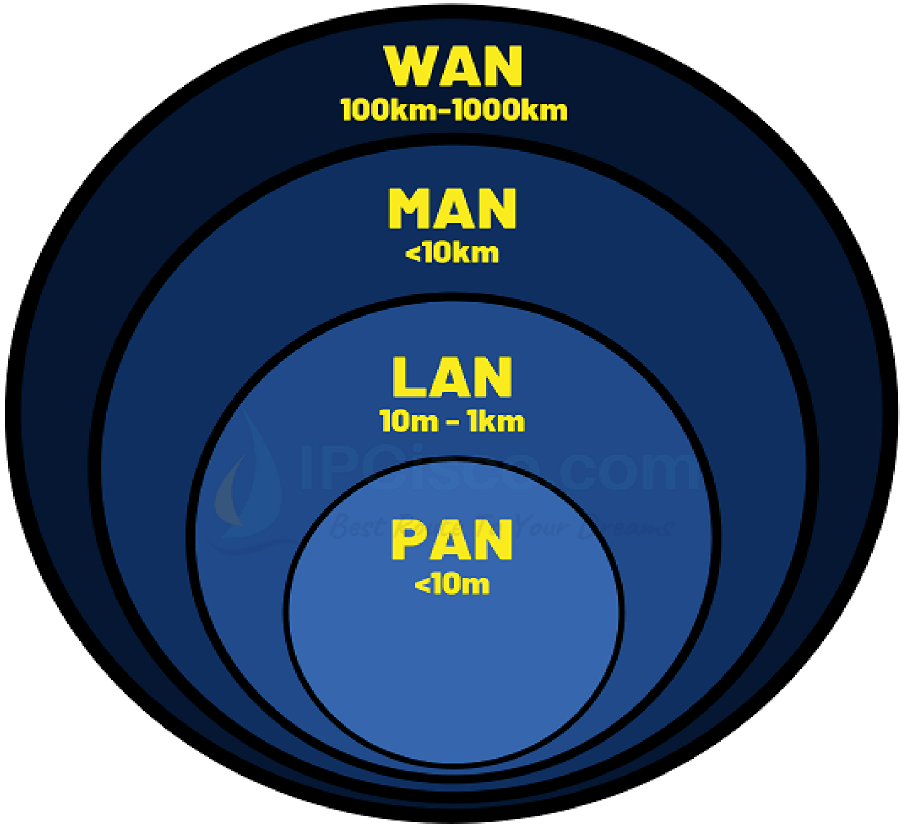
UNIT 4

Basic Computer Engineering (BT-205)

Prepared by Chetna Singh

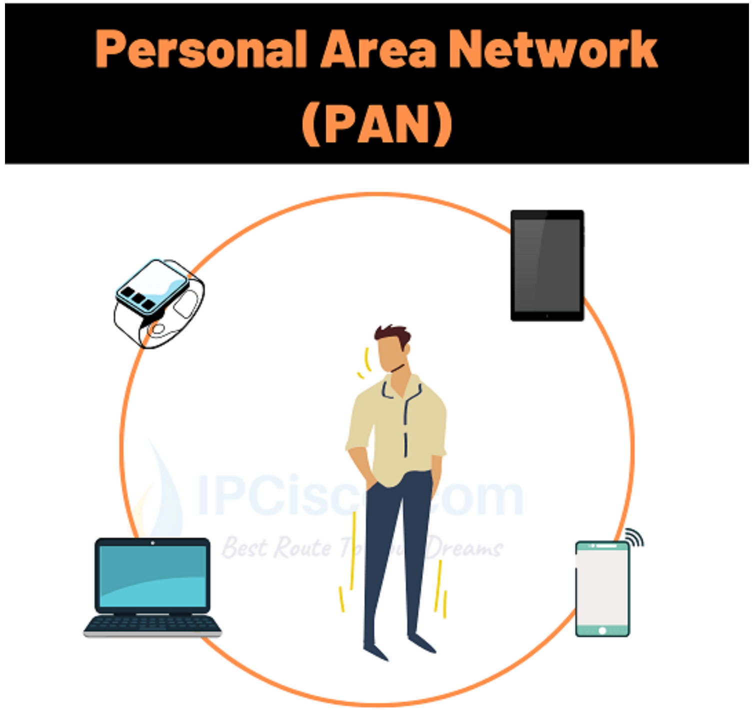
Computer Network

- Computer Network means an interconnection of autonomous (standalone) computers for information exchange. The connecting media could be a copper wire, optical fiber, microwave or satellite.
- There are several types of networks in use today
  - PAN – Personal Area Network
  - LAN - Local Area Network
  - MAN – Metropolitan Area Network
  - WAN - Wide Area Network



Computer Network

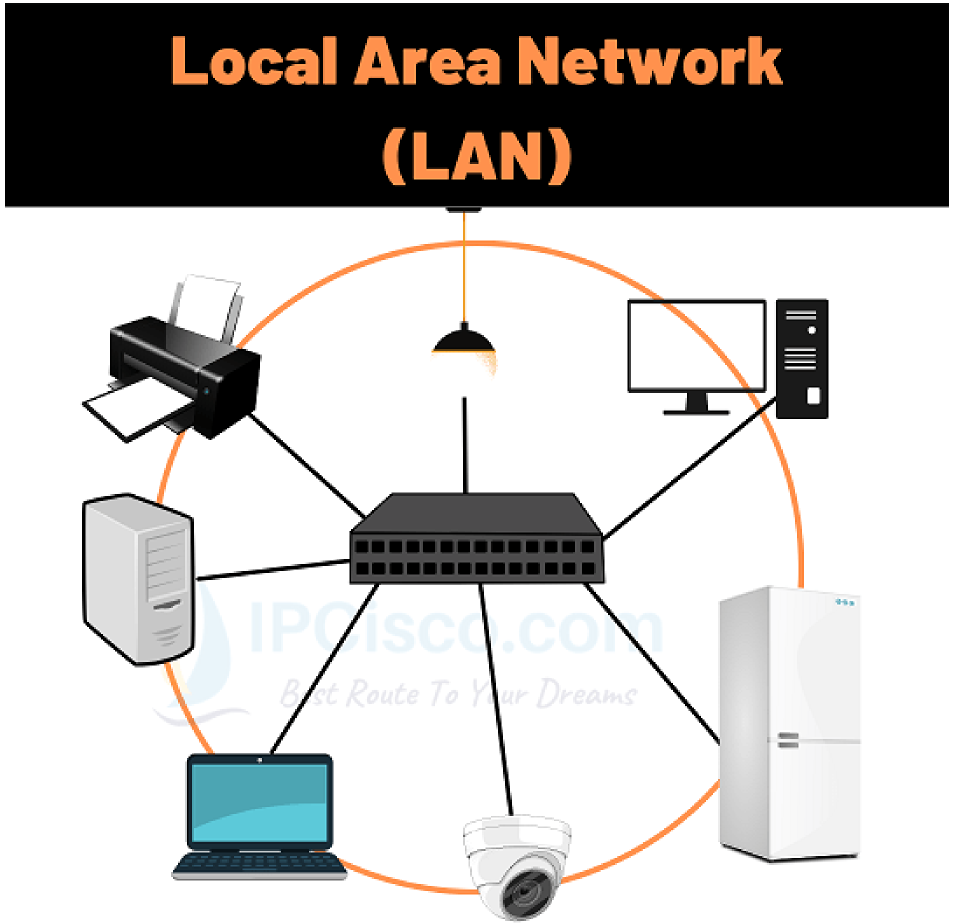
- ➢ The smallest network type is PAN (Personal Area Network). A PAN is the network around a single person. It consists of smart phones, laptops, tablets, wearable technology or any other personal digital device.



Computer Network

- LAN (Local Area Network) is a small type of network used in houses, companies, schools or any other small areas.
- These types of networks are used for file sharing, resource sharing, communication in a small area. It is also used to share internet connection in any place.
- For example, the network in your College which you share information or communicate with other members in a LAN.

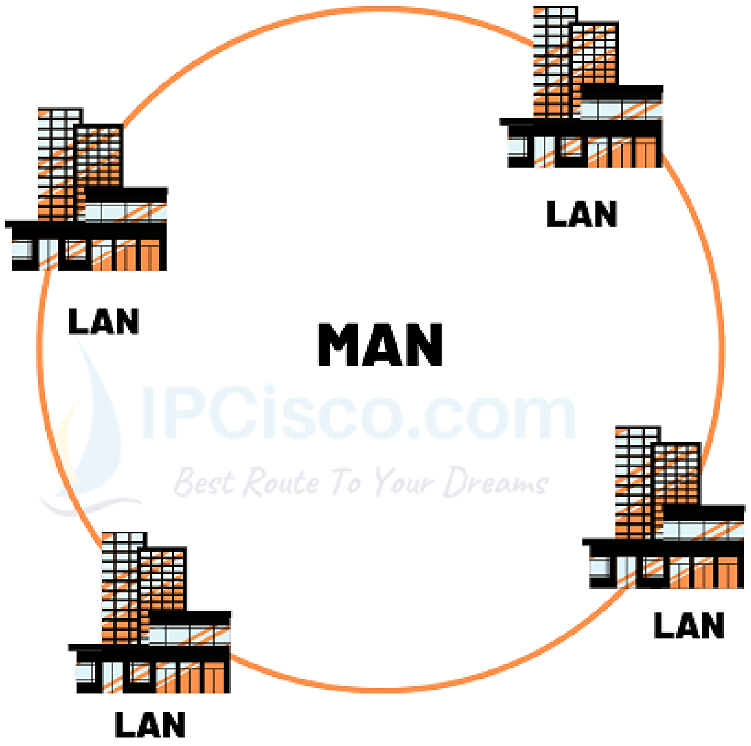
Computer Network



Computer Network

- MAN (Metropolitan Area Network) is another type of networks which is larger than LAN and smaller than WAN.
- It covers medium range areas, in other words several miles. With this characteristic, a MAN can cover a campus, a region or even a city.
- In MANs, mainly fiber optic cables are used. This is because the covered distance.
- MANs are costly networks and it need experienced network engineers for MAN administration.

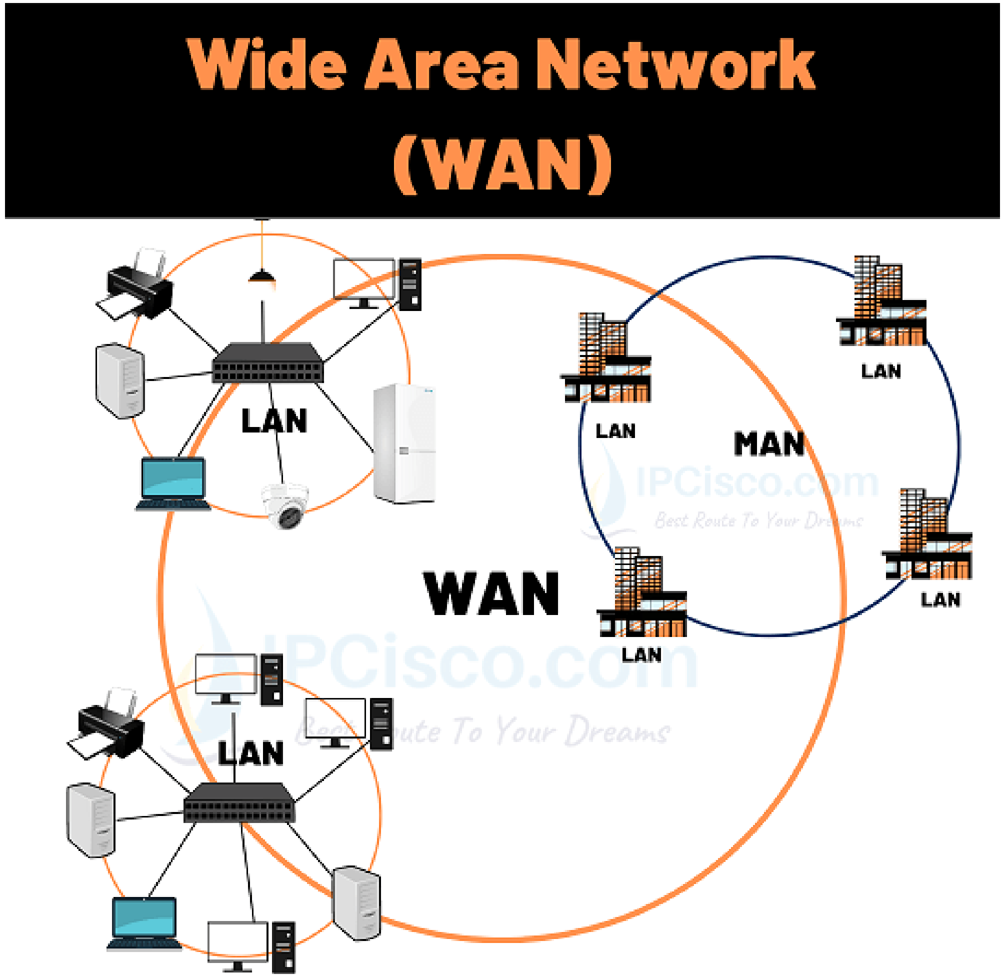
Metropolitan Area Network (MAN)



Computer Network

- ➢ WAN (Wide Area Network) is the largest network type used in computer networks. It covers large geographical areas.
- ➢ WANs can also connect other small and medium networks like LANs and MANs.
- ➢ Building a WAN is very costly. It is also hard to manage a Wide Area Network. It needs expert network engineers for building, maintenance and troubleshooting.

Computer Network



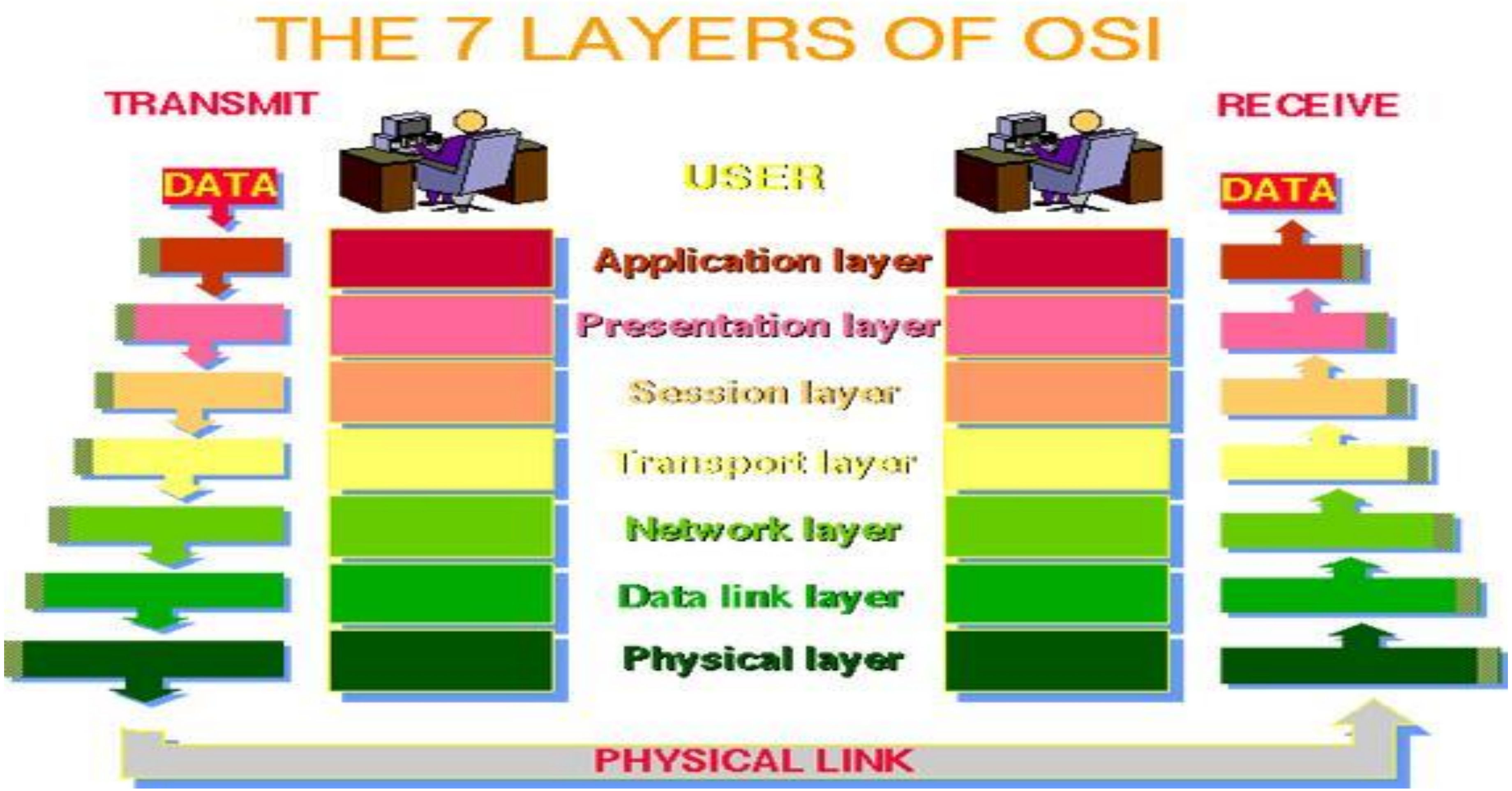
Networking Goals

- **Resource Sharing** – Many organization has a substantial number of computers in operations, which are located apart. Ex. A group of office workers can share a common printer, scanner etc.
- **High-Reliability** – If there are alternate sources of supply, all files could be replicated on two or, machines. If one of them is not available, due to hardware failure, the other copies could be used.
- **Inter-process Communication** – Network users, located at different geographical locations, may establish interactive session through the network.
- **Flexible access** – Files can be accessed from any computer in the network. The project can be begun on one computer and finished on another.

ISO-OSI reference model

- ISO – International Standard Organisation
- OSI – Open System Interconnection
- OSI model is the collection of set of rules needed by two systems to be agreed upon, to make communication possible.
- Since all rules can not be completely binded into single module because updation of rules is needed many times. So division of rules into different modules make suitable for updation easily.
- Broadly OSI model is divided into 7 layers-

ISO-OSI reference model



ISO-OSI reference model

- **Physical Layer**
- This layer is concerned with transmitting raw bits over communication channel.
- It also deals with electrical, mechanical, and procedural interfaces.
- It specifies the way in which a device must transmit data and also the way in which another device must receive the data.
- Also responsible for setting and terminating the network connection.
- **Data link layer**
- Point to point Error & Flow control.
- Framing.
- Link management.

ISO-OSI reference model

- **Network layer**
- Routing- Finding appropriate route for the packet so that it can reach destination efficiently by help of routing tables.
- Congestion control- Congestion occurs due to overload on the capacity of subnet. It can be controlled by following three ways-
- Internetworking- Interconnecting two or more networks by the use of internetworking devices such as Repeater, bridge, hubs etc.
- **Network layer**
- Establishment & release of connection between two ends.
- End to end error control and flow control
- To divide message into fixed size data blocks known as Transport Protocol data unit.
- To provide Quality of service to upper layers.

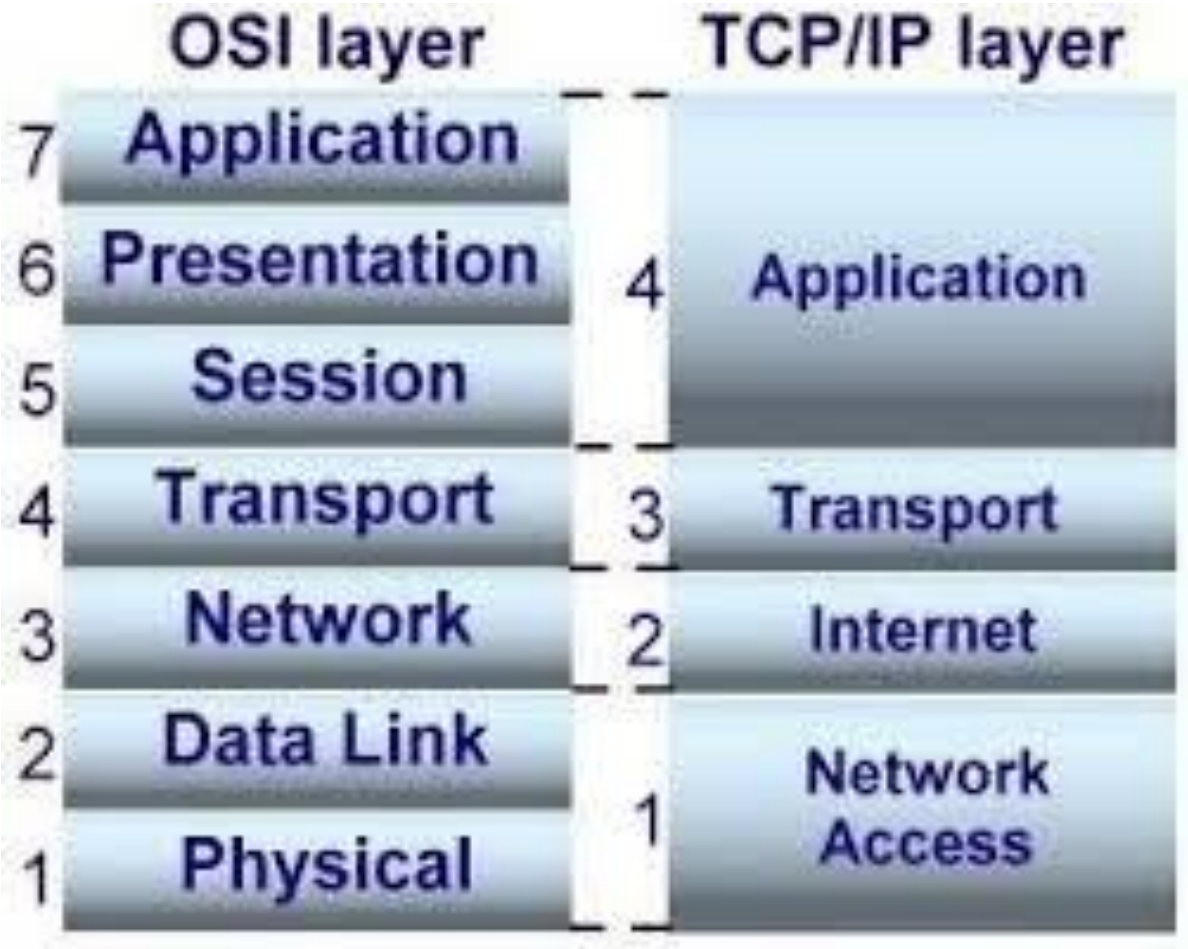
ISO-OSI reference model

- **Session layer**
- To establish session between sender and receiver (Dialog management).
- There are 3 ways to establish session-
  - Simplex
  - Half duplex
  - Full duplex
- **Presentation layer**
- Encryption
- Compression
- Character encoding

ISO-OSI reference model

- **Application layer**
- This layer specify application software implemented by end users for communication. The application software covers variety of services those are possible through computer network.
- Application header bits are appended at last of data packets which make virtual communication possible.

TCP/IP model



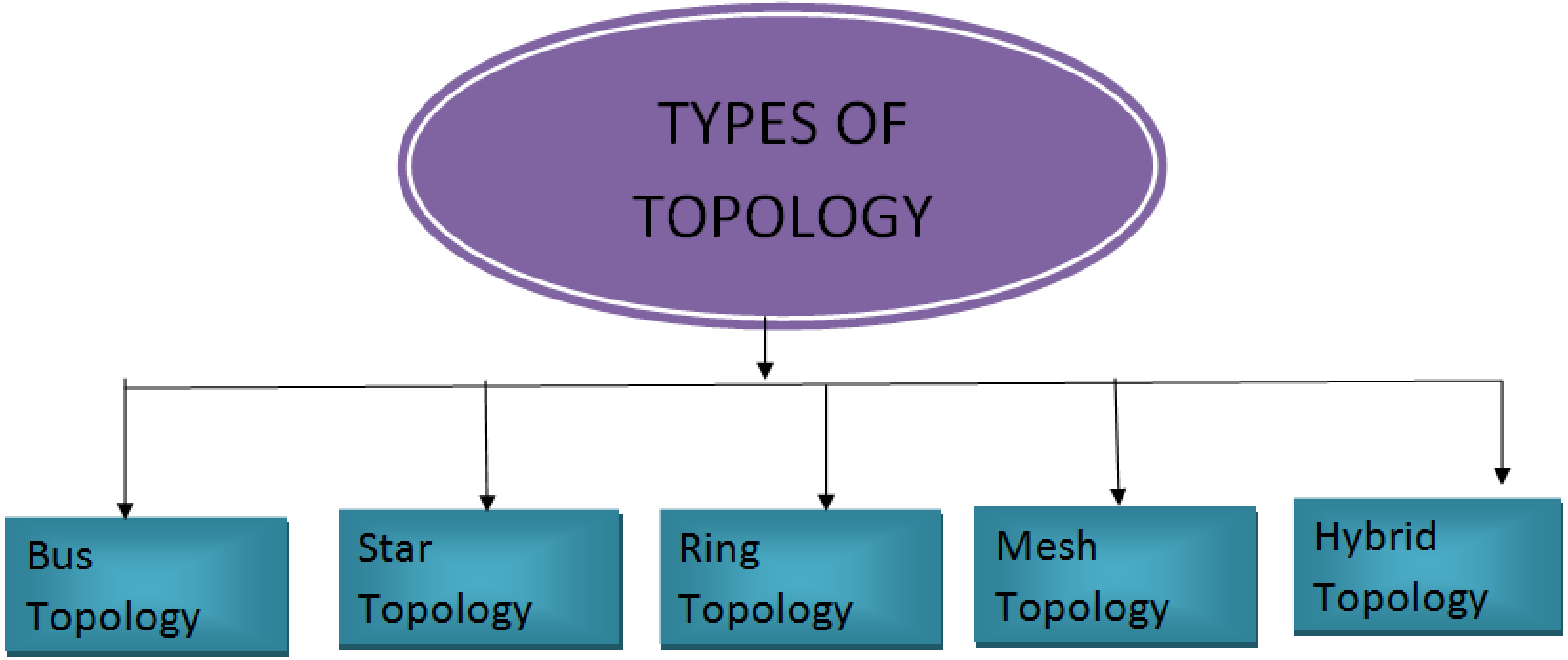
	OSI layer		TCP/IP layer
7	Application	4	Application
6	Presentation		
5	Session		
4	Transport	3	Transport
3	Network	2	Internet
2	Data Link	1	Network Access
1	Physical		

TCP/IP model

- The Internet protocol suite is the computer networking model and set of communications protocols used on the Internet and similar computer networks.
- It is commonly known as TCP/IP, because its most important protocols, the Transmission Control Protocol (TCP) and the Internet Protocol (IP), were the first networking protocols defined in this standard.
- Link Layer, containing communication technologies for a single network segment (link).
- Internet Layer, connecting hosts across independent networks, thus establishing internetworking.
- Transport Layer handling host-to-host communication.
- Application Layer, which provides process-to-process application data exchange.

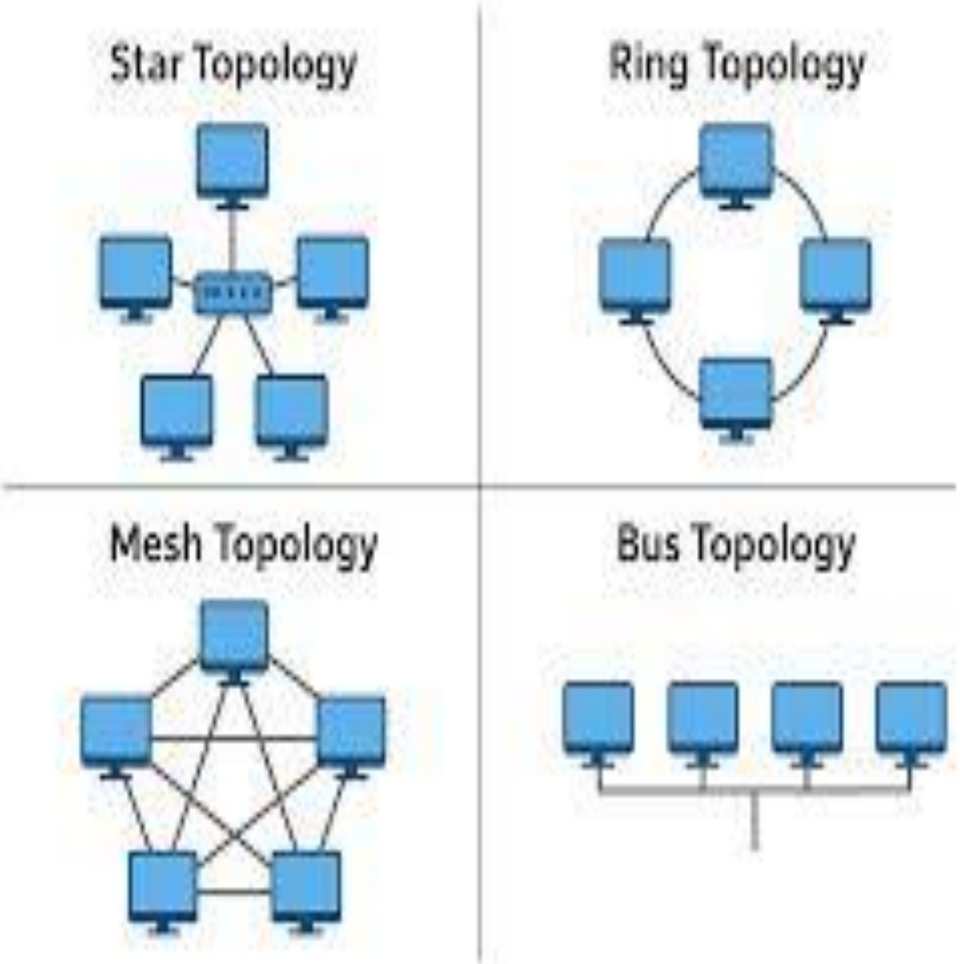
Network Topology

- Network topology refers to the arrangement or layout of computers, cables, and other devices in a network — basically how they are connected.



Network Topology

- ➢ Ring topology: A configuration that connects all nodes in a closed loop on which messages travel in one direction.
- ➢ Star topology : A configuration that centers around one node to which all others are connected and through which all messages are sent.
- ➢ Bus topology : All nodes are connected to a single communication line that carries messages in both directions.
- ➢ Mesh Topology : Every device connects directly to every other device. Provides high reliability and redundancy. Expensive and complex to set up.



Internet: The Network of Networks

- The Internet is a massive, global network connecting billions of computing devices (computers, servers, smartphones, etc.) worldwide.
- It is the physical infrastructure that enables data transmission.
- It is a global system of interconnected computer networks that use the Internet Protocol (TCP/IP) to communicate.
- Think of the Internet as the road system—the cables, routers, and switches that allow traffic (data) to move from one point to another.

Internet: The Network of Networks

- **Key Components & Concepts**
- Router: A device that forwards data packets between computer networks. It acts like a traffic cop directing data to its destination.
- IP Address (Internet Protocol Address): A unique numerical label assigned to every device connected to a computer network. (e.g., 192.168.1.1)
- TCP/IP (Transmission Control Protocol/Internet Protocol): The fundamental set of communication protocols used to interconnect network devices on the Internet. TCP ensures reliable delivery, and IP handles the addressing.
- Data Packet: Data is broken down into small, manageable units called packets for efficient transmission across the network.

The World Wide Web (WWW)

- The World Wide Web is an information system that operates on top of the Internet. It is a collection of documents and resources (web pages, images, videos) accessed via the Internet.
- It is a system of interlinked hypertext documents and other resources accessed via the Internet.
- If the Internet is the road system, the WWW is the **content**—the websites, stores, libraries, and houses—that you visit using those roads.

The World Wide Web (WWW)

- **Key Components & Concepts:**
- URL (Uniform Resource Locator): The address used to identify and locate a specific resource (web page) on the Web. (e.g., https://www.google.com)
- HTTP (Hypertext Transfer Protocol): The set of rules used by web browsers and servers to transfer files (like text, image, sound, video, and other multimedia files) that make up the Web.
- Web Browser: Software used to access the Web (e.g., Chrome, Firefox). It interprets HTML and displays the web page.
- HTML (Hypertext Markup Language): The standard language used to create web pages. It defines the structure of the content.
- Web Server: A computer that stores web content and delivers web pages to clients (browsers) upon request.

E-commerce (Electronic Commerce)

- E-commerce is the activity of buying or selling products and services using computer networks, primarily the Internet and the Web.
- E-commerce is the Commercial transactions conducted electronically on the Internet.

Model	Description	Example
B2C (Business-to-Consumer)	Businesses selling products/services directly to end consumers.	Amazon, Flipkart, Netflix
B2B (Business-to-Business)	Businesses conducting transactions with other businesses.	A component manufacturer selling parts to a car company.
C2C (Consumer-to-Consumer)	Consumers selling to other consumers, often via a platform.	eBay, OLX, classifieds sites.
C2B (Consumer-to-Business)	Consumers offering products/services to businesses.	Freelance graphic designer selling services to a company.

Malicious Softwares

Features	Virus	Worm	Trojan horse
Definition	Viruses are computer programs that connect to other software or programs to harm the system.	A worm is a malware program similar to a virus that doesn't interact with other system applications but instead multiplies and executes itself to slow down and harm the system's performance.	A Trojan Horse is a type of malware that steals sensitive data from a user's system and delivers it to a different location on the network.

Malicious Softwares

Features	Virus	Worm	Trojan horse
Replication	It replicates itself.	It also replicates itself.	It doesn't replicate itself.
Execution	It relies on the transfer.	It replicates itself without human action and utilizes a network to embed itself in other systems.	It is downloaded as software and executed.
Remotely Controlled	A virus could not be remotely controlled.	It may be remotely controlled.	It may also be remotely controlled.
Infection	Viruses spread through executable files.	Worms take advantage of system flaws.	The Trojan horse runs as a program and is interpreted as utility software.

Malicious Softwares

Features	Virus	Worm	Trojan horse
Rate of Spreading	Viruses spread at a moderate rate.	Worms spread at a quicker rate than viruses and Trojan horses.	In addition, the spread rate of Trojan horses is slower than that of viruses and worms.
Purpose	It is primarily utilized to modify or erase system data.	These are utilized to excessive using system resources and slow it down.	It may be utilized to steal user data to obtain access to the user's computer system.

Spywares

- Spyware is a breach of cyber security as they usually get into the laptop/ computer system when a user unintentionally clicks on a random unknown link or opens an unknown attachment, which downloads the spyware alongside the attachment.
- Spyware is a type of software that unethically without proper permissions or authorization steals a user's personal or business information and sends it to a third party. Spyware may get into a computer or laptop as a hidden component through free or shared wares.
- Spyware in many cases runs as a background process and slows down the normal functioning of the computer system.

Anti Spywares

- Antispyware is like a security guard for your computer. Its main job is to find, block, and remove spyware. Think of it this way:
- Spyware = A thief trying to sneak into your house to steal your diary.
- Antispyware = The security guard that catches the thief and kicks them out.
- The security guard (antispyware) works in **two** main ways:

1. **Real-Time Protection:**

- It stands at the "door" of your computer (the internet connection).
- It checks every file that tries to enter.
- If it looks like spyware, the guard says, "Stop! You cannot come in!" and blocks it.

Anti Spywares

2. **Scanning and Removing:**

- ➢ The guard also regularly searches your entire computer for any spies that might have snuck in.
- ➢ When it finds a spy, it catches it and deletes it from your computer.

- ➢ **Why do we need it?**
- ➢ Protect Private Information: Keep your passwords, bank details, and photos safe.
- ➢ Stop Annoying Ads: Some spyware floods your screen with pop-up ads.
- ➢ Keep Your Computer Fast: Spyware can slow down your computer.
- ➢ Stay Safe Online: It helps you browse the internet without being watched.

Cyber Crime

- ➢ Cyber Crime refers to any illegal, criminal, or malicious activity that is carried out using digital technology. This involves computers, computer networks, the internet, or other electronic devices (like smartphones and tablets) either as the primary tool to commit the offense or as the primary target of the offense.
- ➢ It's like a digital robbery or vandalism, but instead of targeting a physical building, the target is a computer or online service. They are of broadly 10 types:
- ➢ **Money Laundering**
- ➢ The process of making "dirty" money (earned from crime) look "clean" (like it came from a legal job).
- ➢ Example: A criminal opens a cash-only laundry shop. They mix their illegal cash with the real laundry money to make it seem like all the profit came from washing clothes.

Cyber Crime

- **Information Theft**
- Stealing someone's personal or private data without permission.
- Simple Example: A hacker breaks into a company's database to steal customers' credit card numbers and passwords.
- **Cyber Pornography**
- Creating, sharing, or viewing pornography (adult content) online, especially when it is illegal.
- Example: This includes posting adult videos on websites or sharing illegal content.

Cyber Crime

- **Email Spoofing**
- Faking the "From" address in an email to make it look like it came from someone else.
- Example: You get an email that looks like it's from your bank, but it's actually from a scammer trying to trick you.
- **Denial of Service (DoS)**
- An attack that floods a website or network with so much fake traffic that it crashes and becomes unavailable for real users.
- Example: Sending thousands of bots to crowd a shop's entrance so that real customers can't get in.

Cyber Crime

- **Cyber Stalking**
- Using the internet to repeatedly harass, threaten, or frighten someone.
- Simple Example: Someone constantly sending you scary messages, watching your social media, and tracking your online activity to make you feel unsafe.
- **Logic Bombs**
- A piece of harmful code secretly placed in a system that is set to activate at a specific time or event.
- Example: A disgruntled employee programs a company's computer to delete important files on a certain date after they've left the job.

Cyber Crime

- **Hacking**
- The act of gaining unauthorized access to a computer system or network.
- Example: Breaking through a website's security to get into its private control panel.
- **Spamming**
- Sending large amounts of unsolicited, irrelevant, or unwanted messages (usually emails) to a large number of people.
- Example: Your email inbox getting flooded with hundreds of ads for miracle pills or fake lottery wins.

Cyber Crime

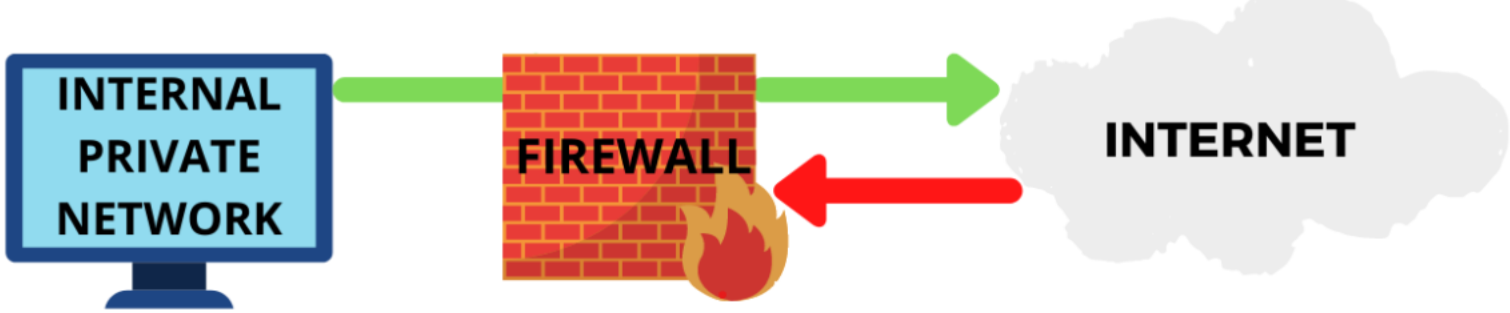
- **Cyber Defamation**
- Damaging someone's reputation by posting false and harmful statements about them online.
- Example: Writing a lie about someone on social media, saying they stole money, to ruin their reputation.

Cyber Security Safety Terms

- **Pharming**
- A cyber attack that secretly redirects you from a real website to a fake one that looks identical.
- Example: You type "www.mybank.com" correctly, but a hacker's trick sends you to a fake copy of the bank's site where they steal your login details.
- In cyber world, it is Like a road sign that has been secretly changed to lead you to a fake store instead of the real one.
- **Firewall**
- A security guard for your computer network. It controls what internet traffic is allowed to enter or leave.
- Example: It acts like a bouncer at a club, checking IDs and only letting authorized data packets in or out, while blocking suspicious ones.
- It is a protective wall between your computer and the internet.

Cyber Security Safety Terms

- **Firewall** not only filters the incoming traffic but also monitors the outgoing traffic to check if the packets are not sent to any suspicious targets.
- A firewall is the first line of security integrated to your network.
- it blocks unwanted suspicious traffic.
- A firewall consists of predefined security regulations on blocking and identifying suspicious traffic and thereby enabling smooth progression on authorized packets.
- Firewall not only blocks unwanted data but also protects a site from malicious data and has the capacity to keep the threat at bay.



Types of Firewalls

1. Packet-Filtering Firewall Checks each packet's IP address, port, and protocol before allowing it. It Works at the Network Layer and is the simplest type. Example: Basic router firewall.
2. Circuit-Level firewall checks and verifies the TCP handshake between source and destination before allowing communication. It works at the session layer and ensures that only legitimate sessions are allowed. Example: SOCKS proxy firewall.
3. Proxy Firewall (Application-Level Gateway)Works as a middleman between user and internet; filters traffic at application layer. Hides the internal network and provides deep inspection. Example: Web proxy server used in colleges.
4. Software Firewall Installed on individual computers or servers to protect that device. Controls app-wise internet access. Example: Windows Defender Firewall.
5. Hardware Firewall is a physical device placed between network and internet for overall protection. Used in offices, data centers. Example: SonicWall hardware firewall.

Cyber Security Safety Terms

- **Computer Ethics & Good Practices**
- The moral rules and responsible behaviors you should follow when using computers and the internet.
- Example: Not copying someone else's work, respecting privacy, not hacking, and being kind to others online.
- Think: "Do unto others online as you would have them do unto you."
- **Introduction of Cyber Laws (about Internet Fraud)**
- Official rules and regulations created by governments to define and punish illegal activities on the internet, like fraud.
- Example: Laws that make it a crime to create a fake online shopping site to steal people's credit card information.
- Think: The police and court system for the internet world.

Cyber Security Safety Terms

- **Good Computer Security Habits**
- Simple, regular actions you take to protect your computer and data from threats.
- Simple Example:
  - Using strong, unique passwords.
  - Installing software updates.
  - Being careful about what links you click.
  - Backing up your data.
- Like locking your door at night, brushing your teeth, or looking both ways before crossing the street—but for your digital life.

Cyber Laws for Internet Fraud

- **Why Do We Need Cyber Laws**: Without specific laws, it would be very difficult to:
- Define what counts as fraud on the internet.
- Investigate and catch criminals who can be in a different country.
- Punish the criminals fairly for their actions.
- **What Do These Cyber Laws Do?**
- Define the Crime: They clearly state that activities like phishing, creating fake websites, and online identity theft are illegal.
- Establish Punishment: They set the penalties for committing fraud, which can include fines and jail time.
- Give Power to Authorities: They grant police and cybercrime cells the legal authority to investigate these digital crimes.
- Provide Jurisdiction: They help determine which court or police force is responsible for handling a case, especially when the victim and criminal are in different cities or countries.

Cyber Laws for Internet Fraud

- In India the main cyber law is the Information Technology Act, 2000.
- Section 66: Punishes identity theft (using someone else's password or digital signature).
- Section 67: Publishing Obscene Material in Electronic Form. It Punishes publishing or transmitting obscene material online.
- Section 43: Deals with penalties for damage to computers and computer systems, which can include introducing viruses or stealing data.
- Section 69: Power to Intercept, Monitor, or Decrypt Information. It gives government the power, under certain conditions, to intercept, monitor, or decrypt any information through any computer resource.

Good Computer Security Habits

- Use Strong, Unique Passwords: Create complex passwords that are difficult to guess and use different passwords for different accounts.
- Enable Multi-Factor Authentication (MFA/2FA): Add an extra verification step beyond just a password, like a code from your phone.
- Keep Software Updated: Regularly install the latest updates for your operating system and applications.
- Be Cautious with Links & Attachments: Avoid clicking suspicious links or downloading unexpected attachments in emails and messages.
- Backup Your Data Regularly: Make frequent copies of your important files to a separate, secure location.
- Use Antivirus/Antimalware Software: Install and maintain security software that can detect and remove malicious programs.
- Be Careful on Public Wi-Fi: Avoid accessing sensitive accounts or data when connected to public, unsecured networks.