference model

Description and Fuction of different layers:-

Layer 1 :- The physical layer :-

1. It is the lowest layer of the OSI Model.
2. It activates, maintains and deactivates the physical connection.
3. It converts the digital / analog bits into electrical signal or optical signals.

layer 2 :- Data link layer :-

1. The main function of this layer is to make sure data transfer is error free from one node to another over the physical layer.
2. Transmitting and receiving data frames sequentially is managed by this layer

layer 3 :- The Network layer :-

1. It acts as a network controller. It manages the subnet traffic.
2. It decides by which route data should take.

layer 4 :- Transport layer

1. It decides if data transmission should be on parallel path or single path.

2. Transport layer can be very complex, depending upon the network requirement.

Layer 5 :- The session layer :-

1. Session layer manages and synchronize the conversation between two different applications.
2. Transfer of data from source to destination session layer stream of data are marked and are resynchronized properly, so that the ends of the messages are not ~~cut~~ cut prematurely, and data loss is avoided.

Layer 6 :- presentation layer :-

1. While receiving the data, presentation layer transform the data to be ready for the application layer.
2. It performs Data compression, Data encryption, Data conversion or Data translation etc.

Layer 7 :- Application layer :-

1. It is the topmost layer.
2. This layer mainly holds application programs to act upon the received and to be sent data.

Merits of OSI reference model :-

1. Protocol of OSI model are very well hidden.
2. protocol can be replaced by new protocol as technology changes.

Demerits of OSI reference model :-

1. Fitting of Protocol is tedious task.
2. It is just used as a reference model.

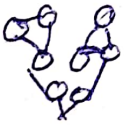
Internetworking Concept & Introduction to Internet :-

Internetworking Concept :- Internetworking, often called interconnecting network, is the practice of connecting different computer networks or network segments to create a larger and more extensive network infrastructure.

Various networking technologies, protocols and devices including routers and switches, are used to enable communication and data exchange between these distinct network.

Interconnect network
↓
Internet

DATE
PAGE



Types of Internetworking :-

1. Intranet
2. Extranet
3. Internet

Introduction to Internet

Internet :- It is a Global network of Computer, (servers or Clients) to exchange information.

* It is a "network of network" that includes millions of private and public, academic, business and government networks (local or Global), linked by copper wires, wireless connections and other technologies.

Application of Internet :-

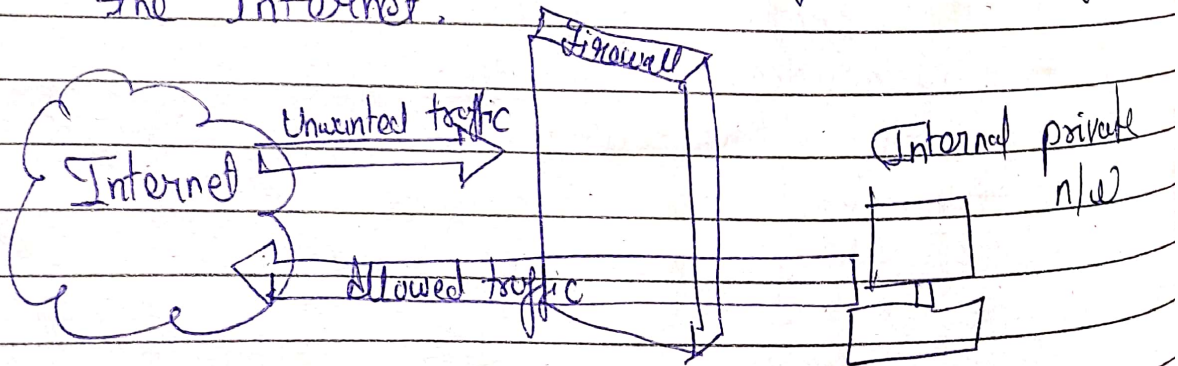
1. Download programs and files
2. E-Mail
3. Voice and Video Conferencing
4. E-Commerce
5. File sharing
6. Information browsing
7. Search the web addresses for access through search engine
8. chatting and many more.

Intranet :-

* Internal company network that uses Internet standards (HTML, HTTP & TCP/IP protocols) & software.
* Accessed only by authorized persons, especially members or employees of the organization.

Firewall :-

* Security device located between firm's internal network (intranet) & external network (internet)
* A firewall is a network security system that manages the network traffic based on some protocol → set of rules.
* Most personal computers use software based firewalls to secure data from threats from the internet.



* Firewalls exist as software and hardware both.

Applications of Intranet :-

* sharing of company policies / rules & regulation
* Access employee database
* Distribution of circulars / office Orders
* Access product & customer data
* Sharing of information of common interest
* Launching of personal / departmental home pages
* Submission of reports.
* Corporate telephone directories.

Extranet :-

* Extranet is an Intranet for outside authorized users using same internet technology.
* Inter-organizational information system.
* enable outsiders to work together with company's employees.
* open to selected suppliers, customers & other business partners.

~~Example~~

Networking Device :-

Network devices are various hardware devices that are used to connect computers, printers etc to a network.

* Switch * Hub * Router * Bridge
* Gateway * NIC card * Repeater * Modem

① Network Interface Card :- * It is also called Ethernet card, Network card, LAN card, Network Adapter Card (NAC) or Network Interface Unit (NIU) or terminal Access point (TAP).

* It is a physical and data link layer device used by computers to connect and communicate with other devices on the LAN

② Wi-fi (Wireless Fidelity) Card :- * is used to connect any device to local network wirelessly.

(Radio & Antena)

* The physical area of the network which provides internet access through Wi-fi is called Wi-fi hotspot or Wifi Access point.

Networking Device :-

Network devices are various hardware devices that are used to connect computers, printers etc to a network.

* Switch * Hub * Router * Bridge
* Gateway * NIC card * Repeater * Modem

② Network Interface Card :- * It is also called Ethernet card, Network card, LAN card, Network Adapter Card (NIAC) or Network Interface Unit (NIU) or terminal Access point (TAP).

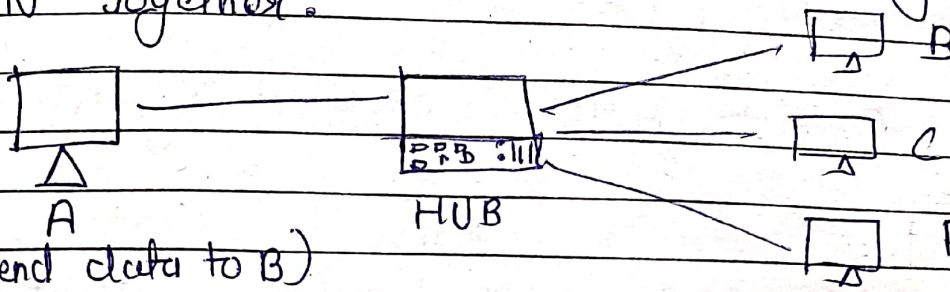
* It is a physical and data link layer device used by computers to connect and communicate with other devices on the LAN

② Wi-fi (Wireless Fidelity) Card :- * is used to connect any device to local network wirelessly.

(Radio & Antena)

* The physical area of the network which provides internet access through Wi-fi is called Wi-fi hotspot or Wifi Access point.

(3) HUB :- HUB is a physical layer device which has multiple ports that are used to connect multiple computers or segments of LAN together.

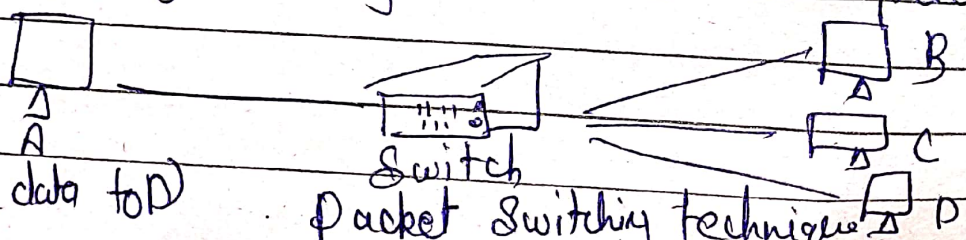


Passive Hub :- allows the signals to be passed without any change.
Active Hubs :- amplify the signals as it moves from one device to another.

Disadvantage :-

* Hub is not secure and safe
* Copying the data packets on all the interface makes it slower and more congested
* To overcome this problem we use of network switch.

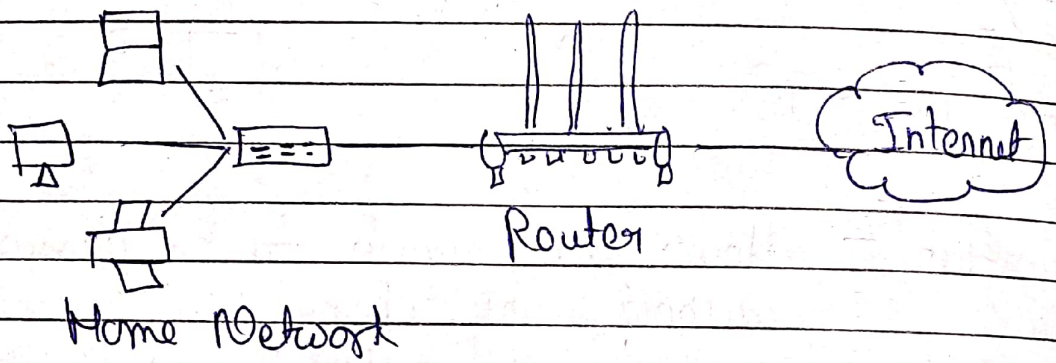
(4) Switch :- Hub just does the work of data forwarding, a switch does "filter and forwarding" which is a more intelligent way of dealing with the data packets. layer 2



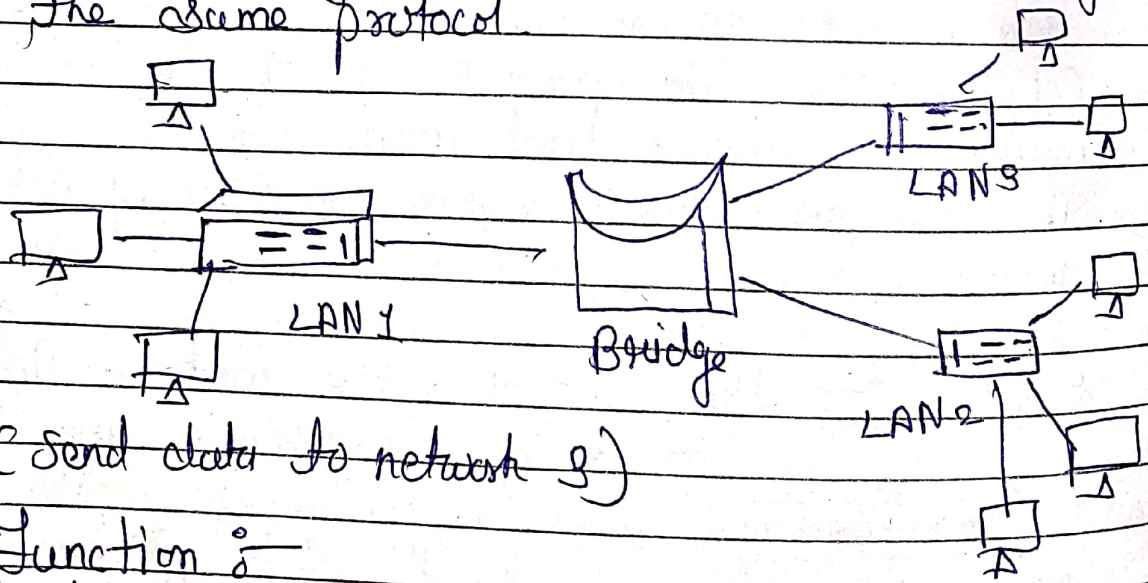
Packet Switching technique

(5) Router :- Router is mainly a Network layer device. It can work like a switch that routes data packets based on their IP addresses. (Costly)

Connects Multiple Network Together



(6) Bridge :- A bridge connects two or more LANs. It operates at data link layer. Bridges handles network that follow the same protocol.

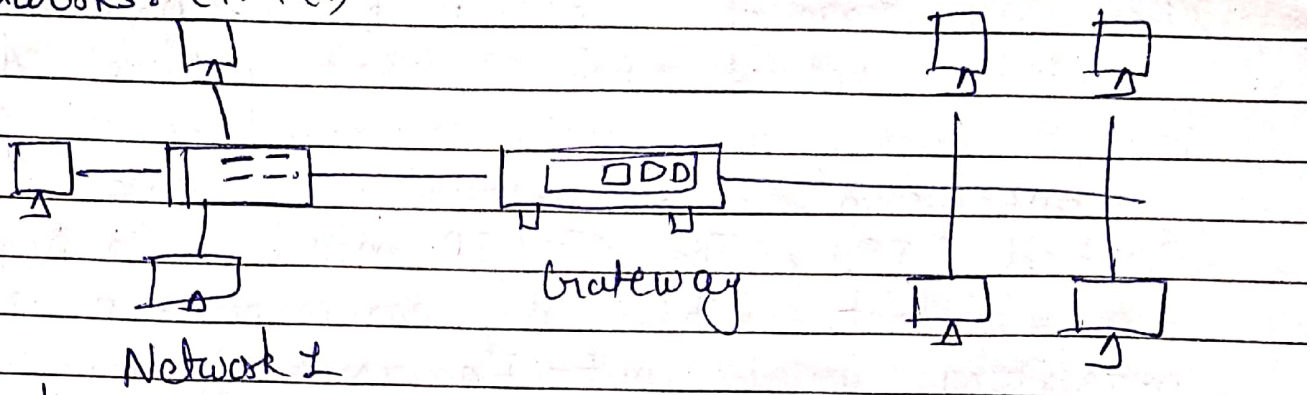


(Send data to network 3)

Function :-
- Filtering
- Forwarding
- blocking

DATE
PAGE

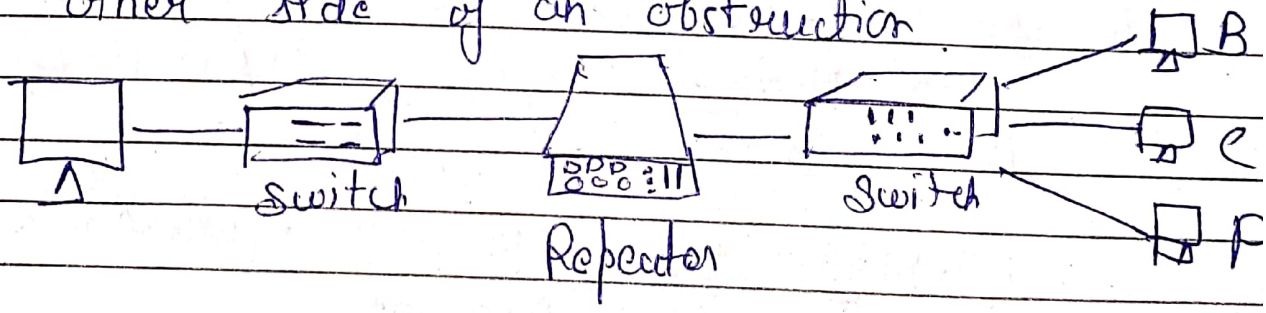
⑦ Gateway :- Gateway is a network device used to connect two or more dissimilar networks. (Protocol)



Function :-

* proxy server
* Firewall
* Malware protection

⑧ Repeater :- Repeater are used to extend transmission so that the signal can cover longer distance or be received on the other side of an obstruction. (Signal regenerator)



⑨ Modem :- Modem stands for Modulator Demodulator. A modem is a networking device of computer network that is used to convert digital signal to analog signal and analog signal to digital signal.

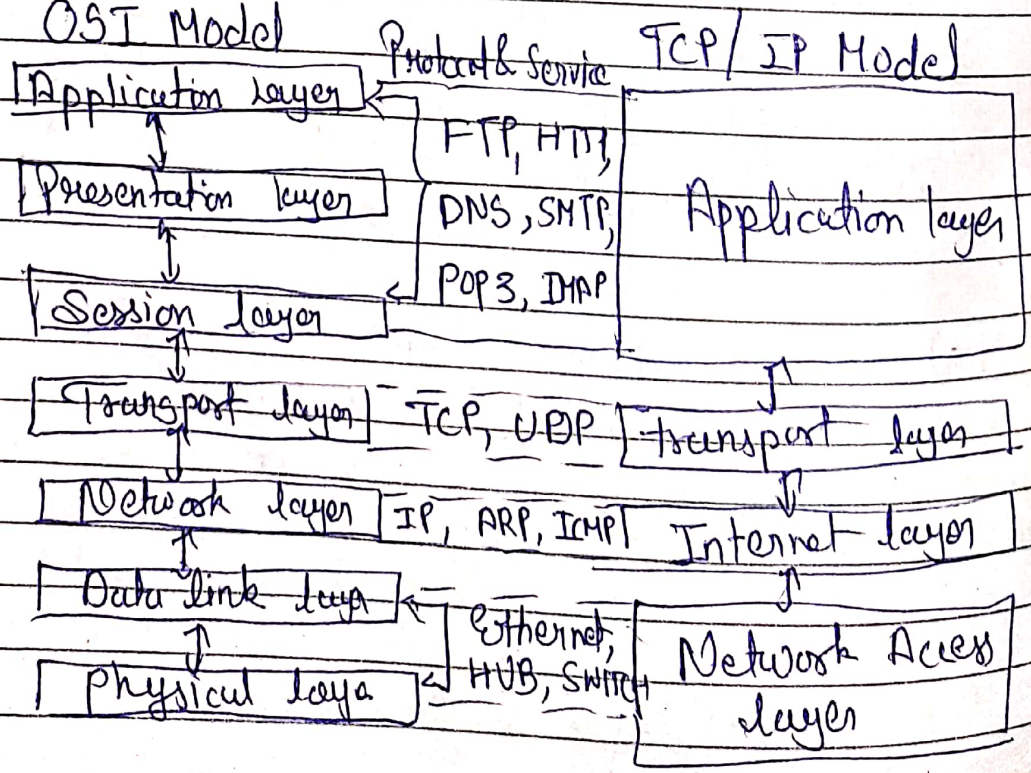
Ex :- Telephone or cable line.

TCP/IP Protocol :-

The full form of TCP/IP is Transmission Control protocol and Internet protocol. As per its name, this model is based on two protocol: Transmission Control protocol (TCP) and Internet protocol (IP). The TCP/IP model is so highly useful that without it, communication in networking would not be as easy for us.

The TCP/IP model is a set of rules designed for storing and transmitting data on the internet.

Protocol :- A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network.



TCP/IP Model

Application

transport

Internet

Network

(1) Network layer :- The network layer is the lowest layer of the TCP/IP model, which is responsible for data transmission in the network. The network layer describes how data is sent in the network. This layer is a combination of the data link layer and physical layer defined in the OSI model. It is responsible for the transmission of data between two devices on the same network.

The function of this layer also includes encapsulating the IP datagram transmitted by the network into frames and mapping the IP address to the pysical address.

(2) Internet layer :- The Internet layer provides connectionless communication in the network, where data is in the form of datagrams.

Datagrams contain the source and destination IP addresses, facilitating the easy sending and receiving of data.

DATE
PAGE

Protocol used in Network layer :-

* IP Protocol :- It stand for Internet protocol, and its main function is to deliver packets from the source to the destination. It has two versions : IPv4 and IPv6.

* ARP :- It stands for Address Resolution Protocol. Its function involves resolving the physical address from the IP address. It has various types, such as RARP, PARP etc.

* ICMP :- It stands for Internet Control Message Protocol. Its function is to inform the host about potential problems that may occur in the network.

(3) Transport layer :- The transport layer provides a solid and reliable connection for data to reach its destination. When data reaches the transport layer, it is divided into data packets and the data is also sequenced.

The Transport layer determines how much data should be sent where it should be sent, and at what rate. It is this layer that ensures data is sent in sequence on the TCP/IP protocol.

Protocol Used in Transport layer :-

1) Transmission Control protocol
2) User Datagram protocol

(4) Application layer :- The Application layer is the topmost layer in the TCP/IP model, responsible for providing communication to users. It sends data to the Transport layer and receives data from it.

Protocols Used in Application layer :-

1. HTTP and HTTPS :- It stand for Hypertext transfer protocol.
Through HTTP, we can access data on the internet, and it transfers data in the forms of text, audio, and video. The full name of HTTPS is HTTP secure. When we use SSL with HTTP, it becomes HTTPS.

2. SNMP :- It stand for Simple Network Management protocol. This is a framework used to manage device on the internet.

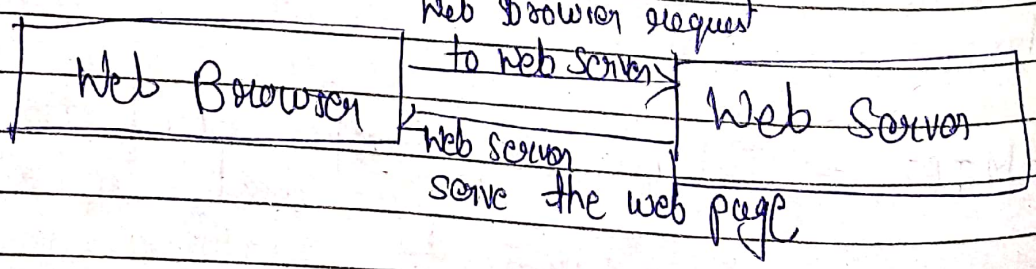
3. SMTP :- Stand for Simple Mail transfer protocol. It is used to sent data from one email address to another in the form of an email.

4. DNS :- Stand for Domain Name System. It is used to map an IP address.

5. SSH :- Stand for Secure shell. It is used for encryption.

WWW (World Wide Web) :- often called the Web, is a system of interconnected webpages and information that you can access using the Internet. It was created to help people share and find information easily, using links that connect different pages together. The Web allow us to browse websites, watch videos, shop online, and connect with other around the world through our computer and phones.

WWW stand for World wide web and is commonly known as the Web. The WWW was started by CERN in 1989. WWW is defined as the collection of different websites around the world.



Features of WWW :-

* WWW is open source
* It is a distributed system spread across various websites.
* It is Cross platform
* It is a Hypertext Information System.

Components of the Web :-

There are 3 component of the Web :-

* Uniform Resource Locator (URL) :- serves as a system for resource on the web.
* Hyper text transfer protocol :- (HTTP) :- Specifies communication of browser and server.
* Hyper text Markup language (HTML) :- defined the structure, organisation and content of a web page.

Computer Security Basics :-

Introduction to viruses :-

* Virus stand for "Virtual Information Resources Under Siege".
  ↓
  यह आविष्कार

* A Computer virus is a piece of software that can 'infect' a computer.

* It install itself to the computers, without the users knowledge or permission.

* It usually attaches itself to other computer program, data files, or the boot sector of a Hard drive, Pendrive etc.

* Malware is short for malicious software
  ↓
  Soc

Virus Names :-

* Malware * Trojan horse * Worm * spyware
* Boot sector virus.

① Worm :- A worm virus refers to a malicious program that replicates itself, automatically spreading through a network. In this definition of computer worms, the worm virus exploits on your security software to steal sensitive

information, install backdoors that can be used to access the system, corrupt files, and do other kinds of harm.

② Malware :- Malware is malicious software that cybercriminals use to damage or destroy computers, steal data, or harm computer network. Example of common malware include viruses, worms, Trojan viruses, spyware, adware and ransomware.

③ Trojans :- A trojan, also known as a Trojan horse, is a type of malware that tricks users into installing it on their computer or device.

Trojans can be delivered in many ways, including :-

* As attachments in emails
* As free to download files
* As videos or music
* As advertisements.

④ Spyware :- Spyware is malicious software that enters a user's computer, gather data from the device and user, and sends it to third parties without their consent.

A commonly accepted spyware definition is a strand of malware designed to access and damage a device without the user's consent.

⑤ Antispyware :- Antispyware is a cybersecurity tool designed to detect and remove spyware.

How it works :-

Anti-spyware software can be integrated with antivirus software or be its own independent product. It uses advanced algorithms and threat intelligence tools to detect spyware

Example of anti-spyware software :-

Avast One, Bitdefender, Surfshark One, McAfee, Norton 360 Deluxe and ESET Essential are some examples of anti-spyware software

Different types of attacks like Money Laundering :-

* Money laundering disguises financial assets without detecting the illegal activity that produced them.
* Online banking and cryptocurrencies have made it easier for criminals to transfer and withdraw money without detection.

The common types of cybercrimes are :-

① Information theft ② Cyber pornography ③ Email spoofing
④ Denial of service (DOS) ⑤ Cyber stalking
⑥ Logic bombs ⑦ Hacking spamming.

① Information theft :- also known as data theft, is the illegal act of obtaining personal, financial, or confidential information. This can include passwords, bank account information, social security numbers and more.

Information theft can be a serious security and privacy breach with severe consequences for both individuals and organizations. Here are some ways to protect yourself from information theft :-

① Secure your connection
② Use strong password
③ Be careful on social media
④ Check websites for security
⑤ Be aware of data breaches (breach)

② Hacking :- An unauthorized user who attempts to or gains access to an information system is known as hacker. Hacking is a cybercrime even if there is no visible damage to the system, because it is an invasion in to the privacy of data.

(3) Cyber stalking :- Cyber stalking involves use of internet to harass someone. The behaviour includes false accusations, threats etc. Normally, majority of cyber stalkers are men and the majority of victims are woman

Cyberstalking is when a cybercriminal uses email, direct messaging or other electronic means to harass, scare or threaten someone with physical harm. It takes different forms, including :- Tracking someone's online activity or physical location.

Consequences of types of Cyber stalking

* Webcam Hijacking * observing location check-ins on social media * looking at geotags to track location

How to Help protect yoursely Against Cyberstalking :

* Develop the habit of logging out of the PC when not in use.

* Set strong and distinctive passwords for your online accounts.

DATE
PAGE

④ Hacking spamming:- Spamming in cybersecurity is the act of sending unsolicited messages, often with commercial or malicious purposes, to a large number of people. E-mails, texts & instant messages can be used as forms of communicat. Spamming can be used to spread malware, steal personal information, or promote scams & phishing schemes.

It can also be used to overload networks & servers, causing them to crash.

It is important for individuals to be cautious when opening emails or messages from unknown senders, & to avoid clicking on suspicious links or providing personal information.

Types of Spam in Cybersecurity:-

① Email spam ② Instant Messaging spam
③ Social Media spam ④ SMS spam
⑤ Voice call spam.

How to protect Yourself from spam:-

① Use spam filters
② Avoid clicking on suspicious links
③ Report spam
④ Installing Cybersecurity Software.

(5) Cyber pornography :— With the increasing approach of internet to the people, there is also an increase in the victimization of women and children for sexual exploitation through internet.

(6) Credit Card Fraud :— In U.S.A half a billion dollers have been lost annually by consumers who have credit cards and calling card numbers. These are stolen from online databases. In present world this cybercrime is emerged as a major threat as numerous cases had been filed in almost every major developed and developing country.

(7) Email Spoofing :- Email spoofing is a threat that involves sending email messages with a fake sender address.

Email protocols cannot, on their own, authenticate the source of an email. Therefore, it is relatively easy for a spammer or other malicious actors to change the metadata of an email.

(8) Denial-of-Service (DoS) :- Denial of service is an attack designed to disable, shut down or disrupt a network, website or service. Typically a malware is used to interrupt or inhibit

the normal flow of data into and out of a system such that, in a short period of time, the ~~for~~ target is rendered useless.

(g) Logic bomb :— A logic bomb is a type of cyber attack that involves a set of instructions that are secretly added to a computer system or application to cause damage. The instructions are de-signed to only execute when certain conditions are met, and can lead to a range of harmful ~~or~~ outcomes.

Cyber Defamation :— (साइबर मानहानि)

"Cyber defamation" vary from country to country, but the fundamental rights covered in the UN Declaration of Human Rights and European Union Fundamental Human Rights.

* Cyber defamation can be divided into two parts — Cyber and defamation.

* Defamation means harming the reputation of person in front of third party (through words or spoken)

* In Cyber defamation internet or computer is used to harm the reputation of other person or lowering the reputation.

* The internet has made many things easier for us through various social networking sites, but one can misuse the facility by publishing false information to this social networking sites.

In India, liability of defamation is two folds:-

* Primary writes:- The person who has written the defamatory content & publish it on the cyberspace.

* Service providers:- The ISP or owner of the site who authorized for publication of such defamatory content.

Various Mediums used:-

* Social Networking site
* Websites
* Email

pharming Security measures firewall :—

Computer Ethics & Good Practics :→

The moral guidelines and principles that are followed for the positive use of a computer system or an information system are known as a computer ethics.

For example, it is unethical to copy a software without the permission of its owner.

Some moral guicklines to the us of computer are as follows :—

1. A Computer should not be used to harm or disturb other people.
2. It is totally unethical to access and destroy the data / information of other people.
3. Developing and intentionally spreading viruses in computers in unethical.
4. Reading other people's email messages is unethical This is attack on their privacy.
5. Spredding rumors or false news through the use of computers is also a seriues crime.

Computer ethics is a set of guidelines that help people use technology responsibly and ethically. It's important to follow computer ethics to protect users' privacy, intellectual property, and system security.

Here are some examples of computer ethics and good practices :-

* Respect privacy :- Don't access other's files or passwords without permission.
* Respect intellectual property :- Don't copy copyrighted software without the author's permission.
* protect your data :- Keep your user ID and password safe, and don't write them down.

Introduction of Cyber law about Internet fraud:-

Cyber law, also known as internet law or digital law, is a set of legal regulations that govern the digital world. It includes laws that address cybercrime, online communication, digital privacy, and e-commerce.

In India, the information Technology Act (IT Act) of 2000 is the primary legislation that deals with cyber crime, data protection and cybersecurity.

The IT Act covers a range of cybercrimes, including:-

* Hacking * Denial-of-service attacks * phishing * Malware attacks * Identity fraud * Electronic theft * Stealing data * Unauthorized accessing into computer

Here are some tips to help you avoid Cybercrime:-

* Don't share your bank information over email or phone calls, even if they seem legitimate.
* Call your bank to verify if any emails or phone calls asking for your bank information are legitimate.
* protect your computer with anti virus software.

Good Computer Security Habits :-

Cyber hygiene ~~means~~ habits means doing certain things to keep your online information safe.

Staying safe online is more important than ever. With hackers and cyber threats lurking around every corner, practicing good cyber hygiene is key to protecting your personal information.

Good Cyber Hygiene Habits to help stay Safe online:-

1. Keep your Wifi network Set Secure :-

2. Use strong passwords :- Use Complex Password that aren't easy to guess, like "12345" or your child's name. Change your password every 90 days or so.

3. Keep your software up to date :- Make sure your antivirus and other software are up to date so they can recognize the latest threats.

4. Back up your data :- Regularly back up your important files and data so you can recover them if needed.

5. Be careful with emails :- Don't open suspicious email, especially if they seem to be from your bank.

6. Avoid downloads from unknown Sources :- Criminals may target software from unknown Sources.