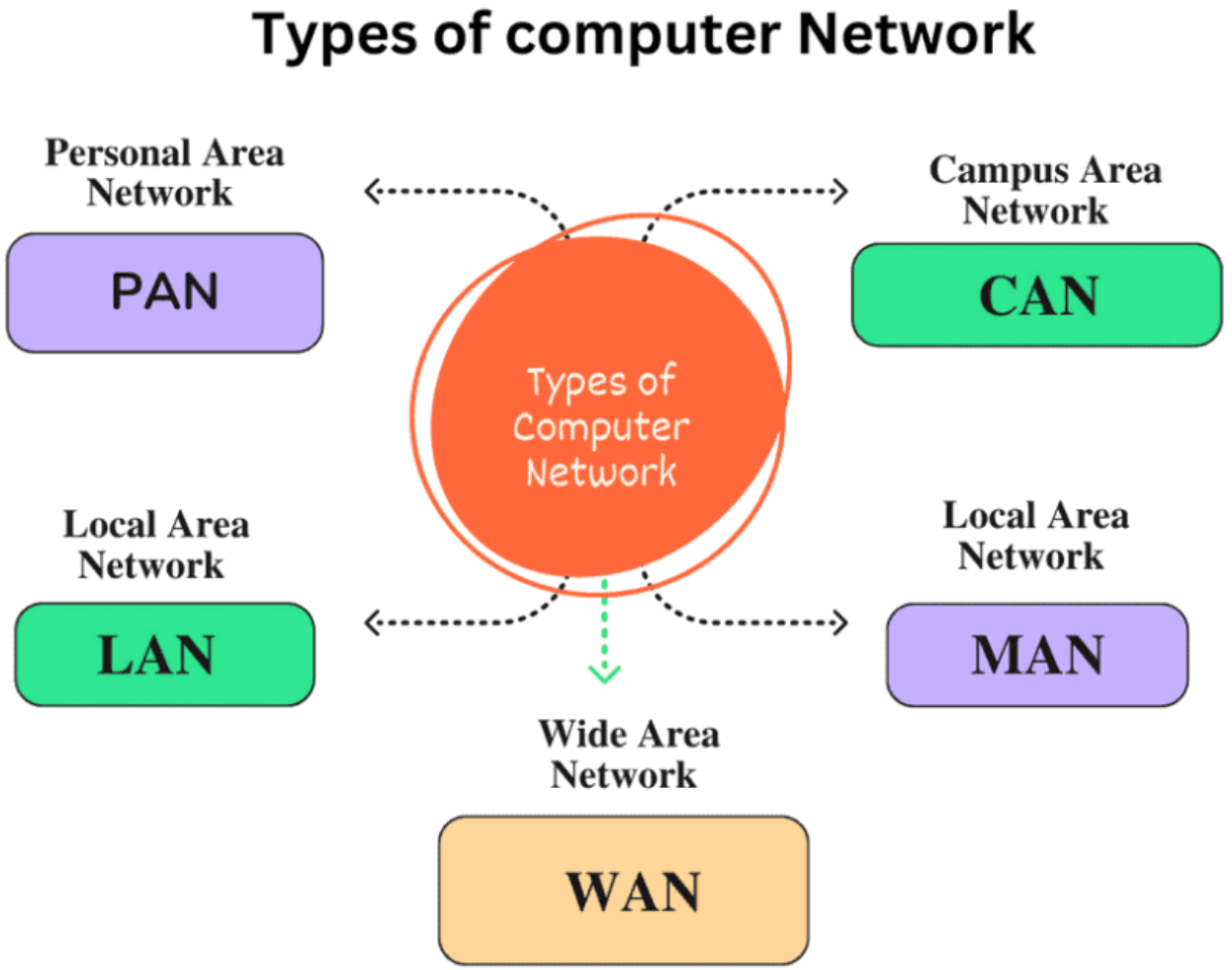
Computer Network

Computer networks are groups of computers linked together to share resources and information. These resources can include hardware devices like printers, data storage, or software applications. Networks can be wired or wireless, and they can be private (like a home network) or public (like the internet)

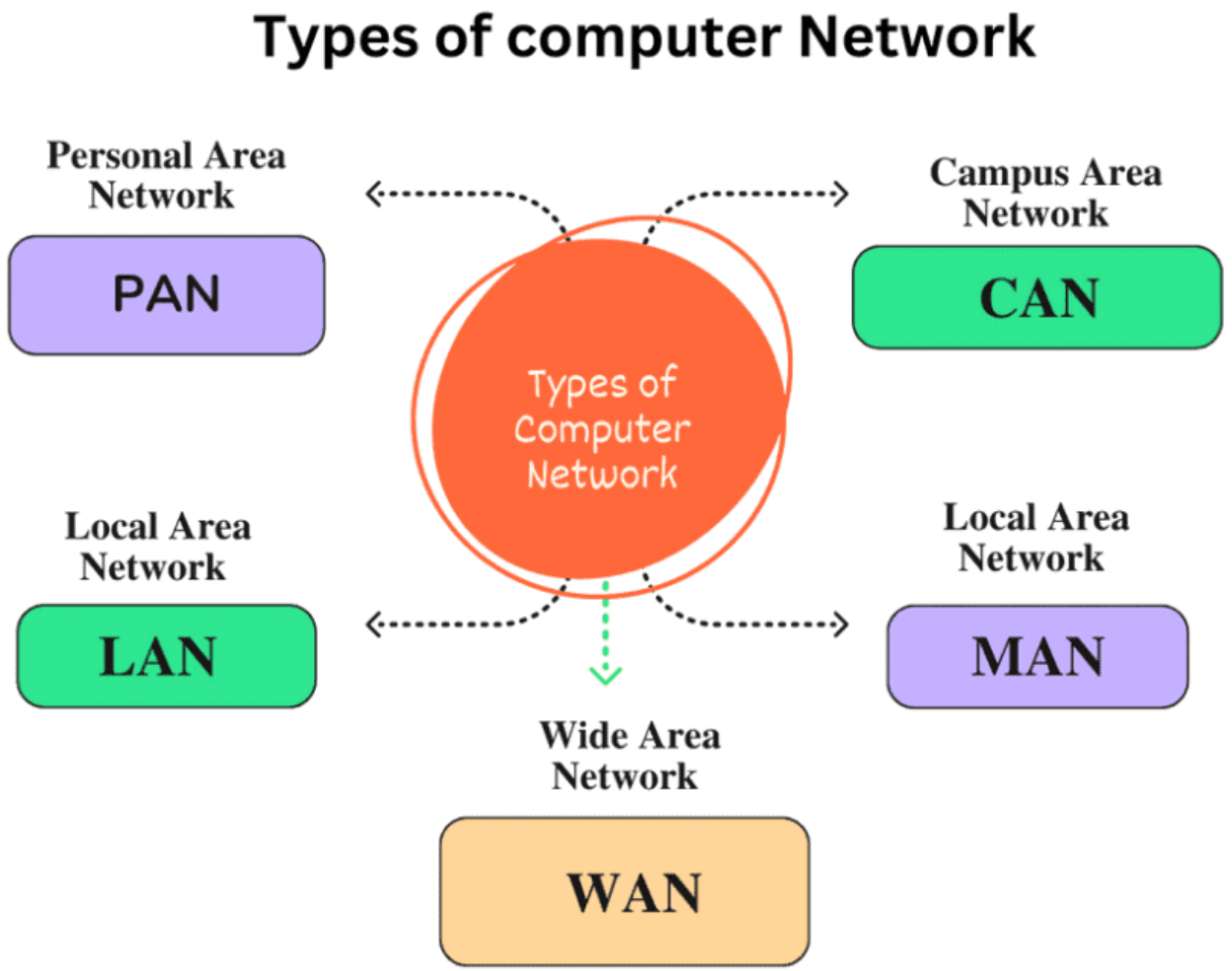
Types Of Computer Network

- **PAN**:
  - Size: Covers a very small geographical area, typically within a few meters of a person.
  - Speed: Can vary depending on the technology used (Bluetooth, Wi-Fi).
  - Privacy: Limited range ensures a relatively private connection.
  - Use: Connects personal devices like smartphones, laptops, printers, and headsets for data sharing and communication within a short range.



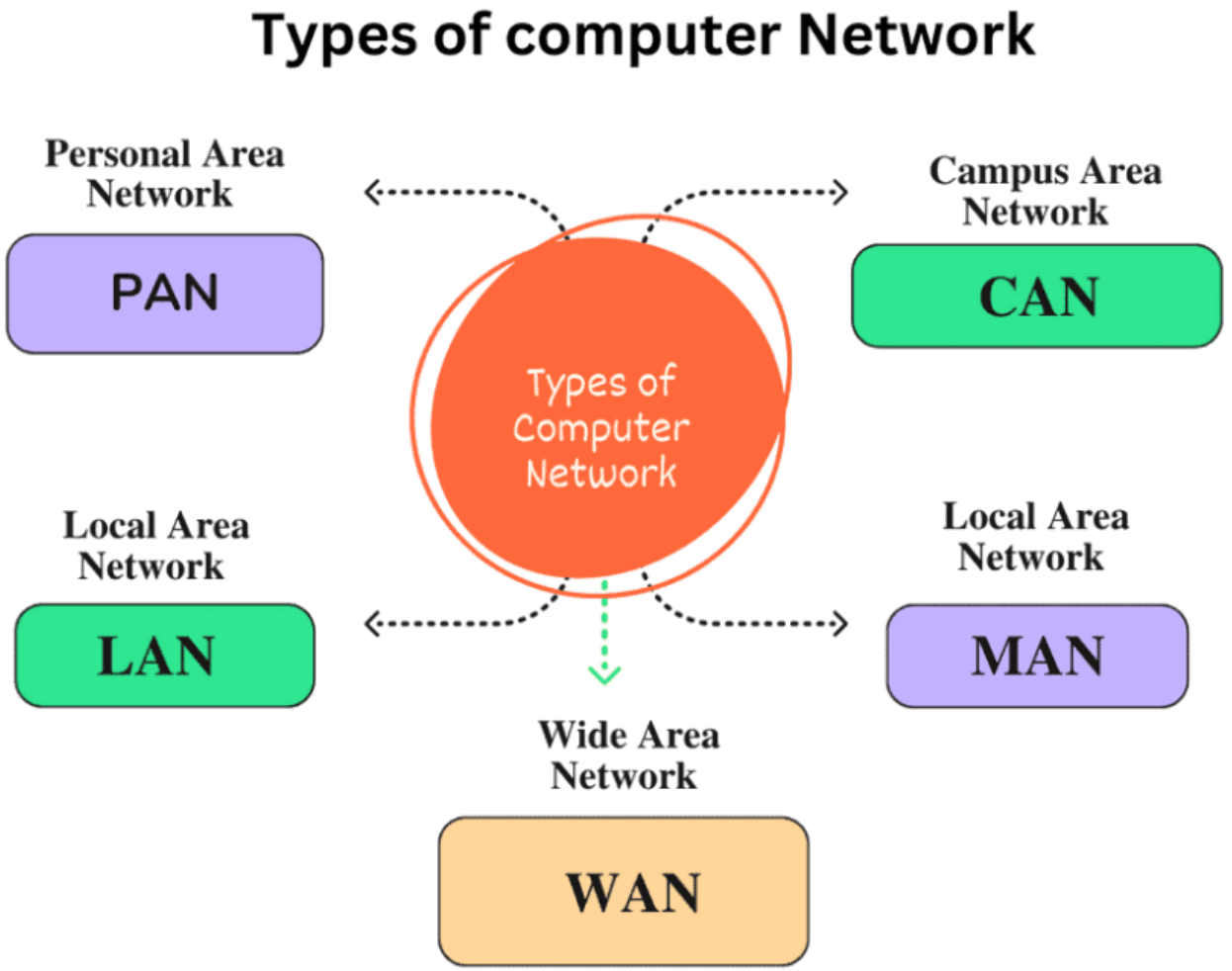
Types Of Computer Network

- **LAN**:
  - Size: Covers a limited geographical area, typically a home, office building, or school campus.
  - Speed: Offers high-speed connections, often using Ethernet cables or Wi-Fi.
  - Privacy: Private network, not accessible to the general public.
  - Use: Ideal for sharing resources like printers, files, and internet access among a small group of devices.



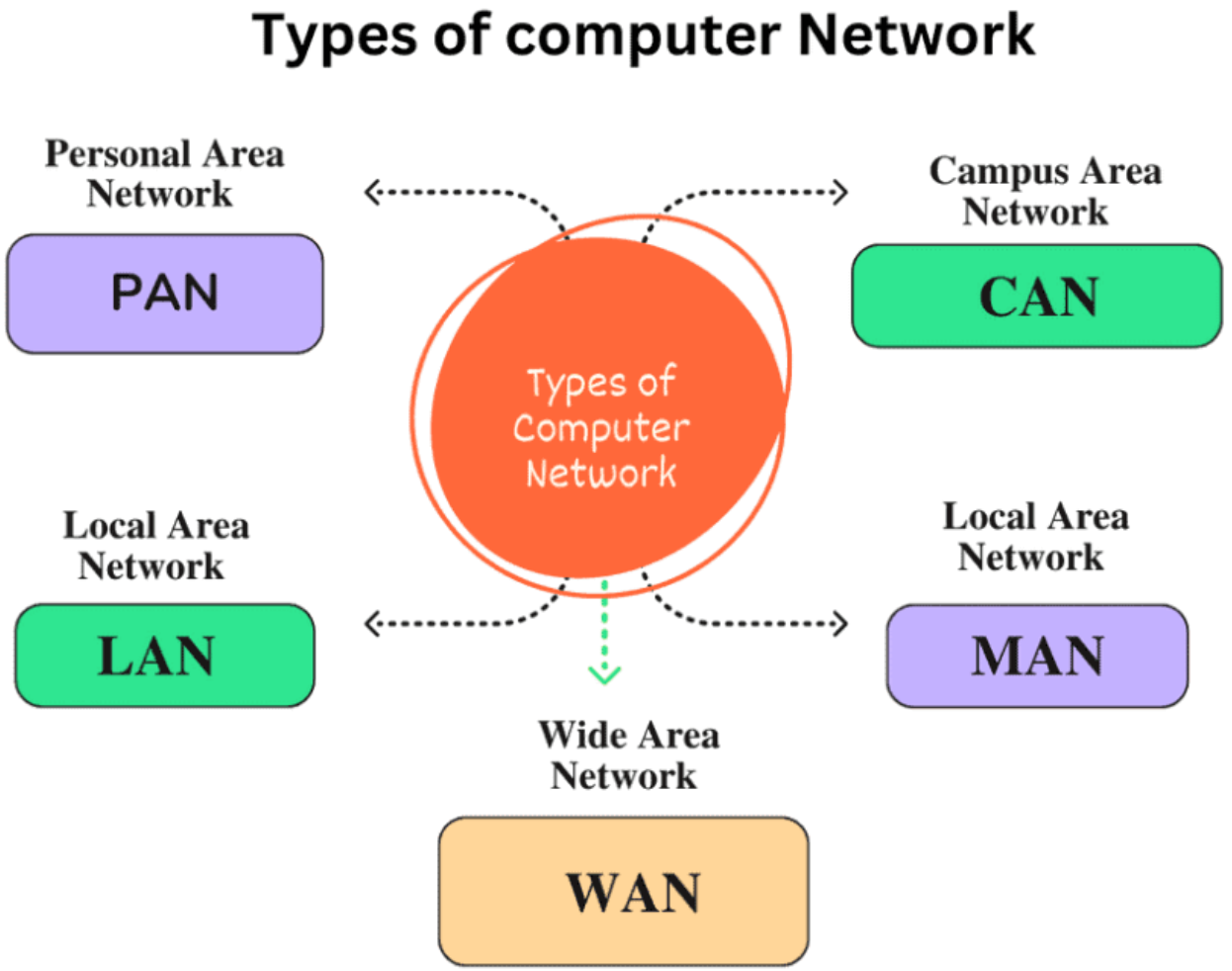
Types Of Computer Network

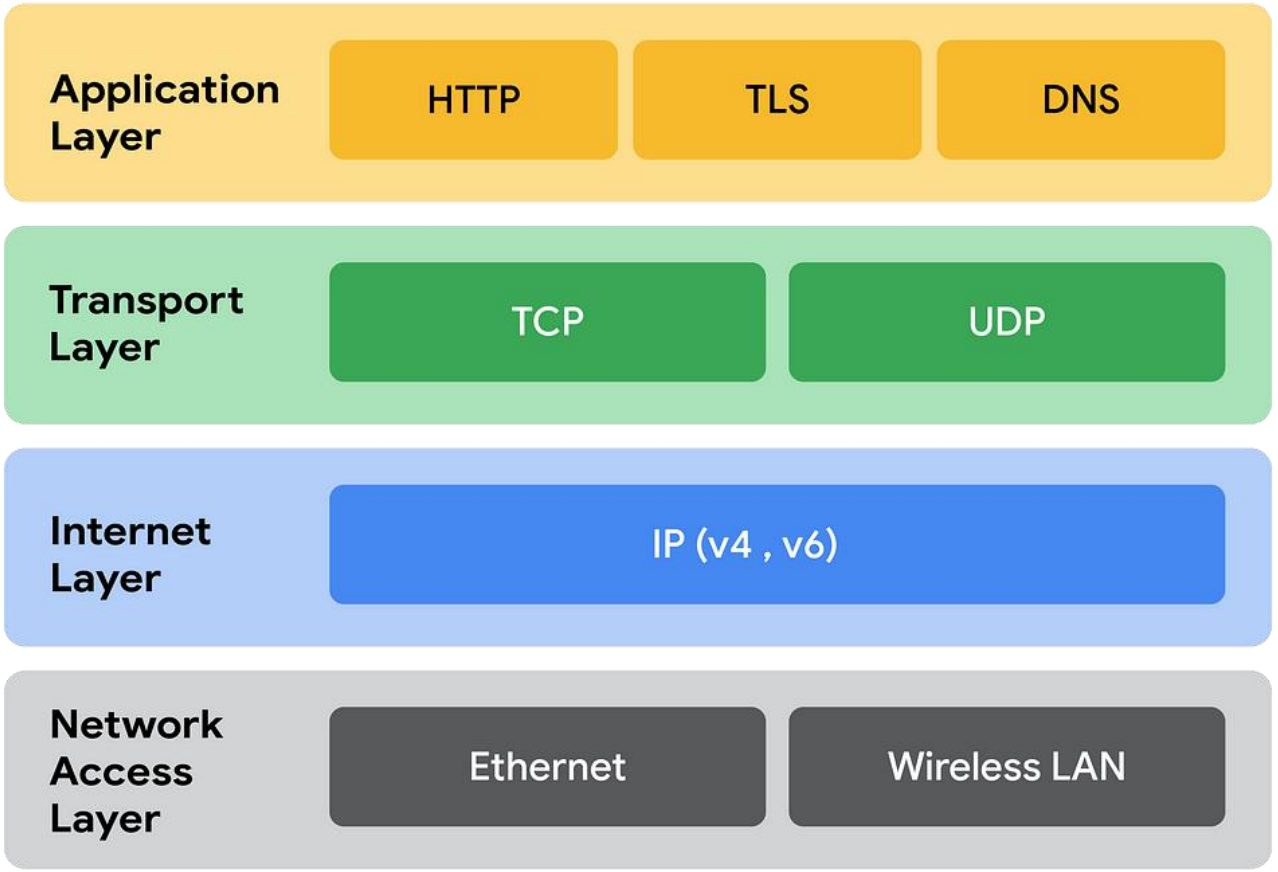
- **MAN** :
  - Size: Covers a larger geographical area than a LAN, typically a city or a large campus.
  - Speed: Offers high-speed connections, often using fiber optic cables or microwave links.
  - Privacy: Can be private or connect multiple private LANs.
  - Use: Connects different LANs within a city, enabling resource sharing and communication between organizations.



Types Of Computer Network

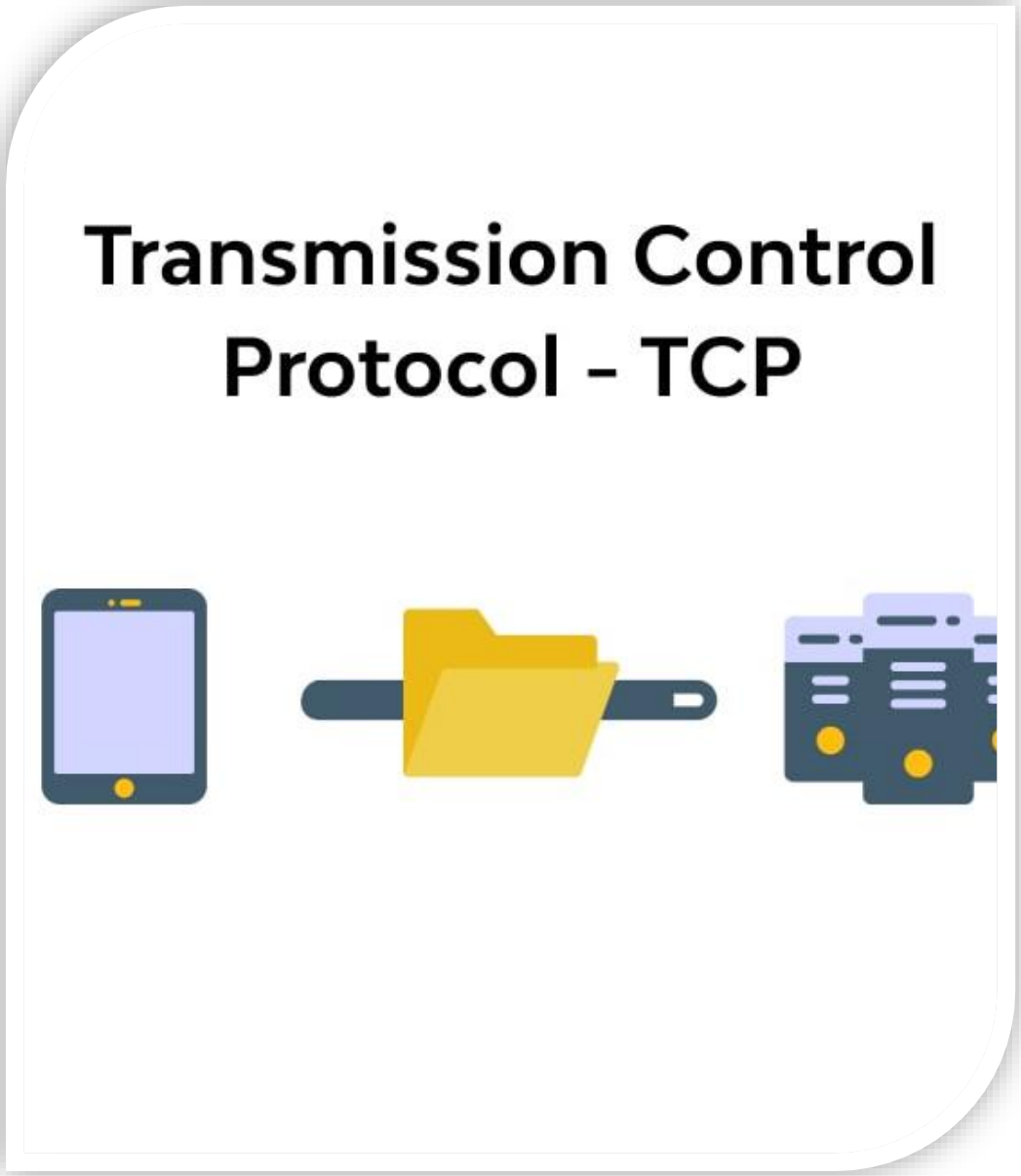
- **WAN** :
  - Size: Spans a large geographical area, covering countries or even the entire globe.
  - Speed: Slower than LANs and MANs due to the vast distances involved.
  - Privacy: Can be private (like a corporate network) or public (like the internet).
  - Use: Connects geographically distant LANs and MANs, allowing for long-distance communication and resource sharing across vast areas





TCP/IP

TCP/IP, which stands for Transmission Control Protocol/Internet Protocol, is the foundation of communication on the internet. It's a suite of protocols that defines how data is transmitted between devices on a network. Here's a breakdown of its key components:



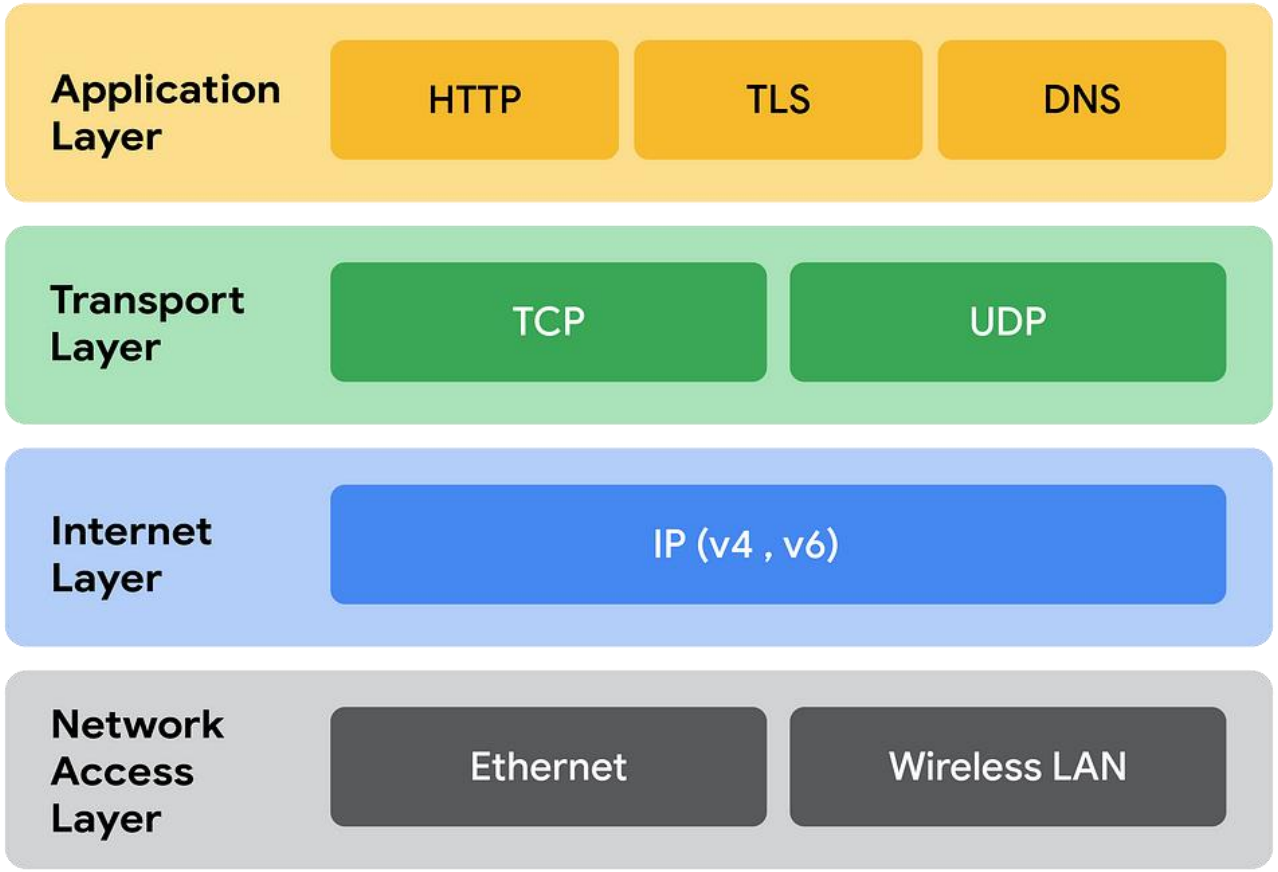
1. Transmission Control Protocol (TCP):

Function: Ensures reliable data delivery.

How it works: Breaks down data into packets, assigns sequence numbers, and acknowledges receipt to guarantee complete and error-free transfer.

Analogy: Imagine sending a long letter by certified mail. Each page is numbered, and you receive confirmation for each received page.

2. Internet Protocol (IP):

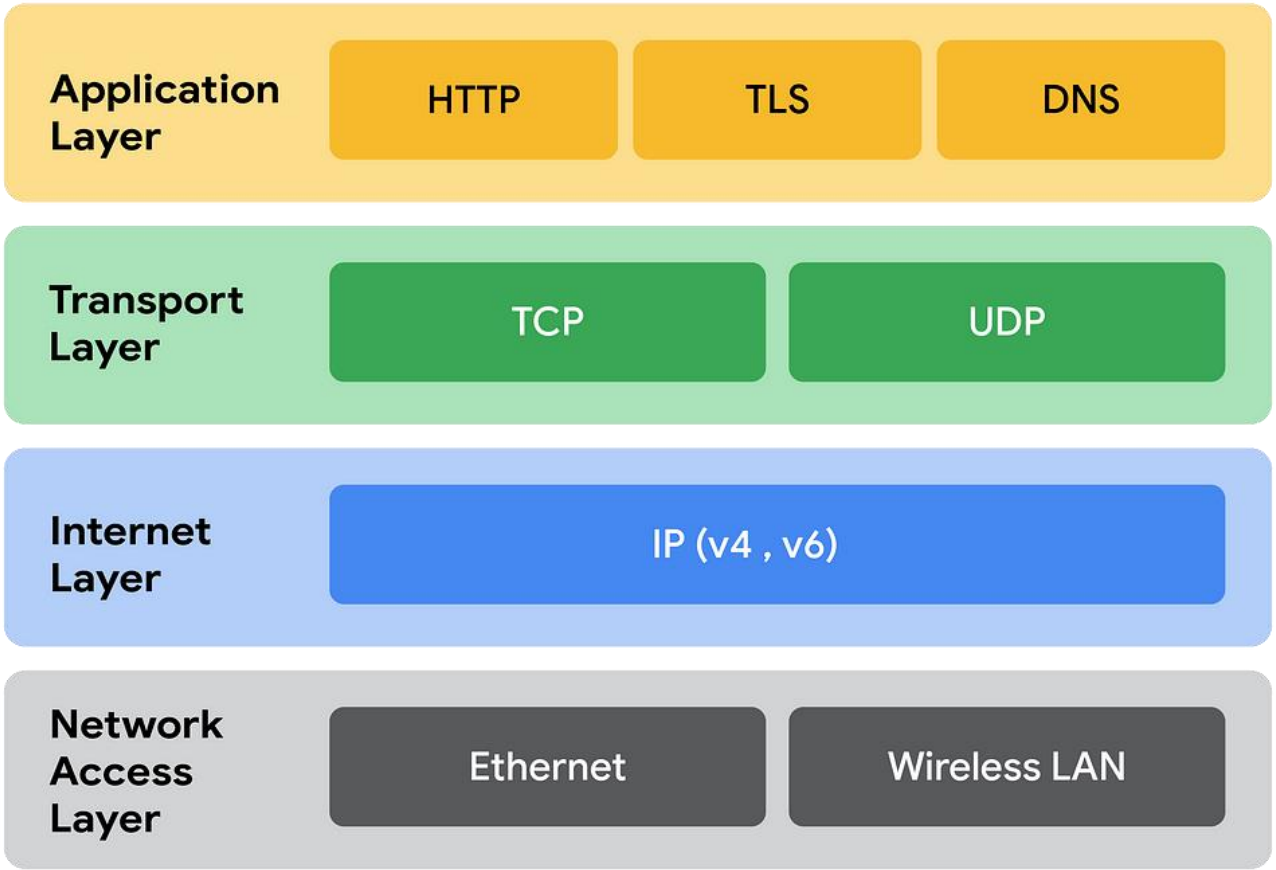


Function: Handles addressing and routing of data packets.

How it works: Assigns a unique IP address (like a house address) to each device on the network. Packets include the sender's and receiver's IP address, allowing routers to direct them to the correct destination.

Analogy: Each house on a street has a unique address. When you mail a letter, you write the recipient's address on the envelope to ensure it reaches the right place.

3. Additional Protocols:

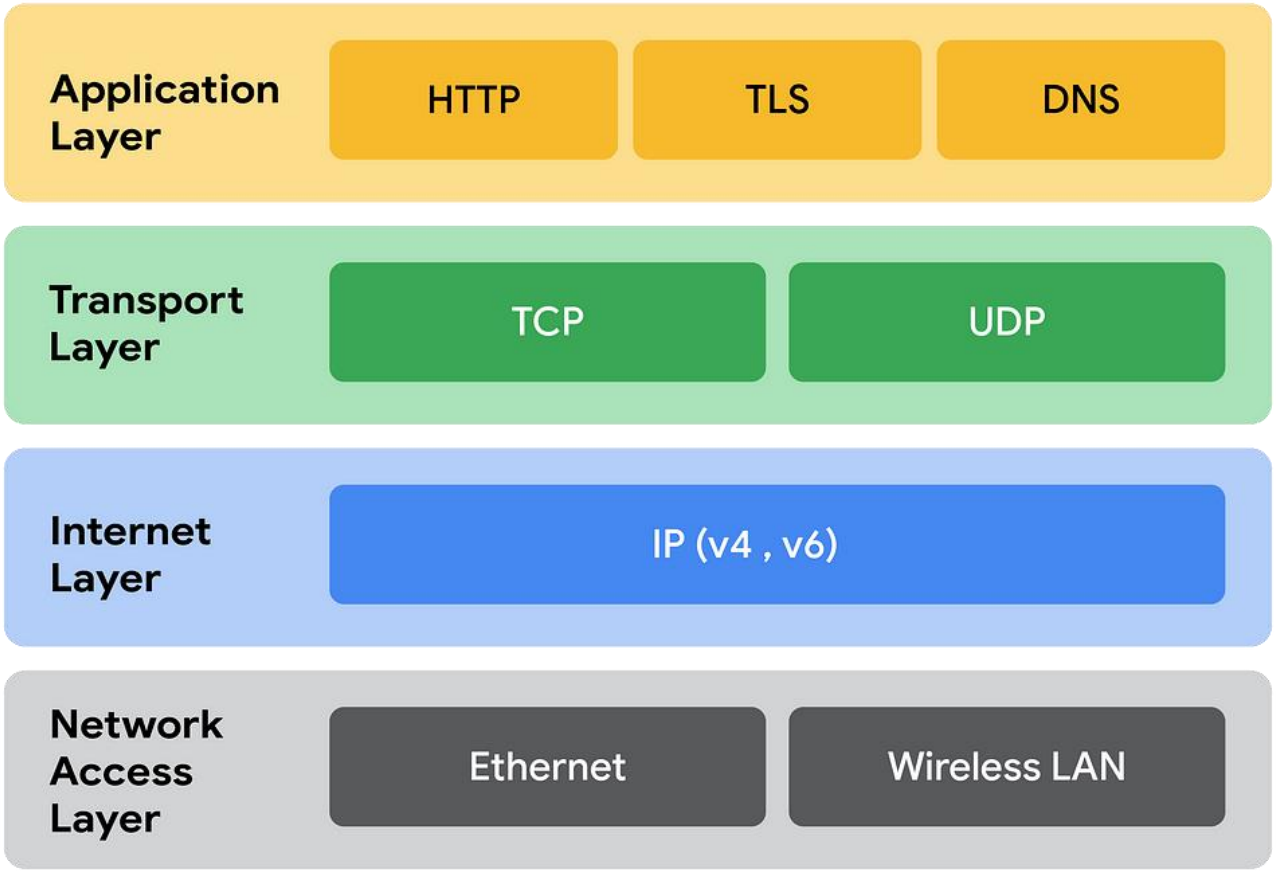


Standardized: Universally used, allowing devices from different vendors to communicate seamlessly.

Modular: Different protocols handle specific tasks, making the system flexible and scalable.

Reliable: TCP ensures data integrity and retransmission in case of errors.

Connectionless: Devices don't need a persistent connection, making it efficient for short data exchanges.



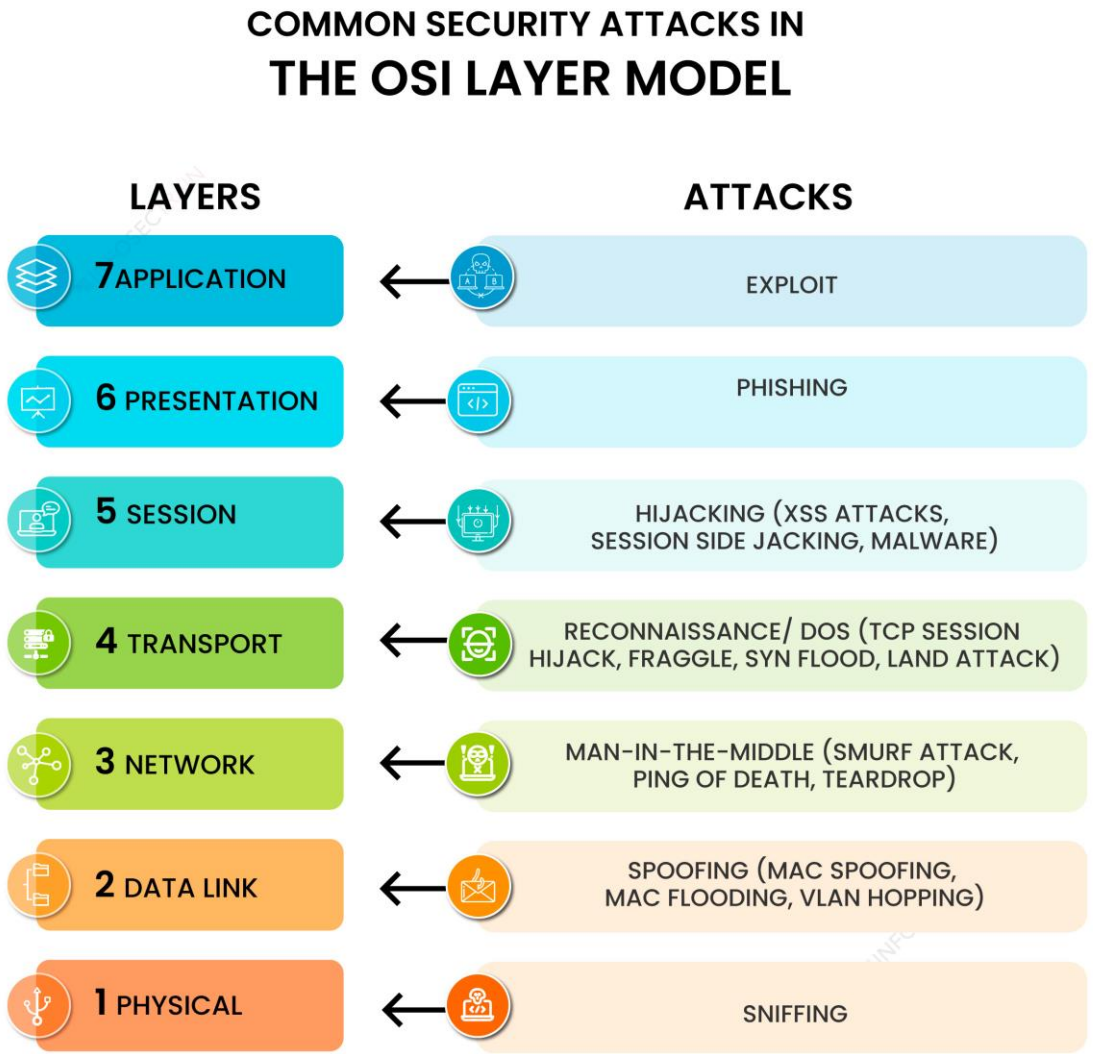
Benefits of TCP/IP:

Standardized: Universally used, allowing devices from different vendors to communicate seamlessly.

Modular: Different protocols handle specific tasks, making the system flexible and scalable.

Reliable: TCP ensures data integrity and retransmission in case of errors.

Connectionless: Devices don't need a persistent connection, making it efficient for short data exchanges.



OSI Model Layer

The OSI Model, also known as the Open Systems Interconnection model, is a conceptual framework used to describe how data is transmitted over a network. It's a layered approach that breaks down the communication process into seven distinct layers, each with a specific function. Here's a breakdown of each layer:

- Layer 1: Physical Layer

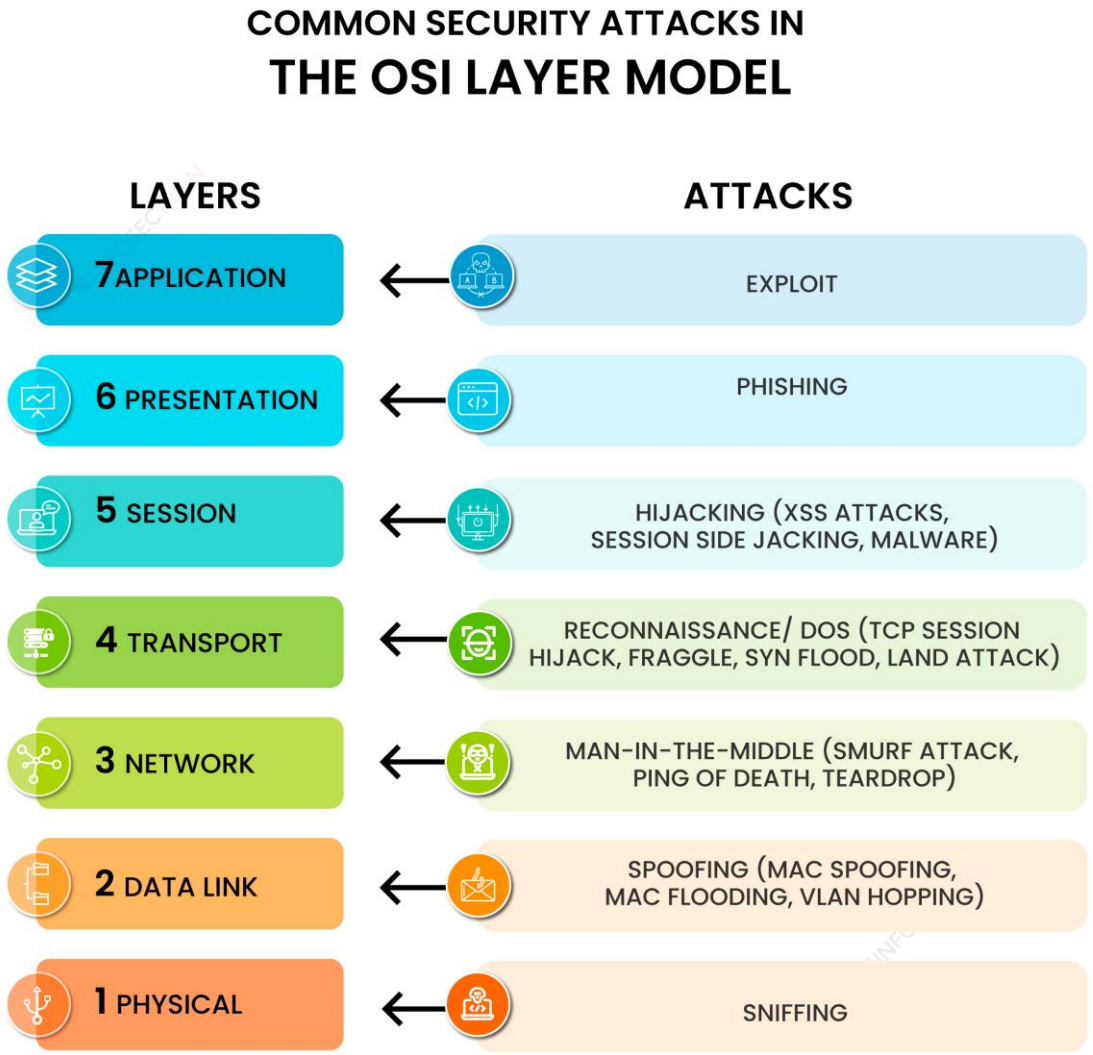
  Function: Transmits data bits across a physical medium like cables or wireless signals.

- Layer 2: Data Link Layer

  Function: Ensures error-free data transmission between directly connected devices.

- Layer 3: Network Layer

Function: Routes data packets across networks by determining the best path to the destination.



OSI Model Layer

- Layer 4: Transport Layer

  Function: Provides reliable data transfer between applications on different devices.

- Layer 5: Session Layer

  Function: Establishes, manages, and terminates sessions between communicating applications.

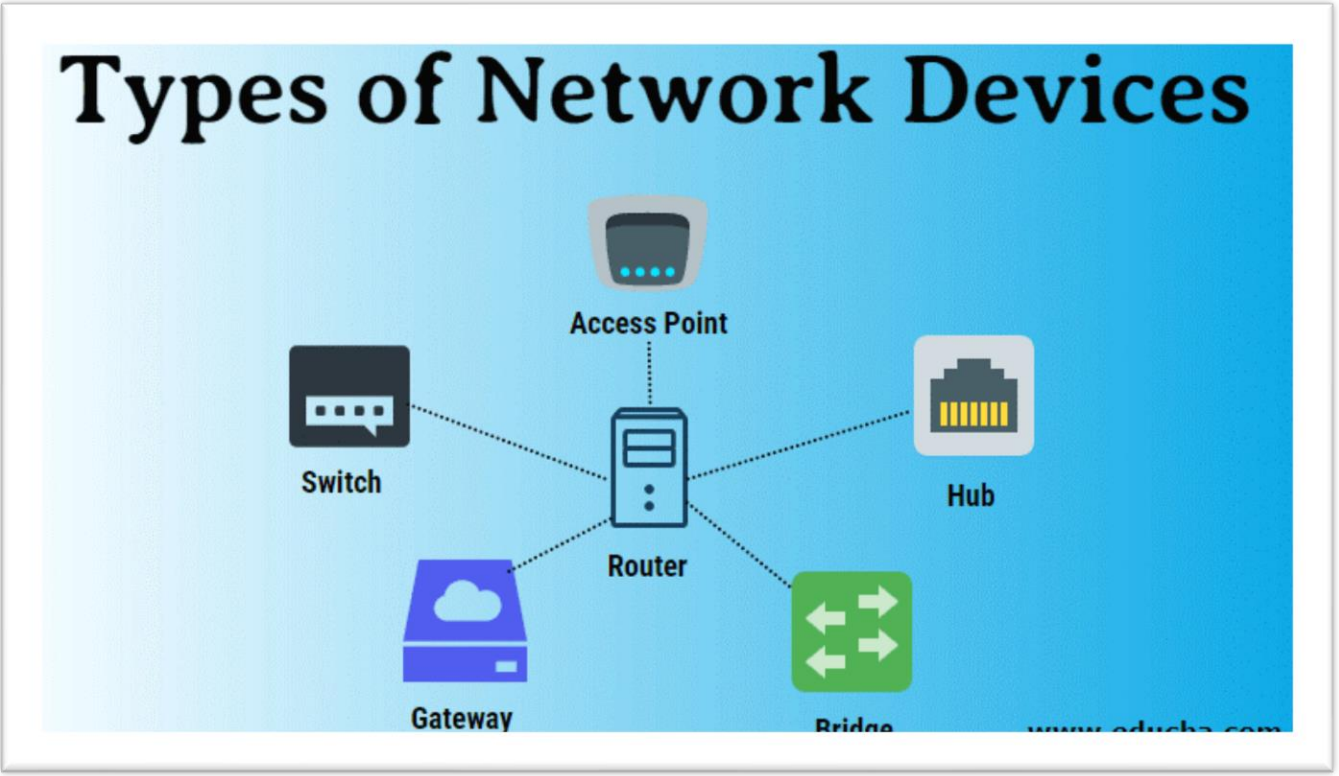
- Layer 6: Presentation Layer

  Function: Prepares data for the application layer by handling data encryption, compression, and formatting.

- Layer 7: Application Layer

  Function: Provides network services directly to user applications.

Network Devices



Switch : Connects multiple devices on a network segment, learning their MAC addresses for efficient data forwarding.

Acts like a traffic director, sending data packets to the specific intended recipient on the network.

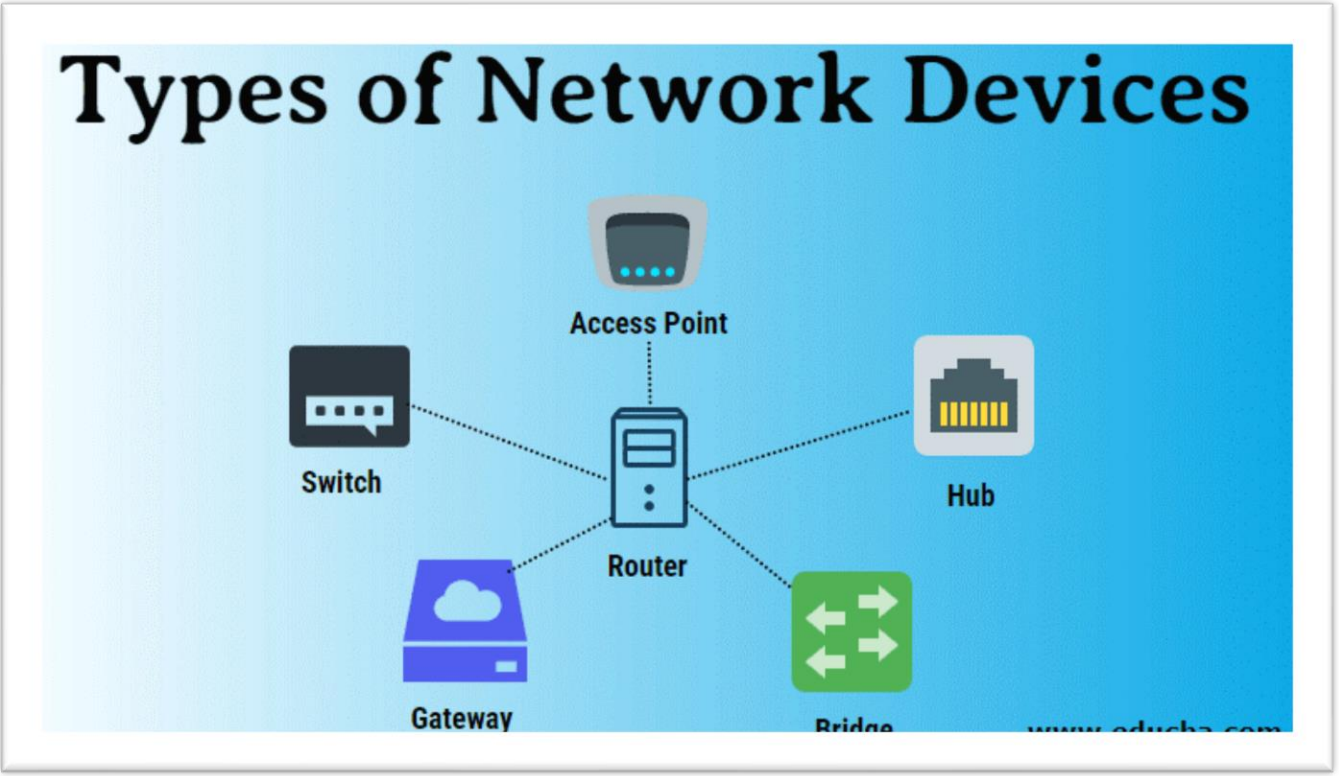
Improves network performance by reducing congestion compared to hubs.

Router : Connects different networks and directs data packets based on their IP addresses.

Acts like a smart traffic controller, determining the best path for data to reach its destination across different networks (like the internet).

Provides internet access to devices on a local network by connecting to an internet service provider (ISP).

Network Devices



Modem : Modulates and demodulates signals, allowing communication between a network and devices using different languages.

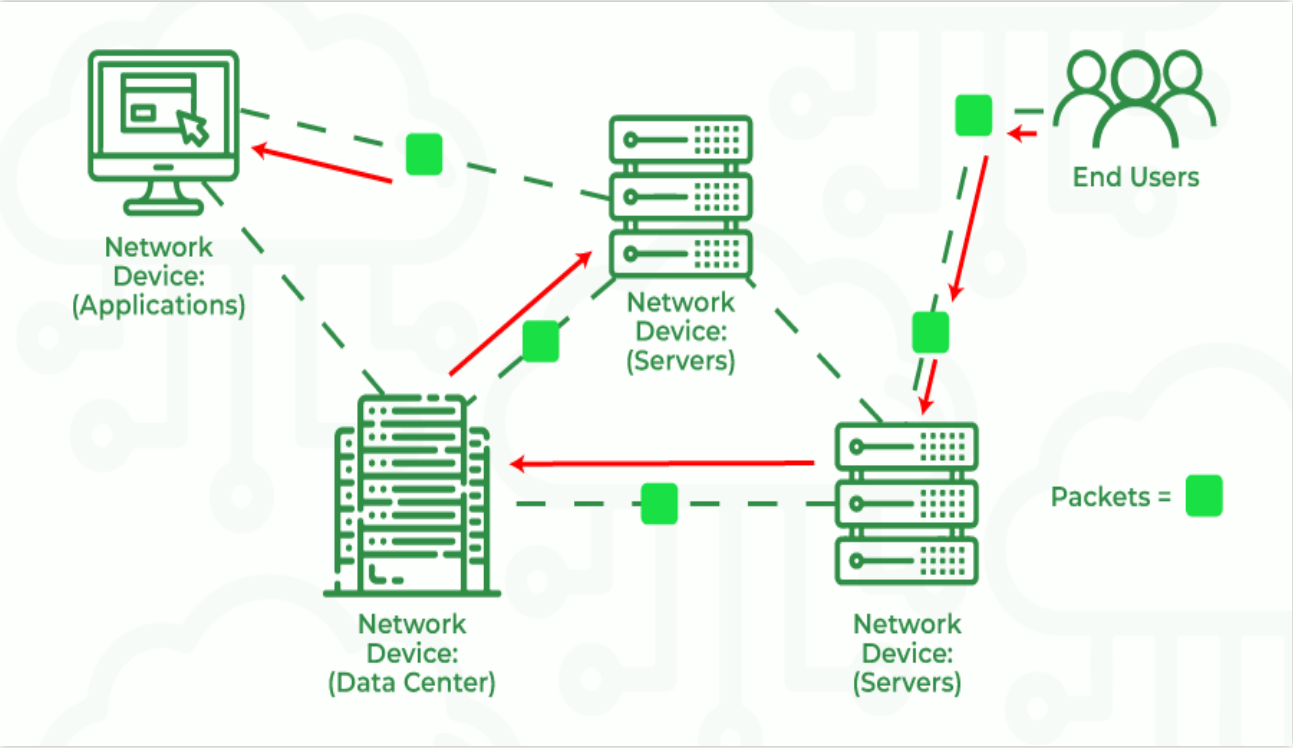
Often used to connect a home network to an ISP by converting digital data from computers into a format suitable for transmission over cable or phone lines.

Access Point (AP) : Creates a wireless local area network (WLAN) by providing Wi-Fi connectivity to devices.

Acts as a central hub for wireless devices to connect and communicate with the wired network.

Often used in homes, offices, and public places to enable Wi-Fi access.

Switching



In computer networking, switching is the process of forwarding data packets to their intended destinations on a network. It's done by network switches, which are hardware devices that connect multiple devices on a network segment.

How does Switching Work?

1. Devices connect to a switch using cables.
2. The switch learns the MAC addresses of connected devices.
3. When a device sends data, the switch forwards it to the destination port based on the MAC address.

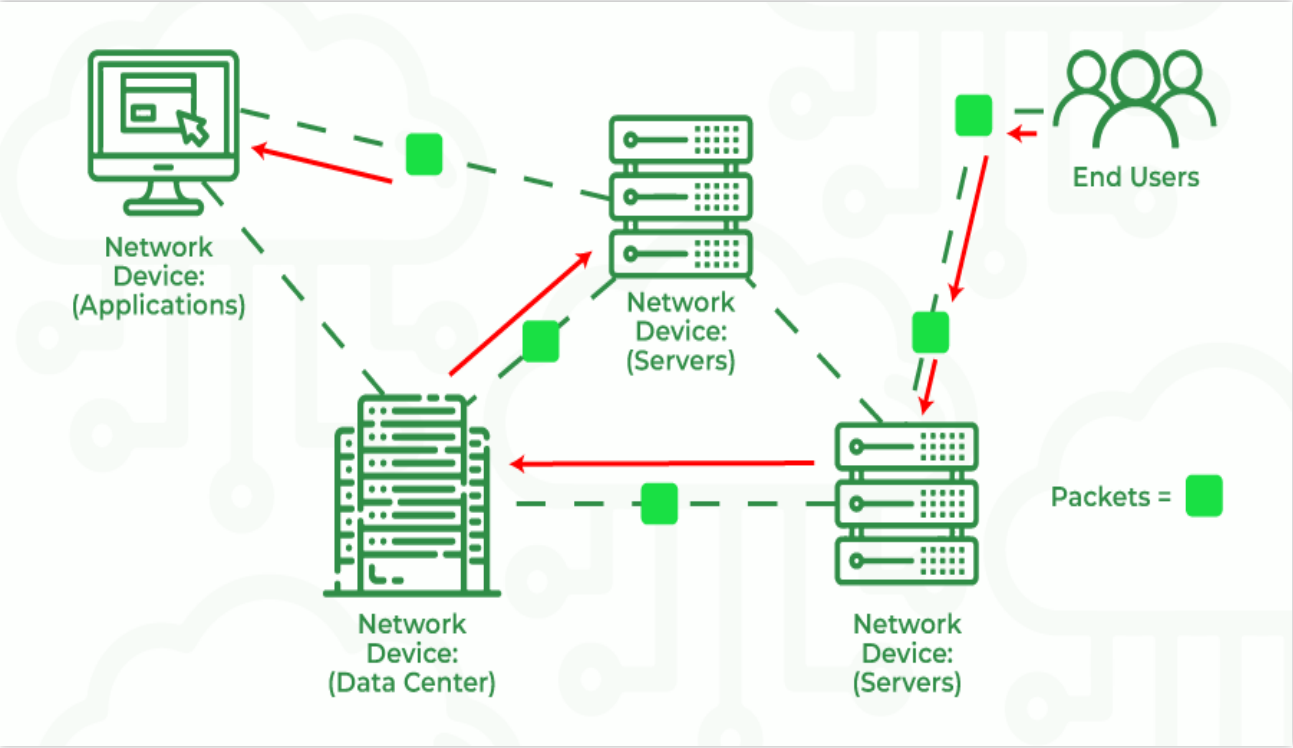
Benefits of Switching:

Reduced congestion

Improved security

Scalability

Switching



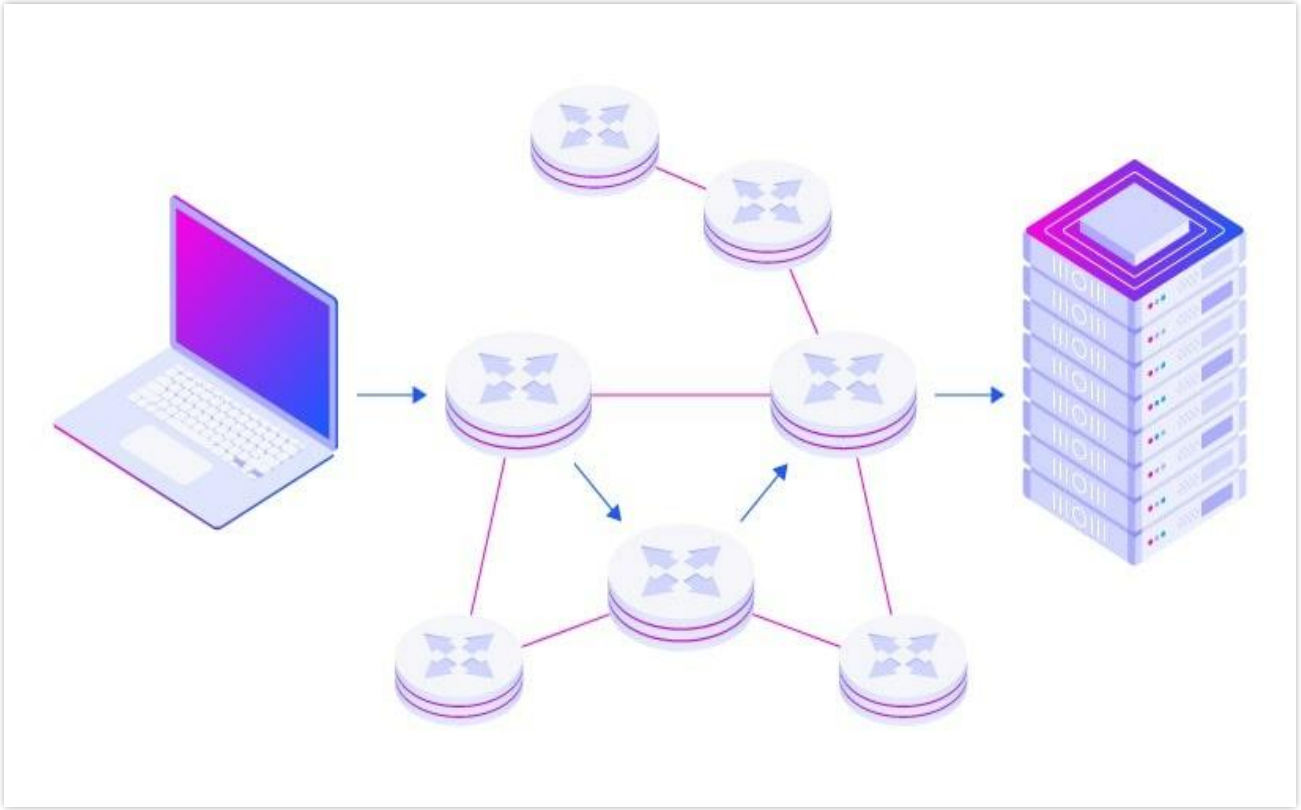
Types of Switching:

- Store-and-forward
- Cut-through
- Content-addressable memory (CAM)

Applications of Switching:

- LANs
- VLANs
- Data centers

Routing

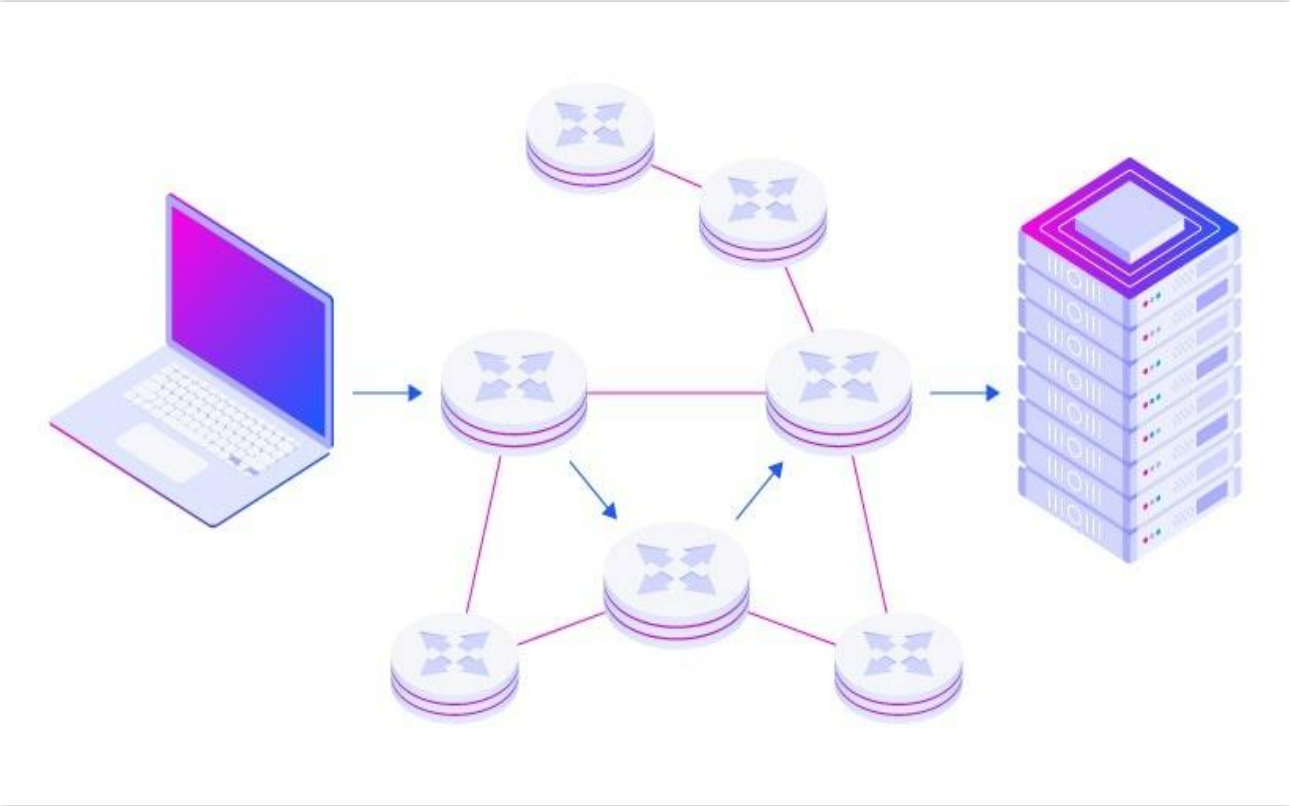


Routing is the process of directing data packets to their intended destinations on a network. It's done by routers, which are devices that connect networks and forward packets based on their IP addresses.

How does Routing Work?

1. Data is broken down into packets, each with a destination IP address.
2. Routers use routing protocols to share information about network paths.
3. Routers choose the best path for each packet based on factors like congestion and distance.
4. Routers forward packets to the next hop on the chosen path.

Routing



Benefits of Routing:

- Efficient data delivery
- Scalability
- Fault tolerance

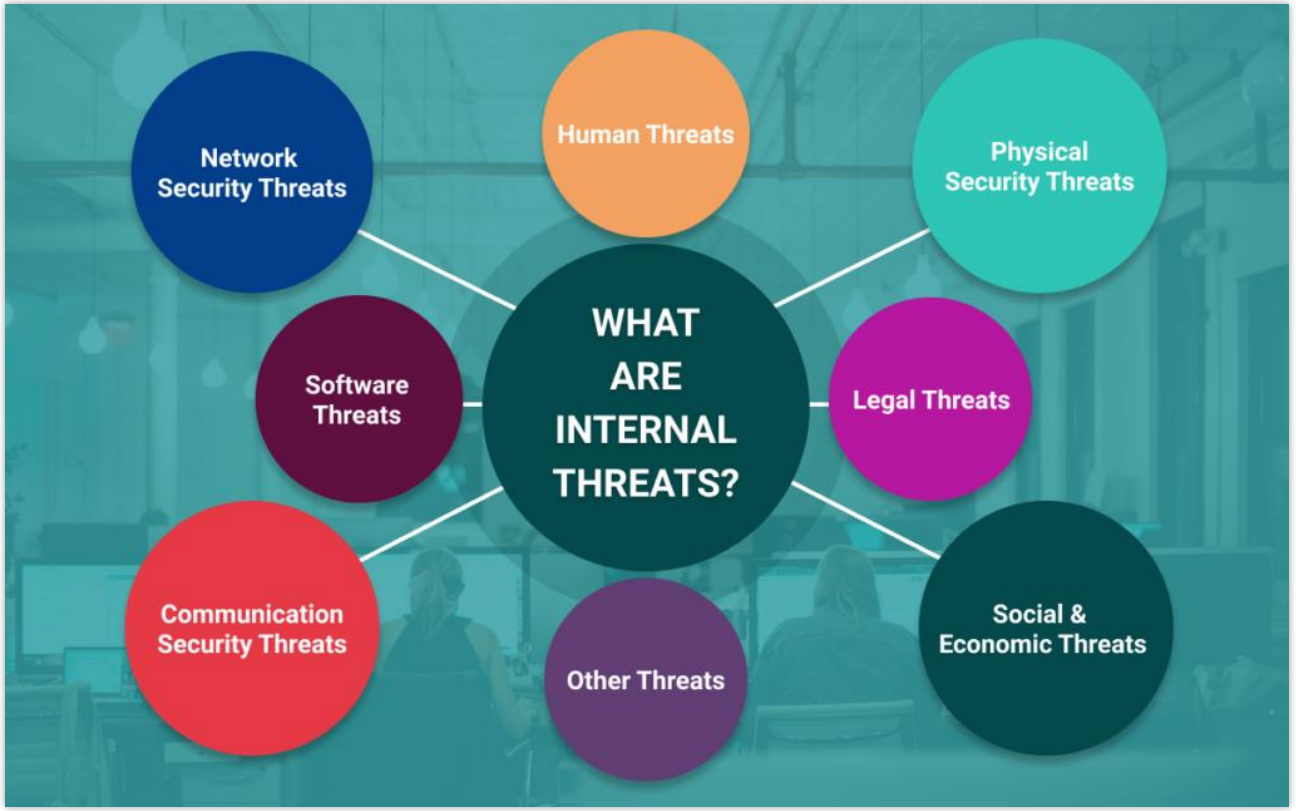
Types of Routing Protocols:

- IGRP: Used within an autonomous system (AS)
- BGP: Used between different ASes
- OSPF: A popular routing protocol

Applications of Routing:

- Internet
- Enterprise networks
- VPNs

Threats



Network threats are malicious activities or events that aim to disrupt, damage, or steal data from a network.

Common Network Threats:

Malware: Software that can infect devices, steal data, or disrupt networks.

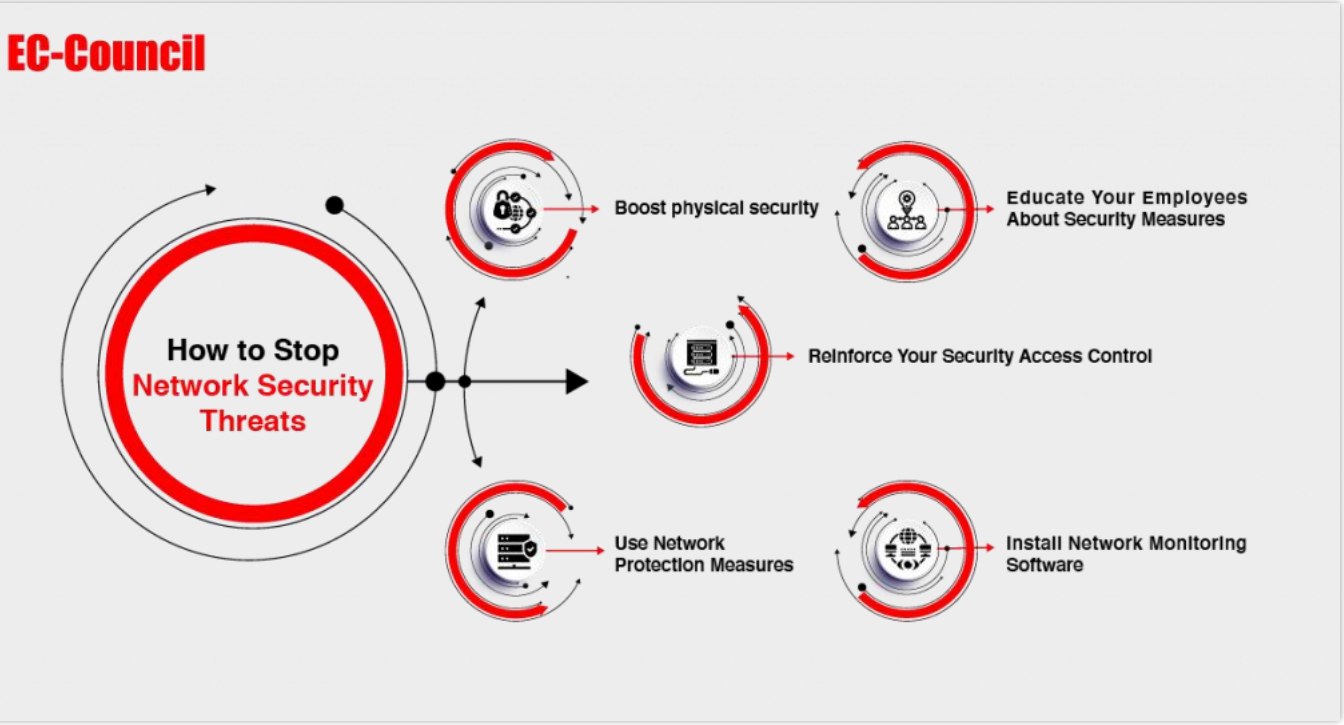
Phishing: Emails or messages that trick users into revealing sensitive information.

DoS Attacks: Overwhelm a network with traffic, making it unavailable to users.

DDoS Attacks: More sophisticated DoS attacks that use multiple devices to flood a network with traffic.

MitM Attacks: Intercept communication between two parties and eavesdrop or alter data.

Security Solutions



Security solutions are tools and strategies to protect your network and data from unauthorized access, theft, disruption, or damage

Key Areas of Security Solutions:

- Network Security: Firewalls, IDS/IPS, VPNs
- Endpoint Security: Antivirus, EDR, DLP
- Access Control: Authentication, authorization, MFA
- Data Security: Encryption, backup, recovery
- Security Awareness Training: Educating users on cybersecurity

Benefits of Security Solutions:

Reduced risk of attacks

Improved compliance

Protected reputation

Conclusion

In conclusion, networks are essential for connecting devices, sharing resources, and accessing information. They have become an integral part of our daily lives, both personally and professionally.

Key Takeaways::

Networks can be classified into different types based on their size, scope, and purpose, such as LANs, WANs, MANs, and PANs.

Networking technologies like Ethernet, Wi-Fi, and cellular networks enable communication between devices over various media.

Network protocols like TCP/IP and HTTP establish rules and guidelines for data transmission and communication between devices.

Network security is critical for protecting networks and data from unauthorized access, threats, and vulnerabilities.

Network troubleshooting and maintenance are essential for ensuring the reliability, performance, and availability of networks.

References

https://en.wikipedia.org/wiki/Local_area_network

https://en.wikipedia.org/wiki/OSI_model

https://www.paloaltonetworks.com/cyberpedia/what-is-a-firewall

https://www.tp-link.com/us/support/faq/227/

https://www.cisco.com/site/us/en/products/networking/switches/index.html

https://en.wikipedia.org/wiki/Network_switch

https://en.wikipedia.org/wiki/Router

https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/network/3-8/reference/guide/routpro.html


Thank you!