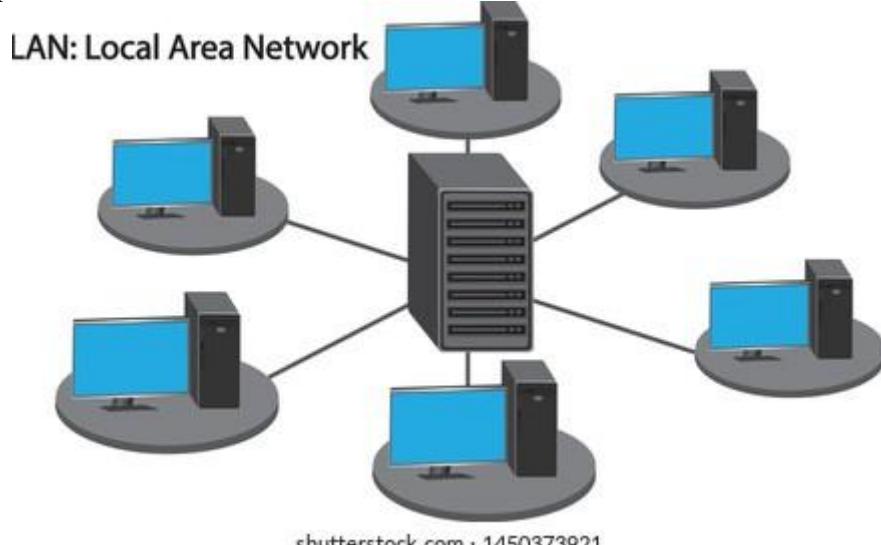


Types of Networks: LAN, MAN, WAN

Local Area Network (LAN)

A Local Area Network, commonly known as LAN, is a computer network that operates in a small geographical area such as a single office, a computer laboratory, a home, or a university campus. It is usually owned, controlled, and maintained by one organization or individual, which makes it more secure and easier to manage compared to larger types of networks. LANs are designed to provide high-speed and reliable communication among devices such as computers, printers, and servers.



shutterstock.com • 1450373921

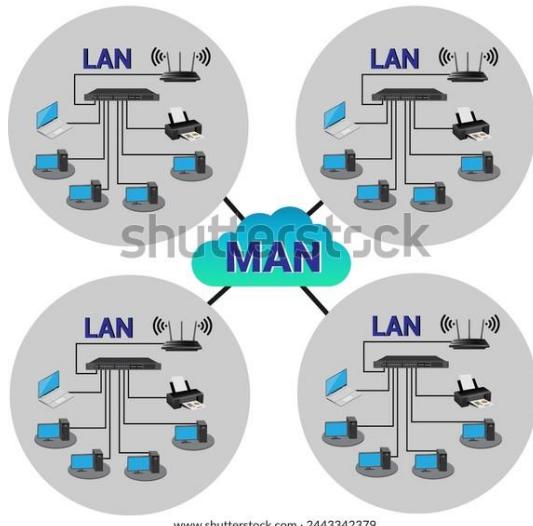
The coverage area of a LAN is typically limited to a few kilometers. LANs use technologies such as Ethernet and Wi-Fi, which are based on IEEE standards like 802.3 and 802.11. The data transmission speeds in LANs are very high, ranging from 100 Mbps to 10 Gbps, and with modern fiber-based LANs even higher speeds are possible. LANs are widely used because they are cost-effective and support resource sharing. In an office LAN, for example, all employees can share the same printer and access common databases. A campus LAN allows students and faculty to share files, use centralized applications, and access the internet.

The major advantages of a LAN are high speed, low error rates, cost-effectiveness, and good security since the entire network is under one administrative control. However, the main limitation is that LANs are confined to a small geographical region and cannot directly cover long distances. Their performance may also degrade when too many devices are connected at the same time, requiring proper design and management.

Metropolitan Area Network (MAN)

A Metropolitan Area Network, or MAN, is a larger network than a LAN and is designed to cover an entire city or metropolitan region. It connects multiple LANs within a city to form a bigger network. MANs are often used by internet service providers, government agencies, and large organizations to provide high-speed connectivity across different parts of a city. The typical coverage of a MAN is between 10 and 50 kilometers, making it ideal for connecting university campuses located in different parts of the city, or linking branches of banks and businesses spread across a metropolitan area.

MAN Metropolitan Area Network



The backbone of a MAN is usually built using high-capacity transmission media such as optical fiber cables, microwave links, or coaxial cables. Technologies like Fiber Distributed Data Interface (FDDI), Asynchronous Transfer Mode (ATM), and Gigabit Ethernet are commonly used in MANs. Data transmission speeds are moderate to high, typically ranging from 10 Mbps to 1 Gbps, depending on the technology and infrastructure used.

A good example of a MAN is the cable television network in a city, where one central provider distributes TV and internet services to thousands of customers across different localities. Similarly, an internet service provider may set up a MAN to provide broadband services across an entire city.

The main advantages of a MAN are its ability to connect multiple LANs over a larger area, its higher capacity backbone which allows faster communication, and its cost-effectiveness compared to WAN when used at the city level. However, MANs are more expensive and complex than LANs and require professional management. They are also more prone to congestion and political or organizational issues, as multiple stakeholders may be involved in operating them.

Wide Area Network (WAN)

A Wide Area Network, or WAN, is the largest type of computer network, spanning across countries and even continents. It interconnects multiple LANs and MANs using long-distance communication technologies such as satellite links, undersea optical fiber cables, and leased telephone lines. The most prominent example of a WAN is the Internet, which connects millions of private, public, academic, business, and government networks across the globe.

The coverage area of a WAN is practically unlimited, often extending thousands of kilometers. Unlike LANs and MANs, which are usually owned and controlled by a single organization, WANs are maintained by multiple service providers such as telecom companies, internet backbone providers, and governments. This shared nature makes WANs more complex to manage.

WAN Wide Area Network



shutterstock.com · 2459981107

The data transmission speeds in WANs are generally lower than in LANs and MANs due to the large distances and the amount of traffic they carry, although modern technologies like high-speed fiber optics, 5G wireless networks, and Multiprotocol Label Switching (MPLS) have significantly improved WAN performance. WANs are essential for businesses that operate internationally, allowing different branches in different countries to communicate and share data. They are also the foundation of services like online banking, global e-commerce, video conferencing, and cloud computing.

The advantages of WANs include global connectivity, resource sharing on a worldwide scale, and the ability to support real-time communication across vast distances. On the downside, WANs are very expensive to build and maintain, they are slower compared to LANs, and they are more prone to security risks such as hacking and data theft due to their large and open nature.

Key Differences: LAN vs MAN vs WAN

Aspect	LAN	MAN	WAN
Full Form	Local Area Network	Metropolitan Area Network	Wide Area Network
Coverage Area	Small area (1–10 km)	City-level (10–50 km)	Global/Continental (1000s km)
Ownership	Single organization	Shared (ISP/government/orgs)	Multiple stakeholders
Speed	Very high (100 Mbps–10 Gbps)	Medium to high (10 Mbps–1 Gbps)	Lower (100 Kbps–100 Mbps+)
Cost	Low	Medium	High
Reliability	Very reliable	Moderate reliability	Less reliable (prone to delays)
Examples	Office Wi-Fi, Ethernet LAN	Cable TV, city broadband	Internet, global banking WAN

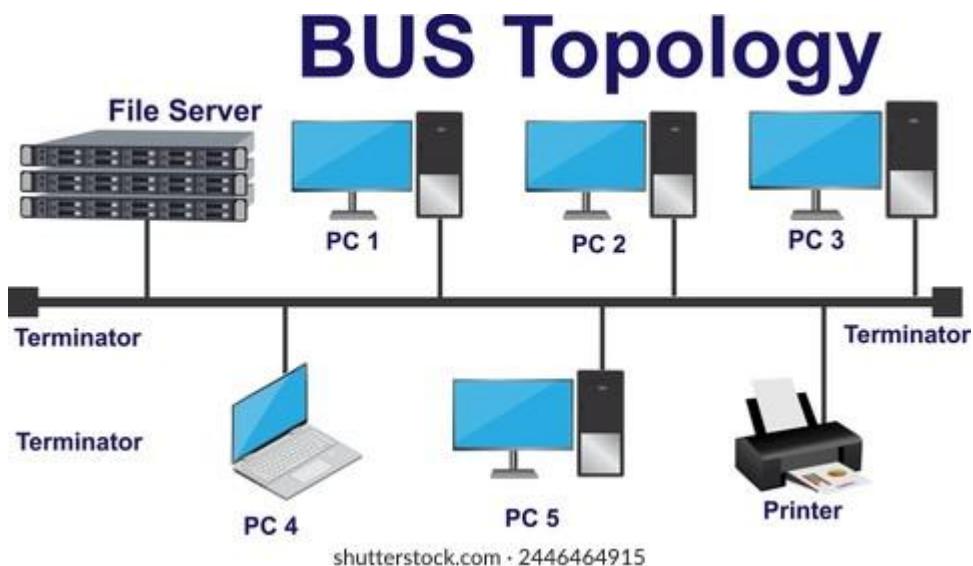
Network Topology (Types)

A network topology refers to the arrangement or physical structure in which the various devices such as computers, printers, switches, or routers are interconnected in a network. It defines not only how the devices are physically connected but also how data flows between them. Topologies can be physical, representing the actual layout of cables and devices, or logical, representing the flow of data regardless of the physical design. The choice of topology affects

the performance, reliability, cost, and scalability of a network. The most common network topologies are bus, star, ring, mesh, tree, and hybrid.

1. Bus Topology

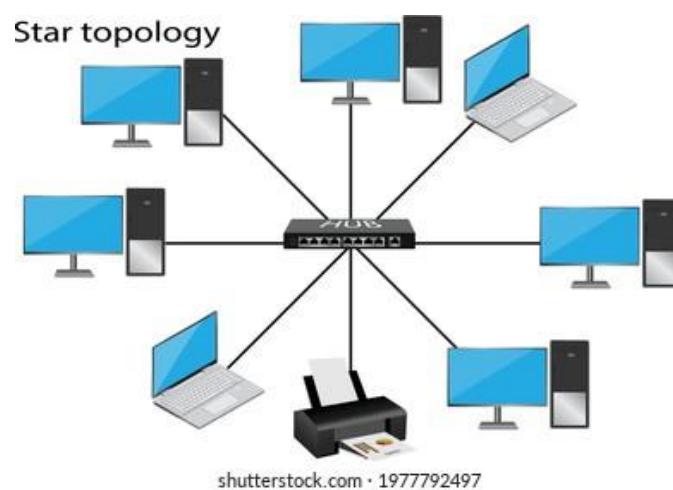
In a bus topology, all devices in the network are connected to a single central cable known as the backbone or bus. Each device has a network interface that allows it to send and receive data over the shared medium. When a device sends data, it is broadcast to all devices on the bus, but only the intended recipient processes the message while others ignore it.



Bus topology is simple to set up and requires less cabling than other topologies, which makes it inexpensive. It was widely used in early Ethernet networks. However, it has significant limitations. If the backbone cable fails, the entire network goes down. As more devices are added, performance decreases because only one device can transmit at a time and collisions may occur. Troubleshooting faults is also difficult since the single cable is a potential point of failure.

2. Star Topology

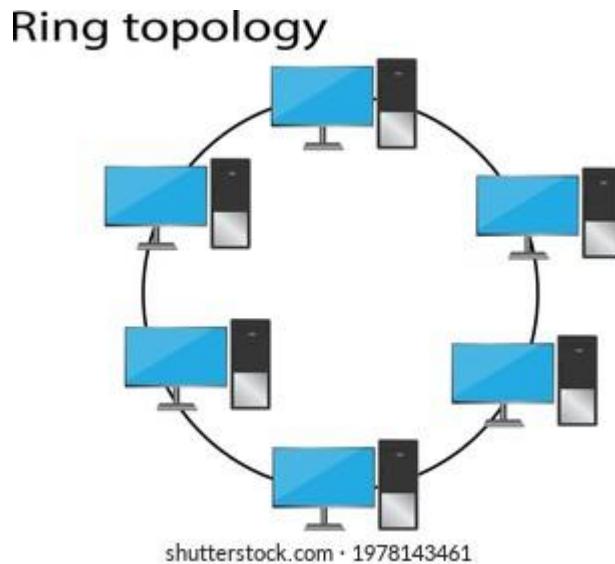
In a star topology, each device is connected to a central device, usually a hub or a switch. The central device acts as a mediator for all network communications. Data sent from one device must pass through the hub or switch before reaching the destination device.



The star topology is widely used in modern networks, especially in Ethernet-based LANs. Its greatest advantage is reliability: if one connection between a device and the hub fails, the other devices remain unaffected. It is also easier to add new devices or troubleshoot problems, as each link is independent. However, the central device is a critical point of failure. If the hub or switch fails, the entire network is disrupted. Star networks also require more cabling than bus networks since each device needs a separate connection to the central hub.

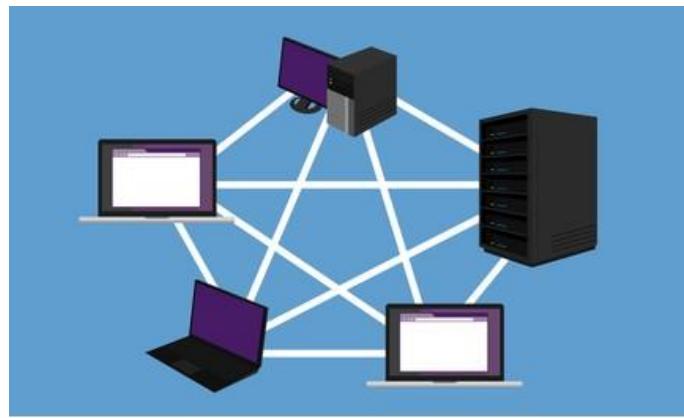
3. Ring Topology

In a ring topology, each device is connected to exactly two other devices, forming a closed loop or ring. Data travels around the ring in one direction, passing through each device until it reaches its destination. Some implementations use tokens to control access, where a token circulates around the ring and only the device holding the token can transmit data.



Ring topology ensures orderly communication without collisions, as only one device transmits at a time. It provides predictable performance even as the network grows. However, the biggest drawback is reliability: if any device or connection in the ring fails, it can disrupt the entire network. To overcome this, some modern implementations use dual rings for redundancy. Ring topology was popular in older technologies like IBM Token Ring but has largely been replaced by Ethernet-based star networks.

4. Mesh Topology



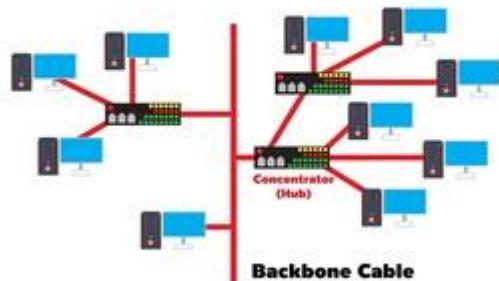
In a mesh topology, every device is connected to every other device in the network. This provides multiple paths for data to travel, which makes the network highly reliable and fault tolerant. If one connection fails, data can take an alternate path to reach its destination. Mesh topology can be either full mesh, where every device has a direct link to every other device, or partial mesh, where only some devices are fully interconnected while others are connected to a few devices.

Mesh topologies are highly reliable and secure since multiple redundant paths exist. They are used in critical networks such as military communication systems and backbone WANs where reliability is more important than cost. However, they require a very large number of connections. For n devices, a full mesh requires $n(n-1)/2$ links, which becomes impractical for large networks. The cabling and setup costs are extremely high, and maintenance is complex.

5. Tree Topology

Tree topology is a hierarchical structure that combines elements of star and bus topologies. Devices are arranged in the form of a tree, with groups of star-configured networks connected to a central backbone cable. The root node is at the top and branches out to other nodes, creating a parent-child relationship.

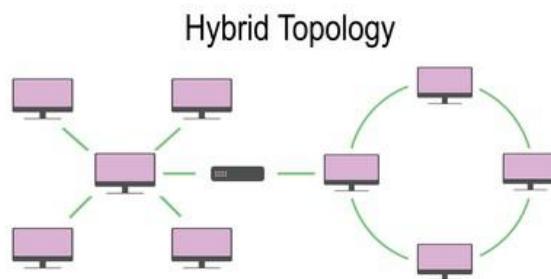
TREE TOPOLOGY



shutterstock.com • 2160054035

Tree topology is suitable for large networks that require expansion. It allows easy addition of new nodes and provides better fault isolation compared to bus topology. However, it still suffers from the disadvantage that if the backbone cable fails, large portions of the network may become disconnected. It also requires a lot of cabling and careful configuration.

6. Hybrid Topology



shutterstock.com • 1822164695

Hybrid topology is formed by combining two or more different types of basic topologies. For example, a large organization may use a mixture of star and bus topologies, or mesh and star, depending on their communication needs and budget. Hybrid topologies are flexible and scalable, allowing designers to choose the best aspects of different topologies.

The main advantage of hybrid topology is that it can be customized to suit specific requirements, providing both reliability and cost efficiency. However, designing and managing hybrid networks can be complex, and they may require advanced hardware such as routers and gateways to handle different segments.

In a five-node mesh, each device (say $M\alpha$, $M\beta$, $M\gamma$, $M\delta$, $M\epsilon$) connects directly to all others. If the link $M\alpha$ – $M\gamma$ goes down, alternate paths such as $M\alpha \rightarrow M\beta \rightarrow M\gamma$ still exist. Connectivity is preserved, though latency might increase.

In a five-node star with central node Core and leaves L1–L5, each leaf connects only to Core. If L2's cable fails, only L2 is isolated; L1, L3, L4, and L5 continue communicating through Core. The real weakness lies in Core: if it fails, the entire network collapses.

In a five-node bus, all nodes N1–N5 share a single backbone. If the backbone breaks between N3 and N4, the bus splits into two islands (N1–N2–N3) and (N4–N5). Nodes within the same segment still communicate, but cross-segment traffic fails.

In a five-node ring, suppose nodes $R\alpha$ – $R\beta$ – $R\gamma$ – $R\delta$ – $R\epsilon$ form a loop. If the link $R\delta$ – $R\epsilon$ breaks, the loop opens into a line, and frames cannot circulate back. Unless the ring is dual or self-healing, communication between opposite halves is interrupted.

1.2 Network Software:

Networking is not just about the physical connection of devices and transmission media; it also requires software protocols and layered designs to ensure proper communication. Network software provides the rules, services, and mechanisms by which devices communicate across local and global networks. It includes concepts such as protocol hierarchies, design issues for layers, connection-oriented and connectionless services, and reliable versus unreliable services.

Protocol Hierarchy

Communication between computers over a network involves several functions, ranging from transmitting raw electrical signals to interpreting high-level application data such as web pages or emails. To manage this complexity, network software is structured in the form of a protocol hierarchy or layered architecture.

Each layer in this hierarchy provides a well-defined set of services to the layer above it while hiding the details of its own implementation. This modular approach allows designers to develop complex systems in manageable parts. For example, when you send an email, the application layer handles composing and reading the message, the transport layer ensures reliable delivery, the network layer selects routes, the data link layer manages error detection in frames, and the physical layer handles the actual transmission of bits.

The hierarchical approach ensures interoperability, flexibility, and ease of troubleshooting. Standard protocol suites such as OSI and TCP/IP are built upon this layered principle.

Design Issues for Layers

While building network layers, certain design issues need to be carefully addressed to ensure efficiency and reliability:

- **Addressing:** Every device must have a unique address so that the intended recipient can be identified. Different layers use different addresses, such as MAC addresses at the data link layer and IP addresses at the network layer.

- **Error Control:** Errors occur due to noise, interference, or hardware faults. Layers must detect and correct errors using mechanisms like checksums, parity bits, or retransmissions.
- **Flow Control:** Sending devices must not overwhelm receiving devices with too much data. Flow control mechanisms ensure that data is transmitted at a rate that the receiver can handle.
- **Multiplexing and Demultiplexing:** A single physical channel often carries data from multiple applications. Multiplexing allows combining several streams of data, while demultiplexing ensures the correct application receives the right data.
- **Connection Establishment and Termination:** Some services require a formal handshake before communication begins and proper closing of the session after transmission ends.
- **Synchronization and Sequencing:** Data sent over a network must arrive in the correct order. Layers must ensure sequencing and synchronization when needed.

These design issues are essential for building reliable and interoperable communication systems.

Connection-Oriented and Connectionless Services

Network services can be classified into two categories based on how communication is established and maintained:

Connection-Oriented Services:

In a connection-oriented service, a dedicated logical path is established between the sender and receiver before any data transfer occurs. This process is similar to making a telephone call where you first dial, establish a connection, talk, and then hang up. The service ensures ordered and reliable delivery of data. Transmission Control Protocol (TCP) in the Internet is an example of a connection-oriented protocol. It sets up a connection through a three-way handshake, transmits data, and closes the connection gracefully.

Connectionless Services

In a connectionless service, data is sent in discrete packets, each of which is routed independently through the network without establishing a dedicated path. This is similar to sending letters by post where each letter may take a different route and may arrive out of order. The Internet Protocol (IP) is a connectionless protocol, as is the User Datagram Protocol (UDP). Connectionless services are faster and have less overhead but do not guarantee reliability or order.

Both types of services have their uses. For critical applications like file transfers or banking, connection-oriented services are preferred. For real-time applications like voice over IP or video streaming, connectionless services are often used to reduce latency.

Reliable and Unreliable Services

Another important distinction in network software is between **reliable** and **unreliable** services.

Reliable Services

Reliable services guarantee that the data sent by the sender is delivered accurately and in the correct order to the receiver. They use acknowledgment, error detection, retransmission of lost packets, and flow control mechanisms. Transmission Control Protocol (TCP) is the prime example of a reliable service. Reliable services are essential for applications where accuracy of data is more important than speed, such as file transfers, emails, or web browsing.

Unreliable Services

Unreliable services do not guarantee delivery, order, or integrity of data. Packets may be lost, duplicated, or arrive out of sequence. However, unreliable services reduce processing overhead, making them suitable for real-time applications where speed is crucial. User

Datagram Protocol (UDP) is an example of an unreliable service. Applications such as live video streaming or online gaming often prefer UDP since occasional packet loss is less noticeable than delays caused by retransmissions.

Network software is the backbone of communication between devices. By organizing communication into layered protocol hierarchies, it allows complex tasks to be managed in simpler, well-defined modules. Each layer faces common design issues such as addressing, error handling, and flow control, which must be handled carefully to provide efficient communication. Services can be either connection-oriented or connectionless, and reliable or unreliable, depending on the needs of the application. Together, these principles form the basis of how modern computer networks such as the Internet function.

When an application communicates across a network, each layer contributes its own addressing. At the **application layer**, a user-friendly name is used, such as library.univ.ac.in (in the alternate scenario, imagine weather.station.local). At the **transport layer**, a process is identified by ports: the sender may choose a random source port Psr (say 52341) aimed at a well-known destination port Pdst (say 25 for SMTP; in the shadow example think 61234→443). At the **network layer**, devices are identified by IP addresses, such as 192.168.5.10 to 192.168.5.25 (alternate: 172.16.8.14 to 10.1.4.9). At the **data link layer**, local delivery is achieved with MAC addresses; these are rewritten on each hop. For example, in the first LAN segment, frames might travel from AA-BB-CC-DD-11-22 to AA-BB-CC-DD-33-44. At the **physical layer**, only the bits (electrical, optical, or radio signals) matter.

The crucial exam insight. **ports and IPs are end-to-end (unchanged), while MACs flip per hop.** If you can phrase it as “Psrc→Pdst and IPsrc→IPdst stay constant, but MACsrc→MACdst is refreshed at each segment,” you’ve got the right reasoning.

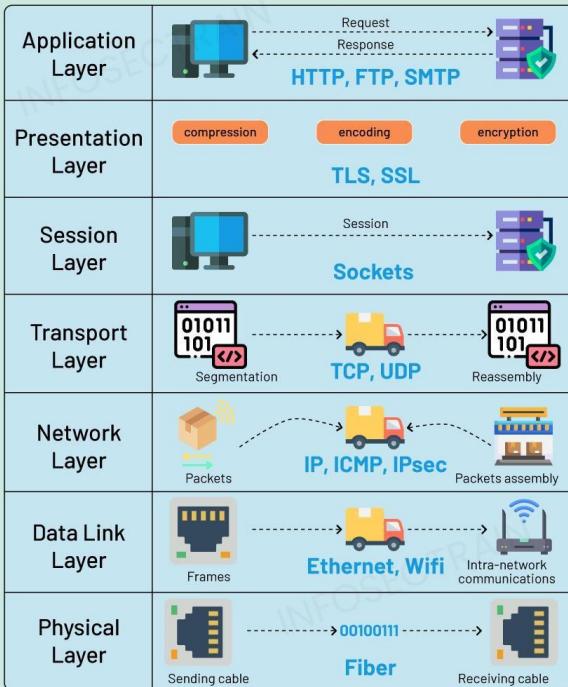
1.3 OSI and TCP/IP Reference Models

Computer networks are complex systems where data must travel from one application on a source device to another application on a destination device, often across multiple physical and logical networks. To handle this complexity in a systematic way, researchers developed reference models that divide the process of communication into layers, each with specific functions. Two important models dominate the field: the **OSI Reference Model** and the **TCP/IP Reference Model**.

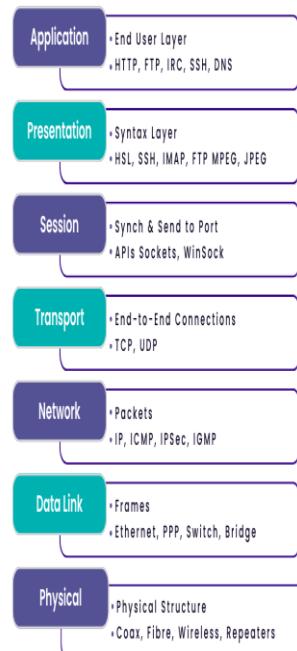
1. OSI Reference Model

The **Open Systems Interconnection (OSI)** model was developed by the International Organization for Standardization (ISO) in the late 1970s and early 1980s. It is a **conceptual framework** that standardizes the functions of a communication system into **seven layers**. The OSI model is not a protocol itself but a guide to understanding and designing interoperable networking systems.

OSI MODEL LAYERS



7 Layers of OSI Model



The Seven Layers of OSI

1. Physical Layer

The lowest layer deals with the transmission of raw bits over a physical medium such as cables, fiber optics, or radio waves. It defines hardware specifications, voltage levels, signal timing, connectors, and data rates. It ensures that when one side sends a binary 1, the other side receives it as a binary 1, not a 0.

2. Data Link Layer

This layer is responsible for framing, error detection, error correction, and medium access control. It ensures reliable transmission of data frames between two directly connected nodes. Technologies such as Ethernet (IEEE 802.3) and Wi-Fi (IEEE 802.11) operate at this layer. It uses **MAC addresses** for identifying devices.

3. Network Layer

The network layer provides logical addressing and determines the path data should take through the network. It handles packet forwarding and routing. The Internet Protocol (IP) works at this layer. Devices such as routers operate here.

4. Transport Layer

The transport layer provides end-to-end communication between applications on two devices. It ensures data is delivered reliably, in order, and without errors (in the case of TCP). It provides services like segmentation, reassembly, flow control, and error recovery.

5. Session Layer

This layer manages sessions or dialogues between applications. It establishes, maintains, and terminates communication sessions. It handles synchronization, checkpoints, and recovery. For example, in a video call, the session layer helps maintain the connection.

6. Presentation Layer

The presentation layer ensures that data is in a usable format for the application layer. It deals with translation (from different character sets or encoding schemes),

encryption/decryption, and compression. For instance, it converts an ASCII-encoded text file into EBCDIC if necessary.

7. Application Layer

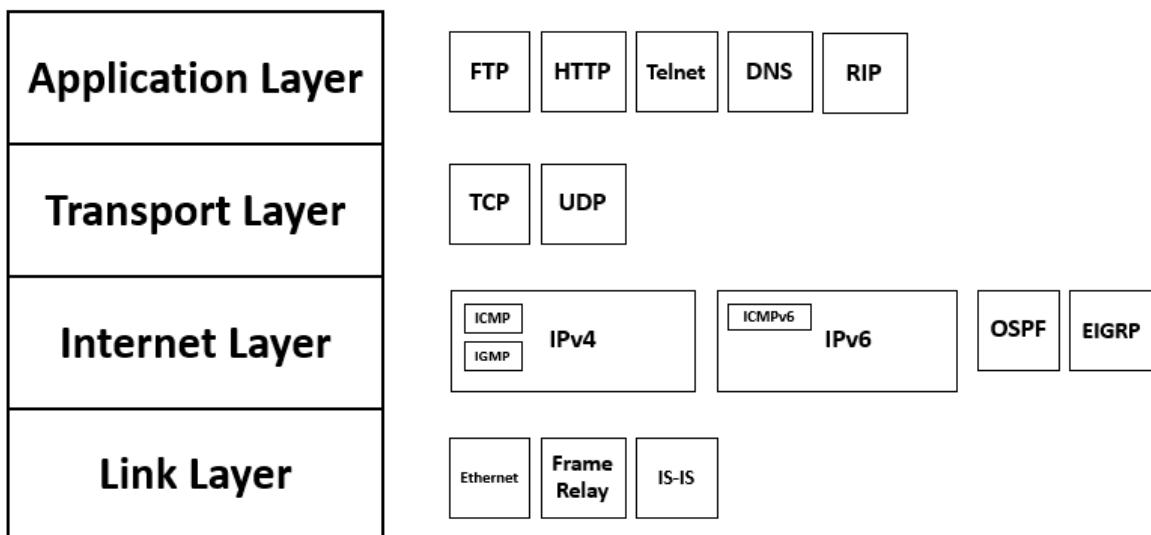
The topmost layer directly interacts with the end user. It provides services such as email (SMTP), web browsing (HTTP/HTTPS), and file transfer (FTP). It is the interface between the user and the network.

Importance of OSI Model

The OSI model provides a **clear separation of concerns**, helping designers and engineers troubleshoot, teach, and develop new networking technologies. Even though it is largely theoretical, it influenced the design of real-world networking protocols.

2. TCP/IP Reference Model

While the OSI model was being developed, the United States Department of Defense was also working on a practical networking framework to support research and military communication. This became known as the **TCP/IP Reference Model**. TCP/IP is not just a model but also a **protocol suite** that underpins the modern Internet.



Layers of TCP/IP

The TCP/IP model has **four layers** that correspond roughly to groups of OSI layers:

1. Network Access Layer

This layer includes the physical and data link aspects of communication. It defines how bits are transmitted over physical media and how devices on the same network identify each other. It encompasses hardware technologies like Ethernet, Wi-Fi, and protocols for framing and addressing.

2. Internet Layer

The Internet layer corresponds to the OSI network layer. It is responsible for logical addressing, routing, and packet delivery across networks. The key protocol here is the **Internet Protocol (IP)**, which comes in two versions: IPv4 and IPv6. Other protocols include ICMP (for error messages and diagnostics) and ARP (for resolving IP addresses to MAC addresses).

3. Transport Layer

The transport layer ensures end-to-end communication between applications. It defines how data is segmented, transmitted, and reassembled. The two main protocols are **Transmission Control Protocol (TCP)**, which provides reliable, connection-oriented

service, and **User Datagram Protocol (UDP)**, which provides fast but unreliable, connectionless service.

4. Application Layer

The application layer in TCP/IP includes everything that involves direct interaction with software applications. Protocols here include HTTP, FTP, SMTP, DNS, and many others. Unlike OSI, TCP/IP does not distinguish between application, presentation, and session functions, merging them all into a single layer.

Importance of TCP/IP Model

The TCP/IP model is more practical and widely adopted. It directly supports the Internet, making it the foundation of global communication. Unlike the OSI model, TCP/IP was not developed as a theoretical exercise but as a working standard tested and implemented in real networks.

Comparison of OSI and TCP/IP Models

Aspect	OSI Model	TCP/IP Model
Full Form	Open Systems Interconnection Model	Transmission Control Protocol / Internet Protocol Model
Developed by	International Organization for Standardization (ISO)	U.S. Department of Defense (DoD), later standardized by IETF
Year of Development	1978 (published as ISO standard in 1984)	1970s (ARPANET project, practical deployment in 1983)
Number of Layers	7 layers	4 layers
Layer Names	Physical, Data Link, Network, Transport, Session, Presentation, Application	Network Access, Internet, Transport, Application
Approach	Theoretical / Conceptual framework for standardizing communication	Practical implementation model for communication across real-world networks
Function Grouping	Functions are separated into 7 well-defined layers	Functions are combined (Session, Presentation, Application → Application layer; Physical & Data Link → Network Access layer)
Protocol Dependency	Protocol-independent, a reference model	Protocol-specific (centered around TCP and IP)
Reliability	Provides reliable communication through clear responsibilities per layer	Provides reliability mainly through TCP at the transport layer
Flexibility	More rigid and layered; each layer strictly defined	More flexible; layers not as strictly separated
Usage	Mainly used as a teaching and conceptual tool	Used in practice; forms the basis of the Internet
Examples of Protocols	Does not itself specify protocols; instead, protocols are mapped to its layers	Defines actual protocols such as TCP, UDP, IP, ARP, HTTP, FTP, DNS
Adoption	Limited adoption in real networks	Widely adopted; global standard for networking

Let Host X in LAN-A send data to Host Y in LAN-B, with Router Z between them. At the **transport layer**, the segment always carries the same source port Psr and destination port Pdst (for example, 49120→8080; imagine 56001→22). At the **network layer**, the packet always shows source address IPx and destination address IPy (say 192.168.10.7→192.168.20.15; think 10.0.3.11→172.16.9.4).

At the **data link layer**, however, each hop is reframed. In the first hop (LAN-A), the Ethernet frame goes from MAC MA1 (X's NIC, e.g., 00-11-22-33-44-55) to MAC MZ1 (Router Z's LAN-A interface). Router Z strips this, consults its routing table, and forwards on LAN-B with new addresses: now the frame is from MAC MZ2 (Router Z's LAN-B NIC, say 66-77-88-99-AA-BB) to MAC MY (Y's NIC).

So, across both hops the **ports remain Psr→Pdst, IPs remain IPx→IPy**, but the **MAC addresses are rewritten per link (MA1→MZ1, then MZ2→MY)**.

1.4 Overview of Connecting Devices

In a computer network, different types of hardware devices are required to connect computers and enable communication. These devices operate at various layers of the OSI model and serve different purposes, such as amplifying signals, filtering traffic, connecting different networks, or translating between protocols. The most common connecting devices are the Network Interface Card (NIC), Repeater, Hub, Bridge, Router, and Gateway.

1. Network Interface Card (NIC)

The Network Interface Card is the basic hardware component that allows a computer or device to connect to a network. It is sometimes called a network adapter or LAN card. Each NIC has a unique MAC (Media Access Control) address, which is used to identify the device at the Data Link Layer.

NICs can be wired, using Ethernet cables, or wireless, using Wi-Fi standards. They handle both the physical connection to the medium (like copper cables or radio waves) and the framing of data for transmission. Without a NIC, a device cannot participate in a network.

In modern computers, NICs are usually integrated into the motherboard, although external NICs (USB or PCI cards) are also available for upgrades. For example, a laptop's built-in Wi-Fi adapter is its NIC.

2. Repeater

A Repeater is a device that operates at the Physical Layer of the OSI model. Its function is to regenerate and amplify signals that weaken as they travel over long distances.

When data is transmitted over cables, the electrical signals degrade due to attenuation and noise. A repeater receives these weak signals, amplifies them, and retransmits them in their original strength. This extends the coverage of a network beyond its normal cable length limitations.

Repeaters do not filter or manage traffic; they simply regenerate all signals, whether useful or not. For example, Ethernet has a distance limitation of 100 meters for twisted-pair cables. A repeater can be placed at the end of the cable to extend the network.

3. Hub

A Hub is a simple networking device that operates at the Physical Layer. It connects multiple devices in a star topology. When a device sends data to the hub, the hub broadcasts the data to all other connected devices, regardless of the intended destination.

There are two types of hubs: active hubs, which regenerate and forward signals like repeaters, and passive hubs, which simply distribute the signals without amplification.

Hubs are inexpensive but inefficient because they generate a lot of unnecessary traffic and can cause data collisions. Modern networks have largely replaced hubs with switches, which are more intelligent. An example of a hub is an early Ethernet hub used in small office networks during the 1990s.

4. Bridge

A Bridge operates at the Data Link Layer of the OSI model. Its purpose is to divide a large network into smaller segments, reducing congestion and improving performance.

A bridge examines the MAC address of incoming frames and decides whether to forward or filter them. If the destination MAC address belongs to the same segment as the sender, the bridge does not forward the frame. If the destination is in another segment, the bridge forwards it to that segment.

In this way, bridges reduce unnecessary traffic and collisions. Bridges are used in LANs to connect two or more network segments. For example, two floors of an office building may each have a LAN, and a bridge can connect them into one larger LAN.

5. Router

A Router is a more advanced device that operates at the Network Layer of the OSI model. Its main role is to connect different networks together and direct packets to their destinations based on IP addresses.

Routers maintain routing tables that contain information about possible paths to different networks. When a packet arrives, the router examines its destination IP address and determines the best path for it. Routers can also perform functions such as Network Address Translation (NAT), firewall filtering, and Quality of Service (QoS) management.

Routers are essential for the Internet, as they enable communication between different networks across the globe. For example, a home Wi-Fi router connects the devices inside the home LAN to the Internet through an ISP. Large organizations use enterprise routers to manage connections between their branch offices and data centers.

6. Gateway

A Gateway is the most complex connecting device. Unlike repeaters, hubs, bridges, and routers, which generally connect similar networks, a gateway can connect networks using different protocols or architectures. It operates at multiple layers of the OSI model, often including the Application Layer.

A gateway acts as a translator, converting data from one format to another so that communication can take place between otherwise incompatible systems. For example, a gateway can connect a TCP/IP-based network with a legacy system using a different protocol. Gateways are commonly used in enterprise systems where internal networks need to communicate with external applications or systems. For example, a payment gateway translates communication between a merchant's system and a bank's financial network.

Guided and Unguided Transmission Media

In computer networks, the medium used to transmit data from one device to another is known as the **transmission medium**. It forms the physical path that carries signals representing data. Transmission media can be broadly divided into two categories: **guided media** and **unguided media**.

Guided transmission media refers to media where signals are confined to a physical path such as cables and wires. In contrast, **unguided transmission media** does not use any physical conductor; instead, signals are transmitted through the air or space in the form of

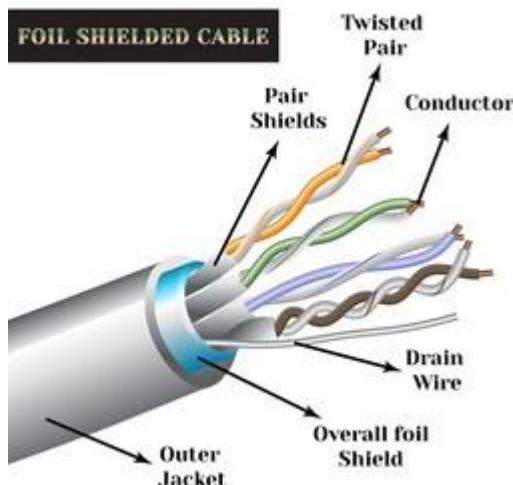
electromagnetic waves. Both types of media have distinct characteristics, advantages, disadvantages, and applications.

1. Guided Transmission Media

Guided media are also known as **wired media** or **bounded media** because data signals are directed and confined within a physical path. The transmission capacity, signal quality, and reliability depend on the physical properties of the medium, such as material, thickness, and shielding.

a) Twisted Pair Cable

Twisted pair is the most common guided medium, consisting of pairs of insulated copper wires twisted together. The twisting reduces electromagnetic interference from external sources and crosstalk between adjacent pairs.



shutterstock.com · 406533088

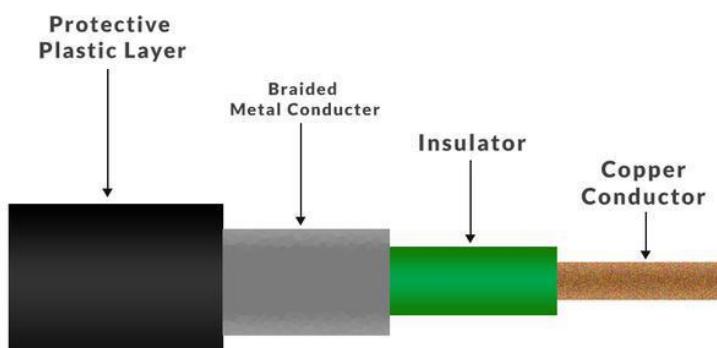
There are two types:

- **Unshielded Twisted Pair (UTP):** Widely used in Ethernet LANs and telephone lines. It is inexpensive and easy to install but more prone to interference.
- **Shielded Twisted Pair (STP):** Similar to UTP but with an additional shielding layer to provide better protection from interference. It is used in environments with high electrical noise.

Twisted pair cables typically support data rates up to 1 Gbps and distances of about 100 meters without repeaters.

b) Coaxial Cable

Coaxial cable consists of a central copper conductor surrounded by an insulating layer, a metallic shield, and an outer insulating jacket. This layered design provides excellent shielding against interference, making coaxial cables more reliable than twisted pair.

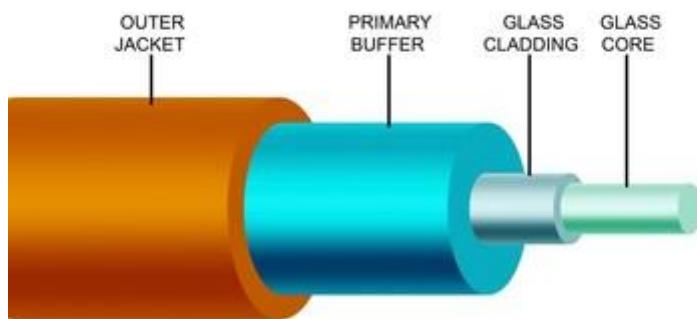


Coaxial cables were once widely used in LANs (10Base2, 10Base5 Ethernet) but are now more common in cable television and broadband internet. They support higher bandwidth and longer distances than twisted pair, typically several kilometers with amplifiers.

c) Optical Fiber Cable

Optical fiber is the most advanced guided medium. It uses thin strands of glass or plastic fibers to transmit data as pulses of light generated by lasers or LEDs. Since light signals are immune to electromagnetic interference, optical fiber provides extremely high bandwidth and long-distance communication.

Optical Fiber Cable



shutterstock.com - 2309153889

There are two types:

- **Single-mode fiber (SMF):** Allows only one mode of light to propagate, enabling very long-distance communication (tens to hundreds of kilometers) with high bandwidth.
- **Multimode fiber (MMF):** Allows multiple light modes to propagate, suitable for shorter distances (up to a few kilometers).

Optical fiber is used in backbone networks, undersea cables, and high-speed internet connections. Its advantages are massive bandwidth, low attenuation, and immunity to interference. The disadvantages are high installation costs and the need for specialized equipment.

2. Unguided Transmission Media

Unguided media are also known as **wireless media** or **unbounded media**. In this case, signals travel through the atmosphere or space using electromagnetic waves. These media do not require physical conductors, making them ideal for mobility and long-distance communication. The propagation of signals depends on frequency, antenna design, and environmental conditions.

a) Radio Waves

Radio waves are low-frequency signals (3 kHz to 1 GHz) that can travel long distances and penetrate buildings. They are omnidirectional, meaning antennas can both transmit and receive signals in all directions.

Radio waves are used in AM/FM radio, cordless phones, Wi-Fi networks, and mobile communications. They are inexpensive to deploy but suffer from interference, limited bandwidth, and security risks due to their broadcast nature.

b) Microwaves

Microwaves have higher frequencies (1 GHz to 300 GHz) and travel in straight lines. They require line-of-sight between transmitter and receiver, which means towers or antennas must be aligned properly.

Microwave communication can be terrestrial (between towers on Earth) or satellite-based (where a signal is sent to a satellite and relayed back to another location). Microwaves are used in satellite TV, mobile phones, radar, and long-distance telephone communication. Their main disadvantages are signal attenuation due to rain and the need for careful alignment.

c) Infrared Waves

Infrared signals operate at even higher frequencies than microwaves, typically 300 GHz to 400 THz. They are used for very short-range communication, such as remote controls, infrared data transfer between devices, and some wireless sensors.

Infrared cannot penetrate walls, so it is secure from external eavesdropping. However, it requires direct line-of-sight and is sensitive to environmental conditions like sunlight.

d) Satellite Communication

Satellites act as relay stations in space that receive signals from Earth and retransmit them to other locations. Communication satellites operate in various frequency bands, such as C-band, Ku-band, and Ka-band.

Satellite links are crucial for global broadcasting, GPS, internet in remote areas, and military communication. They provide wide coverage but are expensive to deploy and maintain. They also suffer from high latency because signals must travel long distances to geostationary satellites.