## UNIT-I

**Introduction:** Types of Computer Networks, Broadband Access Networks, Mobile and Wireless Access Networks, Content Provider Networks, Transit networks, Enterprise Networks, Network technology from local to global, Personal Area Networks, Local Area Networks, Home Networks, Metropolitan Area Networks, Wide Area Networks, Internetworks, Network Protocols, Design Goals, Protocol Layering, Connections and Reliability, Service Primitives, The Relationship of Services to Protocols ,Reference Models, The OSI Reference Model, The TCP/IP Reference Model, A Critique of the OSI Model and Protocols, A Critique of the TCP/IP Reference Model and Protocols.

# 1.Types of Computer Networks

## 1.1 PAN (Personal Area Network)

### Overview of Personal Area Network (PAN)

A **computer network** is a group of **computers and devices connected together** so they can **talk to each other** and **share resources** like files, data, internet, printers, and applications.

There are **different types of computer networks**, and they are **classified** based on:

- How **large** the area is (like a room, building, or entire country),
- What the **network is used for** (personal, business, or public use),
- And how the **devices are connected** (wired or wireless).

✓ **Personal Area Network (PAN)**

A **Personal Area Network (PAN)** is a small network that connects **devices around one person**, usually within a short range of about **10 meters (33 feet)**.

This network includes personal devices like:

- Computers or laptops
- Mobile phones or tablets
- Printers
- Speakers, game consoles, and other gadgets
- PDAs (Personal Digital Assistants)

The idea of PAN was first developed by **Thomas Zimmerman** and his team at **MIT's Media Lab**.

PANs are very useful at **home, small offices**, or for **personal use** because they are:

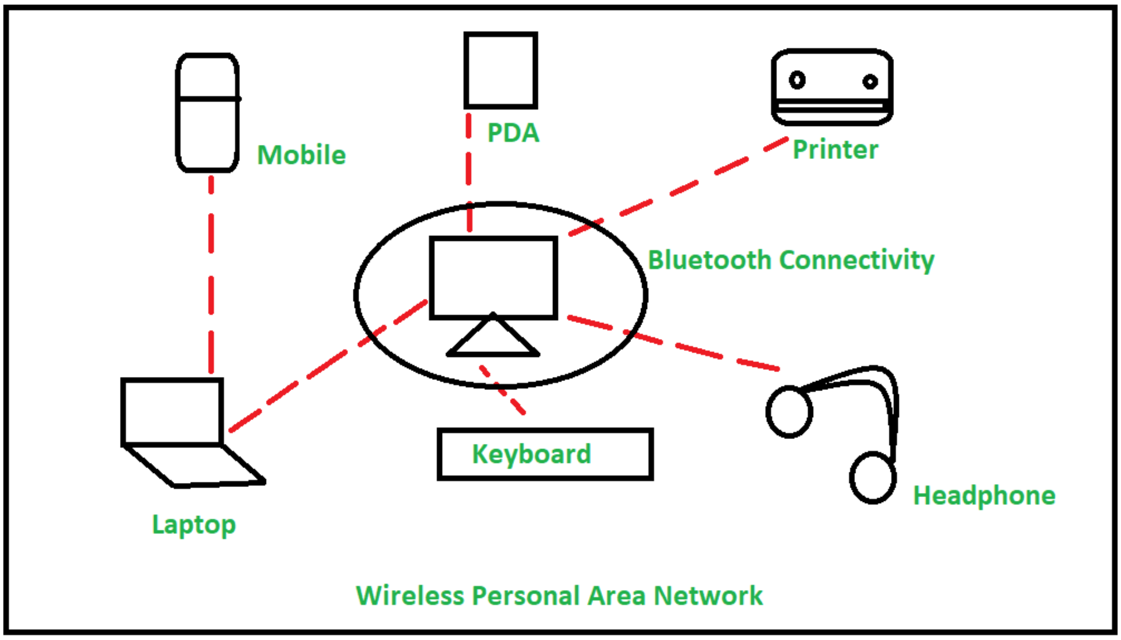
- **Flexible** (easy to use and move)
- **Efficient** (work well for small tasks)

✓ **Types of Personal Area Network (PAN):**

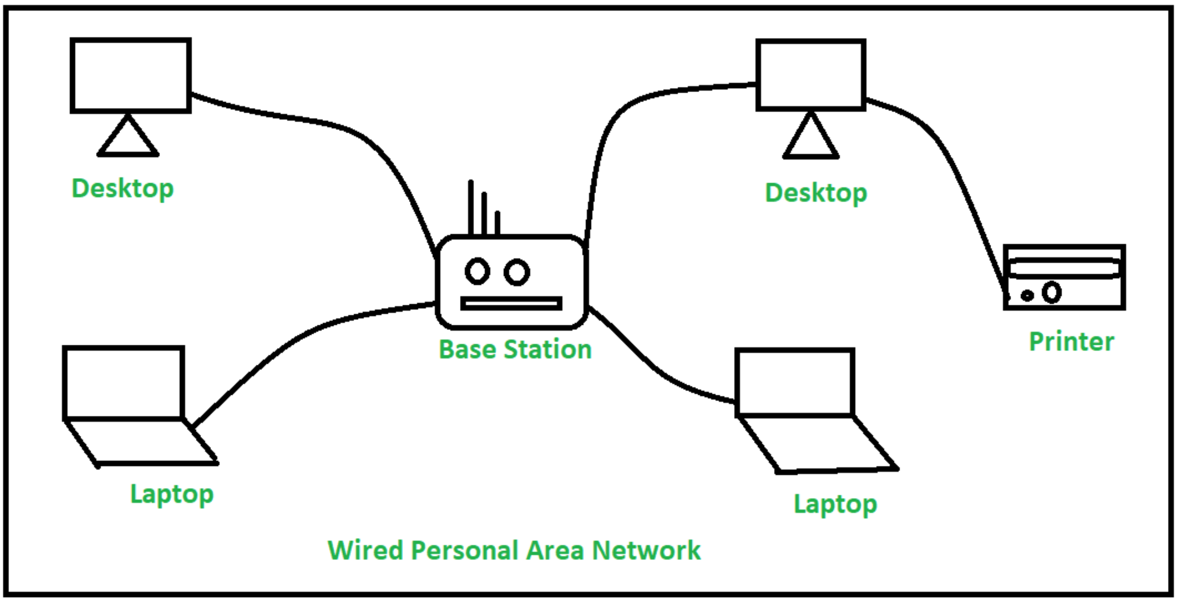
Personal Area Network can be of 2 types depending upon its connection i.e., Wireless PAN, and Wired PAN.

These are explained as following below.

1. **Wireless PAN** –Wireless Personal Area Network (WPAN) is connected through signals such as infrared, ZigBee, Bluetooth and ultrawideband, etc.



2. **Wired PAN -** Wired PAN is connected through cables/wires such as Firewire or USB (Universal Serial Bus).



✓ **Examples of PAN:**

1. **Body Area Network**: This is a **personal mobile network** that moves with a person.

   For example, when someone connects their **smartphone to Bluetooth headphones** and walks in a market — this is called a **Body Area Network**.

2. **Offline Network**: In this type, **multiple devices are connected without internet** using **Bluetooth or Wi-Fi**.
   **Example:** At home, your **computer, printer, mouse, and speakers** are connected to each other through PAN to share data or print documents. This small local setup works without needing the internet.
3. **Home Office Network**: When someone **works from home**, they may set up a **separate PAN** for work devices.

   This is **different from the network used by home appliances**. It helps keep office work devices like laptops, printers, and phones connected and organized separately from personal or entertainment devices.

✓ **Advantages and disadvantages of PAN -**

These are some of the Advantages of PAN:

- PAN is relatively flexible and provides high efficiency for short network ranges.
- It needs easy setup and relatively low cost.
- It does not require frequent installations and maintenance
- It is easy and portable.
- Needs fewer technical skills to use.

These are some of the disadvantages of PAN:

- Low network coverage area/range.
- Limited to relatively low data rates.
- Devices are not compatible with each other.
- Inbuilt WPAN devices are a little bit costly.

✓ **Applications of PAN -**

- Home and Offices
- Organizations and the Business sector
- Medical and Hospital
- School and College Education
- Military and Defense

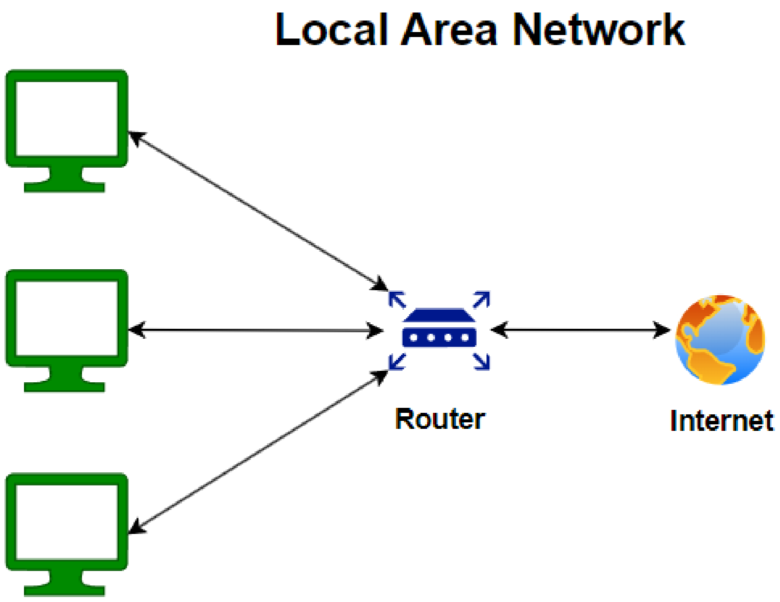
## 1.2 LAN Full Form - Local area network

A **Local Area Network (LAN)** is a small network that connects devices within a **single place** like a **home, office, school, or campus**.

- LAN covers a **short distance** (within a building or nearby rooms).
- The **internet speed** in a LAN usually ranges from **10 Mbps to 100 Mbps**, though today it can be even faster.
- Common **network layouts (topologies)** used in LANs include:
  - **Bus**
  - **Ring**
  - **Star**

**History of LAN:**

- LAN technology started in the **1970s**.
- One of the earliest LAN systems was the **Cambridge Ring**, developed in **1974** at **Cambridge University**.



**Local Area Network**

✓ **How do LANs Work?**

A **router** is like the **main center** in a LAN that connects the network to the **internet**.

- In a **home**, one **router** is usually enough.
- In **larger networks** (like in offices), **network switches** are also used. Switches help send data (called packets) more **quickly and efficiently** between devices.

✓ **How Devices Connect in LAN**

LAN devices usually connect in two ways:

1. **Ethernet** – This is a **wired** way of connecting devices using cables. It works at the **physical layer** and **data link layer** of the **OSI model**.
2. **Wi-Fi** – This is a **wireless** method that connects devices to the LAN **without cables**, using **radio signals**.

✓ **Examples of Devices in LAN**

Devices that commonly connect to a LAN include:

- **Servers**
- **Desktops** and **laptops**
- **Printers**
- **Game consoles**
- **Smart home (IoT) devices** like smart TVs, lights, etc.

✓ **Where LAN is Used**

LANs are mostly used in **offices** and **homes**:

- In offices, they allow staff to **share printers**, **access files**, or **use the internet**.
- In homes, they connect all devices like phones, TVs, and computers to work together.

✓ **Types of LAN (Local Area Network) – Simple Explanation**

LANs can be set up in **different ways**, depending on how devices connect and communicate. These are called **LAN architectures**:

**1 Client/Server LAN**

- In this type, many devices (called **clients**) are connected to a **central server**.
- The **server**:
  - o Manages network traffic
  - o Controls access to apps and files

  - Stores data

- Any device like a **computer, phone, or tablet** using apps or internet is a **client**.
- Devices can connect to the server using **wires (Ethernet)** or **wireless (Wi-Fi)**.

**2 Peer-to-Peer (P2P) LAN**

- This LAN type is **smaller** and has **no central server**.
- All devices (peers) are **equal** and **share resources directly** with each other.
- Devices connect to each other using a **router or switch**.
- Commonly used in **homes** and for **simple file sharing**.

**3 Ethernet LAN**

- **Ethernet** is the **most common** type of LAN.
- It defines:
  - **Network speed**
  - **Type of cable**
  - **Network cards/adapters**
- It supports both **wired** and **wireless** setups.

**4 Token Ring LAN**

- An **older LAN technology**, not used much today.
- It uses a **token** (a small data packet) that moves around the network.
- Devices can only send data when they have the token.
- Speed: Up to **100 Mbps**.

**5 Cloud-Managed LAN**

- This LAN is **controlled using cloud-based software**.
- The cloud manages:
  - **Network setup**
  - **Security**
  - **Access control**
  - **Performance**
- It is very useful for **businesses** with **many branches or devices**, because it is **easy to manage remotely**.

- ✓ **What is a Virtual LAN?**

The same physical network can have its traffic divided into two networks using virtual LANs, or VLANs. Imagine establishing two independent LANs in the same room, each with its own router and Internet connection. Similar to that, but with only one router and one Internet connection required, VLANs divide networks virtually rather than physically.

VLANs are beneficial for network management, particularly in very large LANs. Administrators may much more simply control the network by segmenting it. (Subnets, another method of segmenting networks for increased efficiency, differ greatly from VLANs.)

- ✓ **Differences Between Wired LAN, Wireless LAN, and Virtual LAN**
  - **Wired LAN**

A wired LAN connects devices like, servers, IoT devices, and other electronic devices to a company network using switches and Ethernet cables. For small organization, or businesses with a limited number of devices, a wired LAN might just consist of a single, unmanaged switch with Ethernet ports to connect all the devices.

  - **Wireless LAN**

A wireless LAN allows devices to connect to the network without physical cables. Wireless LAN or WLANs transfer data over radio waves using wireless technology. This type of LAN is commonly found in homes, offices, coffee shops, and restaurants where mobility is important. WLANs enable devices such as computers, smartphones, and tablets to connect to the internet or other shared resources. For example, connecting mobile to the hotspot is a wireless LAN.

Wireless LANs use the IEEE 802.11 standards to transmit data between devices and the network through the wireless system. In many cases, WLANs are preferred over wired LANs due to their flexibility and cost efficiency, as they eliminate the need for extensive cabling. Businesses considering WLANs as their main form of connectivity often have users who primarily depend on mobile devices like smartphones and tablets.

  - **Virtual LAN**

In larger LANs that connect thousands of devices, more hardware, software, and configuration are needed to maintain optimal network performance. This is where virtual LANs (VLANs) become useful.

✓ **What Equipment is Needed to Set up a LAN?**

For setting up a Local Area Network (LAN) requires many type of hardware and, depending on the complexity of the network, some additional components for enhanced functionality and performance. Here is a list of the essential equipment needed to set up a basic LAN-

- **Router: -** This is the central device that is used to connect the LAN to the internet.
- **Modem: -** This it required only if connecting to the internet. Modem convert the signals from your Internet Service Provider (ISP) to a router usable.
- **Switch (optional for larger networks): -** Used to expands the number of devices that can be connected to the LAN.
- **Ethernet Cables: -** It is used to connect devices to the router or switch.
- **Network Interface Cards (NICs)**: - It is required for each device that is connect to the LAN through Ethernet.
- **Wireless Access Point (if wireless connectivity is needed):-** Allows wireless devices to connect to the LAN.
- **Devices**: - Device you want to connect like Laptop, Computers, smartphones, tablets, smart TVs, and other devices.

✓ **How do LANs Relate to the Rest of the Internet?**

The Internet is like a huge web made up of smaller webs. Imagine each small web as a LAN, which is a bunch of devices connected, like in a school or an office. These LANs connect to bigger networks called autonomous systems (AS), which are like super highways for data.

An AS is a massive network with its own rules for sending data and managing certain addresses. Think of it like a big city full of streets and highways.

When you are on the Internet, it is like your LAN is a tiny street in a big city, which is part of an even larger network. And just like people in different cities can chat by traveling through roads and highways, computers on different LANs can talk to each other by sending data across these big networks.

So, the Internet is like a big family of networks, with LANs connecting to bigger networks, all working together to let us share information and connect with people all over the world.

✓ **LAN Security**

LANs face several security risks that can endanger the safety of data and network operations:

- **Insider Threats**: Employees with access to sensitive information may accidentally compromise LAN security. For instance, falling victim to phishing scams could allow unauthorized devices onto the network.

- **Vulnerable LAN Sockets**: LAN outlets in public areas like hallways or reception areas can pose risks if left unattended. Visitors or outsiders might connect to these outlets and gain access to the internal network.
- **Viruses and Malware**: These malicious programs can cause data loss, disrupt computer operations, and spread to other connected devices. They often enter LANs through removable media or email attachments.
- **Open Ports**: The router connecting a LAN to the internet has open ports that cybercriminals could exploit to infiltrate the network. Changing router admin credentials regularly helps mitigate this risk.
- **Rogue Access Points (APs)**: Unauthorized APs or ad hoc networks created by users without proper security measures can allow attackers to intercept network traffic.

Protecting a LAN involves addressing these risks through proactive measures like educating employees about cybersecurity, securing LAN outlets, using antivirus software, managing router settings, and monitoring network activity for unauthorized access points.

## ✓ 5 popular LAN Topologies

Network topologies describe how devices in a LAN are connected and how data moves between them. Popular types of topologies include:

- **Star Topology**: All devices connect to a central hub or switch. Data flows through the hub, which directs it to the appropriate device. If one device fails, it doesn't affect others.
- **Ring Topology**: Devices form a closed loop where data travels in one direction. Each device acts as a repeater to strengthen the signal. Data passes through each device until it reaches the destination.
- **Mesh Topology**: Devices are interconnected with multiple paths between them. If one path fails, data can take an alternative route. This redundancy enhances reliability but requires more cabling and configuration.
- **Bus Topology**: Devices are connected in a line along a single cable. Data travels along the cable, and each device receives all transmissions, but only the intended recipient processes the data.
- **Tree Topology:** Tree topology is a network setup where devices are arranged in a hierarchy, like branches of a tree.

### ✓ What are the Benefits of a LAN?

- **Privacy:** LAN is a private network; thus, no outside regulatory body controls it, giving it a privacy.
- **High Speed:** LAN offers a much higher speed(around 100 mbps) and data transfer rate comparatively to WAN.

- **Supports different transmission mediums:** LAN support a variety of communications transmission medium such as an Ethernet cable (thin cable, thick cable, and twisted pair), Fiber and wireless transmission.
- **Inexpensive and Simple:** A LAN usually has low cost, installation, expansion and maintenance and LAN installation is relatively easy to use, good scalability.

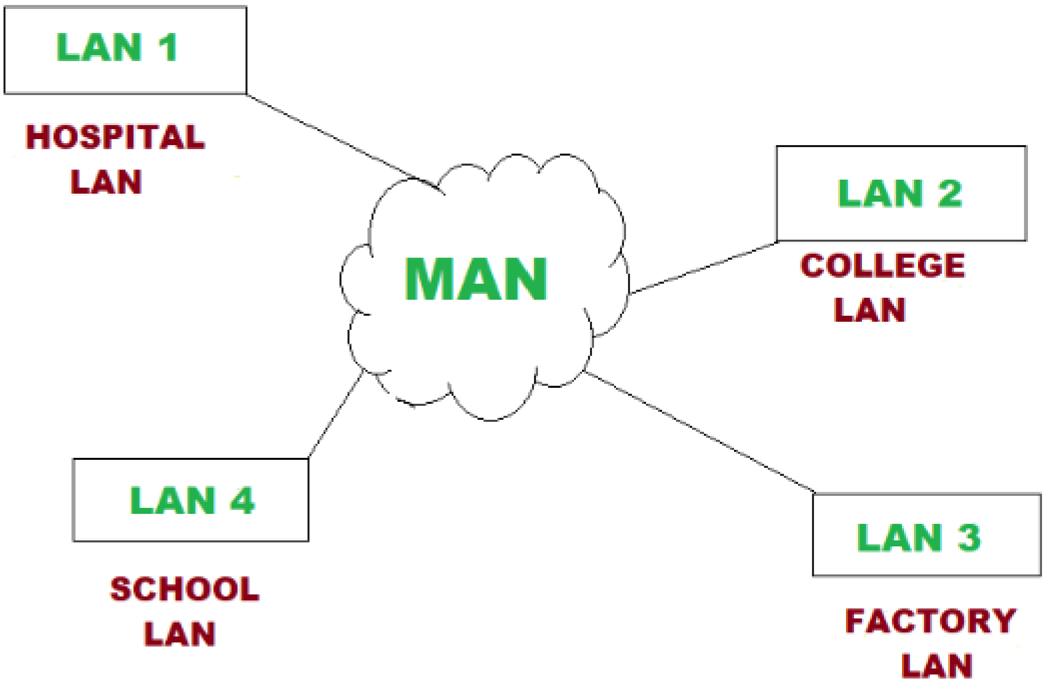
✓ **What are the Drawbacks of LAN?**

- The initial setup costs of installing Local Area Network is high because there is special software required to make a server.
- Communication devices like an ethernet cable, switches, hubs, routers, cables are costly.
- LAN administrator can see and check personal data files as well as Internet history of each and every LAN user. Hence, the privacy of the users is violated
- LANs are restricted in size and cover only a limited area
- Since all the data is stored in a single server computer, if it can be accessed by an unauthorized user, can cause a serious data security threat.

## 1.3 MAN Full Form in Computer Networking

A Metropolitan Area Network (MAN) is a type of computer network that spans over a metropolitan area, typically a city. It provides high-speed data communication services such as video, audio, and data transfer between multiple LANs (Local Area Networks) and WANs (Wide Area Networks). The main purpose of a MAN is to connect different LANs in a city to share resources and exchange data, as well as to provide internet access to users. A MAN typically covers a geographic area of several kilo meters and is larger than a LAN but smaller than a WAN.

**MAN** stands for **Metropolitan Area Network**. It is a computer network that connects number of LANs to form larger network, so that the computer resources can be shared. This type of network covers larger area than a LAN but smaller than the area covered by a WAN which is designed to extend over the entire city. MAN is specially designed to provide high-speed connectivity to the users in which the speed ranges in terms of Mbps. The architecture of MAN is quite complicated hence, it is hard to design and maintain.



- ✓ **History of MAN**

When LANs are establishes in 1994 in order to provide data communication in building and offices, the businesses are primarily relied on public switched telephone networks for the interconnection of LANs. But the telephone network was not capable enough to handle that much of traffic. Hence, to overcome this problem it was suggested that LANs are connected using the single-mode optical fiber lines, which results in the creation of metropolitan area network (MAN) to provide the interconnection of LANs efficiently. These Fiber optic MANs are owned and operated by private organizations or businesses, and did not necessarily have full integration with the public wide area network (WAN) through gateways.

- ✓ **Characteristics of MAN**

- It can cover the area which ranges from 5 to 50 km, which can carry from a group of buildings to the whole city.
- In MAN, data rates are moderate to high.
- In MAN, mostly used medium is optical Fibers which results in high-speed connectivity.
- MAN, networks provide high reliability because the error rate in this network is very less.
- A MAN network can use a variety of access technologies, such as wireless, Fiber-optic, or copper-based connections, to provide connectivity to different devices and networks.
- **Hybrid topology:** A MAN network may use a combination of different topologies, such as a ring, bus, or star topology, depending on the specific requirements of the network.

✓ **Advantages of MAN**

- MAN offers high-speed connectivity in which the speed ranges from 10-100 Mbps.
- The security level in MAN is high and strict as compared to WAN.
- It supports to transmit data in both directions concurrently because of dual bus architecture.
- MAN can serve multiple users at a time with the same high-speed internet to all the users.
- MAN allows for centralized management and control of the network, making it easier to monitor and manage network resources and security.

✓ **Disadvantages of MAN**

- The architecture of MAN is quite complicated hence; it is hard to design and maintain.
- This network is highly expensive because it required the high cost to set up Fiber optics.
- It provides less fault tolerance.
- The Data transfer rate in MAN is low when compare to LANs.

✓ **Examples of MAN**

- Cable TV network.
- Used in government agencies.
- University campuses.
- Used in hospitals to connect multiple buildings

✓ **Uses of MAN Network**

A Metropolitan Area Network (MAN) has several uses, including:

1. **Resource Sharing:** A MAN allows multiple LANs in a metropolitan area to share resources such as printers, storage devices, and other peripherals.
2. **Data Exchange:** A MAN provides a high-speed communication channel for the exchange of data between different LANs.
3. **Internet Access:** A MAN can provide high-speed internet access to users in a metropolitan area.
4. **Video and Audio Streaming:** A MAN can support video and audio streaming for applications such as video conferencing and multimedia presentations.
5. **Backup and Recovery:** A MAN can provide backup and recovery services for data stored on multiple LANs.

6. **Disaster Recovery:** A MAN can provide a secondary communication channel in the event of a disaster or other emergency that disrupts the primary communication channel.
7. **Centralized Management:** A MAN allows centralized management of network resources, making it easier to monitor and manage the network.

✓ **Issues of MAN Network**

Like any other type of computer network, a Metropolitan Area Network (MAN) also faces several issues, including:

1. **Security:** MANs can be vulnerable to security threats such as hacking, malware, and unauthorized access.
2. **Scalability:** As the network grows and more users are added, the network may become congested, leading to performance issues.
3. **Reliability:** MANs can be affected by network outages, which can cause significant disruptions to the network.
4. **Interoperability:** Different LANs may use different technologies and protocols, making it difficult to interconnect them in a single MAN.
5. **Cost:** Implementing and maintaining a MAN can be expensive due to the high-speed equipment and infrastructure required.
6. **Latency:** The distance between different LANs can cause latency, affecting the speed and performance of the network.
7. **Bandwidth Limitations:** MANs can be limited by the bandwidth of the underlying network infrastructure, making it difficult to support high-bandwidth applications such as video conferencing.

✓ **Additional Information**

- **MAN**s can be both wired and wireless. Wired MANs use Fiber optic cables for high-speed connectivity, while wireless MANs use radio frequencies for communication.
- **MANs can be classified into two types**: synchronous and asynchronous. Synchronous MANs use a clock to ensure that all data is transmitted at the same speed, while asynchronous MANs do not use a clock and rely on start and stop bits to indicate the beginning and end of each data packet.
- MANs can be used in a variety of industries, including finance, education, healthcare, and government. For example, MANs can be used in hospitals to share patient records and medical imaging data between different departments.

- MANs can be interconnected with other networks, such as WANs and the internet, through gateways or routers. This allows users in a MAN to access resources and services outside of the network.
- MANs can be managed centrally or locally. In a centrally managed MAN, network resources are managed from a central location, while in a locally managed MAN, network resources are managed at the individual LAN level.
- MANs can provide Quality of Service (QoS) features, which prioritize certain types of traffic (such as video or voice) over others to ensure that they are transmitted with minimal delay and jitter. QoS can be implemented through techniques such as traffic shaping, packet prioritization, and bandwidth allocation.

✓ **How are MAN Networks Constructed?**

A metropolitan area network (MAN) is a system of two or more local area networks situated at a bigger geographical area than a Local Area Network but smaller than a Wide Area Network, usually covering a city or a metropolitan area.

**Process of MAN Network Constructed**

**1. Network infrastructure**

- Core Layer
  - The core of MAN is usually designed using high-capacity fiber optic cables.
  - They form the central hub of the network interconnecting several parts and powerful router and parts and switches are used to control data flow and routing within the MAN.
- Distribution layer
  - The whole data from multiple origins and ready it for distribute to the core layers or end-users.

**2. Connection to local area network (LANs)**

- The access layer adds routers, switches and other devices that directly combine end-users or LANs to the MAN.t This is where most user interface with the network.

**3. Internet and External connection**

- These devices manage connection between the MAN and the broads internet or other outer networks, they handle data routing, security and sometimes load balancing.

**4.Network management and Security**

- This helps in control optimal operations and troubleshooting problems. Tools and system are in locate to monitors network performance, traffic patterns, and potential issues.
- These have various security such as firewall, encryption, VPNs, and other security protocols are implemented to secure data and ensure safe access.

**5. Redundancy and Failovers**

- Critical parts frequently have backup system in locate to take over in case of failures make sure continuous network operation.
- System and plans are in locate to recover from unfortunate failure or disasters.

**6. Scalability and Flexibility**

- The network is frequently structured in a modular fashion, allowing for easy growth or reconfiguration as the needs of the users or organize change.
- A MAN can help various technologies, including Ethernet, wireless, and optimal connections, distributing flexibility in network design and deployment.

Apart from the Fiber optic links, MANs may integrate different wireless technologies, such as microwave links or Wi-Fi, to connect various LANs over smaller distances inside a metropolitan area. In general, MAN combines both wired and wireless technologies to construct the network infrastructure that connects a few LANs spread over the metropolitan area efficiently.

## 1.4 WAN (Wide Area Network)

A WAN (Wide Area Network) is to connect multiple smaller Local Area Networks (LANs). It is a computer network designed. WANs can help in communication, the sharing of information, and much more between systems or devices from around the world through a WAN provider.

✓ **What is a WAN?**

**WAN** stands for **Wide Area Network**. It is a computer network that covers a large geographical area consisting of two or more LANs or MANs. These networks are established with leased telecommunication circuits, in which two sides which are connected have routers that connect the LAN of both sides together in a network to facilitate communication.

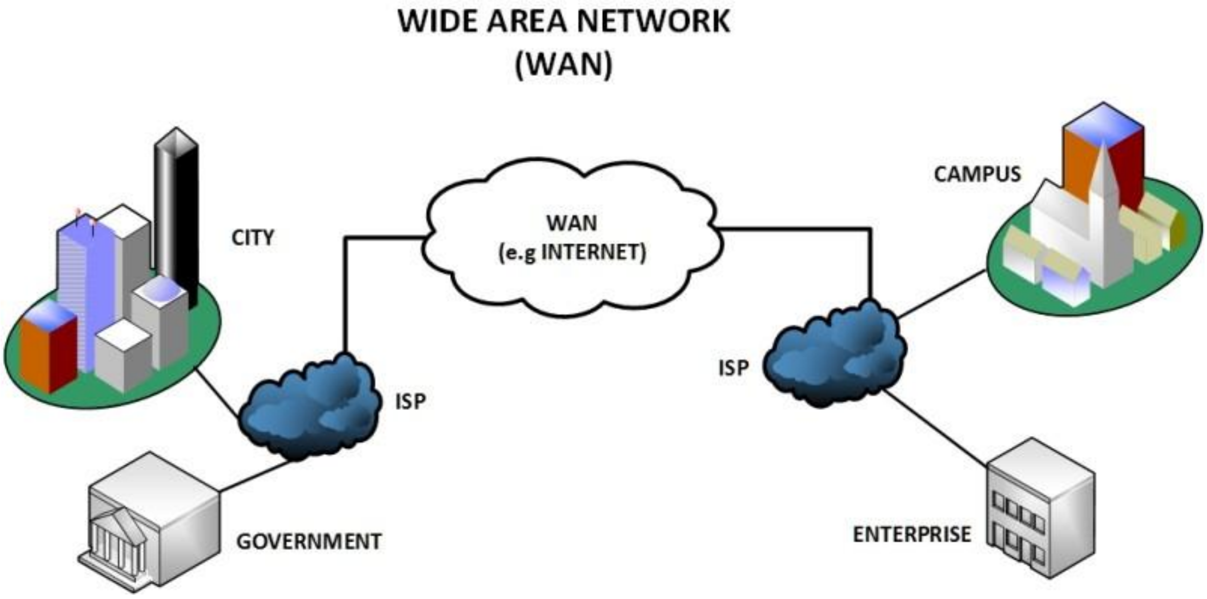
**WAN Full Form**

- ✓ **History of WAN**

The roots of WAN are connected to the U.S Department of defence which developed ARPANET to let researchers communicate and share computer resources remotely. The connection can be circuit-switched telephone lines, radio wave transmission or optical Fiber transmission. It is used to exchange data with users all over the world, they can be client, employee, buyer, seller, student, etc. WAN can transmit data, image, audio data, video data over large distances.

- ✓ **What is a WAN Router?**

An organisation can access a carrier network by using a WAN router, sometimes referred to as an edge router or border router, which routes data packets between WAN locations. Packet over SONET/SDH (PoS), Multiprotocol Label Switching (MPLS), ATM, and Frame Relay are many WAN protocol were developed.



- ✓ **What is Software-Defined WAN (SD-WAN)?**
  - It is a technique for making WAN architectures easier to construct, run, and administer is software-defined WAN (SD-WAN). It relies on virtualization, overlay networks, application-level policies and onsite SD-WAN devices and software platforms.
  - SD-WAN improves the efficiency of data transfer across a WAN by shifting traffic to less expensive network links to replace more expensive leased or MPLS lines.

- ✓ **Types of WAN Technologies**

  There are mainly two technologies that are used in the WAN network design.

  - **Circuit switching**: Circuit switched networks operate on the virtual connection principle, which dictates that all messages will take the same way and that resources along this path are set aside for this connection.
  - **Packet Switching:** The size of a packet in a packet switched network is dictated by the outgoing link, and these packets may follow different route. These packets are ready to collected and reassembled at the destination.
  - **TCP/IP protocol suite**: TCP/IP is a protocol suite of foundational of the internet protocols used to interconnect devices on Internet and other computers networks or device network. Full form of TCP/IP is Transmission Control Protocol/Internet Protocol.
  - **Router:** A router is a networking device which transfers data packets between device networks and also we can say it is used to interconnect LANs to form a wide area network (WAN).
  - **Packet over SONET/SDH (PoS):** Packet over SONET and SDH is a communication protocol used for WAN transport. When using optical fiber and SONET or SDH communication protocol used to defines how point-to-point links communicate.
  - **Multiprotocol Label Switching (MPLS):** Multi Protocol Label Switching (MPLS) is an IP packet routing technique and also a network routing optimization technique that routes IP packet through paths via labels instead of looking at complex routing tables of routers.

- ✓ **Characteristics of WAN**
  - **Broader Reach:** The reach of WAN in terms coverage of geographical area is very high which can be a region, country, or the world itself.
  - **Higher Capacity:** The capacity of WAN in terms of number of LANs or WANs connected in a network is very high, which results in connection of large number of user over different location all around the globe.
  - **Use of Public Carrier:** WAN uses telephone network, cabled system, satellites etc for connection and transmission purpose which are easily available.

- **Resource Sharing:** WAN enables its users to share data and information over large area. Computer resources can be accessed remotely which makes transmission and exchange of data very easy.

✓ **Advantages of WAN**

- It covers large geographical area which enhances the reach of organisation to transmit data quickly and cheaply.
- The data can be stored in centralised manner because of remote access to data provided by WAN.
- The travel charges that are needed to cover the geographical area of work can be minimised.
- WAN enables a user or organisation to connect with the world very easily and allows to exchange data and do business at global level.

✓ **Disadvantages of WAN**

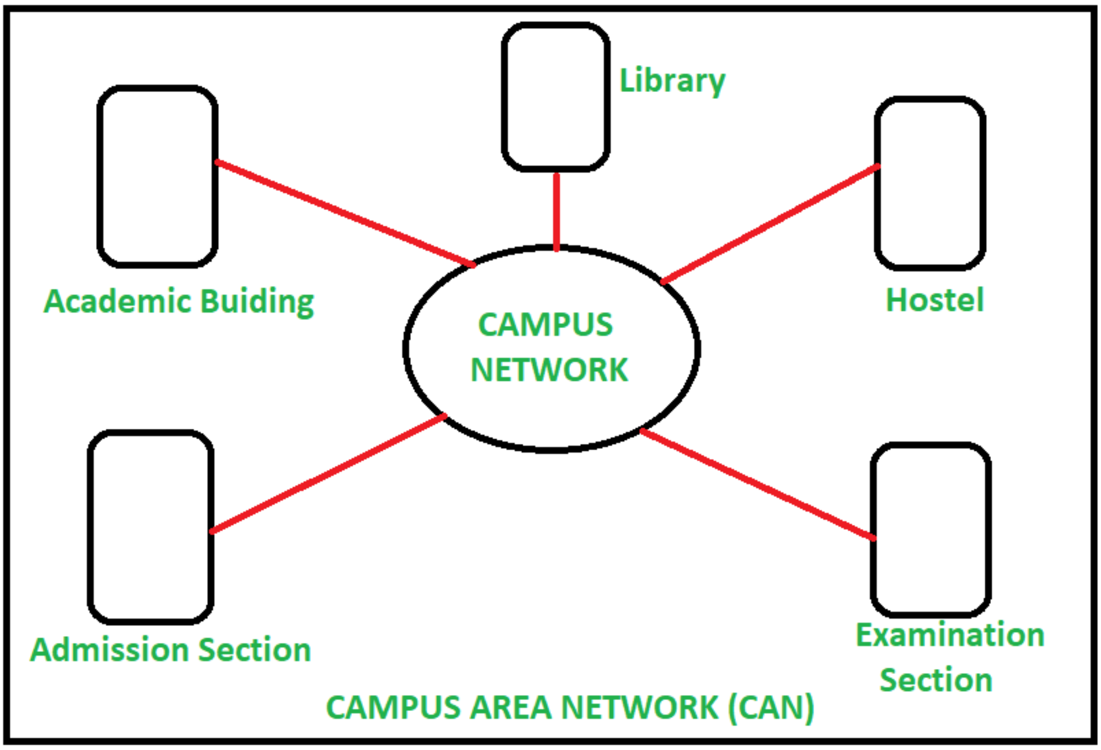
- Traffic congestion in Wide Area Network is very high.
- The fault tolerance ability of WAN is very less.
- Noise and error are present in large amount due to multiple connection point.
- The data transfer rate is slow in comparison to LAN because of large distances and high number of connected system within the network.

## 1.5 Overview of CAN (Campus Area Network)

**Campus Area Network (CAN)** is a group of interconnected Local Area Networks (LAN) within a limited geographical area like school campus, university campus, military bases, or organizational campuses and corporate buildings etc. A Campus Area Network is larger than Local Area Network but smaller than Metropolitan Area Network (MAN) and Wide Area Network (WAN). This Campus Area Network also called as Corporate Area Network. Sometimes this network is also referred as Residential Network or ResNet as it is only used by residents of specific campus only. Campus Area Network is network of interconnected Local Area Networks where these LANs are connected via Switches and routers and create a single network like CAN. Campus Area Network covers areas of around 1 to 5 km range and it can be both wired or wireless connectivity.

**Example of CAN:** Let us think about a university where university networks interconnect academic building, admission building, library, account section, examination section, placement section etc of an institution when connected with each other combine to form Campus Area Network (CAN).

The below figure illustrates a Campus Area Network:



**Infrastructure of CAN:** Within a limited geographical area, LANs are interconnected with help of Switches and Routers and connects buildings to buildings of a single campus where all networking resources like wiring, hubs, switches, routers etc are owned by organization itself. In this, they use same kind of technologies like Local Area Network only interconnection between different buildings is there. Nodes in a campus network are interconnected by means of Optical Fiber media, i.e., Fiber optics and takes advantage of 10-Gigabit Ethernet technology. Besides this 10-Gigabit ethernet technology, Wi-Fi hotspots and hot zones are different ways of accessing network.

**Benefits of CAN:**

- **Speed -** Communication within a CAN takes place over Local Area Network (LAN) so data transfer rate between systems is little bit fast than Internet.
- **Security -** Network administrators of campus take care of network by continuous monitoring, tracking, and limiting access. To protect network from unauthorized access firewall is placed between network and internet.
- **Cost effective -** With a little effort and maintenance, network works well by providing fast data transfer rate with multi-departmental network access. It can be enabled wirelessly, where wiring and cabling costs can be managed. So, to work with in a campus using CAN is cost-effective in view of performance.

## 1.6 SAN (Storage Area Network)

A dedicated, fast network that gives storage devices network access is called a **Storage Area Network (SAN)**. SANs are generally made up of several technologies, topologies, and protocols that are used to connect hosts, switches, storage elements, and storage devices. SANs can cover several locations.

Data transfer between the server and storage device is the primary goal of SAN. Additionally, it makes data transmission across storage systems possible. Storage area networks are primarily used to connect servers to storage devices including disk-based storage and tape libraries.

✓ **Types of Storage Area Networks (SAN)**

- **Fibre Channel (FC):** A Fibre Channel is one of the maximum broadly used SAN storage connections. It presents excessive-velocity, low-latency connectivity between servers and storage devices with the use of fibre optic cables. Fibre Channel helps factor-to-factor, arbitrated loop, and switched fabric topologies. It gives excessive throughput, reliability, and scalability, making it suitable for traumatic enterprise environments.

- **Internet Small Computer System Interface(iSCSI):** iSCSI is a storage protocol that transmits SCSI commands over TCP/IP networks, permitting servers to get the right of entry to faraway storage devices using fashionable Ethernet connections. ISCSI offers a value-effective alternative to Fibre Channel, leveraging current Ethernet infrastructure and TCP/IP networks. It presents features such as block-level garage access, multipathing, and CHAP authentication.

- **NVMe over Fabrics (NVMe-oF):** NVMe over Fabrics extends the NVMe garage protocol over excessive-pace networks, together with Ethernet or Fibre Channel, to offer low latency.

- **Fibre Channel over Ethernet (FCoE):** Fibre Channel over Ethernet encapsulates Fibre Channel frames into Ethernet packets, allowing Fibre Channel site visitors to be transmitted over Ethernet networks. FCoE enables the convergence of storage and data networks, lowering infrastructure complexity and fees. It leverages Ethernet's sizable adoption and familiarity at the same time as preserving Fibre Channel's overall performance characteristics.

- **Serial Attached SCSI(SAS):** Serial Attached SCSI is a factor-to-point garage protocol designed to attach servers to garage gadgets using high-pace serial connections. SAS gives overall performance akin to Fibre Channel but with less difficult cabling and decrease expenses. It helps direct-connected garage (DAS) and may be used in SAN environments with SAS switches or routers.

✓ **Advantages of SANs**

- Increased accessibility of applications
- Storage is available through numerous pathways for improved dependability, availability, and serviceability and exists independently of applications.
- Improved functionality of the programme
- Storage Area Networks (SANs) transfer storage processing from servers to different networks.
- High availability, scalability, flexibility, and easier management are all made feasible by central and consolidated SANs.
- By using a remote copy, remote site data transfer and vaulting SANs shield data from malicious assaults and natural disasters.
- Straightforward centralised administration
- SANs make management easier by assembling storage media into single images.

✓ **Disadvantages of SANs**

- If client PCs require high-volume data transfer, SAN is not the best option. Low data flow is a good fit for SAN.
- More costly
- It is quite challenging to keep up.
- Sensitive data may leak since every client computer has the same set of storage devices. It is best to avoid storing private data on this network.
- A performance bottleneck is the result of poor implementation.
- Maintaining a data backup in the event of a system failure is challenging.
- Too costly for small businesses
- need a highly skilled individual

Today, many businesses are growing fast online, so they need to store a lot of data. They use systems like **ERP (Enterprise Resource Planning)** to connect different parts of the company, and **data warehouses** to save old data for reports. Because of this, the **need for storage has increased**.

In the past, companies stored data in fixed places like data centers. But now, they need **faster and more flexible ways** to manage their data.

Many companies use **RAID systems** to protect data. But to use these systems well, they must connect them to a special network called **SAN (Storage Area Network)**. SAN helps to

**store and access data better and faster**, making it easier for businesses to handle large amounts of data.

In a **Storage Area Network (SAN)**, storage devices like hard drives are connected as **nodes** on a **high-speed network**. These storage devices can be **easily connected or removed** from servers whenever needed. This makes SAN very **flexible**.

Many companies now offer **SAN solutions**, and they use their **own network designs (called proprietary topologies)**. The main advantage is that the **storage devices don't have to be close to the servers**—they can be placed far away and still work well. These systems also give businesses **more options** for **speed and connections**.

Older storage software can also work with SAN by using **Fibre Channel networks**. Fibre Channel helps transfer the old **SCSI protocol** over a network. Because of this, the devices connected to a SAN **look like SCSI devices** to the server, even though they are working over a new, high-speed network.

Current architectural alternatives for SAN include the following:

- Point to point connection between the storage system and servers via Fibre Channel.
- Use of Fibre Channel switches to connect Multiple RAID systems, tape libraries and so on to servers.
- Use of Fibre Channel hubs and switches to connect servers and storage system in the different configuration.

✓ **Main advantages claimed are following:**

- Flexible for many to many connectivity among servers and storage device with the help of fibre channel hubs and switches.
- Up to 10 Km separation between a server and a storage system using appropriate fibre optic cables.
- Better isolation capabilities allowing the nondisruptive addition of new servers and peripherals.

Use of SANs are increasing rapidly but it still facing many problems such as combining storage option from multiple vendors and dealing with evolving standards of storage management software and hardware. Most major companies are evaluating SAN as a viable option for database storage.

✓ **Features of Storage Area Networks (SAN)**

- Users may more easily scale up or down the storage space to suit their demands using SANs since they make it convenient to add or remove storage devices from their storage networking systems. Furthermore, servers continue to function normally even when scaling up or down. Because users do not need to restart or stop these servers, there is less downtime because the apps can continue to function.

- Cybercriminals could potentially gain access to data kept on a storage system. That is why having top-notch security measures is essential for a sound storage network system. SAN security features are excellent. With SANs, users can limit unauthorised access to data by using a virtual SAN.
- They also have security protocols, such as an access control list (ACL), which makes them one of the best storage networking systems.
- SAN provide good disk utilization.

✓ **Protocols Used in SAN**

There are multiple protocols used by Storage Area Networks (SAN), Below are some mentioned protocols supported by the Storage Area Network:

- **Fibre Channel Protocol (FCP):** It is the Storage Area Network protocol that is most frequently utilised. It is a Fibre Channel (FC) network mapping of a SCSI command.
- **Internal Small Computer Interface (ISCSI):** Internet SCSI, or Internet Small Computer System Interface, is what it stands for. It is the SAN protocol's second-largest block. The SCSI commands are transferred via an Internet protocol (IP) ethernet after being encapsulated in an ethernet frame.
- **Fibre Channel Over Internet (FCoE):** The acronym for "Fibre Channel Over Internet" is FCoE. This protocol bears resemblance to the iSCSI. It transfers over an IP Ethernet network by enclosing the fibre channel inside an Ethernet datagram.
- **Non-Volatile Memory Express (NVMe):** NVMe, or Non-Volatile Memory Express, is an acronym. Additionally, it is a SAN protocol that uses PCI to access flash storage.

## 1.7 EPN (Enterprise Private Network) or Enterprise Networks

A type of private network which an enterprise company uses to connect its branches is known as an enterprise private network. The initial networking was made possible in the 1970s by AT&T. Enterprise private network can be made in various ways that include: - Virtual private network (VPN) Local area network (LAN) Wide area network (WAN) Cloud-based network The purpose of EPN is to have high-speed internet and data [...]

A type of private network which an enterprise company uses to connect its branches is known as an enterprise private network. The initial networking was made possible in the 1970s by AT&T.

Enterprise private network can be made in various ways that include: -

- Virtual private network (VPN)
- Local area network (LAN)
- Wide area network (WAN)
- Cloud-based network

The purpose of EPN is to have high-speed internet and data sharing within an organization. Companies can use Wi-Fi within their offices to share the internet and resources. Also, routers, switches, Fiber optics, virtual devices, and modems are used in making this type of private network.

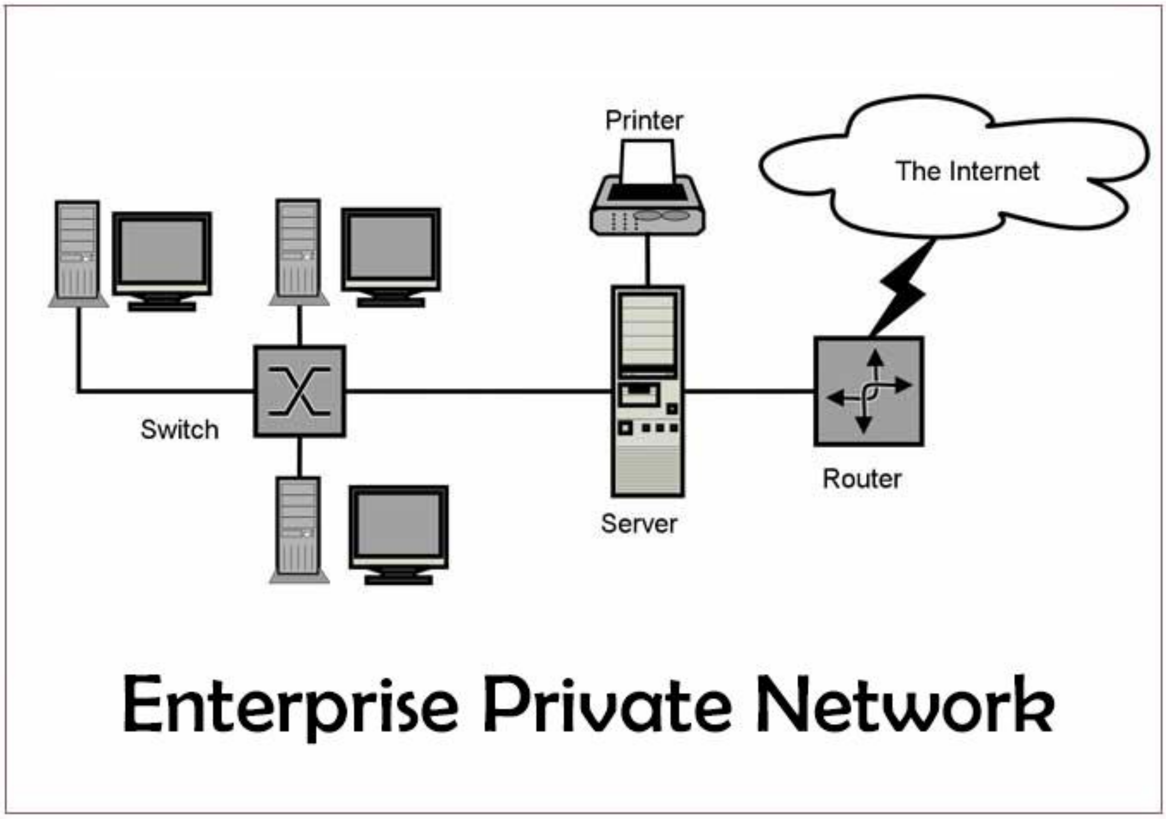


**Diagram of EPN**

Security is also an important issue in making the enterprise network. There are placed different firewalls near access points to have the secure transfer of data among computers. The high speed of data transfer can be made using Fiber optics. If different branches of the company are very close to each other than LAN is best for making the private network. But if branches of the company are far away from each other than WAN is a better choice. If WAN is used to make a private network, then a dedicated leased line is given by ISP to connect different branches of the company.

Making an enterprise network also involves secure sharing of data that is done by using cloud-based services. Employees of the company can store their data on cloud-based servers. Data is placed securely on the cloud and can be retrieved 24/7.

VPN also plays an important role in making a private network. People across the organization securely communicate with one another. The special IP is assigned to each user and the original IP is not shared with other users. The data is also encrypted before sending it on the streamline.

✓ **Features of Enterprise private network (EPN)**

Some benefits of EPN are: -

- EPN has higher security than other types of public networks
- EPN uses cloud storage for storing and retrieval of data
- The messages are encrypted before sending
- It is best for business users
- Different offices are centralized together through EPN
- This network is scaled up quickly without a lot of expense
- EPN is cost-effective for big companies

✓ **Examples of Enterprise private network (EPN)**

- Connecting different shops of the company
- Communication network between head office and remote office of the company
- Connecting hospital branches from different cities together
- Sharing of data like live videos among different university campuses

## 1.9 VPN (Virtual Private Network)

**What is VPN? How It Works, Types of VPN**

A **VPN (Virtual Private Network)** is a powerful tool that enhances **online privacy**, protects sensitive data, and enables secure access to the internet. In today's interconnected world, **online privacy** and **data security** are more important than ever. One of the best ways to protect yourself and enhance your internet experience is by using a **VPN (Virtual Private Network)**. Whether you are looking to **secure your data**, **bypass geo-restrictions**, or simply want to **maintain your anonymity online**, a VPN is an invaluable tool.

This guide will explain **what VPN is**, **how it works**, and the **different types of VPNs** available to suit your needs in 2025.

***Disclaimer****: Always select a reliable VPN service to ensure maximum security and avoid potential risks.*

✓ **What Is a VPN**

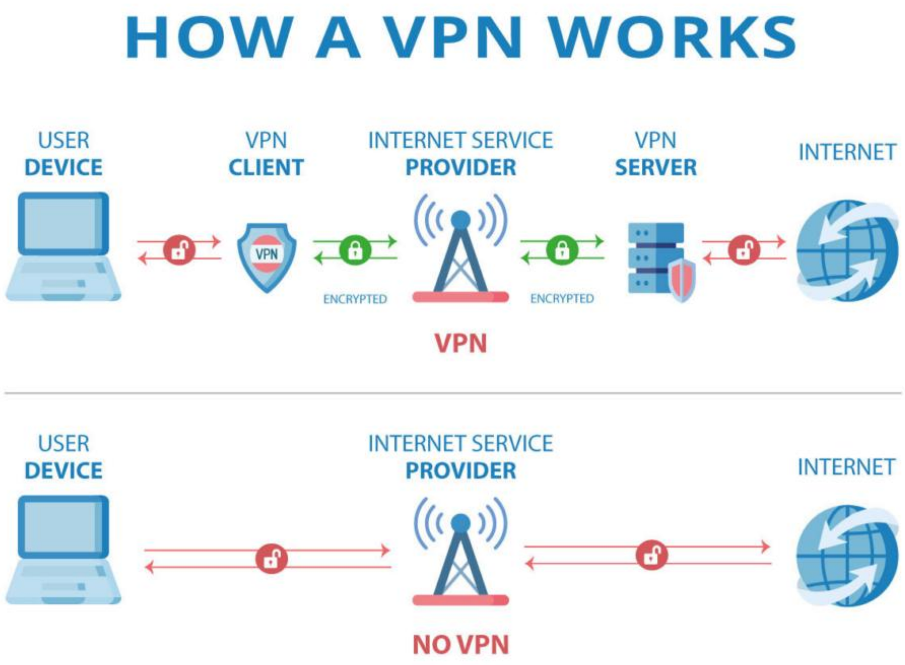
A **VPN (Virtual Private Network)** is a technology that creates a secure, encrypted connection between your device and the internet. It essentially acts as a private tunnel for your internet traffic, preventing hackers, ISPs, and even governments from monitoring your activities. When using a VPN, your **IP address** is masked, and your online actions are routed through a remote server, making it harder to track your online activity.

✓ **Key Benefits of Using a VPN:**

1. **Privacy Protection**: A VPN hides your IP address, ensuring that your browsing habits and activities remain private.
2. **Security on Public Networks**: Public Wi-Fi networks are often insecure, but a VPN encrypts your connection, making it safer to browse the internet on networks like those in cafes or airports.
3. **Bypass Geo-restrictions**: A VPN allows you to access content that may be blocked in certain regions (such as streaming platforms, social media sites, etc.).
4. **Prevent Data Throttling**: Some ISPs throttle your connection speed when you stream or play games. A VPN can bypass this, allowing for faster internet speeds.
5. **Accessing Remote Work Resources**: A VPN enables secure access to private networks, making it ideal for businesses and remote workers.

✓ **How Does a VPN Work**

A VPN works by creating an encrypted tunnel between your device and a remote server. Here's the process simplified:



1. **Connection Establishment**: When you activate a VPN on your device, it connects to a server operated by the VPN provider.

2. **Encryption**: The VPN encrypts your data (**information, files, web traffic**) so that it's unreadable to anyone trying to intercept it, whether it's a hacker on the same Wi-Fi network or an entity trying to monitor your browsing.
3. **Traffic Redirection**: Your device's internet traffic is routed through the VPN server, which can be located in any country. This makes it appear as though you're browsing from the server's location, masking your actual IP address.
4. **Decryption**: Once your data reaches the VPN server, it is decrypted and sent to the destination (such as a **website, app, or service**). Any response from the server is then sent back to you through the encrypted tunnel.

This **end-to-end encryption** ensures that your sensitive data stays private and your location remains anonymous.

✓ **Types of VPN**

VPNs come in various types, each catering to different needs, from individual privacy to enterprise-level solutions. Below are the main types of VPNs:

**1. Remote Access VPN**

A **Remote Access VPN** allows individual users to connect to a network remotely, such as accessing work files from home. It's ideal for people who need secure access to a private network from anywhere.

**2. Site-to-Site VPN**

A **Site-to-Site VPN** is used to connect two networks, often used by businesses with multiple office locations. It securely links two private networks over the internet, enabling employees to access resources from both locations.

**3. Mobile VPN**

A **Mobile VPN** is designed for mobile devices like smartphones and tablets. It ensures stable connections even when switching between different networks (such as from Wi-Fi to mobile data) and is used in industries like healthcare and logistics where users need continuous access while moving.

**4. MPLS VPN (Multiprotocol Label Switching)**

An **MPLS VPN** is used mainly by large businesses and enterprise networks. It routes data between different locations through an efficient network that prioritizes data traffic. It's often more complex and provides more scalability compared to traditional VPNs.

**5. PPTP VPN (Point-to-Point Tunneling Protocol)**

**PPTP** is one of the oldest VPN protocols and is known for being fast but less secure compared to others. It is rarely used in modern systems due to its vulnerabilities, but it's still available on some legacy systems.

**6. L2TP/IPsec VPN (Layer 2 Tunneling Protocol with IPsec)**

**L2TP** combined with **IPsec** offers more security than PPTP. It uses encryption to secure data, making it a popular option for users who need a reliable, moderately secure connection.

**7. OpenVPN**

**OpenVPN** is a highly secure, open-source VPN protocol known for its flexibility and strength in encryption. It's often used for custom VPN setups and is highly configurable, making it a popular choice for advanced users.

**8. IKEv2/IPsec VPN (Internet Key Exchange version 2)**

**IKEv2** is a fast, stable, and secure VPN protocol that works well on mobile devices. It automatically reconnects when the device switches between networks, providing continuous service without interruptions.

✓ **Advantages of Using a VPN**

1. **Privacy Protection**: VPNs keep your online activities private and anonymous, preventing third parties from tracking you.
2. **Bypass Geo-Restrictions**: VPNs enable you to access content that might be restricted in your country or region, such as streaming services (Netflix, BBC iPlayer).
3. **Enhanced Security**: With end-to-end encryption, VPNs protect your data from hackers, especially on public Wi-Fi networks.
4. **Prevents Data Throttling**: VPNs help avoid internet speed throttling imposed by your Internet Service Provider (ISP), particularly when streaming or gaming.
5. **Safer Online Transactions**: VPNs help protect sensitive information like bank details when conducting transactions online.
6. **Access Work Resources Remotely**: Securely access your work or school network, even from remote locations.

✓ **Disadvantages of Using a VPN**

1. **Slower Speeds**: Using a VPN may slow down your internet speed due to the encryption process and server routing.
2. **Not All VPNs Are Equal**: Some VPN services may log your data or provide subpar protection, so it's essential to choose a **reliable VPN provider**.

3. **Can Be Blocked**: Certain websites or countries may block VPN access, limiting your ability to connect to certain services.
4. **Requires Configuration**: Setting up a VPN may require a bit of technical knowledge, especially if you're doing it manually.
5. **Cost**: While there are free VPNs available, premium VPNs offer more reliable services and better security, which can be a recurring expense.

✓ **How to Choose the Right VPN for Your Needs?**

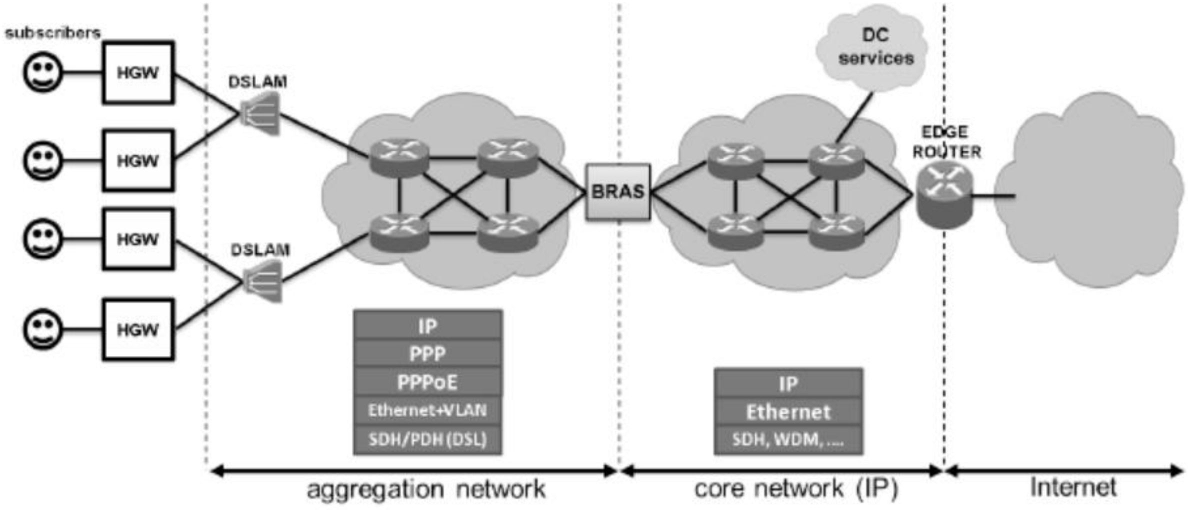
When selecting a VPN, consider the following factors:

1. **Security Features**: Look for strong encryption, no-logs policies, and secure protocols (e.g., OpenVPN, IKEv2).
2. **Speed**: If streaming or gaming is a priority, choose a VPN with high-speed servers.
3. **Location of Servers**: More server locations provide better access to geo-blocked content.
4. **Device Compatibility**: Ensure the VPN is compatible with your devices (Windows, Mac, Android, iOS).
5. **Customer Support**: Choose a VPN with excellent customer support in case you encounter issues.

## 2. Broadband Access Networks – Explained in Simple English

**Definition:**

**Broadband Access Networks** are the technologies that help users connect to the internet at **high speed** over long distances. These networks provide **continuous internet access** to homes, offices, and organizations.



✓ **Why “Broadband”?**

- "Broadband" means **wide bandwidth** — it can carry **large amounts of data** quickly.
- Unlike old dial-up connections, broadband is **always ON** and does not block your phone line.

✓ **Types of Broadband Access Networks:**

**1. DSL (Digital Subscriber Line)**

- Uses **telephone lines** to provide internet.
- You can **talk on the phone and use the internet at the same time**.
- Speed: Medium (up to 100 Mbps)
- **Example:** BSNL DSL broadband

**2. Cable Modem**

- Uses **TV coaxial cables** to give internet access.
- Faster than DSL in many cases.
- Speed: High (up to 1 Gbps)
- **Example:** ACT Fibernet, Hathway

**3. Fiber Optic (FTTH – Fiber To The Home)**

- Uses **light signals through glass fibers** for super-fast internet.
- Very **high speed and stable** connection.
- Speed: Very High (up to 10 Gbps or more)
- **Example:** Jio Fiber, Airtel Xstream Fiber

**4. Wireless (Wi-Fi, Mobile Data, 4G/5G)**

- No cables needed – uses **radio signals**.
- Includes **mobile broadband** (like Jio 4G/5G, Airtel).
- Speed: Varies from medium to very high.
- Best for portable use.

**5. Satellite Internet**

- Used where cable or fiber is **not available** (remote areas).
- Requires a **dish antenna** to communicate with satellites.
- Speed: Moderate, but **higher delay (latency)**.

- **Example:** HughesNet, Starlink

### 6. Fixed Wireless Access (FWA)

- Uses **antennas** to provide internet over short distances.
- Faster than satellite, used in cities or villages.
- Used by ISPs when fiber is not feasible.

### Features of Broadband Access:

- **Always ON** – no need to connect again and again.
- **Faster** than dial-up.
- Can support **multiple devices** (like phones, laptops, TVs).
- Allows video calls, streaming, online games, cloud use, etc.

### Real-Life Example:

You connect your laptop to your home Wi-Fi, which is provided by Jio Fiber. That Fiber cable is part of a **broadband access network**, letting you browse the web, stream HD movies, and download files quickly.

## 3 Mobile and Wireless Access Networks – Explained Simply

### Definition:

**Mobile and Wireless Access Networks** are technologies that allow devices like smartphones, laptops, or tablets to **connect to the internet without wires** — either **while moving** (mobile) or within a fixed area (wireless).

✓ **Difference Between Mobile & Wireless Access:**

| Type | Meaning | Example Use |
|---|---|---|
| **Mobile Access** | Internet access **while moving** | Using mobile data (4G/5G) on your phone |
| **Wireless Access** | Internet access **without cables**, but usually **stationary** | Using Wi-Fi at home or office |

✓ **Types of Mobile and Wireless Access Networks:**

### 1. Wi-Fi (Wireless Fidelity)

- Wireless internet in a **limited area** (like home, school, or office).
- Devices connect using a **Wi-Fi router**.
- Based on **IEEE 802.11 standards**.

- **Range:** Up to 100 meters indoors.
- **Speed:** 50 Mbps to 1 Gbps (depends on the router).

**Example:** Airtel Broadband Wi-Fi at home

**2. Cellular Networks (2G, 3G, 4G, 5G)**

- Allows mobile devices to access internet **anywhere within coverage**.
- Connects via **mobile towers**.
- Based on standards like **GSM, UMTS, LTE, 5G-NR**.

| **Generation** | **Technology** | **Speed** | **Use Case** |
|---|---|---|---|
| 2G | GSM | ~50 Kbps | Calls & SMS |
| 3G | UMTS | ~2 Mbps | Basic internet |
| 4G | LTE | ~100 Mbps | HD video, online games |
| 5G | 5G-NR | >1 Gbps | Smart cities, IoT, AR/VR apps |

- **Example:** Jio 5G, Airtel 4G

**3. Bluetooth**

- Short-range wireless network for **device-to-device** communication.
- Used for **headphones, printers, file sharing**, etc.
- **Range:** Up to 10 meters
- **Speed:** ~2-3 Mbps
- **Example:** Connecting phone to Bluetooth speaker

**4. Infrared (IR)**

- Wireless, **line-of-sight** communication.
- Rarely used now (older phones, TV remotes).
- Short-range, **slow speed**.
- **Example:** TV remote control

**5. Zigbee / Z-Wave / LoRa**

- Low-power wireless networks for **IoT (Internet of Things)**.
- Used in **smart homes**, agriculture, industrial monitoring.
- Long battery life, small data size.
- **Example:** Smart bulbs, smart locks, environmental sensors

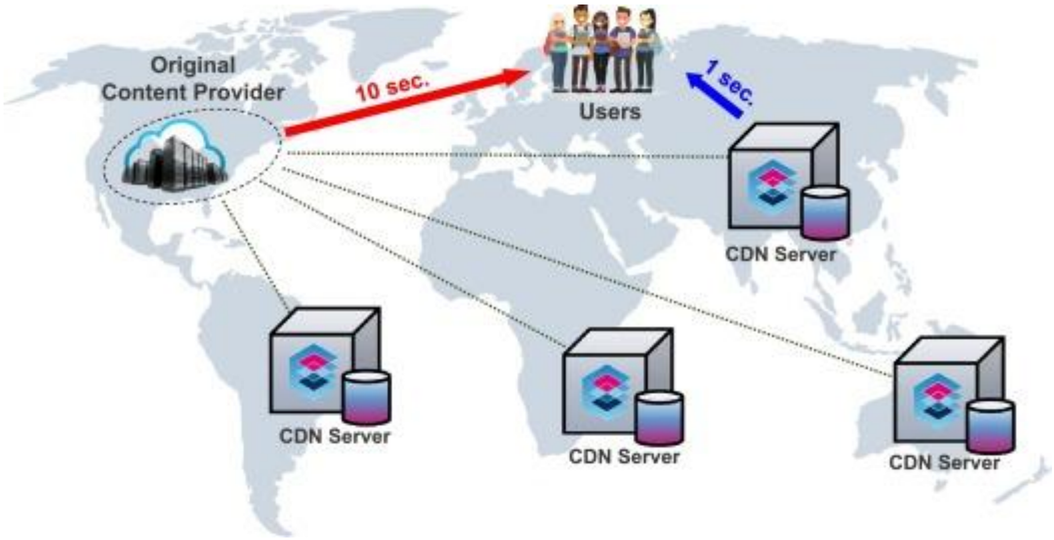
**Common Uses:**

- Browsing internet on mobile.
- Wi-Fi access in cafes, airports, schools.
- Video calling (Zoom, WhatsApp).
- Mobile payment apps (PhonePe, Google Pay).
- Location tracking, smart home devices.

## 5 Content Provider Networks – Explained Simply

**Definition:**

**Content Provider Networks** are systems or platforms that **host, manage, and deliver digital content** (like videos, music, web pages, apps) to end-users over the internet.



They **own or control** the servers and infrastructure that deliver content such as:

- Videos (e.g., YouTube)
- News (e.g., Times of India)
- Apps (e.g., Google Play Store)
- Social media (e.g., Facebook)

**Simple Example:**

When you watch a movie on **Netflix** or a video on **YouTube**, that content is delivered to you through **content provider networks**. These platforms have **data centers and servers** around the world to deliver fast and reliable service.

✓ **Main Features:**

| Feature | Explanation |
|---|---|
| Content Hosting | Stores videos, images, websites, and app files |
| Content Delivery | Sends content to users via **CDNs** (Content Delivery Networks) |
| Scalable Infrastructure | Supports **millions of users at the same time** |
| Optimized for Speed | Uses caching and edge servers for faster delivery |
| Analytics Support | Tracks content usage, traffic, and performance |

✓ **Popular Content Providers:**

| Provider | Type of Content | Example Use |
|---|---|---|
| **YouTube** | Videos, livestreams | Watching tutorials, movies |
| **Netflix** | TV shows, movies | Streaming entertainment |
| **Spotify** | Music, podcasts | Listening to music |
| **Facebook** | Social media content | News feed, stories, ads |
| **Google Play** | Apps, games, books | Downloading apps |
| **Amazon** | E-commerce product content | Viewing product details, reviews |

✓ **How It Works (Simplified Steps):**

1. **Content Creation:** User or company uploads videos, blogs, or apps to the provider's platform.
2. **Storage in Servers:** Stored in data centers around the world.
3. **User Request:** You click a video or app.
4. **Content Delivery:** Sent to your device using the **nearest server** (via CDN) for fast response.
5. **Display on Screen:** Content is shown with minimal delay.

✓ **Technologies Used in Content Provider Networks:**

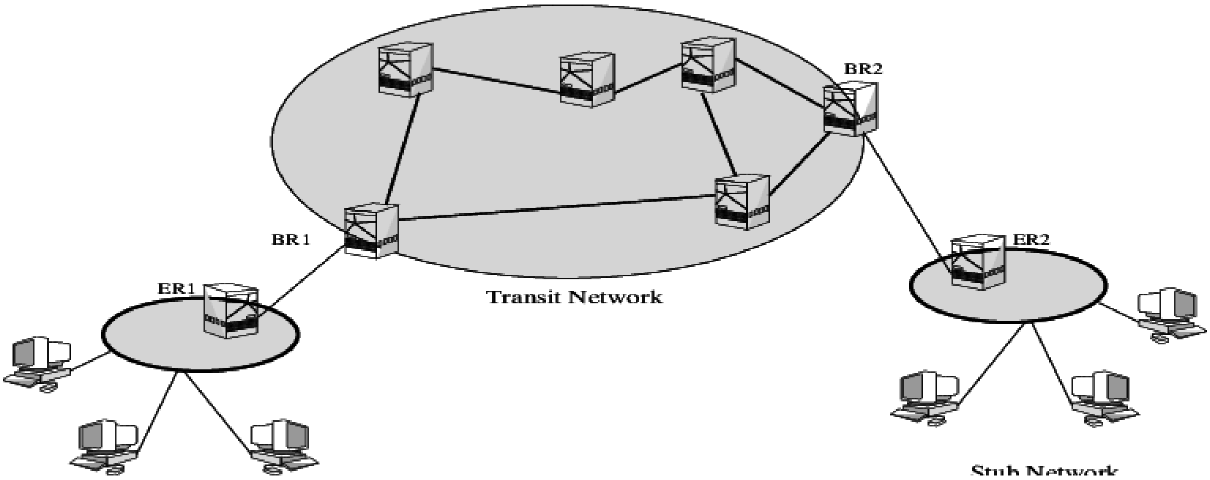
| **Technology** | **Purpose** |
|---|---|
| **CDN (Content Delivery Network)** | Speed up content delivery by using nearby servers |
| **HTTP/HTTPS** | Protocols for web content transfer |
| **Caching** | Store frequently accessed content for faster access |
| **Load Balancers** | Distribute user traffic efficiently |
| **Data Centers** | Large server farms to host content |

## 6 Transit Networks – Simple Explanation

**Definition:**

**Transit Networks** are **high-capacity backbone networks** that help **move internet traffic between different networks**, such as:

- Between **ISPs (Internet Service Providers)**
- Between **Content Providers and Users**
- Between **Data Centers and Regional Network**



**Key Components in the Image:**

**1. Transit Network (Center cloud):**

- Acts as the **backbone** of the overall network.
- Interconnects other networks, such as enterprise or stub networks.
- Typically made up of **core routers or high-speed switches**.

- Offers high-speed **data transit** between branches or regions.

**2. Stub Networks (Left and Right ovals):**

- Smaller, local networks that connect to the larger transit network.
- Stub networks don’t carry transit traffic—they only send/receive traffic through the backbone.
- These could be individual office networks, branch offices, or local departments.

✓ **Labeled Routers and Devices:**

| Label | Meaning | Function |
|---|---|---|
| **BR1, BR2** | **Border Routers** | Connect stub networks to the transit network. Route data between enterprise and backbone. |
| **ER1, ER2** | **Edge Routers** | Located on the **edge** of a stub network. Interface between internal devices (PCs, local servers) and the external (BR) router. |

**Traffic flow: Host → ER → BR → Transit Network → BR → ER → Host**

✓ **Example Walkthrough:**

Let us say a computer in the left stub network wants to send data to a computer in the right stub network:

1. The source PC sends data to **ER1**.
2. **ER1** forwards the data to **BR1**.
3. **BR1** sends the data through the **Transit Network**, possibly via multiple routers.
4. Data arrives at **BR2**, which forwards it to **ER2**.
5. **ER2** sends the data to the destination PC.

They act like **highways of the internet**, connecting smaller local roads (like your home or office network) to the global internet.

**Simple Example:**

When you open a website from your phone in India, and that website is hosted in the USA, your request **travels across multiple transit networks** (international Fiber cables, routers, etc.) to reach the server — and the response comes back the same way.

✓ **How It Works (Step-by-step):**

1. You open a website (e.g., www.example.com).
2. Your ISP (like Airtel, Jio) sends that request to a **Transit Network**.
3. The Transit Network carries the request across the globe to the content server.
4. The server sends data back to you through **another Transit Network**.
5. The data reaches your ISP, then your device.

✓ **Technologies and Protocols Used:**

| **Protocol / Tech** | **Full Form** | **Purpose** |
|---|---|---|
| **BGP** | Border Gateway Protocol | Routing data between large networks |
| **MPLS** | Multi-Protocol Label Switching | Fast data forwarding |
| **IP** | Internet Protocol | Addressing and delivery of packets |
| **DWDM** | Dense Wavelength Division Multiplexing | High-speed fiber optic transmission |
| **Peering Links** | (N/A) | Agreements for direct traffic exchange |

✓ **Major Transit Network Providers:**

| **Provider** | **Region / Speciality** |
|---|---|
| **Level 3 (Lumen)** | Global backbone network |
| **NTT Communications** | Asia-Pacific and global connectivity |
| **Tata Communications** | Strong Indian and international presence |
| **Cogent Communications** | Low-cost global transit |
| **AT&T** | North American backbone |

✓ **Benefits of Transit Networks:**

- Enables **global connectivity** for users and services
- Supports **high-speed, long-distance communication**
- Works behind the scenes to **route and deliver internet traffic**
- Offers **redundancy and reliability** in case of failure

## 7 Network Technologies: From Local to Global, Point-to-Point, Shared

This topic covers **how networks operate** across various distances (local to global) and how data is transmitted (point-to-point or shared). It is crucial for students to understand **how networks are built, scale up, and manage communication paths**.

### 1. From Local to Global

This refers to the **scale and coverage** of a network:

| Scale | Type | Example | Devices Used | Why it Matters |
|---|---|---|---|---|
| **Local** | PAN, LAN | Home Wi-Fi, Office LAN | Wi-Fi Router, Switch, PC | For fast internal communication |
| **Regional** | MAN | College Campus, City Fiber Network | MAN routers, Ethernet switches | Links large buildings or branches |
| **Global** | WAN/Internet | Internet, VPNs between countries | OLTs, Core Routers, Submarine cables | Allows worldwide communication |

**Real-life Example**:

- You send an email from your phone at home (local Wi-Fi).
- It travels through your ISP (regional).
- It reaches a server in the US (global WAN).

### 2. Point-to-Point Communication

**Definition:**

In **point-to-point (P2P)** communication, **data travels directly between two devices**, without being shared with others.

**Examples:**

- A **USB cable** from your laptop to a printer.
- A **dedicated leased line** between two bank branches.
- **Bluetooth** connection between mobile and wireless earbuds.

**Devices Used:**

- Ethernet cable (RJ45), Serial cable
- Modem, Router
- Microwave Dish (for long-distance P2P links)

**Why You Should Know:**

- P2P is the simplest form of connection.
- Foundation of **secure**, **private** and **dedicated** communications.
- Used in **IoT**, **edge computing**, and **remote device setup**.

### 3. Shared Communication

**Definition:**

In **shared networks**, **multiple devices use the same communication channel**, and must take turns or share bandwidth.

**Examples:**

- Your home Wi-Fi (many devices share bandwidth)
- Ethernet LAN with a hub
- Cable TV network

**Devices:**

- Network Hub (old tech)
- Wi-Fi Routers
- Switches (layer 2 and layer 3)

**Drawback:**

- Collisions and congestion if too many devices send at once.

**Why You Should Know:**

- Understand **bandwidth allocation** and **network performance**.
- Learn how **contention and collision** affect data flow.
- Important in **network design**, **performance tuning**, and **troubleshooting**.

# 8 Home Networks

A **Home Network** is a **small-scale network** set up in a residential home. It connects multiple digital devices such as computers, smartphones, smart TVs, gaming consoles, printers, and IoT devices so they can share internet access, files, and devices like printers or speakers.

✓ **Definition:**

A **Home Network** is a type of **Local Area Network (LAN)** used within a home environment to connect digital devices together using **wired (Ethernet)** or **wireless (Wi-Fi)** technologies.

✓ **Key Features:**

| Feature | Description |
|---|---|
| **Scope** | Covers a single house or apartment |
| **Devices connected** | Smartphones, laptops, smart TVs, routers, printers, IoT devices |
| **Connection types** | Wi-Fi (wireless), Ethernet cables (wired) |
| **Network device** | Wireless router (often includes modem + firewall + switch) |
| **Control** | Managed by the user (basic configuration via router interface) |

✓ **Real-Life Example:**

At home, you may have:

- A **Wi-Fi router** that gives internet access.
- Your **laptop**, **smartphone**, and **smart TV** all connect to the router wirelessly.
- A **printer** connected via Wi-Fi or USB to your laptop.
- A **CCTV camera** streaming video to your mobile app over the same home network.

✓ **Uses of Home Networks:**

| **Use Case** | **Explanation** |
|---|---|
| Internet Sharing | All devices share a single internet connection via router |
| File Sharing | Share files between devices without USB drives |
| Printer & Device Sharing | Multiple users can print from one wireless printer |
| Smart Home Automation | Connect and control smart bulbs, thermostats, locks, and cameras |
| Streaming & Gaming | Stream Netflix on Smart TV, or play online games on PS5/Xbox |
| Parental Controls & Monitoring | Manage kids' internet usage and block harmful content via router settings |

**Components of a Home Network:**

| **Component** | **Role** |
|---|---|
| **Router** | Central device that connects to ISP and routes traffic to devices |
| **Modem** | Connects to Internet via ISP (often built-in with router) |
| **Switch** | Optional – for more Ethernet ports if needed |
| **Wi-Fi Access Point** | Built-in or separate – provides wireless access |
| **Devices** | Smartphones, PCs, Smart TVs, IoT devices |
| **Firewall** | Often part of the router – protects against external attacks |

**Advantages:**

- Easy to set up and manage.
- Cost-effective (one router for many devices).
- Provides centralized control.
- Allows automation and smart living.

**Disadvantages:**

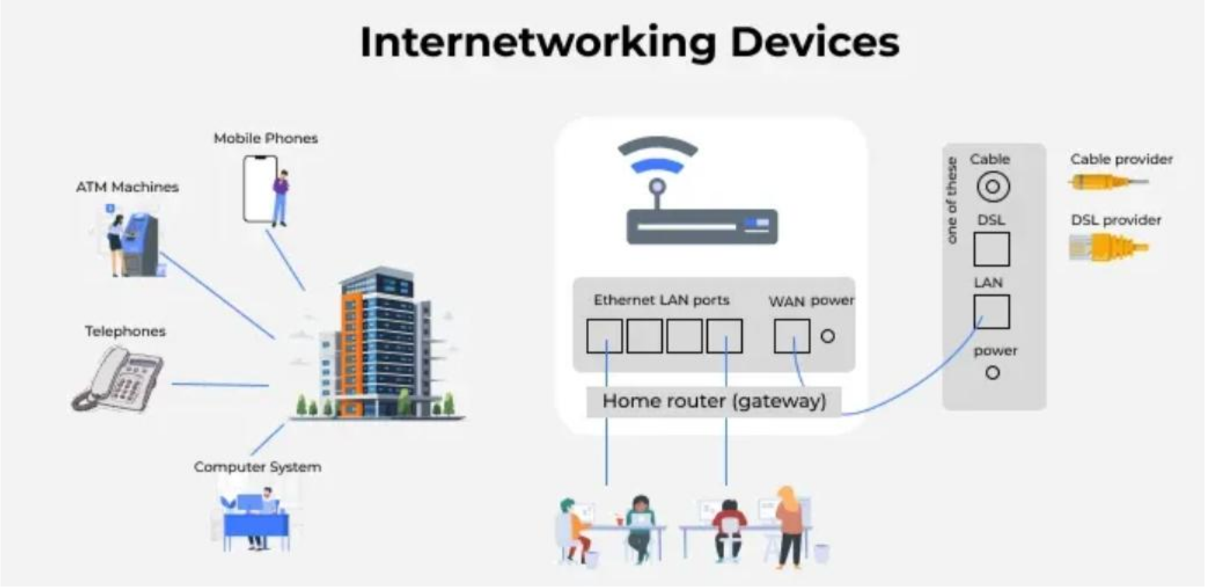
- Can be insecure if not properly configured (e.g., default passwords).
- Bandwidth sharing may reduce speed when many devices are active.
- Signal interference in large homes or with thick walls.

## 9 Internetworks

**Internetworking** is made from two words: **"inter"** and **"networking"**, which means **connecting different networks or devices together**. These connections are made using special devices like **routers** or **gateways**. The old name for internetwork was **Catenet**.

Internetworking can happen between many types of networks—such as **public, private, commercial, industrial, or government** networks. So, an internetwork is just a group of **separate networks that are connected** using intermediate devices, making them act like **one large network**.

Internetworking also refers to the **technology, tools, and methods** used to **create and manage** these large, connected network systems.



To make different networks **communicate** with each other, each part of the network uses the same **communication rules**, such as **TCP (Transmission Control Protocol)** and **IP (Internet Protocol)**.

When two networks follow the same communication rules, we call it **internetworking**.

Internetworking was created to **solve the problem of sending data through many network links** from one point to another.

There is a small difference between **network extension** and **internetworking**:

- If you use a **hub or switch** to connect two LANs, it is just an **extension of the LAN**.
- If you connect them using a **router**, it becomes **internetworking**.

Internetworking happens at **Layer 3 (Network Layer)** of the **OSI model**.

The best real-life example of internetworking is the **Internet**, which connects many different networks around the world.

There is chiefly 3 units of Internetworking:

1. Extranet
2. Intranet
3. Internet

Intranets and extranets might or might not have connections to the net. If there is a connection to the net, the computer network or extranet area unit is usually shielded from being accessed from the net if it is not authorized. The net isn't thought-about to be a section of the computer network or extranet, though it should function as a portal for access to parts of the associate degree extranet.

1. **Extranet -** It is a network of the internetwork that is restricted in scope to one organization or entity however that additionally has restricted connections to the networks of one or a lot of different sometimes, however not essential. It is the very lowest level of Internetworking, usually enforced in an exceedingly personal area. Associate degree extranet may additionally be classified as a Man, WAN, or different form of network however it cannot encompass one local area network i.e. it should have a minimum of one reference to associate degree external network.
2. **Intranet -** This associate degree computer network could be a set of interconnected networks, which exploits the Internet Protocol and uses IP-based tools akin to web browsers and FTP tools, that are underneath the management of one body entity. That body entity closes the computer network to the remainder of the planet and permits solely specific users. Most typically, this network is the internal network of a corporation or different enterprise. An outsized computer network can usually have its own internet server to supply users with browsable data.
3. **Internet -** A selected Internetworking, consisting of a worldwide interconnection of governmental, academic, public, and personal networks based mostly upon the Advanced analysis comes Agency Network (ARPANET) developed by ARPA of the U.S. Department of Defense additionally home to the World Wide Web (WWW) and cited as the 'Internet' to differentiate from all different generic Internetworks. Participants within the web, or their service suppliers, use IP Addresses obtained from address registries that manage assignments.

**Why Internetworking Was Needed – Simple Explanation**

**Internetworking** was developed to solve some major problems in early networks:

1. **Isolated LANs**: Different offices or departments had their own LANs (Local Area Networks) that were **not connected**. This made **communication between them difficult**.
2. **Duplicate Resources**: Every department needed **its own copy** of the same hardware and software. This meant **extra cost**, and each department also needed its own **support staff**.
3. **No Central Management**: There was **no central way** to control or fix network problems. Every office had to manage its own network separately, which was inefficient.

✓ **Internetwork Addressing**

**Internetwork addressing** helps identify devices on a network. These addresses can identify a single device or a group of devices. The type of address used depends on the **protocol** and **layer** in the OSI model.

There are **three main types of internetwork addresses**:

**1. Data Link Layer Addresses (Physical/Hardware Address)**

- These addresses are used to **identify each physical connection** on a device.
- Also called **hardware addresses** because they are built into the device.
- These addresses usually **do not change** and belong to the **Data Link Layer**.
- A computer typically has **one network connection**, so it has **one data link address**.
- A **router**, which connects to many networks, will have **multiple data link addresses**.

**2. MAC Address (Media Access Control Address)**

- MAC addresses are a **special type** of data link address used mostly in **LANs**.
- Each network device (like a computer or printer) has a **unique MAC address**.
- A MAC address is **48 bits long** and written as **12 hexadecimal digits** (example: 00:1A:2B:3C:4D:5E).
- The first 6 digits identify the **manufacturer** (this is called the **OUI - Organizational Unique Identifier**).
- The last 6 digits are **unique to the device**, given by the manufacturer.
- MAC addresses are usually **permanently stored** in the device's memory (called **burned-in address** or **BIA**), but temporarily copied into RAM when the device runs.

**3. Network Layer Addresses (Logical Address)**

- These addresses belong to the **Network Layer** (like IP addresses).
- Unlike MAC addresses, **network-layer addresses can change**.
- These addresses are also called **logical or virtual addresses**.
- The IP address depends on **how the network is set up**, not just the device.
- Computers and routers may have **more than one network-layer address**, depending on the number of protocols and interfaces they support.

✓ **Challenges in Internetworking:**

**1. Connecting Different Systems**

The first big challenge is **connecting many different systems** that may use different technologies.

For example, some offices may use **different types of cables** or **run at different speeds**.

Getting all these systems to **communicate properly** is a tough task.

**2. Maintaining Reliability**

- A good internetwork must always offer **stable and reliable service**.
- People and companies **depend on the network** to access important files, applications, or services.
- If the network is **unreliable or often down**, it causes problems for users.

**3. Effective Network Management**

- Managing the internetwork from **one central place** is important.
- This includes:
  - Fixing problems (troubleshooting),
  - Managing performance,
  - Keeping the network **secure and updated**.
- All these tasks must be done properly for the network to **run smoothly**.

**4. Ensuring Flexibility**

- The network should be **easy to grow** and **ready for new technologies**.
- Flexibility allows the network to **add new devices**, **support more users**, and **handle new services** without big changes.

✓ **Advantages:**

- **Increased connectivity: I**nternetworking enables devices on different networks to communicate with each other, which increases connectivity and enables new applications and services.
- **Resource sharing:** Internetworking allows devices to share resources across networks, such as printers, servers, and storage devices. This can reduce costs and improve efficiency by allowing multiple devices to share resources.
- **Improved scalability:** Internetworking allows networks to be expanded and scaled as needed to accommodate growing numbers of devices and users.
- **Improved collaboration:** Internetworking enables teams and individuals to collaborate and work together more effectively, regardless of their physical location.
- **Access to remote resources:** Internetworking allows users to access resources and services that are physically located on remote networks, improving accessibility and flexibility.

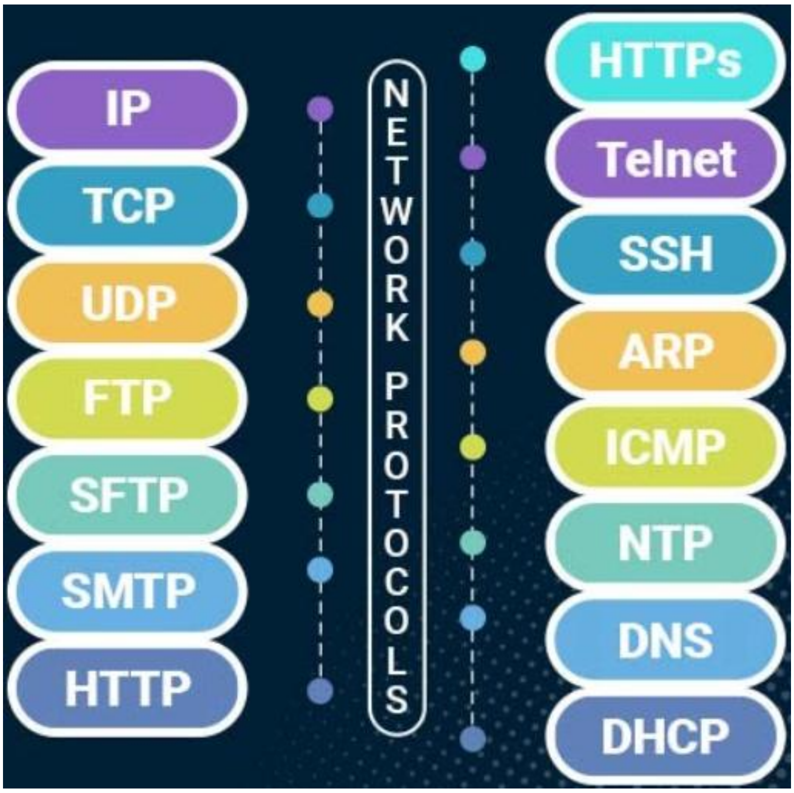
✓ **Disadvantages:**

- **Security risks:** Internetworking can create security vulnerabilities and increase the risk of cyberattacks and data breaches. Connecting multiple networks together increases the number of entry points for attackers, making it more difficult to secure the entire system.

- **Complexity:** Internetworking can be complex and requires specialized knowledge and expertise to set up and maintain. This can increase costs and create additional maintenance overhead.
- **Performance issues:** Internetworking can lead to performance issues, particularly if networks are not properly optimized and configured. This can result in slow response times and poor network performance.
- **Compatibility issues:** Internetworking can lead to compatibility issues, particularly if different networks are using different protocols or technologies. This can make it difficult to integrate different systems and may require additional resources to resolve.
- **Management overhead:** Internetworking can create additional management overhead, particularly if multiple networks are involved. This can increase costs and require additional resources to manage effectively.

## 10 Network Protocols

Network protocols are rules and standards that define how data is transmitted and received over a network. Think of them as languages or instructions that computers follow to talk to each other.



✓ **Why are Network Protocols Important?**

- They ensure reliable communication between devices.
- They help organize and manage data transmission.
- They allow interoperability (different devices and systems can work together).

## ✓ Types of Network Protocols (with Full Forms):

**1. Communication Protocols**

These manage the way data is sent and received between devices.

- **HTTP** (HyperText Transfer Protocol) – Used to access websites.
- **HTTPS** (HyperText Transfer Protocol Secure) – Secure version of HTTP.
- **FTP** (File Transfer Protocol) – Used to transfer files over a network.
- **SMTP** (Simple Mail Transfer Protocol) – Used to send emails.
- **POP3** (Post Office Protocol version 3) – Used to retrieve emails.
- **IMAP** (Internet Message Access Protocol) – Another way to retrieve and manage emails.
- **Telnet** (Telecommunication Network) – Remote login protocol.
- **SSH** (Secure Shell) – Secure remote login.

**2. Network Management Protocols**

Used to manage, monitor, and troubleshoot networks.

- **SNMP** (Simple Network Management Protocol) – Monitors network devices.
- **ICMP** (Internet Control Message Protocol) – Sends error messages like “host unreachable.”
- **ARP** (Address Resolution Protocol) – Finds MAC address from IP address.
- **RARP** (Reverse Address Resolution Protocol) – Finds IP address from MAC address.

**3. Routing Protocols**

Used by routers to determine the best path to send data.

- **IP** (Internet Protocol) – Main protocol that routes data.
- **IPv4** (Internet Protocol version 4) – Commonly used version of IP.
- **IPv6** (Internet Protocol version 6) – Newer version with more address space.
- **BGP** (Border Gateway Protocol) – Routes between big networks (like ISPs).

- **OSPF** (Open Shortest Path First) – Finds the fastest path.
- **RIP** (Routing Information Protocol) – Shares routing information.

**4. Security Protocols**

Protect data from being accessed or stolen.

- **SSL** (Secure Sockets Layer) – Encrypts data for secure communication.
- **TLS** (Transport Layer Security) – Improved version of SSL.
- **IPSec** (Internet Protocol Security) – Secures IP communication.

**5. Wireless and IoT Protocols**

Used for wireless communication and smart devices.

- **Wi-Fi** (Wireless Fidelity) – Wireless internet.
- **Bluetooth** – Short-range device communication.
- **Zigbee** – Used in smart home devices.
- **NFC** (Near Field Communication) – Used in contactless payments.
- **MQTT** (Message Queuing Telemetry Transport) – Lightweight protocol for IoT.

**Real-Life Example:**

When you open a website:

1. **DNS (Domain Name System)** converts the name (like google.com) into an IP address.
2. **HTTP/HTTPS** is used to send and receive web pages.
3. **TCP/IP (Transmission Control Protocol / Internet Protocol)** manages how the data is broken into packets and sent.
4. **ICMP** might alert if something goes wrong.

**Why Should You Learn Protocols?**

- They form the base of everything done on a computer network.
- Helpful in careers like networking, cybersecurity, web development, and cloud computing.
- Good understanding helps in solving real-world technical problems.

## ✓ Essential Network Protocols Table

| Protocol | Full Name | Purpose | OSI Layer | Example Use |
|---|---|---|---|---|
| **IP** | Internet Protocol | Routing and addressing packets across networks | Network | Sending data across the Internet |
| **TCP** | Transmission Control Protocol | Reliable, connection-oriented communication | Transport | Web page loading, file transfers |
| **UDP** | User Datagram Protocol | Fast, connectionless communication | Transport | Streaming, online games |
| **ICMP** | Internet Control Message Protocol | Error reporting and network diagnostics | Network | Ping, Traceroute |
| **ARP** | Address Resolution Protocol | Resolves IP addresses to MAC addresses | Data Link | Sending packets on LAN |
| **RARP** | Reverse Address Resolution Protocol | Resolves MAC to IP | Data Link | Booting diskless systems |
| **DNS** | Domain Name System | Translates domain names to IP addresses | Application | Visiting websites (e.g., google.com) |
| **HTTP** | Hypertext Transfer Protocol | Web browsing, data exchange | Application | Accessing websites |
| **HTTPS** | HTTP Secure | Encrypted web communication | Application | Online banking, secure login |
| **FTP** | File Transfer Protocol | Transfers files between computers | Application | Uploading/downloading files |
| **TFTP** | Trivial File Transfer Protocol | Simple file transfers without authentication | Application | Booting devices like routers |

| | | | | |
|---|---|---|---|---|
| **SFTP** | Secure File Transfer Protocol | Secure file transfer over SSH | Application | Transferring confidential files |
| **SMTP** | Simple Mail Transfer Protocol | Sending emails | Application | Outgoing mail (Gmail, Outlook) |
| **POP3** | Post Office Protocol v3 | Receiving emails, downloads and deletes | Application | Accessing mail on one device |
| **IMAP** | Internet Message Access Protocol | Receives and syncs email | Application | Reading mail on multiple devices |
| **DHCP** | Dynamic Host Configuration Protocol | Automatically assigns IP addresses | Application | Connecting to Wi-Fi |
| **NTP** | Network Time Protocol | Synchronizes clocks on a network | Application | Time settings in routers/switches |
| **SNMP** | Simple Network Management Protocol | Monitors network devices | Application | Manage switches, routers |
| **Telnet** | Terminal Network Protocol | Remote text-based access (insecure) | Application | Older remote system management |
| **SSH** | Secure Shell | Secure remote access via command line | Application | Server administration |
| **RTP** | Real-time Transport Protocol | Transports audio/video in real-time | Transport | Video conferencing |
| **RTSP** | Real Time Streaming Protocol | Controls streaming media servers | Application | Live streaming apps |
| **MPLS** | Multi-Protocol Label Switching | Fast packet forwarding using labels | Data Link | Telecom and enterprise networks |

| | | | | |
|---|---|---|---|---|
| **BGP** | Border Gateway Protocol | Inter-domain routing between large networks | Network | Internet backbone routing |
| **OSPF** | Open Shortest Path First | Finds the best path for data within a network | Network | Enterprise routing |
| **EIGRP** | Enhanced Interior Gateway Routing Protocol | Cisco proprietary routing | Network | Cisco-based routing systems |
| **CDP** | Cisco Discovery Protocol | Discovers nearby Cisco devices | Data Link | Network troubleshooting (Cisco) |
| **LLDP** | Link Layer Discovery Protocol | Vendor-neutral device discovery | Data Link | Discover devices on LAN |
| **IPSec** | Internet Protocol Security | Encrypts network traffic | Network | VPN connections |
| **TLS/SSL** | Transport Layer Security / Secure Sockets Layer | Encrypts web traffic | Transport | HTTPS communication |
| **PPP** | Point-to-Point Protocol | Connects two directly connected computers | Data Link | Dial-up and VPN connections |
| **L2TP** | Layer 2 Tunneling Protocol | Supports VPN over internet | Data Link | VPN tunnels |
| **GRE** | Generic Routing Encapsulation | Encapsulates packets for tunnel connections | Network | VPN and tunneling |

### Why you should learn this

- **Interviews**: Protocol questions are common in networking jobs.
- **Certifications**: CCNA, Network+, and security exams all test protocols.
- **Real-world understanding**: Helps in troubleshooting, managing networks, and building secure systems.

## 11 What Are Protocol Design Goals?

Protocols are **rules** for communication between devices.

**Design goals** ensure that these rules help create a **fast, reliable, scalable, and secure** network.

✓ **Major Design Goals of Network Protocols**

| Design Goal | Explanation (Simple English) | Example |
|---|---|---|
| **1. Correctness** | The protocol must do the **right thing**: no confusion, no wrong delivery. | TCP ensures that all parts of a file are received correctly. |
| **2. Simplicity** | Keep it **simple to understand**, use, and implement. | UDP is simple—just send data, no checks. |
| **3. Robustness** | Should **handle errors**, failures, and still work well. | TCP resends data if it gets lost. |
| **4. Efficiency** | Use **minimum time, memory, and bandwidth**. | Data compression in HTTP reduces data usage. |
| **5. Scalability** | Must work well even with **millions of devices**. | IP addressing works across the globe. |
| **6. Security** | Should protect data from **hackers or misuse**. | HTTPS uses encryption to secure websites. |
| **7. Interoperability** | Should allow **different devices and vendors** to work together. | Wi-Fi works on all brands: Samsung, Apple, HP, etc. |
| **8. Flexibility** | Must be **adaptable** to new technologies or needs. | IPv6 supports more addresses for future devices. |
| **9. Fairness** | Each device or user should get a **fair share** of resources. | Routers distribute bandwidth fairly. |
| **10. Fault Tolerance** | If one part fails, network should still **keep running**. | Internet reroutes traffic if a cable breaks. |
| **11. Quality of Service (QoS)** | Some services (like video calls) need **better speed or less delay**. | VoIP protocols give voice packets higher priority. |

**Real-Life Example:**

- Think of a **traffic system** as a protocol.
  - It must be **correct** (red = stop),
  - **efficient** (minimize jams),

  - **secure** (no misuse),
  - **scalable** (for small towns and big cities),
  - and **flexible** (add flyovers or smart lights).

Same rules apply in **computer networks**.

## 11 What Is Protocol Layering?

**Protocol layering** is the **concept of dividing network communication into separate layers**, each with its own specific function.

This is done so that **each layer only focuses on its job** and can interact with layers above or below it without knowing the full system.

### Why Use Protocol Layers?

Think of sending a letter:

- You write it (Application)
- Put it in an envelope (Transport)
- Address it (Network)
- Hand it to a postman (Data Link)
- It travels on roads (Physical)

Same for networks — **layer by layer processing**.

### Benefits of Protocol Layering

| **Benefit** | **Meaning** |
|---|---|
| **Modularity** | Each layer does its own job independently. |
| **Simplicity** | Easier to design, test, and maintain. |
| **Interoperability** | Devices from different vendors can work together. |
| **Scalability** | Can handle changes and new technologies easily. |
| **Troubleshooting** | Problems can be diagnosed at the specific layer. |

- ✓ **Popular Layer Models**

**1. OSI Model (7 Layers)**

| Layer No. | Layer Name | Function Example |
|---|---|---|
| 7 | Application | User interaction (e.g., Chrome, WhatsApp) |
| 6 | Presentation | Data format, encryption (JPEG, SSL) |
| 5 | Session | Manages sessions (start/stop communication) |
| 4 | Transport | Reliable delivery (TCP, UDP) |
| 3 | Network | Routing (IP address, routers) |
| 2 | Data Link | MAC address, frames (Switch, Ethernet) |
| 1 | Physical | Cables, Wi-Fi, electrical signals |

**Mnemonic**: All People Seem to Need Data Processing

**2. TCP/IP Model (4 Layers) – Practical Model**

| Layer No. | Layer Name | Equivalent OSI Layers | Example Protocols |
|---|---|---|---|
| 4 | Application | 7,6,5 | HTTP, FTP, DNS, SMTP |
| 3 | Transport | 4 | TCP, UDP |
| 2 | Internet | 3 | IP, ICMP |
| 1 | Network Access | 2,1 | Ethernet, Wi-Fi, ARP |

**Real-Life Analogy: Sending a Parcel**

| Step | OSI Layer |
|---|---|
| Write the letter | Application |
| Translate language | Presentation |
| Start a phone call | Session |
| Use delivery service | Transport |
| Assign postal address | Network |
| Pack and label the box | Data Link |
| Deliver physically | Physical |

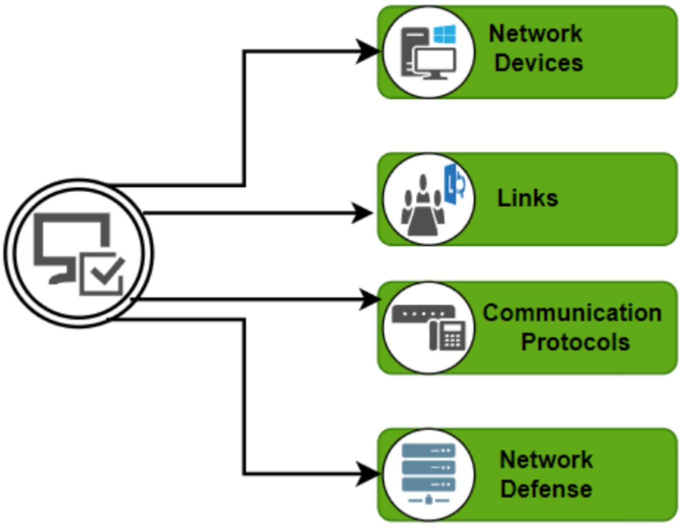
**Key Terms**

- **Encapsulation**: Each layer adds its own header to the data as it moves down.
- **Decapsulation**: Each layer removes its header when data moves up at the receiver's side.

## 12 Connections and Reliability

### ✓ Connections in Computer Networks

In networking, a **connection** refers to the **communication link** between two or more devices (computers, servers, routers) that allows the exchange of data.



**Types of Connections:**

| Type | Description | Example |
|---|---|---|
| **Wired (Physical)** | Uses cables (e.g., Ethernet, Fiber optics) for data transmission. | LAN with Ethernet cables |
| **Wireless** | Uses radio waves, infrared, or satellite signals. | Wi-Fi, Bluetooth, 5G |
| **Point-to-Point** | Direct connection between two devices. | Router ↔ PC via Ethernet |
| **Multipoint (Broadcast)** | Multiple devices share a single link. | Switch connected to many PCs |
| **Circuit-switched** | Dedicated path is established for the whole session. | Traditional telephone network |
| **Packet-switched** | Data is sent in packets independently. | Internet (TCP/IP) |

- ✓ **Network Reliability**

**Network Reliability** refers to the **ability of a network to consistently perform** its intended function without failures or downtime.

- ✓ **Factors Affecting Reliability:**

| Factor | Explanation |
|---|---|
| **Redundancy** | Extra paths/devices (e.g., backup links) to prevent single point of failure |
| **Error Detection/Correction** | Mechanisms like checksums and ACKs to ensure data is correct |
| **Fault Tolerance** | Ability of a system to keep working even if part of it fails |
| **Bandwidth and Load** | High capacity reduces congestion and improves reliability |
| **Hardware Quality** | Better routers, switches = fewer hardware-related failures |
| **Protocols Used** | TCP provides reliability; UDP does not |
| **Maintenance** | Regular updates and monitoring prevent failures |

**Measuring Reliability:**

| Metric | Description |
|---|---|
| **Availability** | % of time network is operational (e.g., 99.9% uptime) |
| **Mean Time Between Failures (MTBF)** | Average time between two failures |
| **Mean Time To Repair (MTTR)** | Time it takes to fix a failure |

- ✓ **Improving Network Connections and Reliability:**
  - Use **high-quality cables** and **wireless access points**.
  - Implement **redundant paths** (like dual internet links).
  - Apply **security protocols** (firewalls, encryption).
  - Perform **regular maintenance** and monitoring.
  - Use **smart routing protocols** (OSPF, BGP) for dynamic path selection.
  - Use **cloud-based failover systems** for data backup and load balancing.

**Real-Life Example:**

Your video-calling your friend:

- If your network is **connection-oriented (TCP)**, the call might pause to fix dropped packets.
- If it is **connectionless (UDP)**, the call continues smoothly but might lose some words.
- If your internet is **reliable**, the call is smooth and high-quality.
- If not, the call drops or buffers — showing **low reliability**.

## 12 Service Primitives

✓ **What are Service Primitives?**

**Service Primitives** are the basic operations (or commands) used by one layer in a network to **communicate with the layer directly below it**.

They define **how services are requested or provided** between layers in a network (like OSI or TCP/IP models).

Think of them like **instructions** for interaction between layers.

✓ **Why are Service Primitives Important?**

- Help in **managing communication** between software and hardware layers.
- Provide a **standard way** to use network services (like sending or receiving data).
- Useful in **protocol design and implementation**.

✓ **Types of Service Primitives**

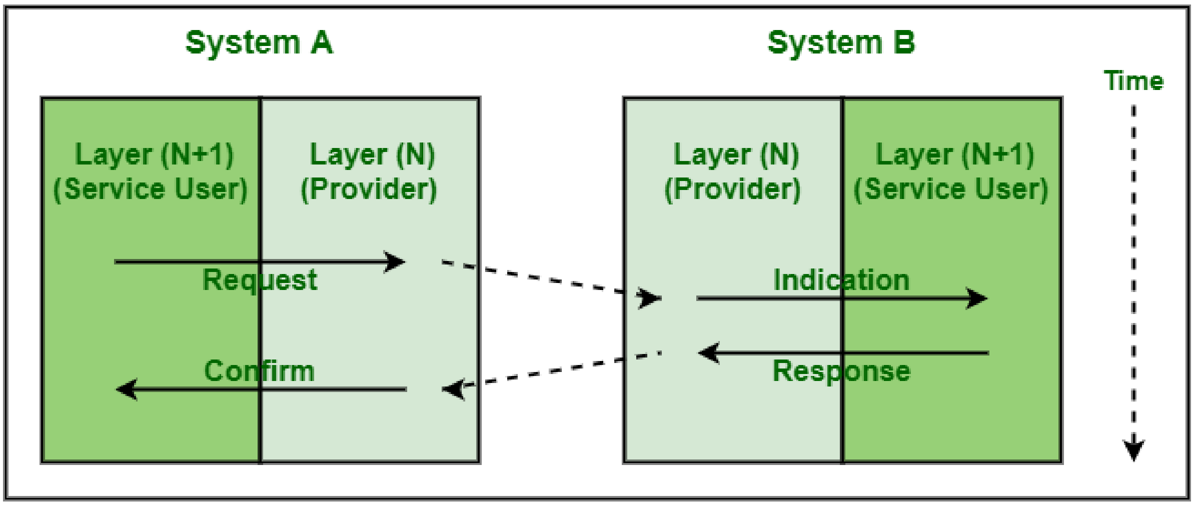
There are **five** main types of service primitives:

| **Primitive** | **Meaning** | **Real-Life Example** |
|---|---|---|
| REQUEST | Used by the sender to **ask** for a service | "Send this message to the network" |
| INDICATION | Used by the lower layer to **inform** the upper layer of an event | "You received a message!" |
| RESPONSE | Used by the upper layer to **reply** after an indication | "Okay, I'm ready to receive it" |

| | | |
|---|---|---|
| CONFIRM | Sent to **confirm** a request was successfully completed | "Your message was sent successfully" |
| PRIMITIVE | A general term referring to any of the above | Any communication between layers |

**Common Service Primitive Sequence (Example: Sending Data)**

Here is how the **data transfer** process happens using primitives:



Primitives for Connection between Peer Protocol Entities

✓ **Real-World Analogy: Sending a Courier**

| Step | Network Primitive | Analogy |
|---|---|---|
| You give a parcel to courier | REQUEST | You request the courier to send your parcel |
| Courier knocks on door | INDICATION | They indicate a delivery is here |
| Receiver opens the door | RESPONSE | The receiver responds to receive the parcel |
| Courier updates status | CONFIRM | Courier confirms delivery was successful |

## 14 The Relationship of Services to Protocols

### 1. Basic Definitions

| Term | Simple Definition |
|---|---|
| **Service** | What one layer offers to the layer **above it**. It defines **what** can be done (e.g., send/receive data). |
| **Protocol** | A set of rules or agreements used for communication between **peer layers** (same layer on different devices). It defines **how** the service is carried out. |

### 2. Relationship in One Line:

**Services** define *what* is done, and **protocols** define *how* it is done.

### 3. Real-Life Analogy: Postal System

| Concept | Postal Example |
|---|---|
| **Service** | Sending and receiving letters |
| **Protocol** | Rules: How to address envelopes, postage, delivery steps |

### 4. How They Work Together (Layered Communication)

Imagine a computer sending a file to another computer:

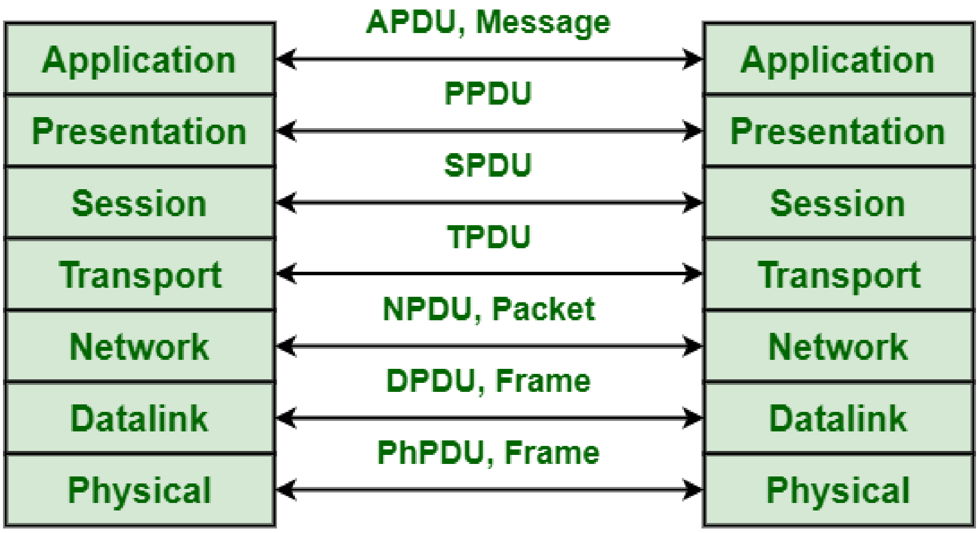
**Computer A:**

- **Application layer** uses a **service** to send a file.
- This service goes down through the layers (transport, network…).
- At each layer, a **protocol** is used to format and send the data to **Computer B**.

**Computer B:**

- The layers on this side use **protocols** to understand and process the received data.
- Each layer provides **services** upward to the next layer.

### 5. Visual Diagram



Protocol Data Unit

### OSI Layer-wise Protocol Data Units (PDUs)

| OSI Layer | PDU Name | Description |
|---|---|---|
| Application | **APDU** | Application Protocol Data Unit (Message) |
| Presentation | **PPDU** | Presentation Protocol Data Unit |
| Session | **SPDU** | Session Protocol Data Unit |
| Transport | **TPDU** | Transport Protocol Data Unit |
| Network | **NPDU** | Network Protocol Data Unit (Packet) |
| Data Link | **DPDU** | Data Link Protocol Data Unit (Frame) |
| Physical | **PhPDU** | Physical Protocol Data Unit (Frame/Bits) |

### Relationship of Services to Protocols

- **Service:** What a layer provides to the layer above it (e.g., reliable data transfer).
- **Protocol:** The rules and conventions used by the same layer on different devices to communicate (e.g., TCP, IP, HTTP).

**Example:**

- The **Transport layer** provides **reliable data transfer service** to the **Session layer**, using the **TCP protocol**.
- The data unit used at the Transport layer is called **TPDU** (Transport Protocol Data Unit).

## 15 Reference Models in Computer Networks

Reference models are **frameworks** that help us understand how communication happens between devices in a computer network. These models break the communication process into **layers**, each with specific responsibilities.

### 1. What is a Reference Model?

A **reference model** is a **theoretical framework** that explains how data travels from one device to another using different layers.
Each layer:

- Has a **specific function**
- Talks only to the layer **above and below it**
- Uses **protocols** to communicate with its peer layer in another device

### 2. Popular Reference Models

| Model | Layers | Usage |
|---|---|---|
| **OSI Model** | 7 Layers | Theoretical model, used for learning and design |
| **TCP/IP Model** | 4 or 5 Layers | Practical model, used in real-world internet communication |

### 3. OSI (Open Systems Interconnection) Model – 7 Layers

| Layer No. | Layer Name | Purpose (Simple Words) | Example Protocols |
|---|---|---|---|
| 7 | **Application** | Provides user services (e.g., email, browser) | HTTP, FTP, SMTP |
| 6 | **Presentation** | Translates, encrypts, compresses data | SSL, JPEG, MPEG |
| 5 | **Session** | Manages sessions between apps (start/stop) | NetBIOS, RPC |
| 4 | **Transport** | Reliable delivery, error recovery | TCP, UDP |
| 3 | **Network** | Routing and addressing | IP, ICMP |
| 2 | **Data Link** | Node-to-node data transfer, MAC addressing | Ethernet, PPP |
| 1 | **Physical** | Physical connection – wires, voltages | USB, Bluetooth, Ethernet cables |

**4. TCP/IP Model – 4 or 5 Layers**

| Layer No. | Layer Name | Purpose | Example Protocols |
|---|---|---|---|
| 4 | **Application** | Combines OSI layers 5–7 | HTTP, FTP, SMTP, DNS |
| 3 | **Transport** | End-to-end communication | TCP, UDP |
| 2 | **Internet** | Logical addressing and routing | IP, ICMP, ARP |
| 1 | **Network Access** | Physical + Data link (from OSI) | Ethernet, Wi-Fi, PPP |

## 16 A Critique of the OSI Model and Protocols

The OSI (Open Systems Interconnection) model is a **conceptual framework** used to understand and design how different computer systems communicate. While it is widely taught and useful for learning, it has several **limitations and criticisms** when applied in practice.

### Why Critique the OSI Model?

Because the OSI model:

- Is **idealistic**, not practical in real networks.
- Was developed **after** real-world protocols like TCP/IP were already in use.
- Tries to **force-fit** strict layer boundaries, which does not always reflect how networks work.

### Main Criticisms of the OSI Model

| Critique Point | Explanation (Simple Words) | Example |
|---|---|---|
| **1. Too Complex** | Has 7 layers, which can be overkill for simple networking needs. | Many real protocols (e.g., TCP/IP) combine layers. |
| **2. Not Practical** | It is theoretical and doesn't match how real protocols (like TCP/IP) operate. | TCP/IP only uses 4 layers. |
| **3. Layer Duplication** | Some functions (like error checking) appear in multiple layers. | Both Transport and Data Link layers handle errors. |
| **4. Layer Dependency Issues** | Some layers depend on others too strictly, making updates hard. | Upgrading Presentation Layer without affecting Application Layer is tricky. |

| | | |
|---|---|---|
| **5. Delayed Development** | OSI model came **after** many protocols were already being used. | By the time OSI came, TCP/IP was already standard. |
| **6. Vendor Disagreement** | Many hardware and software vendors did not agree on implementing full OSI. | IBM and Microsoft preferred TCP/IP stack. |
| **7. No Clear Standards for Some Layers** | Layers like Session and Presentation are vague or rarely implemented directly. | Few applications use "Session Layer" protocols separately. |
| **8. Inefficiency in Performance** | Layer-by-layer communication can slow things down. | Protocol stacks may skip or merge layers to save time. |

## 17 A Critique of the TCP/IP Reference Model and Protocols

The **TCP/IP model** is a practical and widely used reference model that forms the foundation of the **Internet**. It was developed in the 1970s and became the **de facto standard**. Although extremely successful, it also has several **limitations and criticisms** from a conceptual and design standpoint.

### Why Critique the TCP/IP Model?

Even though TCP/IP works well in practice, it was not designed with the **same conceptual clarity** as the OSI model. It **focuses more on protocols than structure**, and that leads to some **design flaws or inconsistencies**.

### Main Criticisms of the TCP/IP Model

| **Critique Point** | **Explanation (Simple Words)** | **Example** |
|---|---|---|
| **1. Lacks Clear Layer Separation** | Layers are not as clearly defined as OSI. | No distinct Presentation or Session layer. |
| **2. Mixing of Concepts** | Protocols and services are mixed within layers. | TCP is both a protocol and a service provider. |
| **3. No Standard for Interfaces** | The model does not clearly define how layers communicate. | OSI defines service access points; TCP/IP doesn't. |

| | | |
|---|---|---|
| **4. No Proper Session or Presentation Layers** | It skips some layers needed for modern applications. | Encryption, compression handled at app level, not defined in model. |
| **5. Protocol-Oriented, Not Service-Oriented** | Model was built around existing protocols, not abstract services. | OSI separates what should be done from how it is done. |
| **6. Original Model Focused on Connection-Oriented Communication** | Initially emphasized TCP, less focus on UDP or real-time traffic. | Streaming applications prefer UDP, which was later adapted. |
| **7. Less Flexibility** | Adapting to newer services is harder than in OSI model. | Integration of security (like IPSec) was not planned initially. |
| **8. Poor Fit for Modern Network Functions** | Concepts like mobility, multicast, QoS are not native. | Mobile IP and other overlays had to be added later. |

**Beginner-Level Certifications (Entry-Level)**

| Certification | Provider | Who It's For |
|---|---|---|
| **CompTIA Network+** | CompTIA | Beginner-level foundational networking knowledge |
| **Cisco Certified Support Technician (CCST)** | Cisco | High school/college students; pre-CCNA level |
| **IT Fundamentals (ITF+)** | CompTIA | Beginners new to IT |

**Intermediate-Level Certifications**

| Certification | Provider | Focus Area |
|---|---|---|
| **Cisco Certified Network Associate (CCNA)** | Cisco | Routing, switching, IP, network basics |
| **CompTIA Security+** | CompTIA | Network security fundamentals |
| **Juniper JNCIA** | Juniper Networks | Juniper technologies and basic networking |
| **Microsoft Certified: Security, Compliance, and Identity Fundamentals** | Microsoft | Network security and access management basics |
| **Fortinet NSE 1-3** | Fortinet | Entry-level security networking skills |

**Advanced-Level Certifications**

| Certification | Provider | Specialization |
|---|---|---|
| **Cisco Certified Network Professional (CCNP)** | Cisco | Advanced routing, switching, automation |
| **CompTIA Linux+** | CompTIA | Network operations on Linux systems |
| **Juniper JNCIS / JNCIP / JNCIE** | Juniper | Intermediate to expert in Juniper networks |
| **AWS Certified Advanced Networking - Specialty** | Amazon | Cloud networking and hybrid infrastructure |

| | | |
|---|---|---|
| **Fortinet NSE 4-8** | Fortinet | Network security and advanced FortiOS features |
| **Microsoft Certified: Azure Network Engineer Associate** | Microsoft | Designing and implementing Azure networks |

**Expert-Level Certifications (High Prestige)**

| **Certification** | **Provider** | **Description** |
|---|---|---|
| **Cisco Certified Internetwork Expert (CCIE)** | Cisco | One of the most respected certifications in networking |
| **CompTIA CASP+ (Advanced Security Practitioner)** | CompTIA | Enterprise-level security and networking |
| **Certified Information Systems Security Professional (CISSP)** | ISC2 | Covers networking, security, risk management |
| **Certified Information Security Manager (CISM)** | ISACA | Management-focused network security certification |

**Bonus: Vendor-Specific or Niche Certifications**

| **Certification** | **Vendor** | **Focus** |
|---|---|---|
| **HPE Aruba Certified** | Aruba | Wireless and enterprise network solutions |
| **Palo Alto PCNSA / PCNSE** | Palo Alto | Firewall and network security |
| **Check Point CCSA / CCSE** | Check Point | Security appliances and firewall networking |
| **Red Hat Certified Engineer (RHCE)** | Red Hat | Linux networking and administration |
| **Google Cloud Networking Engineer** | Google | Cloud and hybrid networking systems |