Al-Mustaqbal University

College of Science

Security and Networking

Lecture 1

Assis Lec: Hadi Salah

Lecture Objectives

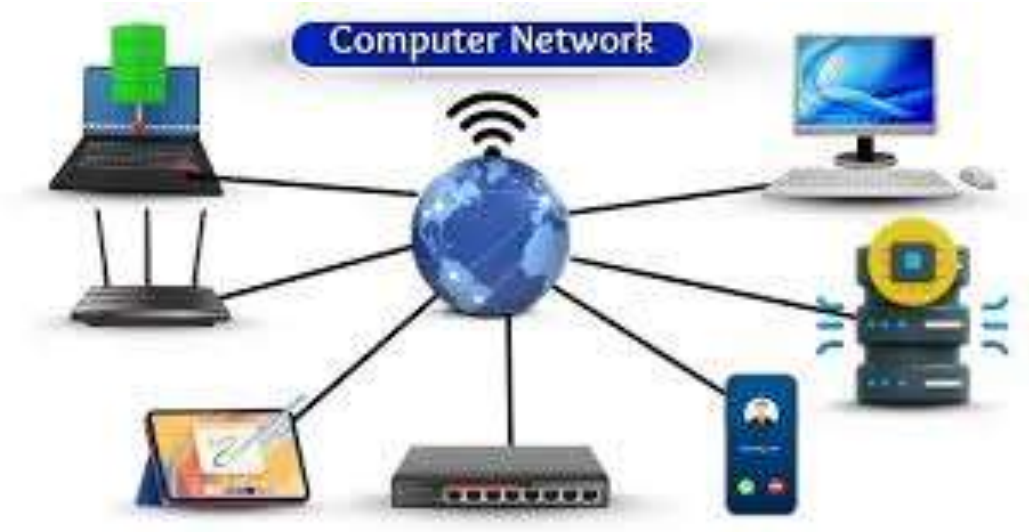
By the end of this lecture, students will be able to:

- Understand the concept of computer networks
- Identify different network types
- Recognize basic network components
- Understand network security principles
- Identify common network threats
- Apply basic troubleshooting techniques

What is a Network?

A computer network is a collection of interconnected devices such as computers, servers, printers, and mobile devices.

These devices communicate with each other to share data, resources, and services efficiently.



Why Do We Need Networks?

Networks allow users to share files and data easily.

They enable sharing hardware resources such as printers and servers.

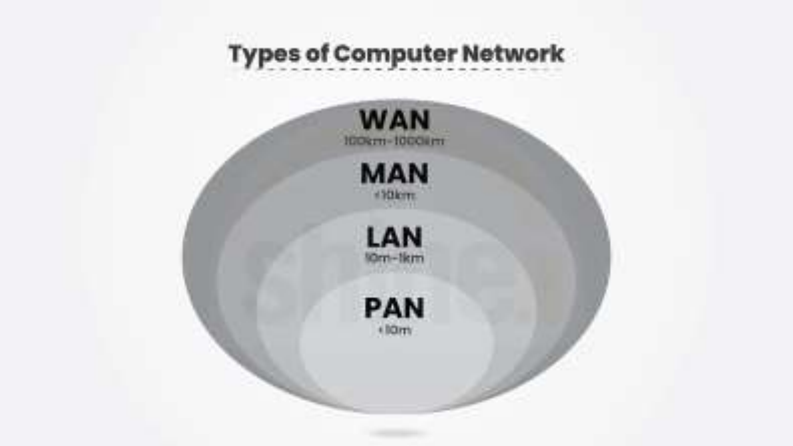
They support communication tools like email and messaging.

They provide access to the internet.

Types of Networks

Networks are classified based on size and coverage area:

- LAN – Local Area Network
- MAN – Metropolitan Area Network
- WAN – Wide Area Network
- PAN – Personal Area Network

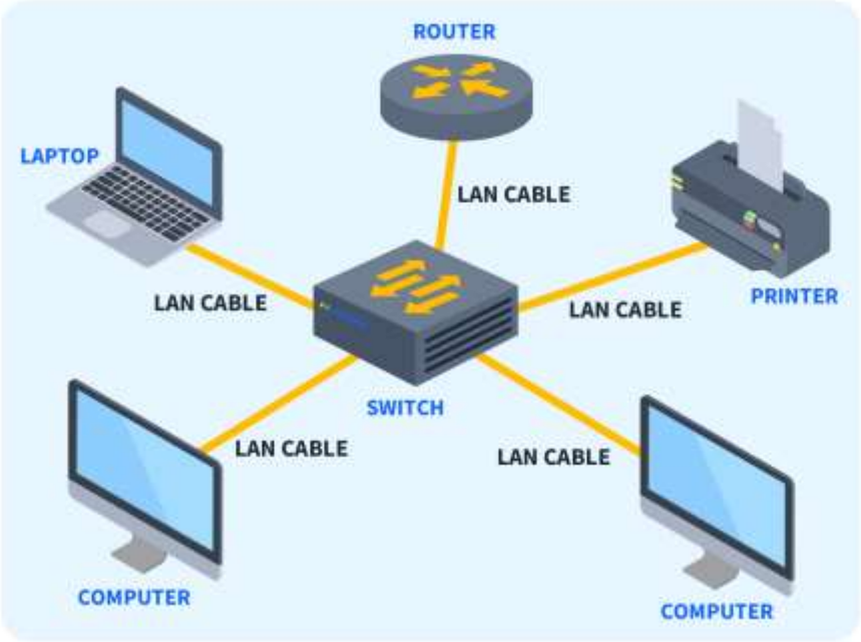


Local Area Network (LAN)

A LAN covers a small geographic area such as a home, office, or school.

It provides high-speed data transfer.

LANs are usually privately owned and managed.

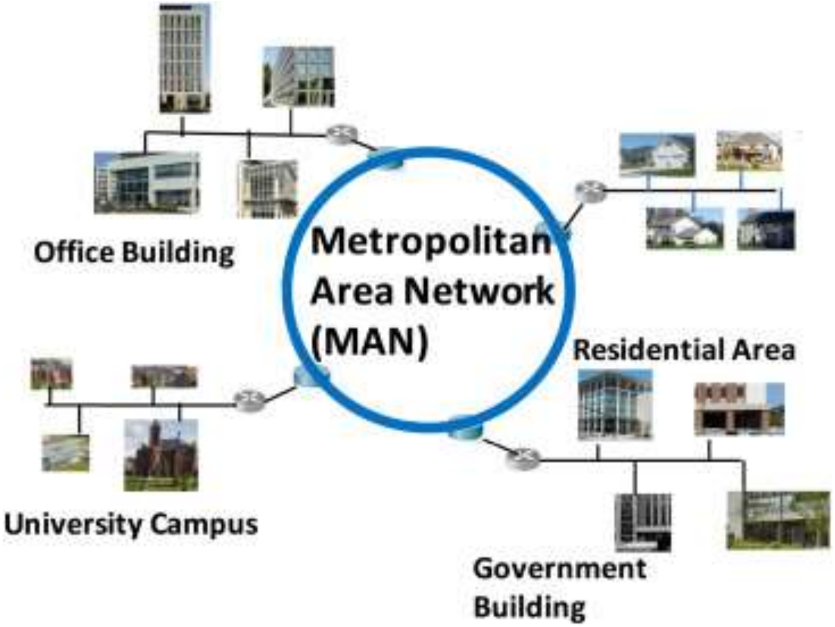


Metropolitan Area Network (MAN)

A MAN covers a city or a large campus.

It connects multiple LANs together.

MANs are commonly used by universities or municipalities.

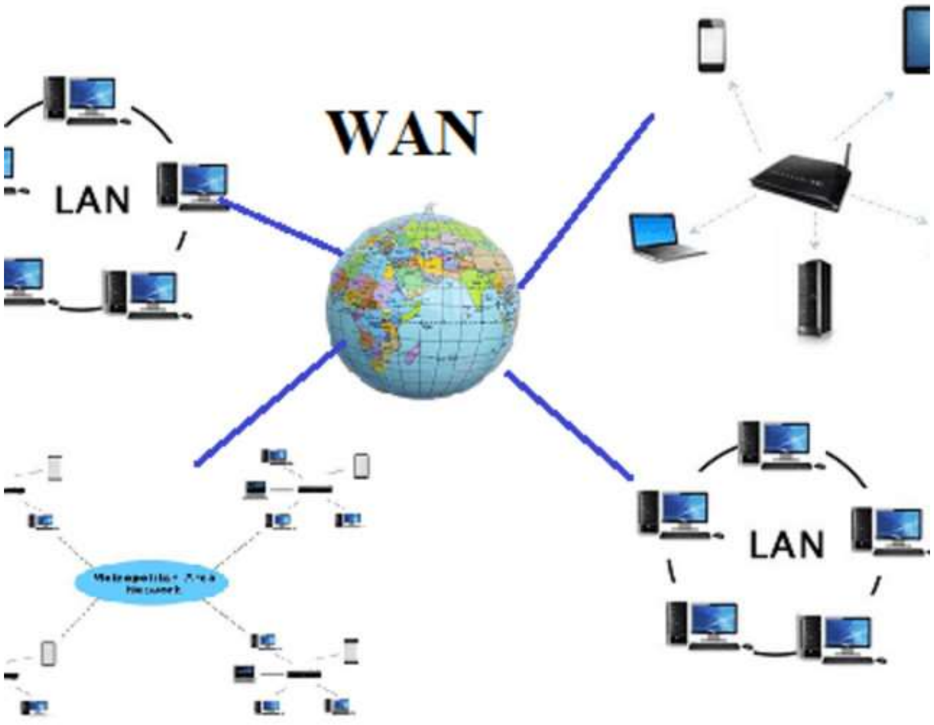


Wide Area Network (WAN)

A WAN covers very large geographic areas such as countries or continents.

It connects multiple LANs and MANs.

The Internet is the best-known example of a WAN.



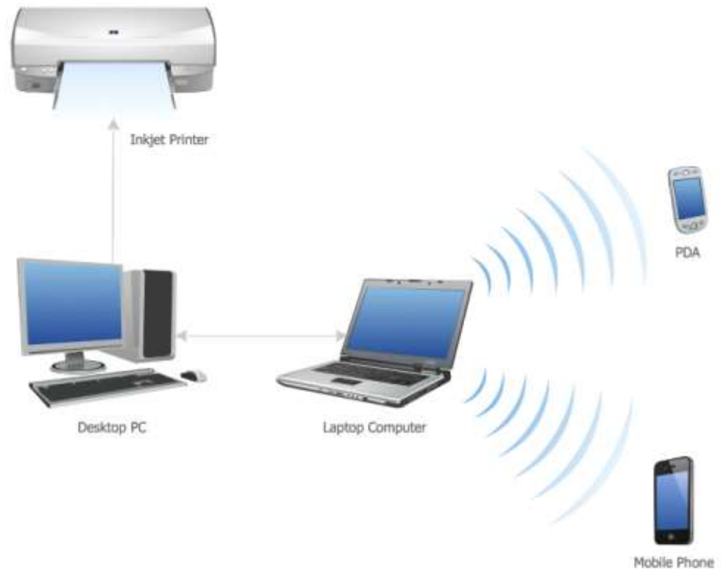
Wide area network (WAN)

Personal Area Network (PAN)

A PAN connects personal devices over a very short range.

Examples include Bluetooth connections and mobile hotspots.

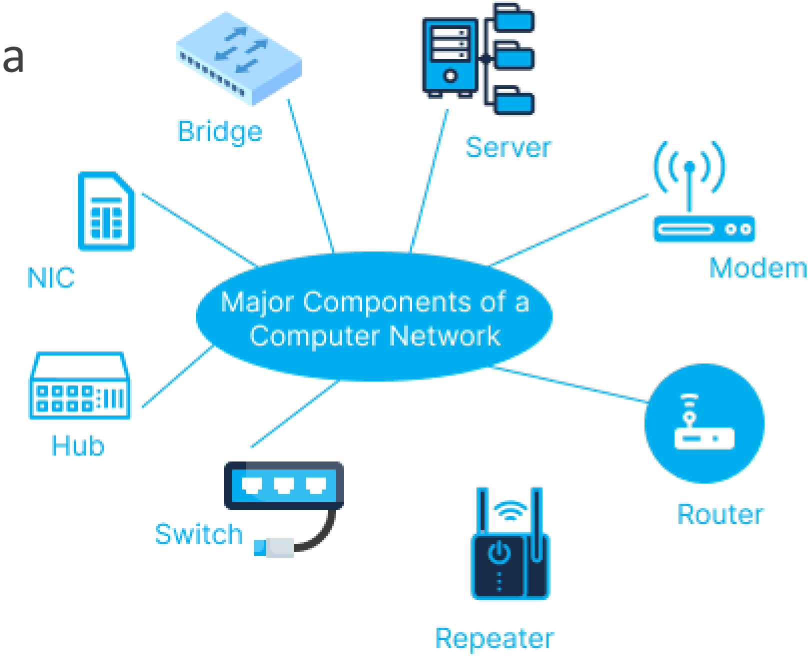
It is commonly used for personal data sharing.



Basic Network Components

Every network consists of:

- End devices such as computers and servers
- Network devices that manage data flow
- Transmission media that carry the data

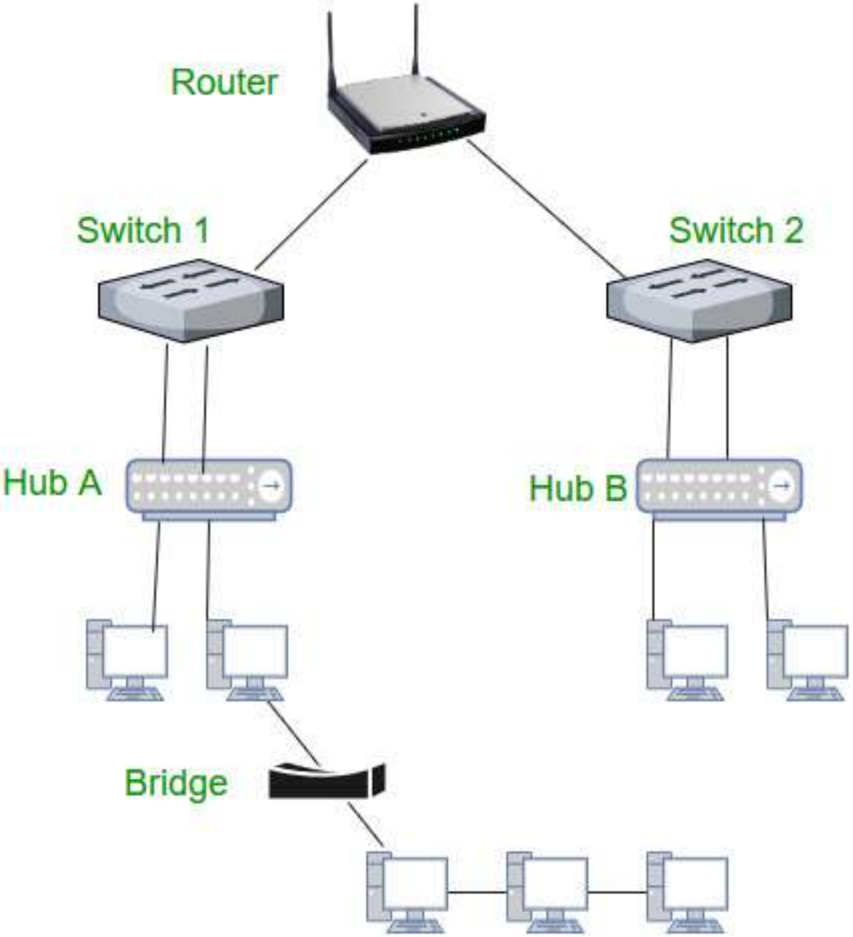


Network Devices

Common network devices include:

- Router
- Switch
- Hub
- Modem
- Access Point

Each device has a specific role in the network.



Router

A router connects different networks together.

It directs data packets between networks.

Routers are essential for internet connectivity.

Switch

A switch connects devices within a local area network.

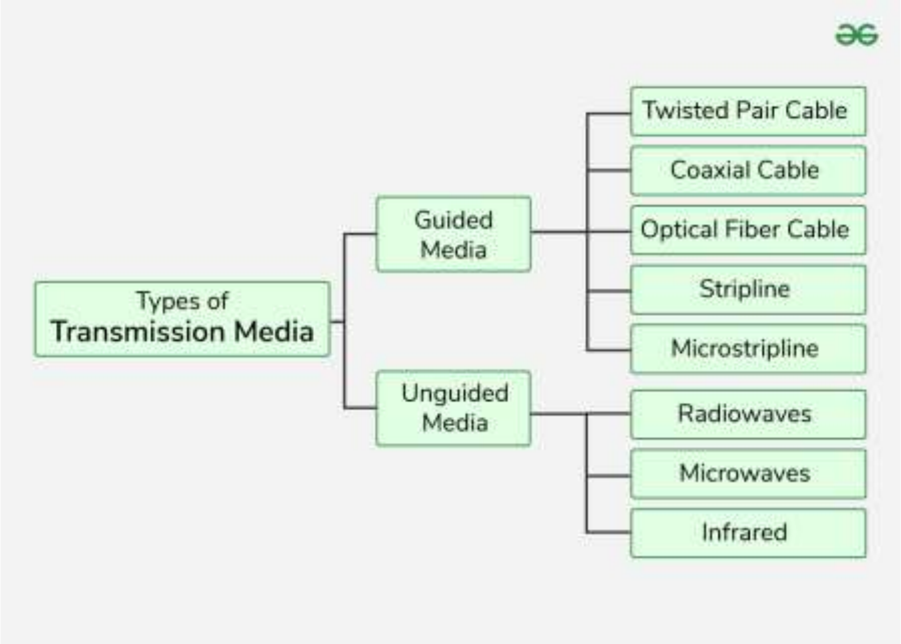
It sends data only to the intended device.

This improves network efficiency and performance.

Transmission Media

Transmission media are the paths through which data travels.

- Wired media such as Ethernet and Fiber Optic cables
- Wireless media such as Wi-Fi



What is Network Security?

Network security involves protectin
networks and data from unauthoriz
access.

It ensures confidentiality, integrity, a
availability of information.

Importance of Network Security

Network security is important to:

- Protect sensitive information
- Prevent data loss and damage
- Ensure continuous system operation
- Defend against cyber attacks

Common Network Threats

Networks face many threats including:

- Malware
- Viruses
- Worms
- Trojans
- Phishing attacks

Threat Type	Definition	How It Spreads	Requires User Action?	Main Purpose	Example
Malware	General term for any malicious software	Varies (files, links, networks)	Sometimes	Damage, spying, control	Spyware, ransomware
Virus	Malicious code that attaches to a legitimate file	Infected files, USB, downloads	Yes	Damage files, disrupt systems	File-infecting virus
Worm	Standalone malware that self-replicates	Network vulnerabilities	No	Rapid spreading, network overload	Conficker
Trojan	Malicious program disguised as legitimate software	Fake software, downloads	Yes	Steal data, create backdoors	Fake antivirus
Phishing Attack	Social engineering attack to steal sensitive info	Emails, fake websites, messages	Yes	Steal passwords, money, identity	Fake bank email

Unauthorized Access

Unauthorized access is the process of gaining entry or access to a system, physical or electronic, without the permission of the owner or administrator. Such access can be obtained by bypassing security measures, exploiting system vulnerabilities or by using stolen credentials. Unauthorized access is a serious violation of privacy laws and can lead to severe consequences, including legal action.

This may involve hacking, password attacks, or insider threats.

Network Security Tools

Various tools are used to protect networks:

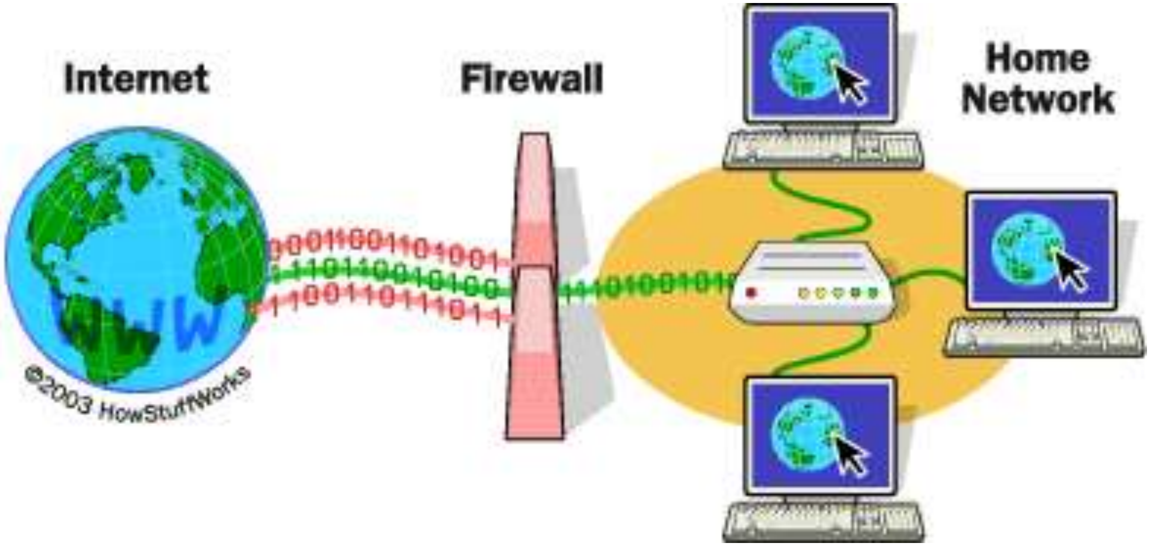
- Firewalls
- Antivirus software
- Encryption techniques
- Authentication mechanisms

Firewall

A firewall monitors incoming and outgoing network traffic.

It allows or blocks data based on security rules.

It acts as the first line of defense.

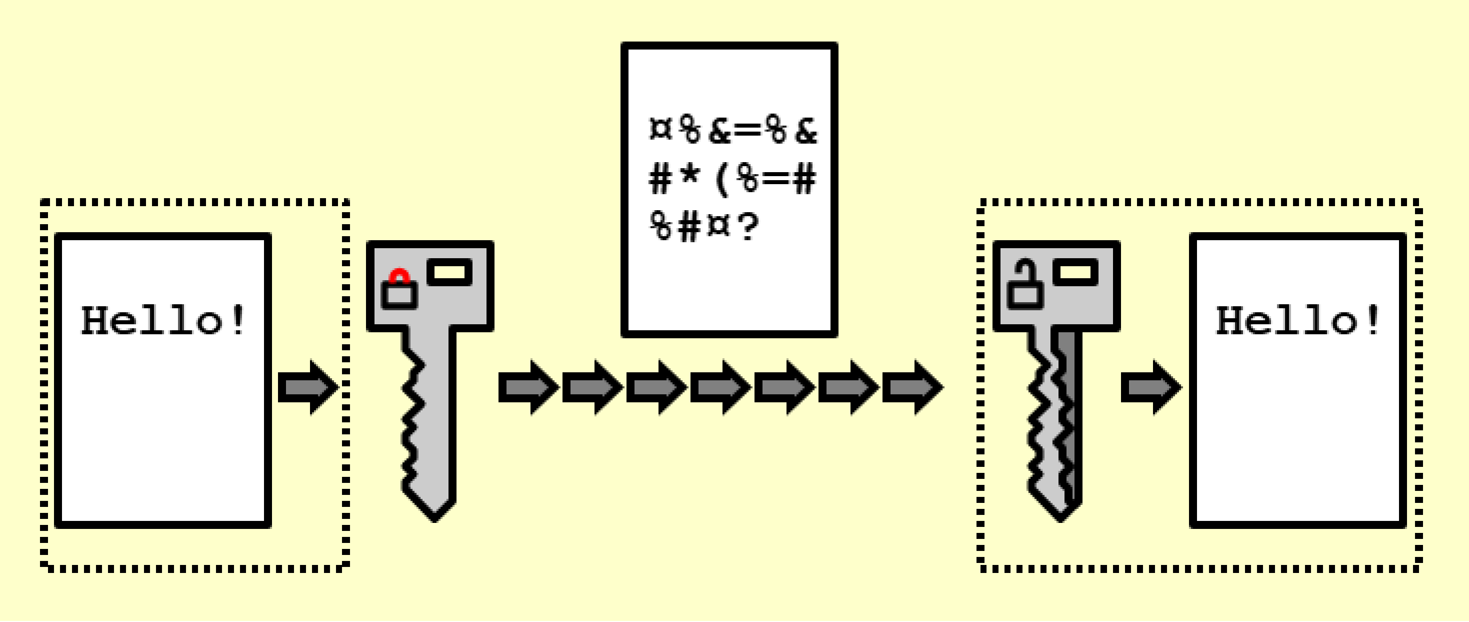


Encryption

Encryption converts readable data into an unreadable format.

It protects data during transmission.

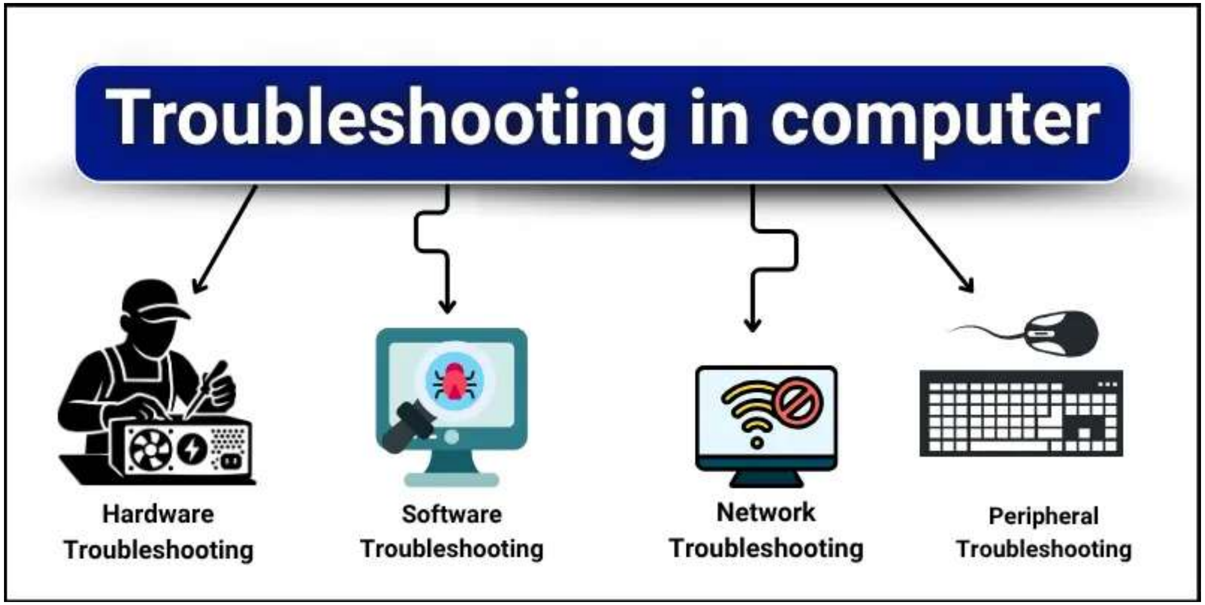
Only authorized users can decrypt the data.



Network Troubleshooting

Network troubleshooting is the process of identifying and resolving network issues.

It helps maintain reliable and efficient network performance.



Common Network Problems

Typical network problems include:

- No internet connection
- Slow network speed
- IP address conflicts
- Hardware failures

Basic Troubleshooting Steps

Basic troubleshooting steps include:

- Checking cables and physical connections
- Restarting network devices
- Verifying IP configuration
- Testing connectivity using ping

Conclusion

Computer networks are essential in modern life.

Network security is critical to protect data.

Basic troubleshooting skills save time and cost.

Understanding networking improves IT and career skills.