UNIVERSITY OF ANBAR
COLLEGE OF SCIENCES
DEPARTMENT OF BIOLOGY

SECURITY AND NETWORKING

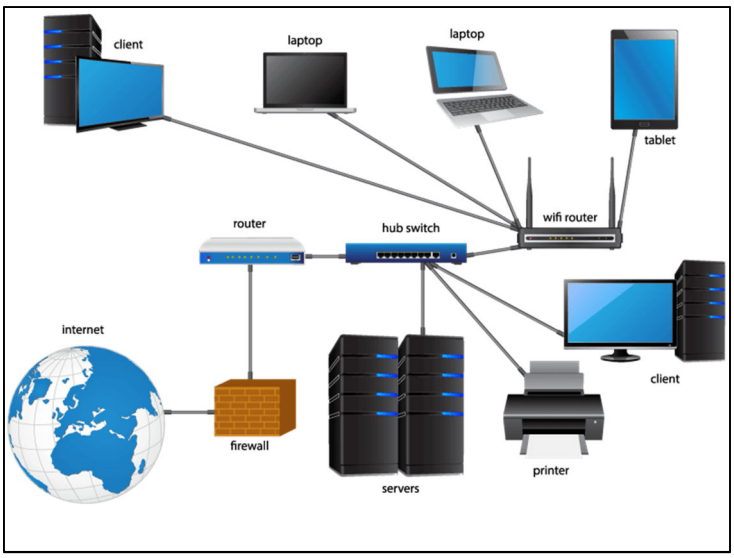
Assef Raad Hmeed

2025

Lecture1: Security and Networking

1. What is a Network?

A **network** is a collection of interconnected devices that communicate with each other to share resources and information. Networks allow computers, servers, printers, and other devices to communicate efficiently, whether they are in the same building (local network) or across the world (wide-area network).



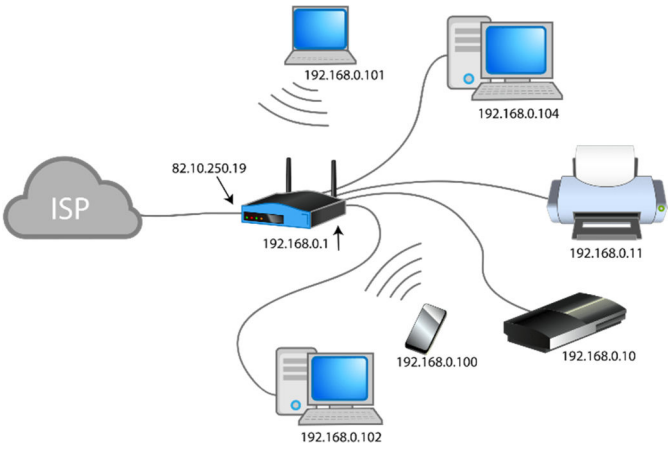
Key Concept:

- **Networking** refers to the process of linking these devices and ensuring they can exchange data reliably and securely.

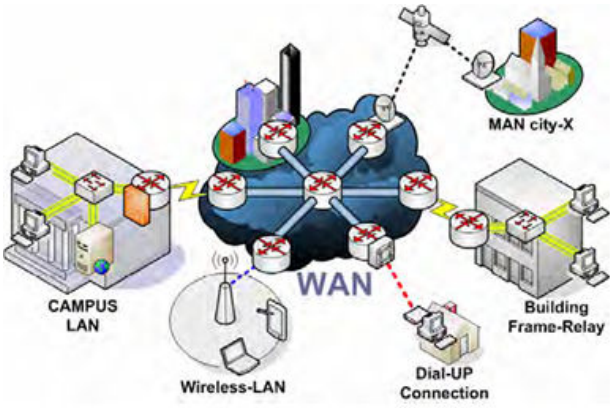
2. Types of Networks

Networks are classified based on their size, ownership, and the technologies used for data transmission. Some of the most common types are:

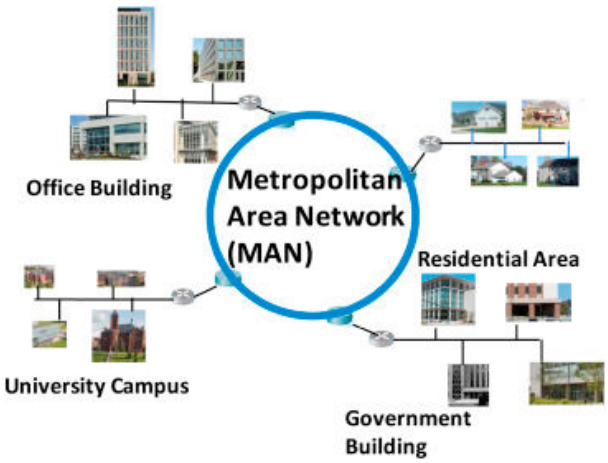
1. **Local Area Network (LAN)**:
    - Covers a small geographical area, such as a home, office, or building.
    - Examples: Ethernet networks, Wi-Fi networks within a house.



2. **Wide Area Network (WAN)**:
    - Covers large geographical areas, such as cities, countries, or continents.
    - The internet is the largest example of a WAN.

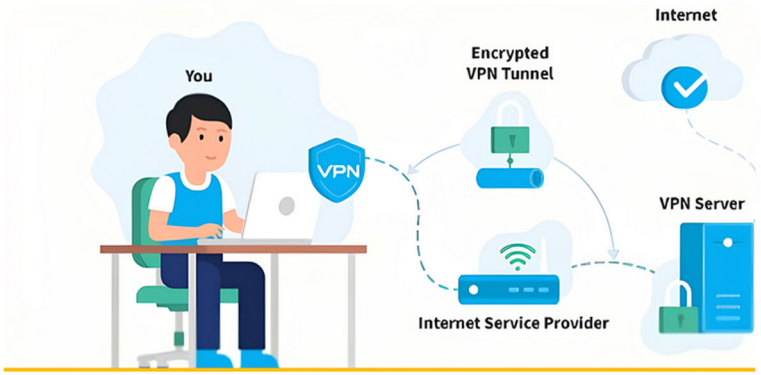


3. **Metropolitan Area Network (MAN)**:
    - Larger than a LAN but smaller than a WAN, typically covering a city.
    - Used by governments or businesses for city-wide connectivity.



4. **Personal Area Network (PAN)**:
    - Very small, usually centered around one person's devices, like Bluetooth or USB connections between a phone and laptop.

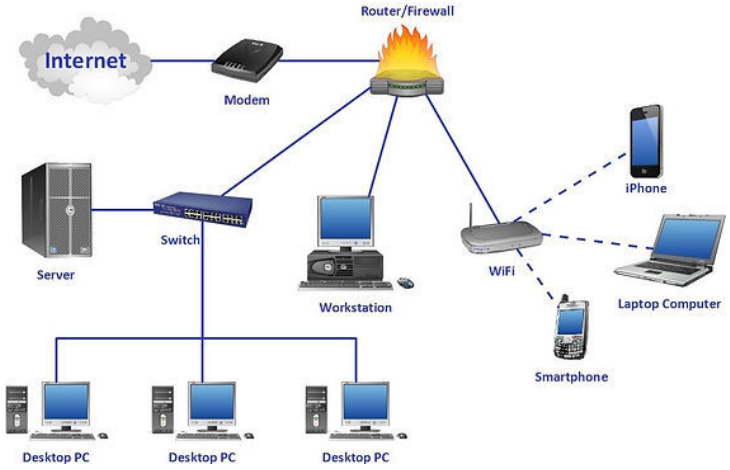
5. **Virtual Private Network (VPN)**:
    - A private network that uses a public network (like the internet) to connect remote sites or users.
    - It creates a secure and encrypted connection to safeguard data from interception.



3. Basic Network Components

To build a functional network, several core components are required:

1. **Nodes (Hosts/Devices)**:
    - Devices like computers, servers, and smartphones that connect to a network.
2. **Switches**:
    - Devices that connect multiple devices within a LAN. They route data to the correct destination.
3. **Routers**:
    - Devices that connect multiple networks (LAN to WAN, for example) and direct data packets to their destination.
4. **Firewalls**:
    - Network security systems that monitor and control incoming and outgoing traffic based on predetermined security rules.
5. **Access Points (APs)**:
    - Devices that allow wireless devices to connect to a wired network using Wi-Fi.
6. **Cabling and Wireless Media**:
    - **Ethernet cables (wired)** or **Wi-Fi (wireless)** connections that provide the means for data to move between devices.



4. Network Security Basics

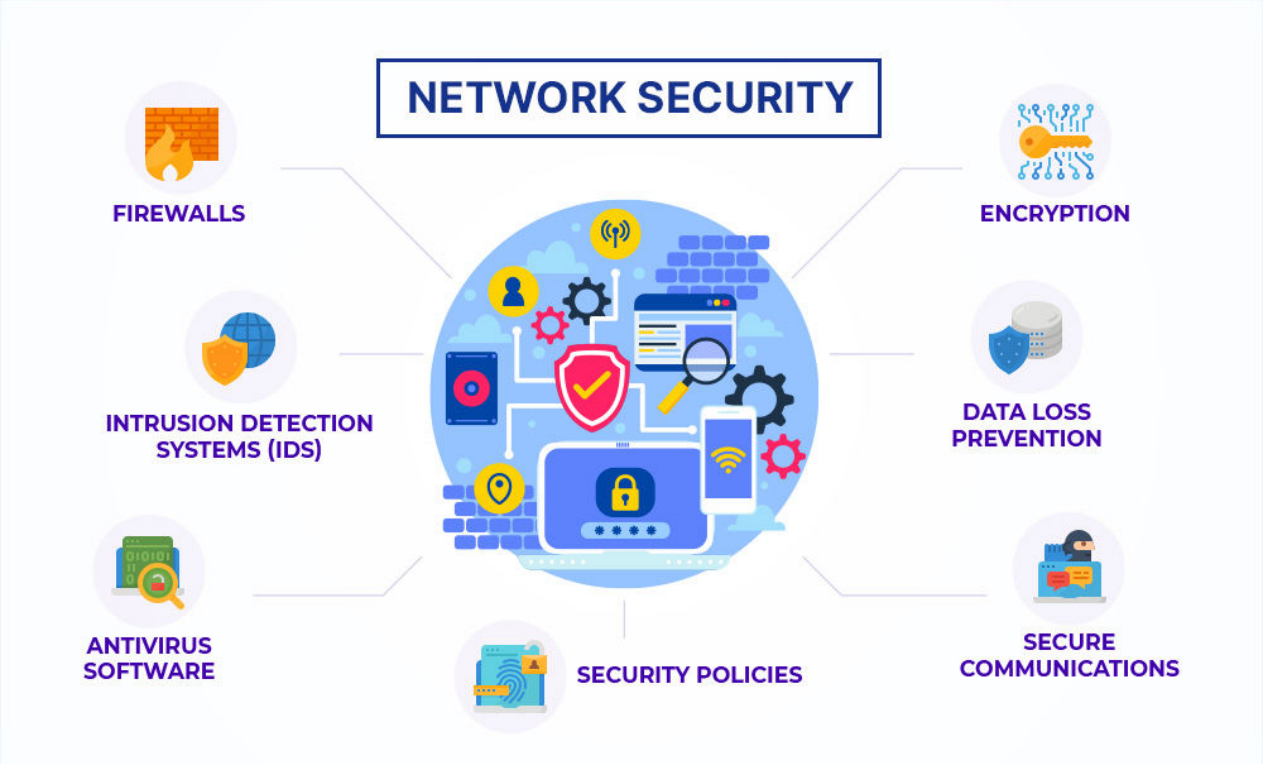
Network Security refers to policies, practices, and technologies used to protect a network and its resources from unauthorized access, misuse, malfunction, or destruction.

Key concepts:

1. **Availability**: Ensures that authorized users have access to the network and data when needed.
2. **Integrity**: Ensures that data is not altered during transmission or storage.
3. **Confidentiality**: Ensures that data is only accessible by authorized individuals.

Security Measures:

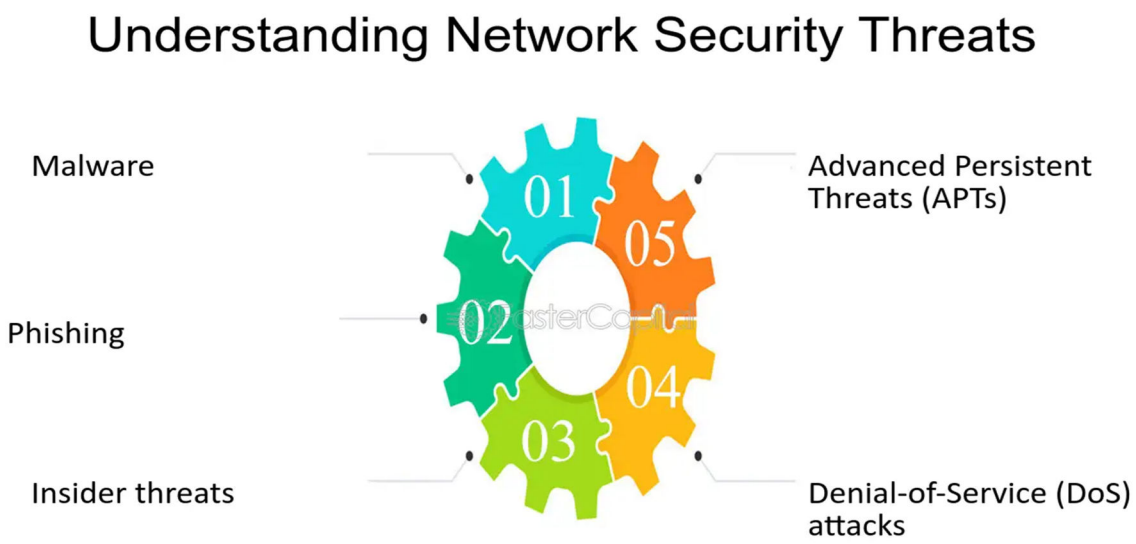
- **Firewalls**: Blocks or permits traffic between different network zones.
- **Encryption**: Converts data into an unreadable format to prevent unauthorized access.
- **Access Control**: Limits who can access the network based on credentials (username/password, multi-factor authentication).
- **Intrusion Detection Systems (IDS)**: Monitors network traffic for suspicious activity.



5. Understanding Network Threats

Modern networks face a variety of threats that can compromise data, reduce availability, or allow unauthorized access. Some common threats include:

1. **Malware** (e.g., viruses, worms, ransomware):
   - Software designed to disrupt, damage, or gain unauthorized access to systems.
2. **Phishing Attacks**:
   - Attempts to trick users into providing sensitive information (like passwords) through deceptive emails or websites.
3. **Denial of Service (DoS) Attacks**:
   - Overwhelms a network or service, making it unavailable to legitimate users.
4. **Man-in-the-Middle Attacks**:
   - An attacker intercepts communications between two parties, potentially altering or stealing data.
5. **Data Breaches**:
   - Unauthorized access to sensitive data, often due to weak security controls or insider threats.



Best Practices to Mitigate Threats:

- Implement strong firewalls.
- Regularly update and patch software and systems.
- Use multi-factor authentication.
- Educate users on safe internet and email usage.