



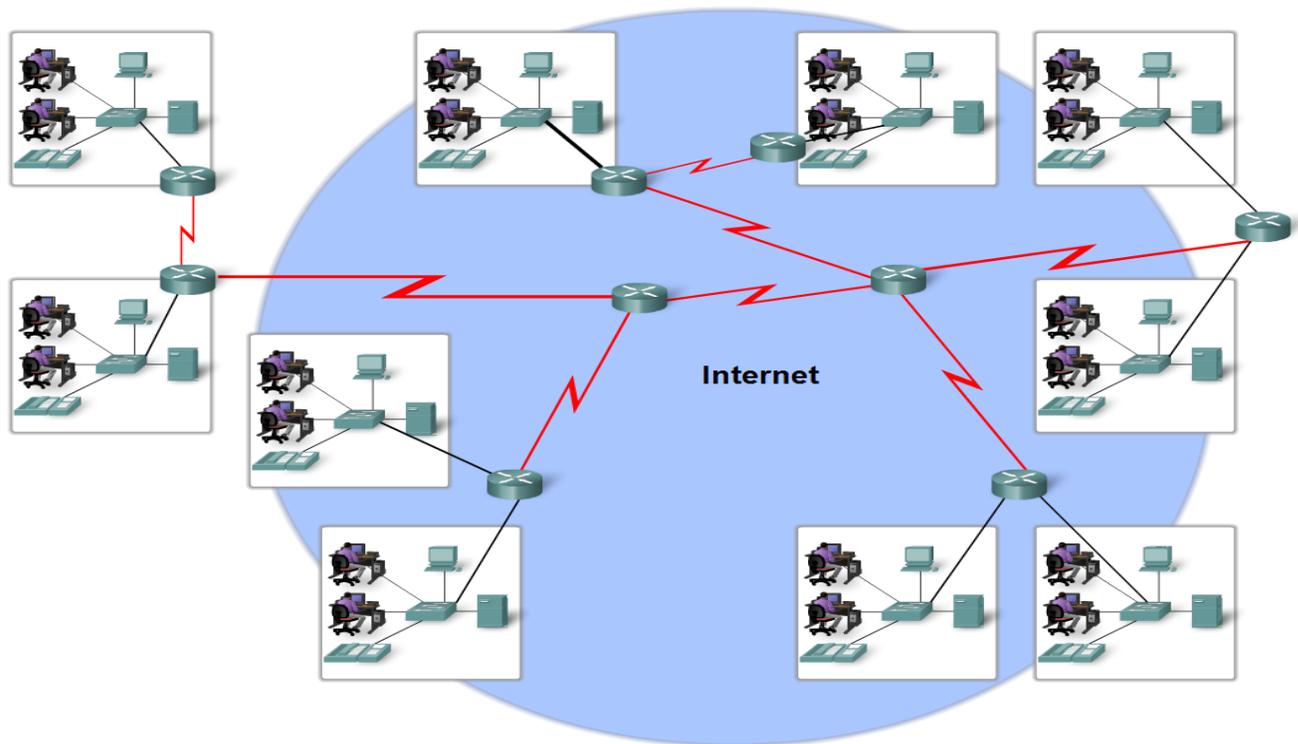
Introduction to Security and Networking

1. Computer Networks – Basic Concepts

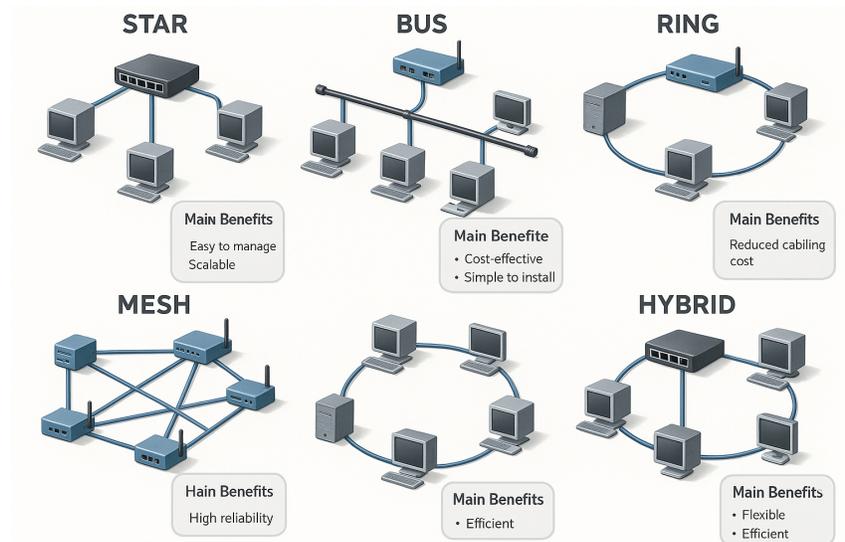
A **Network** is a group of computers and devices connected together to share data, resources, and services.

Why Networks Are Important?

- Share files and data
- Share hardware (printers, scanners)
- Communication (email, chat, video calls)
- Access the Internet



Network Topology: it is the arrangement of devices (nodes) and connections (links) in a computer network.

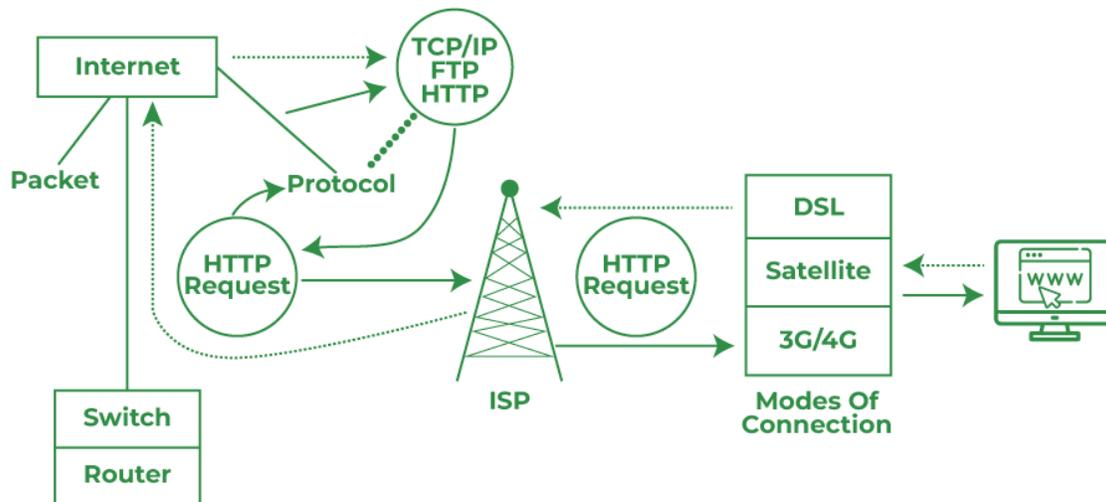


How does a network work?

A **computer network** works by allowing devices to **connect, communicate, and share data and resources** with each other.

Here is a **simple explanation**:

- 1. Devices (Nodes):**
Computers, smartphones, printers, and servers are connected to the network.
- 2. Communication Media:**
Devices are linked using **cables** (Ethernet, fiber) or **wireless signals** (Wi-Fi).
- 3. Network Devices:**
 - **Switches** connect devices within a local network.
 - **Routers** connect different networks and direct data to the correct destination.
- 4. Data Transmission:**
Information is broken into **small packets**. Each packet is sent across the network and reassembled at the destination.
- 5. Protocols:**
Networks follow rules called **protocols** (such as TCP/IP) to ensure data is sent, received, and understood correctly.
- 6. Servers and Services:**
Servers provide services like file sharing, email, and internet access to connected devices.



Advantages of Computer Networking

The fundamental benefits of computer networking include:

- It allows multiple computers to connect and exchange information efficiently.
- It enables sharing of resources such as printers, scanners, and email services.
- It supports fast data and information sharing.
- Electronic communication through networks is more efficient and less expensive compared to communication without a network.

Disadvantages of Computer Networking

The main drawbacks of computer networking include:

- The initial investment in hardware and software can be costly.
- Without proper security measures such as encryption and firewalls, data may be at risk.
- Some network components may become outdated or malfunction over time and require replacement.
- Continuous administration and maintenance are required.
- Network issues such as server failures and cable faults can disrupt operations.



2. Types of Computer Networks

A) Local Area Network (LAN): a LAN connects computers within a small area such as: Home, School, Office, University lab. For **Example:** Computer lab in a university connected via Ethernet or Wi-Fi.

Characteristics:

- Small geographical area
- High data speed
- Low cost
- Usually owned by one organization

B) Wide Area Network (WAN): A WAN covers a large geographical area such as: Cities, Countries, Continents. For example, The **Internet** is the largest WAN in the world.

Characteristics:

- Large distance coverage
- Slower than LAN
- More expensive
- Uses public or leased communication lines

C) Personal Area Network (PAN): Connects devices within a very short personal range, such as Bluetooth connections between a mobile phone and a headset.

D) Metropolitan Area Network (MAN): Covers a city or large campus, such as a university network or a local government network.

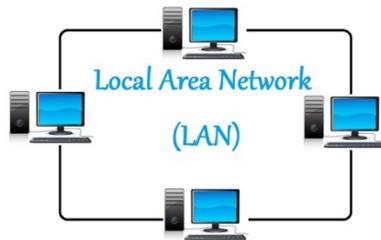
E) Wireless Local Area Network (WLAN): A type of LAN that relies on wireless communication using Wi-Fi instead of physical cables.

F) Home Area Network (HAN):

A small network used within a home to connect personal devices such as computers, smartphones, smart TVs, printers, and smart home devices, usually through Wi-Fi or Ethernet.

G) Campus Area Network (CAN):

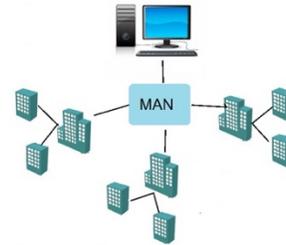
A network that connects multiple local area networks (LANs) within a limited geographic area such as a university campus, school, hospital, or corporate campus.



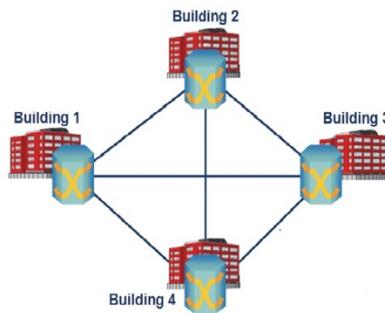
Local Area Network
(LAN)



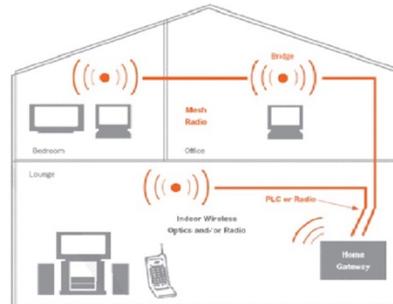
(WAN) Wide Area Network



Metropolitan Area Network



Campus Area Network(CAN)



Home Area Network(HAN)

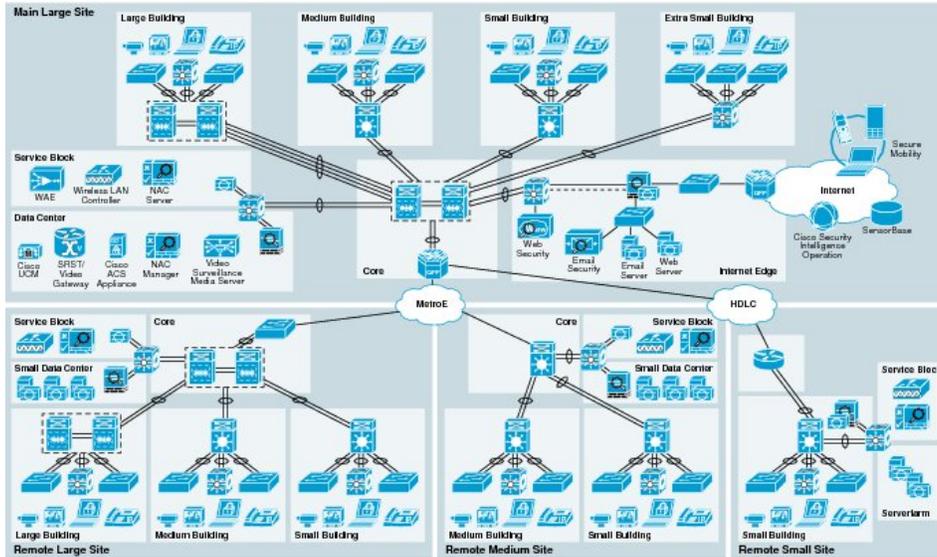
3. Concept of the Internet

The **Internet** is created by the interconnection of networks belonging to Internet Service Providers (ISPs) to provide access for millions of users all over the world.

The **Internet** is a global network of networks that connects millions of computers and devices worldwide.

Key Points

- Uses standard communication protocols (TCP/IP)
- Allows global data exchange
- Operates 24/7



4. Applications of the Internet

Common Internet applications include:

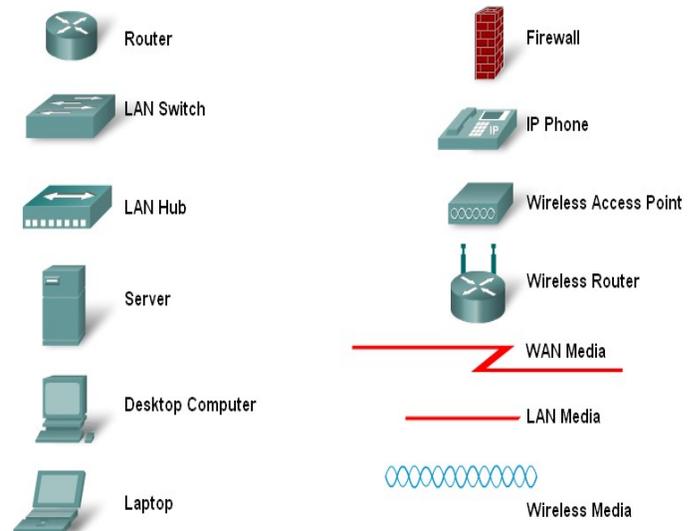
- **Email** – sending and receiving messages
- **Web browsing** – accessing websites
- **Social media** – communication and sharing
- **Online learning** – e-learning platforms
- **E-commerce** – online shopping and banking
- **Cloud services** – Google Drive, OneDrive

5. Connecting to the Internet

To connect to the Internet, we need:

- A device (computer, laptop, smartphone)
- Network interface (Wi-Fi or Ethernet)
- Internet Service Provider (ISP)
- Modem or router

Common Connection Types are Wi-Fi, Mobile data (4G/5G), DSL and Fiber optic.





6. Network security

What Is Network Security?

Network security refers to the policies, practices, and technologies used to **protect a computer network and its data** from unauthorized access, misuse, attacks, and damage.

It ensures that:

- Only **authorized users** can access network resources
- **Data is protected** during storage and transmission
- Network services remain **available and reliable**

Key Elements of Network Security

- **Authentication:** Verifies the identity of users and devices
- **Authorization:** Controls what users are allowed to access
- **Firewalls:** Block unauthorized network traffic
- **Encryption:** Protects data from being read by attackers
- **Antivirus and Anti-malware:** Detect and remove malicious software

Purpose of Network Security:

The main goal of network security is to maintain:

- **Confidentiality** – data is kept private
- **Integrity** – data is not altered without permission
- **Availability** – network services are accessible when needed

In simple terms, **network security protects networks from cyber threats and ensures safe communication which is called CIA**



How Does Network Security Work?

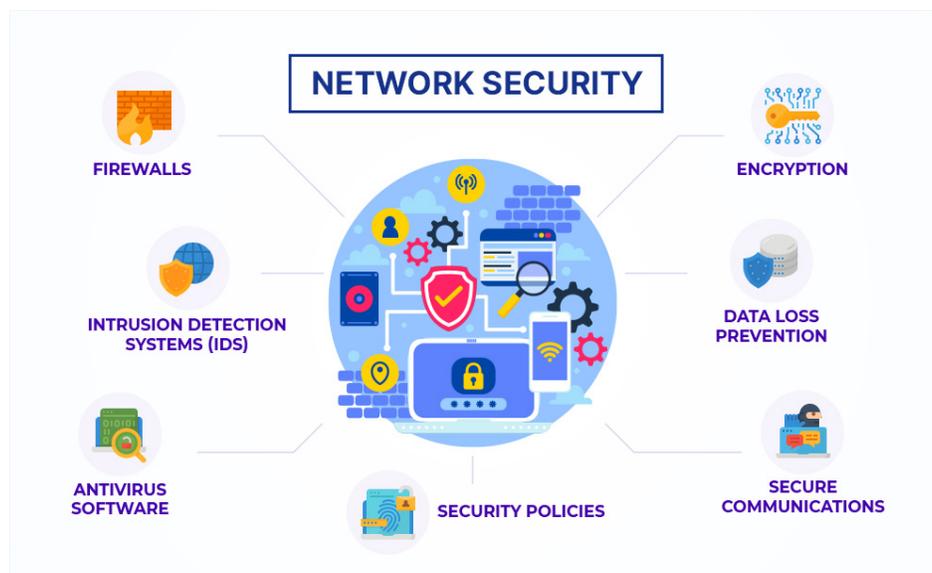
Digital acceleration has enabled businesses to achieve greater efficiency, reduce costs, and improve productivity. However, it has also expanded the attack surface across modern networks. As networks grow to include local area networks (LANs), wide area networks (WANs), Internet of Things (IoT) devices, and cloud computing environments, each new deployment introduces potential security vulnerabilities.

Network security works by **protecting networks, devices, and data** through a combination of policies, controls, and technologies designed to prevent unauthorized access and cyberattacks.

Network Security Basics

The fundamental practices of network security include:

- **Creating strong passwords** to prevent unauthorized access
- **Logging out completely** from shared or public computers
- **Access control** to ensure users can only access permitted resources
- **Encryption** to protect sensitive data and communications
- **Safeguarding networks and software** through updates, firewalls, and security tools





7. Understanding Network Threats

Understanding network threats involves recognizing different types of attacks that can compromise network security. These threats may lead to data breaches, system downtime, and other serious consequences.

Key points include:

- A **network threat** targets a computer network or its connected devices.
- Network threats can **damage, disrupt, or interrupt** systems, applications, and services.
- Different types of network threats have **different objectives**, such as spying, disruption, or financial gain.
- Network security policies should be designed to **identify vulnerabilities and protect against attacks**.
- The ultimate goal of many network attacks is to **steal, modify, or deny access to valuable data**.

8. Network Troubleshooting Basics

What Is Network Troubleshooting?

Troubleshooting is the process of identifying, analysing, and solving problems that occur in a computer system.

During this process, administrators gain visibility into network components and analyze connectivity issues, security-related problems, and performance metrics. Whether the issue is simple or complex, network troubleshooting helps determine the **root cause of problems** and ensures smooth and reliable network connectivity.

Why Is Network Troubleshooting Important?

Even a minor fault in a network component can reduce efficiency and increase downtime. Network troubleshooting is important because it allows IT managers and network administrators to:

- Detect network performance issues in real time
- Improve the **Quality of Service (QoS)** for users
- Prevent downtime and service interruptions
- Reduce costs caused by network outages and potential data loss



In addition, **network monitoring systems** support troubleshooting by tracking key metrics such as packet loss, traffic flow, and network capacity to maintain smooth operations.

Examples of Network Troubleshooting

- Using basic troubleshooting tools such as **ping, tracert, ipconfig, netstat, nslookup, pathping, route, and PuTTY** to diagnose network issues.
- Identifying and fixing common network symptoms such as slow network speed, buffering downloads, laggy video calls, poor VoIP quality, and loss of Internet connection.
- Addressing the four major categories of network issues:
 - Network connectivity issues
 - Bandwidth issues
 - Network device configuration issues
 - IP addressing and configuration issues

Basic Network Troubleshooting Steps

1. **Identify the problem** (determine what is not working).
2. **Gather information** about the symptoms and affected devices.
3. **Check physical connections** such as cables, ports, and power.
4. **Test network connectivity** using troubleshooting tools.
5. **Identify the root cause** of the issue.
6. **Apply a solution** and fix the problem.
7. **Test the network again** to confirm the issue is resolved.
8. **Document the problem and solution** for future reference.

Step-by-Step Troubleshooting Process

