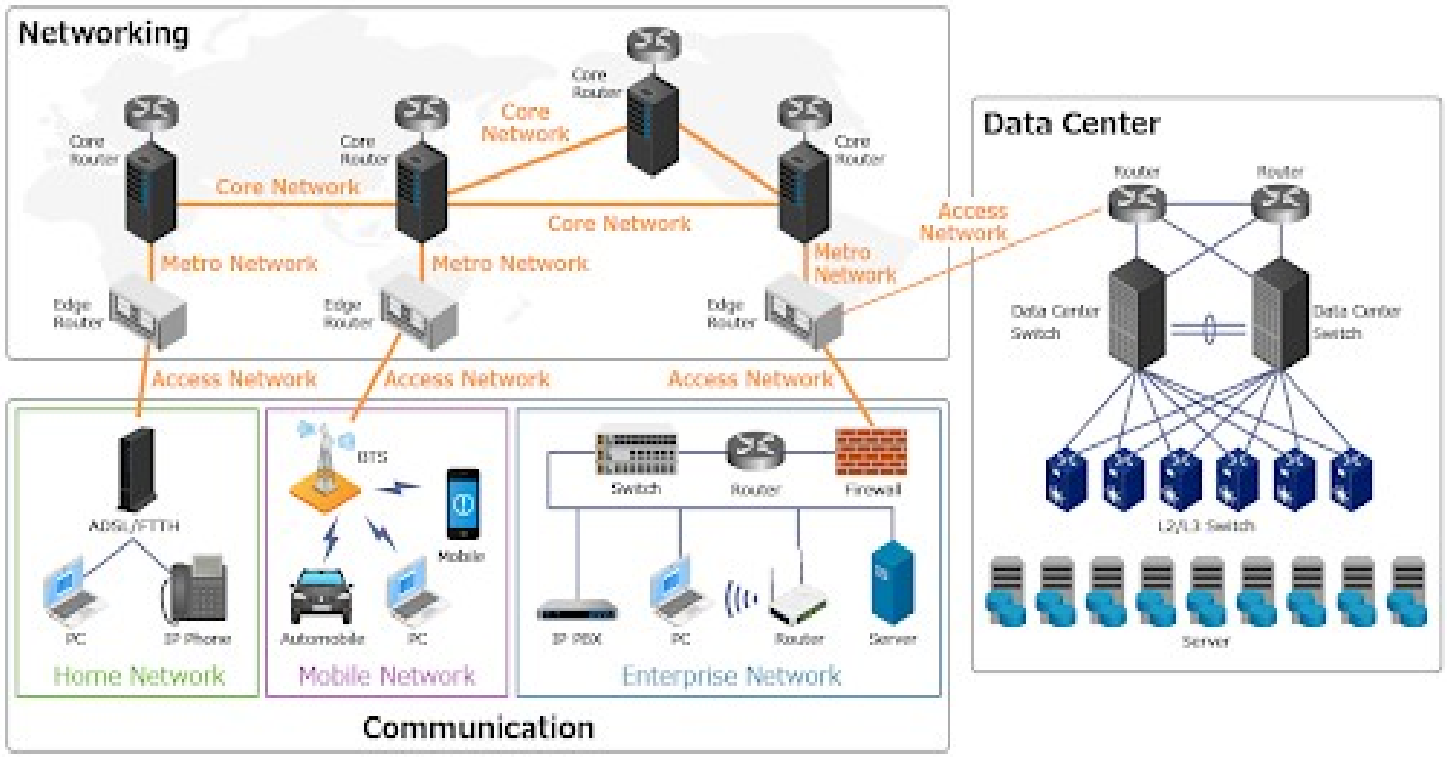
Computer Network

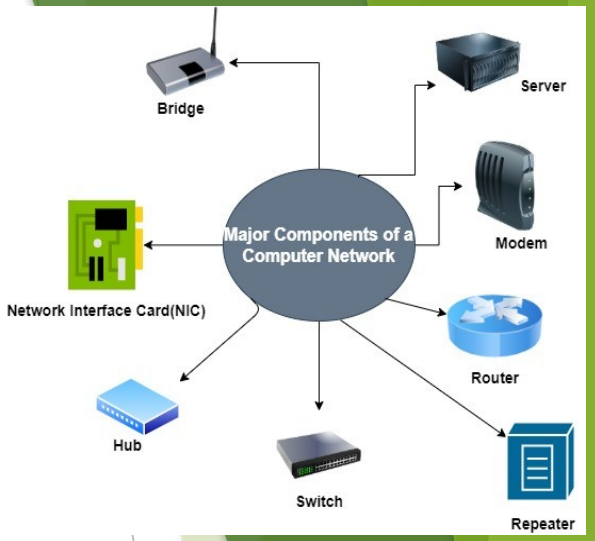
Bca

Network as an infrastructure for data communication

- A network, in the context of data communication, refers to the infrastructure that allows devices and systems to exchange data with each other.
- It provides the necessary connectivity and services for data transmission. Networks are fundamental to modern technology and play a crucial role in variou



key components and aspects of a network infrastructure for data communication



- **Devices:** Networks connect various devices, such as computers, smartphones, servers, routers, switches, and IoT (Internet of Things) devices. These devices may be connected through wired (e.g., Ethernet) or wireless (e.g., Wi-Fi, cellular) connections.
- **Topology:** Network topology refers to the physical or logical layout of the network. Common topologies include star, bus, ring, and mesh. The choice of topology depends on factors like scalability, fault tolerance, and cost.
- **Protocols:** Data communication on a network relies on protocols, which are sets of rules and conventions that govern how data is formatted, transmitted, received, and processed. Examples include TCP/IP (Transmission Control Protocol/Internet Protocol) for the Internet and HTTP (Hypertext Transfer Protocol) for web browsing.

- **Routing:** In larger networks, routing is essential to direct data packets from the source to the destination. Routers are responsible for making decisions about the optimal path for data to travel.
- **Switching:** Network switches are used to create local area networks (LANs) by connecting multiple devices within a single location. They use MAC addresses to determine where to send data within a LAN.
- **Firewalls and Security:** Network security is a critical consideration. Firewalls, intrusion detection systems, and encryption protocols are used to protect data from unauthorized access and cyber threats.

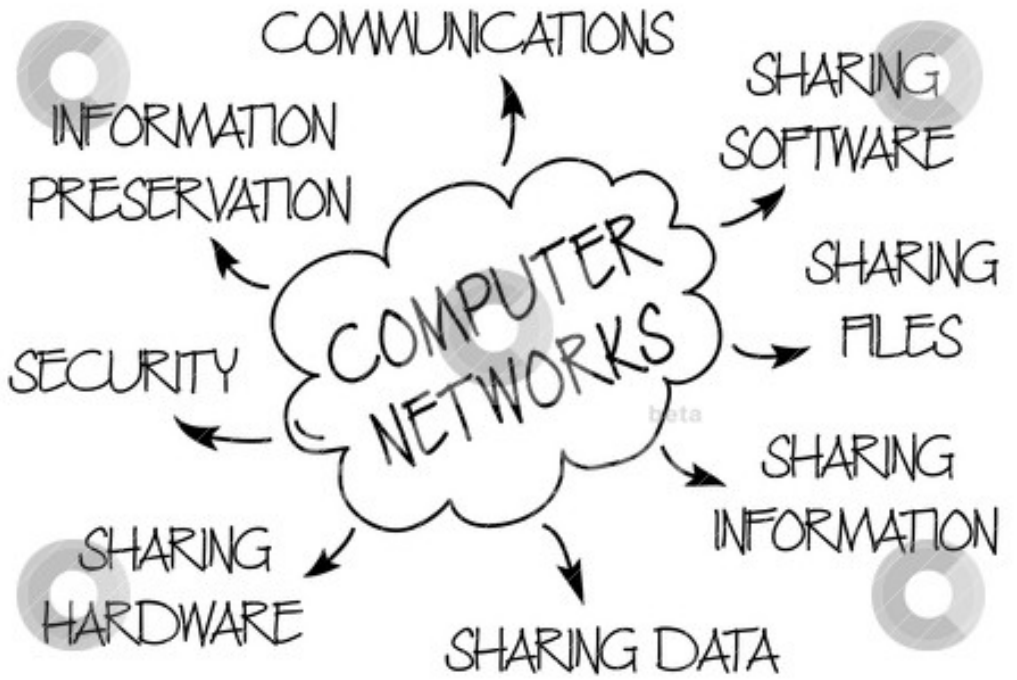
- **Bandwidth and Capacity:** Network infrastructure needs to be designed to handle the required bandwidth and capacity. This involves considerations like the type of data being transmitted, the number of users, and future scalability requirements.
- **Cabling and Connectivity:** For wired networks, the choice of cabling (e.g., Ethernet, fiber-optic) and the quality of connections are important factors that affect network performance.
- **Wireless Networks:** Wireless networks, such as Wi-Fi and cellular networks, have become increasingly prevalent. They provide flexibility and mobility but require careful management of radio frequencies and security.

- **Internet:** The global network of networks, known as the Internet, connects millions of networks and billions of devices worldwide. It operates using standardized protocols and allows data communication on a global scale.
- **Cloud Computing:** Cloud services rely on vast network infrastructures to provide on-demand access to computing resources, storage, and applications over the internet.
- **Virtual Private Networks (VPNs):** VPNs create secure, encrypted connections over public networks, allowing remote users to access private networks as if they were physically present at a specific location.

- **Quality of Service (QoS):** QoS mechanisms prioritize and manage network traffic to ensure that critical applications receive the necessary resources and that network performance meets specific requirements.
- **Monitoring and Management:** Network administrators use monitoring tools and management systems to oversee network performance, troubleshoot issues, and make necessary adjustments.
- **Scalability and Redundancy:** A well-designed network infrastructure should be able to scale to accommodate growing demands and provide redundancy to ensure reliability.

Application of Computer Network

- **Internet Access:** Computer networks provide access to the internet, enabling individuals and organizations to browse websites, send emails, and use various online services.
- **Email Communication:** Networks facilitate email communication, allowing people to send and receive messages and attachments quickly and efficiently.
- **File Sharing:** Networks enable file sharing and data transfer between devices, which is essential for collaboration and data distribution in both personal and professional settings.
- **Resource Sharing:** In a networked environment, devices can share hardware resources such as printers, scanners, and storage devices, reducing costs and increasing efficiency.
- **Remote Access:** Networks enable remote access to computers and systems, making it possible to work from different locations and access resources on distant servers.



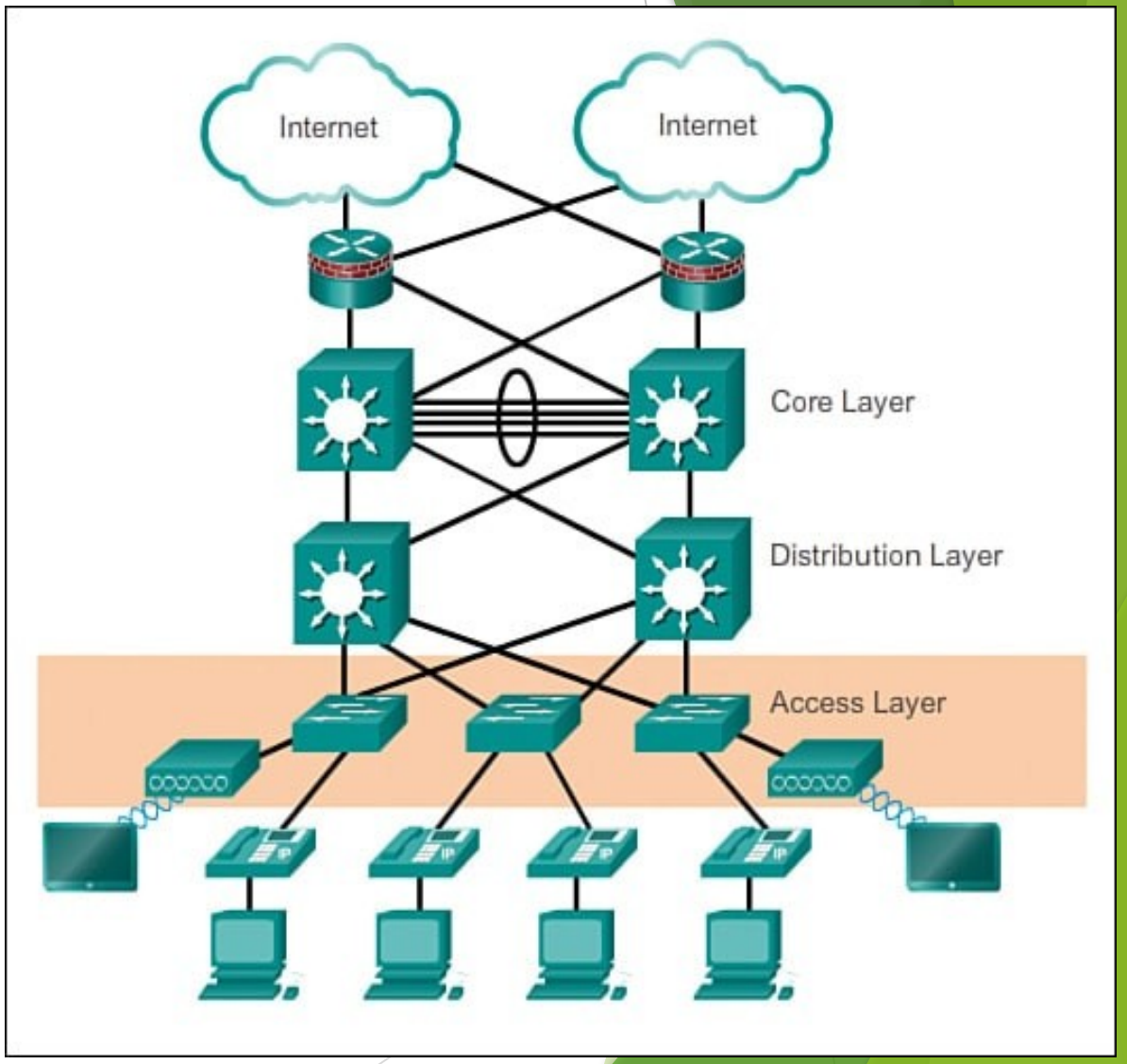
- **Intranets and Extranets:** Organizations use computer networks to create intranets (internal networks) and extranets (extended networks that connect partners or customers). These networks facilitate internal communication, document sharing, and collaboration.
- **VoIP and Video Conferencing:** Voice over Internet Protocol (VoIP) and video conferencing technologies rely on computer networks to enable voice and video communication over the internet, reducing communication costs and enhancing collaboration.
- **Cloud Computing:** Cloud services are hosted on large-scale computer networks, providing on-demand access to computing resources, storage, and applications for businesses and individuals.
- **Online Gaming:** Multiplayer online games rely on computer networks to connect players from around the world, allowing them to interact in virtual environments.
- **Social Media and Content Sharing:** Social media platforms and content-sharing websites rely on networks to connect users and enable the sharing of text, images, videos, and other media.

- **E-commerce:** Online shopping websites and e-commerce platforms operate over computer networks, enabling users to browse and purchase products and services.
- **Banking and Financial Transactions:** Networks are essential for conducting secure financial transactions, including online banking, electronic funds transfers, and credit card processing.
- **Healthcare:** Computer networks support telemedicine, electronic health records (EHRs), and remote patient monitoring, improving healthcare delivery and patient care.
- **Manufacturing and Industrial Control:** Industrial networks control and monitor manufacturing processes, machinery, and automation systems, enhancing efficiency and productivity.
- **Education:** Educational institutions use computer networks for e-learning platforms, online courses, and virtual classrooms, allowing students to access educational resources remotely.

- **Transportation and Logistics:** Networks are used in transportation systems for tracking shipments, managing vehicle fleets, and providing real-time information to travelers.
- **Smart Cities:** Networks play a crucial role in smart city initiatives, enabling the integration of technologies for efficient energy use, traffic management, and public services.
- **IoT (Internet of Things):** IoT devices rely on networks to connect and communicate, enabling applications like smart homes, industrial automation, and environmental monitoring.
- **Government and Public Services:** Governments use networks for e-government services, public safety, and communication between government agencies.
- **Research and Scientific Collaboration:** Networks connect researchers and institutions worldwide, facilitating collaboration on scientific projects and data sharing.

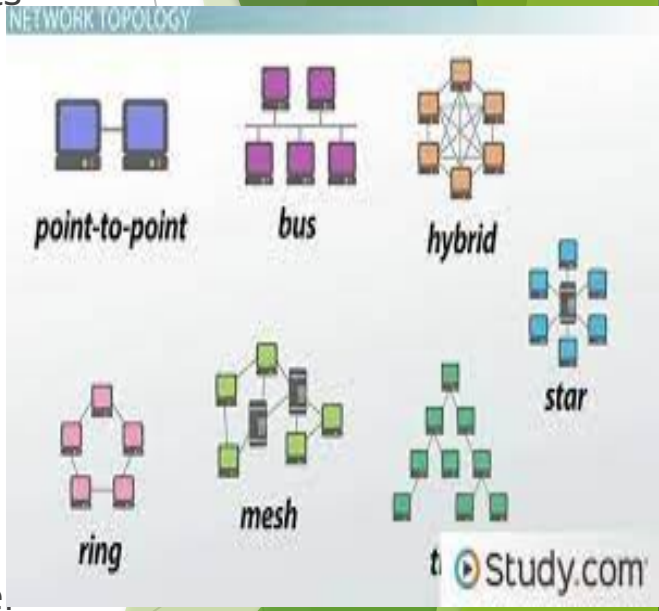
Network Architecture

- Network architecture refers to the design and layout of a computer network.
- It defines how the various components and devices within a network are organized and how they interact with each other.
- Network architecture is a critical consideration when designing, implementing, and maintaining a network, as it directly impacts its performance, scalability, and security.



key aspects of network architecture:

- **Topology:** Network topology defines the physical or logical layout of network components and how they are interconnected. Common network topologies include:
  - **Star Topology:** Devices are connected to a central hub or switch.
  - **Bus Topology:** Devices are connected in a linear fashion along a single backbone.
  - **Ring Topology:** Devices are connected in a closed-loop or ring.
  - **Mesh Topology:** Devices are interconnected in a complex, redundant manner, providing high fault tolerance.
- **Protocol Stack:** Network architecture specifies the protocol stack used for communication. The most common protocol stack is the TCP/IP (Transmission Control Protocol/Internet Protocol) suite, which is the foundation of the internet.
- **Network Layers:** Networks are often organized into layers to separate functionality and provide modularity. The OSI (Open Systems Interconnection) model and the TCP/IP model are two commonly used reference models that define network layers, including physical, data link, network, transport, session, presentation, and application layers.



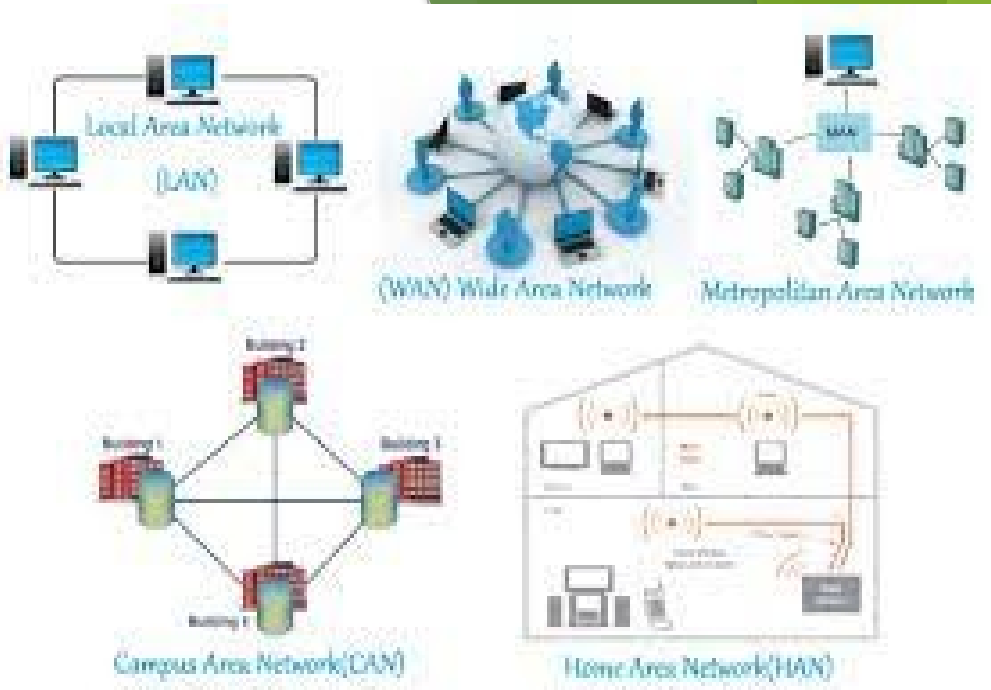
- **Routing and Switching:** Network architecture defines how routing and switching are handled. Routers are responsible for directing traffic between different networks, while switches manage traffic within a network segment.
- **Network Addressing:** It includes the assignment of unique addresses (e.g., IP addresses) to devices on the network and the use of subnets for network segmentation.
- **Security:** Network architecture must consider security measures such as firewalls, intrusion detection systems, encryption, and access control to protect the network from unauthorized access and cyber threats.
- **Scalability:** A well-designed network architecture should be scalable to accommodate growth in the number of devices and increased traffic demands. This often involves the use of hierarchical designs and modular components.
- **Redundancy:** To ensure network availability and fault tolerance, redundancy is built into the architecture. Redundant components, links, and failover mechanisms are used to minimize downtime.

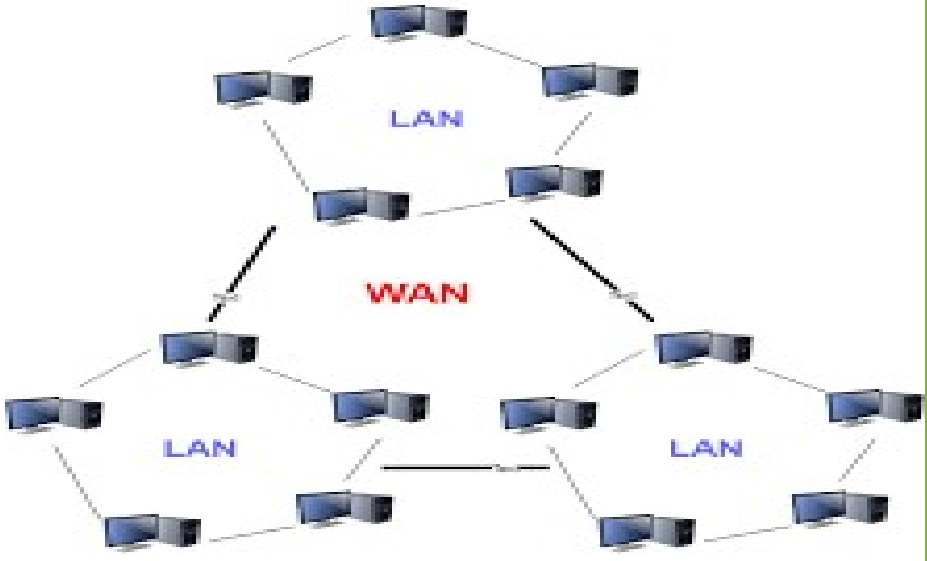
- **Quality of Service (QoS):** In some networks, QoS mechanisms are implemented to prioritize certain types of traffic (e.g., voice or video) to ensure a certain level of performance.
- **Virtualization:** Virtualization technologies allow multiple virtual networks to run on the same physical network infrastructure. This is common in data centers and cloud computing environments.
- **Wireless vs. Wired:** The choice between wireless and wired network architectures depends on factors like mobility requirements, data transfer speeds, and environmental constraints.
- **Cloud Integration:** Modern network architectures often incorporate cloud services and hybrid cloud models, requiring considerations for connectivity to cloud providers and secure data transmission.
- **Monitoring and Management:** Network architecture should include provisions for monitoring network performance, collecting data for analysis, and managing network devices and configurations.

- **Internet of Things (IoT):** IoT devices are integrated into network architectures, requiring special considerations for handling a massive number of connected devices and the associated data traffic.
- **Edge Computing:** Edge computing architectures place computing resources closer to the data source, which requires network design that supports low-latency communication with edge devices.

Type of Computer Network

- **Local Area Network (LAN):**
  - **Scope:** LANs cover a relatively small geographic area, such as a single building, campus, or office.
  - **Purpose:** LANs are used for local data sharing, file storage, printer sharing, and resource sharing within an organization.
  - **Topologies:** LANs can have various topologies, including star, bus, ring, or mesh.
- **Wide Area Network (WAN):**
  - **Scope:** WANs span larger geographic areas, connecting LANs across cities, regions, or even countries.
  - **Purpose:** WANs are used for long-distance data communication, connecting remote offices, branches, and data centers.
  - **Technologies:** WANs often use public or private telecommunications services, including leased lines, MPLS, and the internet.
- **Metropolitan Area Network (MAN):**
  - **Scope:** MANs cover a metropolitan or city-wide area.
  - **Purpose:** MANs provide high-speed connectivity between multiple LANs or data centers within a city.
  - **Examples:** Cable TV networks, city-wide Wi-Fi, and fiber-optic rings.





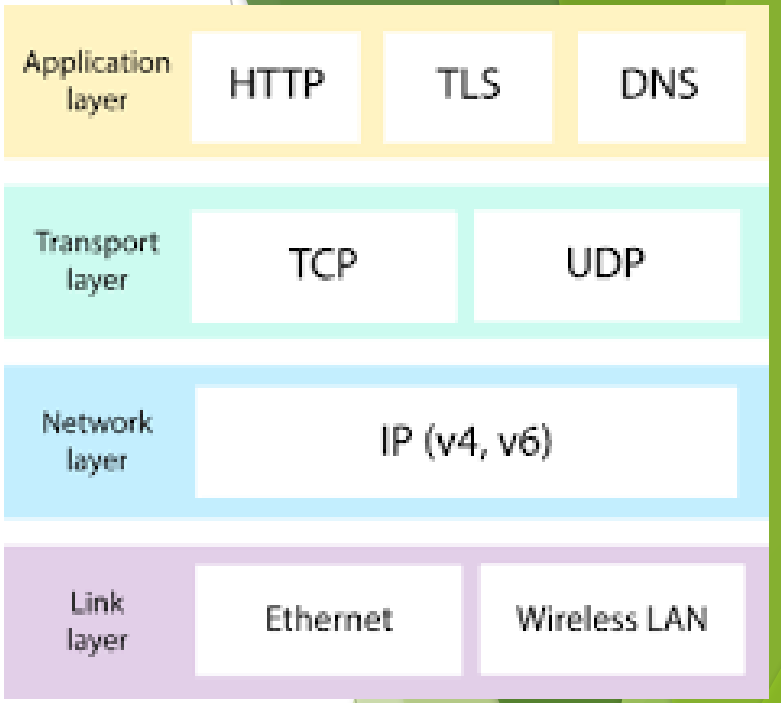
- **Campus Area Network (CAN):**
  - **Scope:** CANs cover a university campus or large corporate campus.
  - **Purpose:** CANs connect multiple buildings within the same campus and facilitate communication between departments or academic units.
- **Storage Area Network (SAN):**
  - **Scope:** SANs are specialized networks designed for high-speed data storage and retrieval.
  - **Purpose:** SANs connect storage devices (e.g., disk arrays, tape libraries) to servers, allowing for efficient and centralized data storage management.
  - **Protocols:** Fibre Channel and iSCSI are common SAN protocols.
- **Virtual Private Network (VPN):**
  - **Scope:** VPNs can operate over LANs, WANs, or the internet.
  - **Purpose:** VPNs provide secure, encrypted communication over untrusted networks, allowing remote users to access private networks or the internet securely.
  - **Types:** Site-to-Site VPNs connect entire networks, while Remote Access VPNs are used by individual users or devices.

- **Wireless Local Area Network (Wi-Fi):**
  - **Scope:** Wi-Fi networks provide wireless connectivity within a limited area, such as homes, offices, or public spaces.
  - **Purpose:** Wi-Fi allows wireless devices to connect to a wired network or the internet without physical cables.
  - **Standards:** Common Wi-Fi standards include 802.11ac (Wi-Fi 5) and 802.11ax (Wi-Fi 6).
- **Cellular Network:**
  - **Scope:** Cellular networks cover large geographic areas and are typically provided by mobile service providers.
  - **Purpose:** Cellular networks enable mobile communication through smartphones and other mobile devices.
  - **Generations:** Cellular networks evolve through generations, such as 2G, 3G, 4G, and 5G, each offering improved speed and capabilities.
- **Peer-to-Peer Network (P2P):**
  - **Scope:** P2P networks can be local or distributed across the internet.
  - **Purpose:** P2P networks allow devices to communicate directly with each other without the need for central servers, often used for file sharing (e.g., BitTorrent).

- **Internet of Things (IoT) Network:**
  - **Scope:** IoT networks connect a vast number of devices and sensors to the internet.
  - **Purpose:** IoT networks enable data collection, monitoring, and control of various smart devices, from appliances to industrial machines.
- **Cloud Network:**
  - **Scope:** Cloud networks refer to the interconnected infrastructure of cloud service providers.
  - **Purpose:** Cloud networks support the delivery of cloud-based services and applications to users and organizations.
- **Sensor Network:**
  - **Scope:** Sensor networks consist of distributed sensors and actuators.
  - **Purpose:** Sensor networks are used for environmental monitoring, surveillance, and data collection in various applications, including agriculture and healthcare.

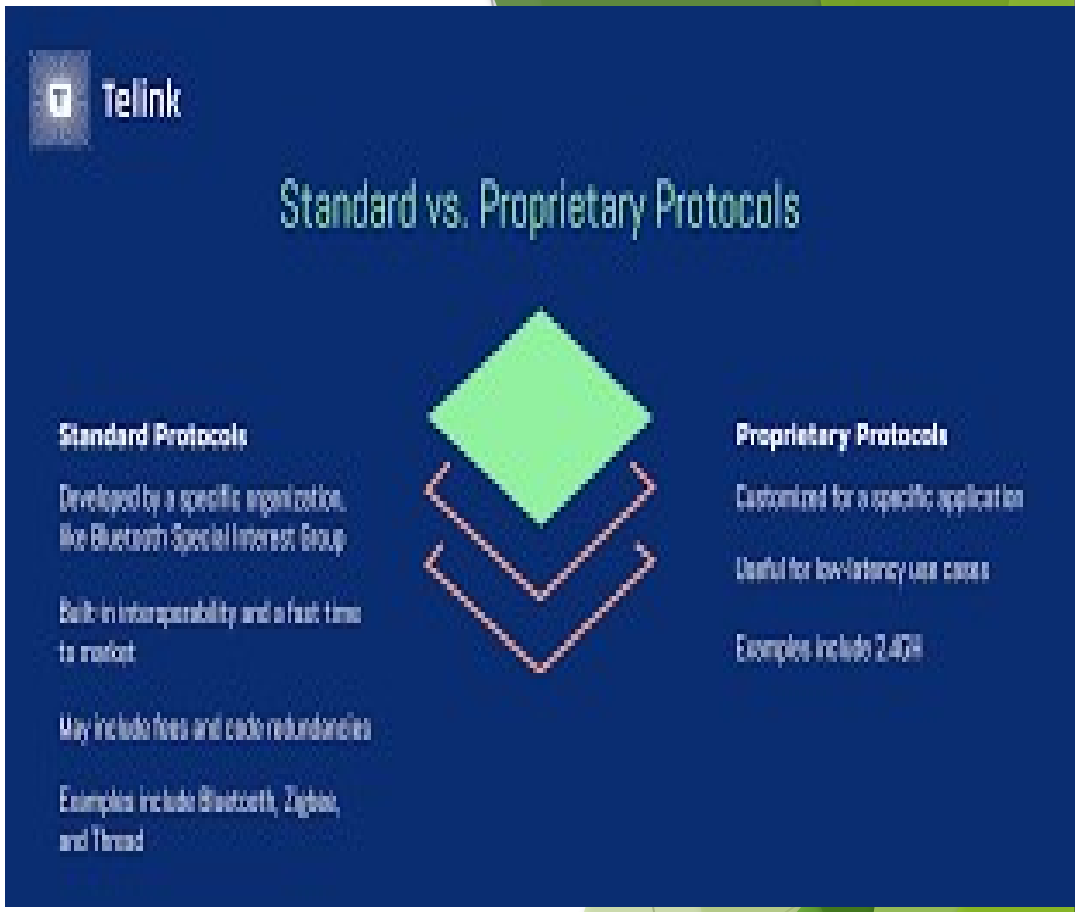
protocol and standards

- Protocols and standards are essential components of computer networks and the broader field of information technology. They ensure interoperability, reliability, and consistency in data communication and system interaction.
- **Definition:** A protocol is a set of rules and conventions that govern how data is formatted, transmitted, received, and processed in a computer network or communication system. Protocols ensure that devices and systems can understand each other and exchange data effectively.
- **Role:** Protocols define the rules for various aspects of communication, including data encoding, error detection and correction, addressing, routing, and the establishment and termination of connections.
- **Examples:** Some common network protocols include:
  - **Transmission Control Protocol (TCP):** Ensures reliable, connection-oriented data transfer, commonly used for web browsing, email, and file transfer.
  - **Internet Protocol (IP):** Provides addressing and routing functions to enable data packets to traverse a network.
  - **Hypertext Transfer Protocol (HTTP):** Governs the transfer of web pages and resources on the World Wide Web.
  - **Simple Mail Transfer Protocol (SMTP):** Manages the sending of email messages.
  - **File Transfer Protocol (FTP):** Facilitates the transfer of files between computers.
  - **Post Office Protocol (POP) and Internet Message Access Protocol (IMAP):** Used for email retrieval.



Standards

- **Definition:** Standards are formalized specifications or criteria that define how products, processes, and systems should be designed, operated, and tested. They establish common ground for quality, safety, interoperability, and performance.
- **Role:** Standards provide a common framework for manufacturers, developers, and organizations to ensure that their products or systems meet certain requirements and can work together seamlessly.
- **Importance:** Standards are crucial for several reasons:
  - **Interoperability:** Standards enable products from different manufacturers to work together, fostering compatibility and choice.
  - **Quality Assurance:** Standards set minimum quality and performance levels, helping ensure product reliability and safety.
  - **Globalization:** In a global economy, standards facilitate trade by providing a common language and set of expectations.
  - **Regulation:** Many industries are subject to regulations that require adherence to specific standards to ensure safety and compliance.

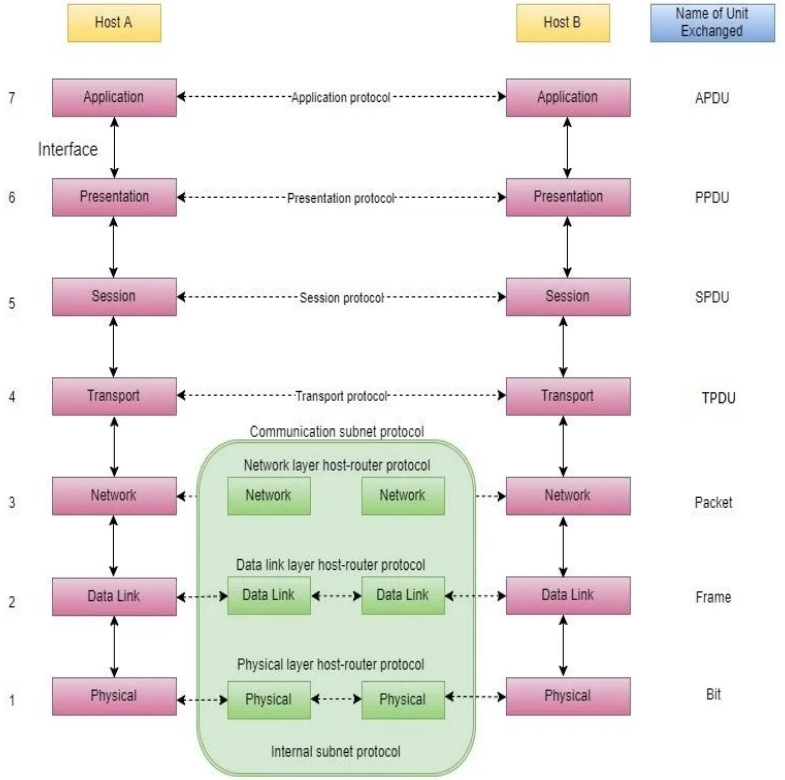


- **Examples:** Various industries have their own sets of standards. In information technology and networking, some notable standards organizations and examples include:
- **IEEE (Institute of Electrical and Electronics Engineers):** Develops standards for networking, wireless communication, and various other technology fields.
- **ISO (International Organization for Standardization):** Publishes a wide range of standards, including those for data security (e.g., ISO 27001), quality management (e.g., ISO 9001), and information technology (e.g., ISO 9000 series).
- **IETF (Internet Engineering Task Force):** Focuses on developing and promoting internet-related standards, including those for internet protocols and technologies.
- **W3C (World Wide Web Consortium):** Develops standards for web technologies, such as HTML, CSS, and XML.

The OSI Reference Model

7. Application	• Provides a user interface
6. Presentation	• Presents Data • Handles encryption and decryption
5. Session	• Maintains distinction between data of separate applications • Provides dialog control between hosts
4. Transport	• Provides End-to-End connections • Provides reliable or unreliable delivery and flow control
3. Network	• Provides Logical Addressing • Provides Path determination using logical addressing
2. Data Link	• Provides media access and physical addressing
1. Physical	• Converts digital data so that it can be sent over the physical medium • Moves data between hosts

7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

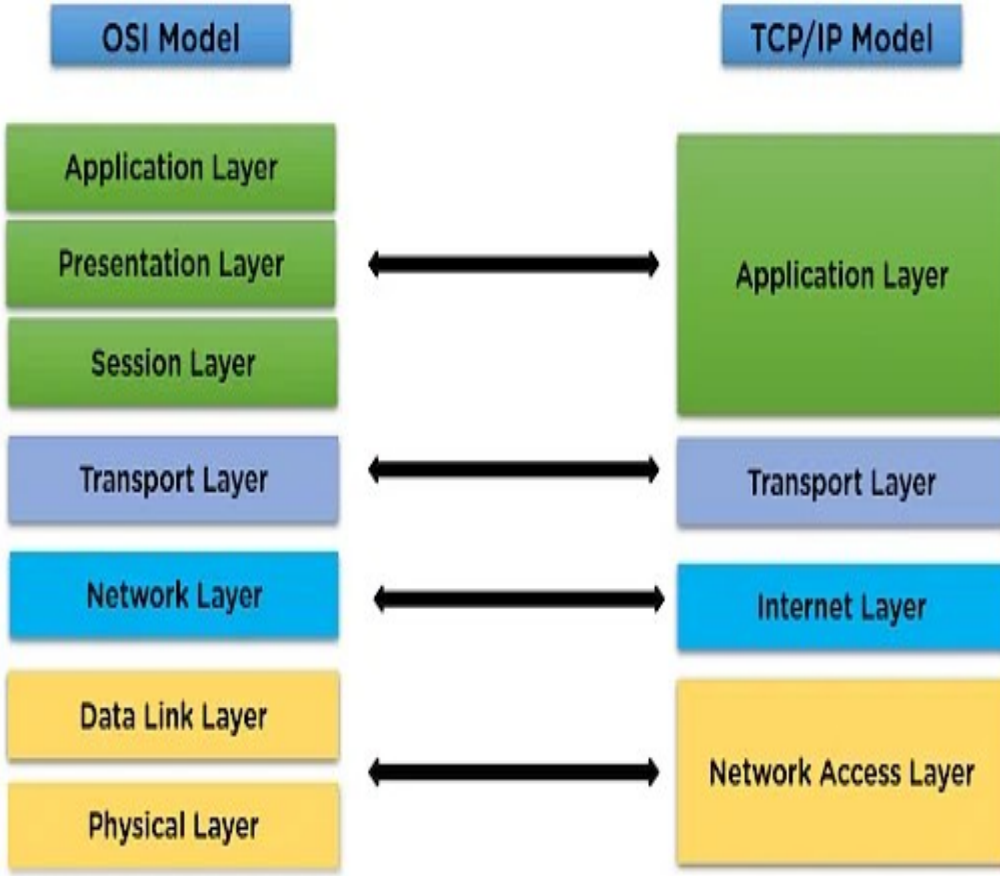


TCP/IP Protocol

The TCP/IP Protocol Suite

Chapter 3

- The TCP/IP protocol suite is a network model with four layers: *Application, Transport, Internetwork, and Network Interface*. These layers correspond to the layers in the OSI reference model.
- A series of documents called *RFCs* define, describe, and standardize the implementation and configuration of the TCP/IP protocol suite. The *InterNIC* is responsible for maintaining these standards.
- Notice in the next slide that the *Application* layer and the *Network Interface* layer of the TCP/IP model support multiple functions that require five different layers in the OSI reference model.



Difference Between Tcp/IP and OSI

TCP/IP	OSI
Implementation of OSI model	Reference model
Model around which Internet is developed	This is a theoretical model
Has only 4 layers	Has 7 layers
Considered more reliable	Considered a reference tool
Protocols are not strictly defined	Stricter boundaries for the protocols
Horizontal approach	Vertical approach
Combines the session and presentation layer in the application layer	Has separate session and presentation layer
Protocols were developed first and then the model was developed	Model was developed before the development of protocols
Supports only connectionless communication in the network layer	Supports connectionless and connection-oriented communication in the network layer
Protocol dependent standard	Protocol independent standard InstrumentationTools.com

Critique

OSI

- Bad timing, by the time the OSI protocols appeared, the competition TCP/IP protocols were already in widespread use.
- Bad technology, both the model and the protocols are flawed, the model along with the associated service definitions and protocols are very complex.

TCP/IP

- The model does not clearly distinguish the concepts of services, interface, and protocol.
- It is not at all general and is poorly suited to describing any protocol stack other than TCP/IP.