Hilla University
College of Medical and Health Technology
Anesthesia department
Computer Networks
Second stage / First course

Lec. No. 2,3,4

Ass. Lec. Zainab Hussein Ali
M.Sc. Information technology

Security and networking

what is network?

A network in technology and telecommunications is a system that connects multiple devices or systems, allowing them to communicate, share data, and resources. Networks come in various types and sizes, ranging from small local setups to vast global infrastructures.

Network Topology

Network topology refers to the physical or logical arrangement of nodes (devices) and connections (communication lines) in a network. The design and layout of a network topology affect performance, scalability, and fault tolerance. Here are the primary types of network topologies:

1. Bus Topology

- Structure: Devices are connected to a single central cable (backbone).

2. Star Topology

- Structure: All devices are connected to a central hub or switch.

3. Ring Topology

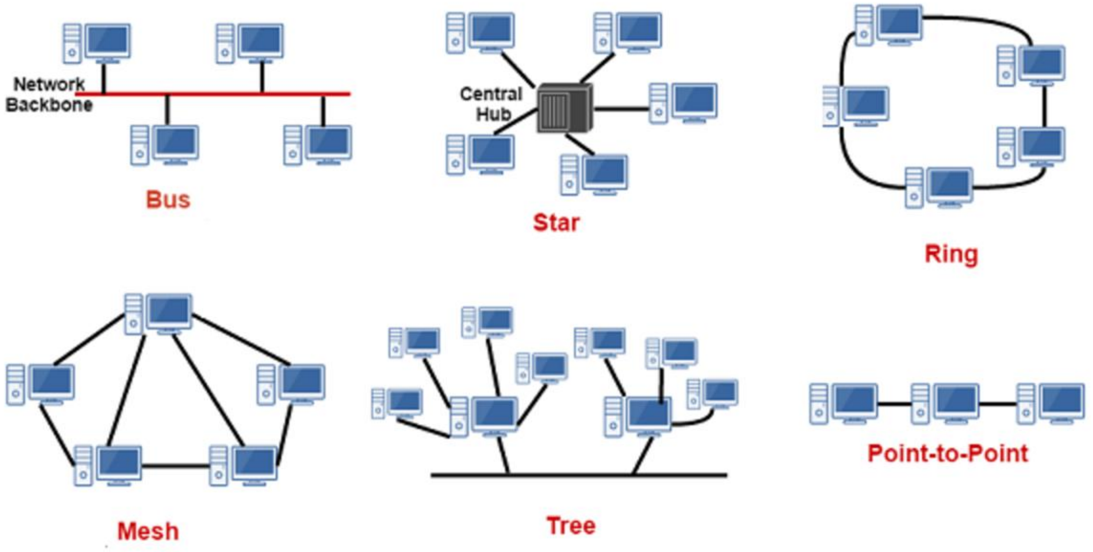
- Structure: Devices are connected in a closed loop, where each device is connected to two other devices.

4. Mesh Topology

- Structure: Each device is connected to multiple other devices, creating a web of connections.

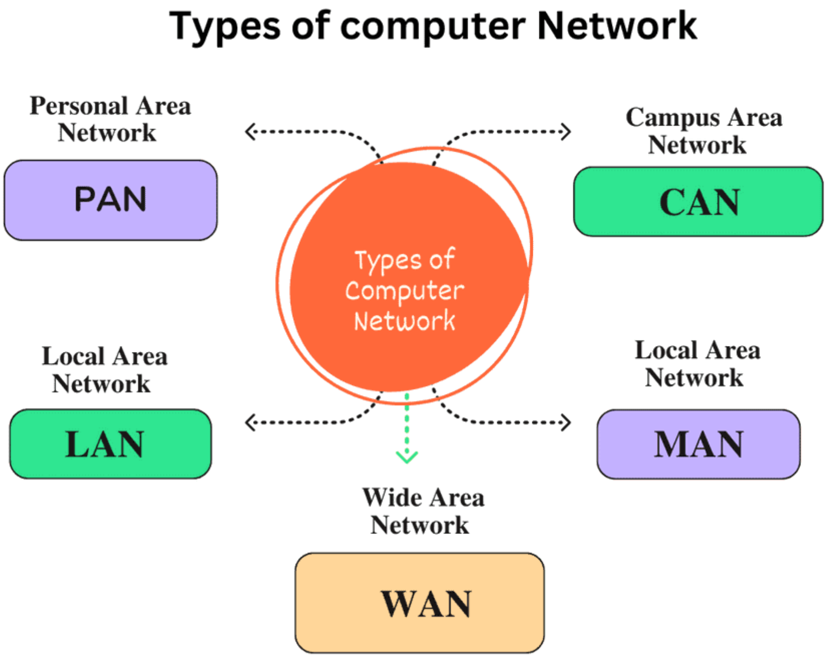
5. Tree Topology

- Structure: A hybrid of bus and star topologies; hierarchical, with multiple star-configured devices connected to a backbone.

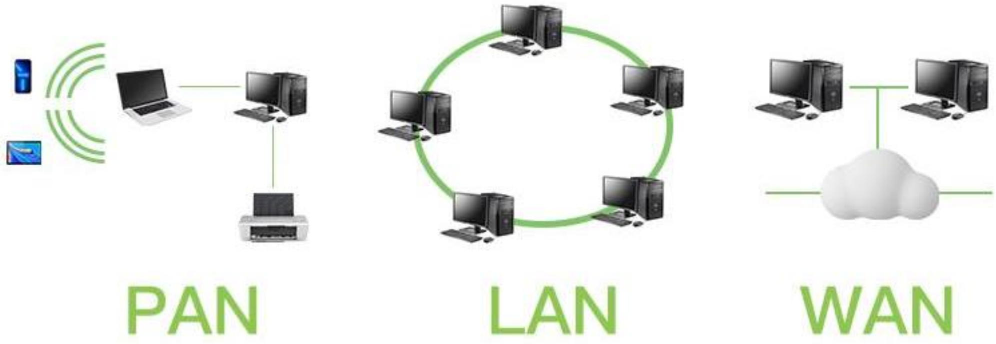


Figer-Network Topology

Here are some common types of networks:

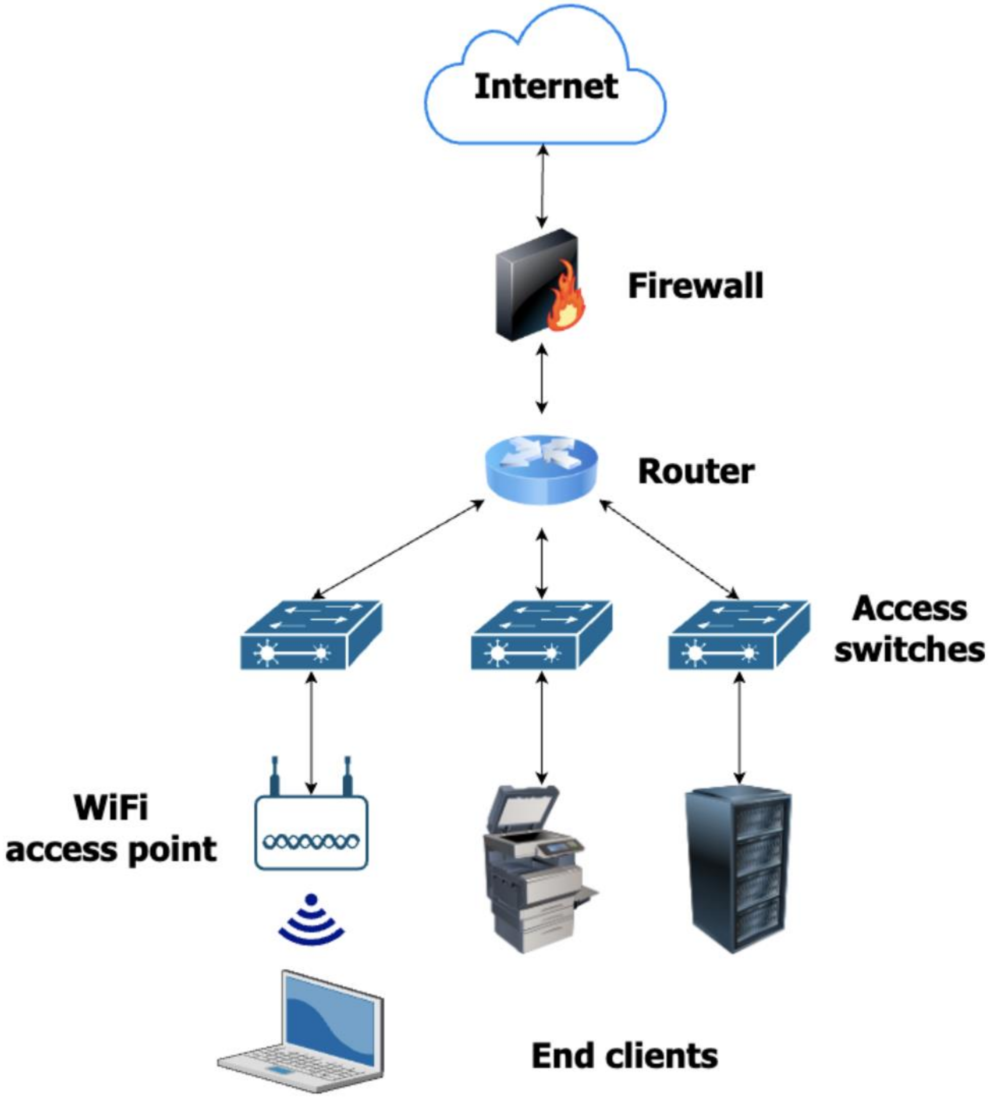


1. **Personal Area Network (PAN)**: A small network typically around a single person, connecting devices like phones, tablets, and laptops, often via Bluetooth or USB.
2. **Local Area Network (LAN)**: A network in a limited area, such as a home, office, or building, allowing computers, printers, and other devices to communicate within a small geographic area.
3. **Wide Area Network (WAN)**: A larger network that connects devices across cities, countries, or globally. The internet itself is a WAN, connecting countless LANs worldwide.
4. **Wireless Local Area Network (WLAN)**: A LAN that uses wireless technology (like Wi-Fi) to connect devices, often used in homes and businesses.
5. **Virtual Private Network (VPN):** A secure network that uses encryption to safely connect devices over the internet, often for accessing private or corporate networks remotely.



Basic network components

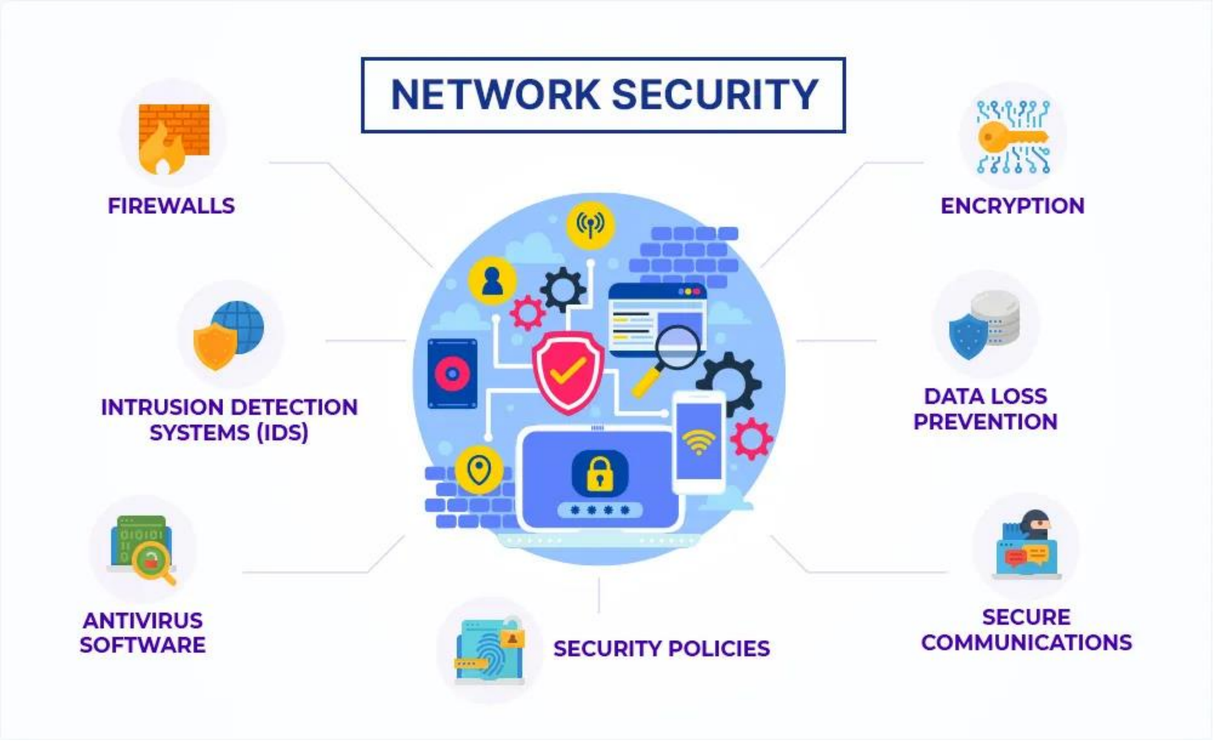
A network consists of several key components that work together to enable communication and data sharing. Here are the essential components of a basic network:



1. **Nodes (Devices):**
   - These are the endpoints in a network, such as computers, servers, printers, smartphones, and any other device that communicates on the network.
2. **Network Interface Card (NIC):**
   - Also called a network adapter, this hardware component allows a device to connect to a network. NICs can be wired (Ethernet) or wireless (Wi-Fi) and are usually built into modern devices.
3. **Transmission Media:**
   - The medium through which data is transmitted between devices. This can be wired (like Ethernet cables, fiber optic cables) or wireless (such as Wi-Fi, Bluetooth, radio frequencies).
4. **Switch:**
   - A device that connects multiple devices within a LAN and forwards data to the correct device. Switches are key for efficient data flow within local networks.
5. **Router:**
   - A device that connects different networks, often linking a LAN to the internet. Routers manage data packets, directing them between the internal network and external networks (such as the internet).
6. **Modem:**
   - A device that converts digital data from a network into the analog signal required for communication over telephone or cable lines (DSL or cable modems are common). Many routers today come with built-in modems.
7. **Firewall:**
   - A security device (software or hardware) that monitors and controls incoming and outgoing network traffic based on predetermined security rules, protecting the network from unauthorized access.

network security basic

Network security is the practice of protecting a network and its resources from unauthorized access. Here are the basics of network security:



Firewall

- A firewall is a security device (either hardware, software, or a combination of both) that monitors and controls incoming and outgoing network traffic

Encryption

- Encryption converts data into a coded format that can only be accessed by authorized parties with a decryption key

Authentication

- Authentication ensures that only authorized users and devices can access network resources. Common methods include:
    - **Username and password** combinations.
    - **Two-factor authentication (2FA) or multi-factor authentication (MFA),** which requires multiple forms of verification.
    - **Biometrics** (fingerprint, facial recognition).

Antivirus and Anti-Malware

- Antivirus and anti-malware software protect devices from malicious software

Data Backup and Disaster Recovery

Regularly backing up data ensures recovery from potential data loss due to cyberattacks, hardware failure, or other incidents

Understanding network threats

Network threats are dangers that can compromise the security, integrity, and availability of a network and its data. Understanding these threats is essential for implementing effective network security. Here’s a breakdown of common network threats:

1. Malware

- Malware is a general term for malicious software designed to harm or exploit a network. Common types include:
    - **Viruses**: Attach themselves to files or programs and spread when opened.
    - **Worms**: Self-replicating malware that spreads across networks without user intervention.
    - **Trojan Horses**: Disguised as legitimate software, Trojans trick users into installing them, which then open a backdoor for attackers.

  - **Ransomware**: Encrypts a user's data and demands a ransom for the decryption key.
  - **Spyware**: Gathers sensitive data from the infected system and sends it to the attacker.

2. Phishing Attacks

- Phishing is a social engineering attack where attackers impersonate legitimate sources to trick users into revealing sensitive information, like usernames, passwords, or credit card details.

3. SQL Injection

- SQL Injection attacks target databases by injecting malicious SQL code into forms or URLs. If successful, attackers can access, modify, or delete sensitive data within the database. SQL injection is particularly dangerous for web applications with poor input validation.

4. Password Attacks

- Attackers may attempt to crack passwords to gain unauthorized access to network resources.

5. Drive-By Downloads

- Drive-by downloads occur when a user visits a compromised website that automatically downloads malicious software to their device. This attack can exploit outdated software, plugins, or vulnerabilities in browsers.

*Mitigation Techniques

To counter these threats, organizations use various security measures, such as firewalls, encryption, multi-factor authentication, intrusion detection/prevention systems, and employee training to raise awareness about social engineering and phishing tactics.

Network Troubleshooting

Network troubleshooting is the process of identifying, diagnosing, and resolving problems within a network. It involves a series of systematic steps to help restore connectivity and optimize network performance. Here are the basic steps and tools commonly used in network troubleshooting:

1. Identify the Problem

- Is the problem affecting a single device or multiple devices?

2. Define the Scope

- Is the problem on a **local device**, on the **local area network (LAN)**, or across the **wide area network (WAN)**?

3. Check Physical Connections

- **Ethernet cables** for wired connections.
- **Power connections** on routers, switches, and other devices.

4. Restart Network Devices

- Restarting devices, such as modems, routers, switches, and even computers, can clear temporary issues and re-establish connections.
- Power cycling a modem or router can also help resolve problems caused by overheating or cache overflow.

5. Check Wireless Settings (for Wi-Fi issues)

- The SSID (network name) and password settings.
- The **signal strength** and ensure that the device is within range of the access point.
- **Channel congestion**: Overlapping channels with neighboring Wi-Fi networks can cause interference.

- Consider **switching to a different channel** if there is interference.