



Al Mustaqbal University

College of Health and Medical Techniques

Computer Science

lecture 1

Network and security

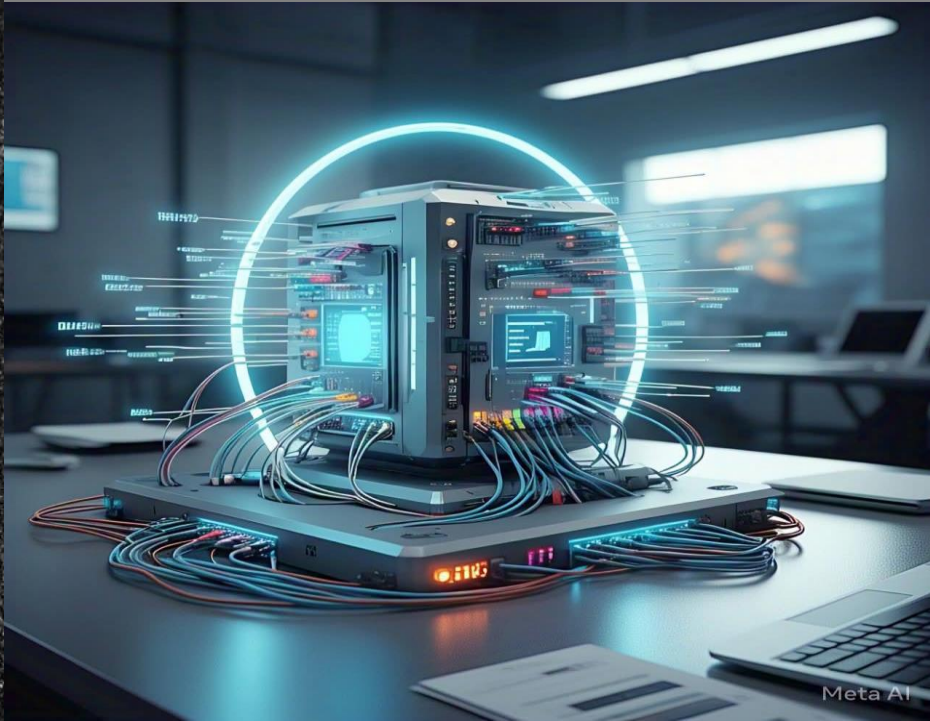
Asst. Lect. Mortada Haider

Introduction to Networks

A **network** is a system of interconnected devices that are capable of sharing data and resources. It allows for communication between devices, such as computers, smartphones, servers, and more. A network enables the sharing of information, files, and other resources like printers or storage.

Types of Networks

There are several types of networks based on their size, purpose, and the technology they use:



1- Local Area Network (LAN):

A LAN connects devices within a small geographic area, such as within a building .

It is often used in homes or businesses.

Example: A company's internal network connecting all employees' computers.

2- Wide Area Network (WAN):

A WAN connects LANs over large geographical distances. The internet is a global WAN.

Example: A business that has offices in different cities or countries.

3- Metropolitan Area Network (MAN):

A MAN is larger than a LAN but smaller than a WAN. It spans a city or large area.

Example: The network that connects several buildings in a city.

4- Personal Area Network (PAN):

A PAN is a small network for personal devices, typically within a range of a few meters.

Example: Connecting a smartphone, tablet, and laptop using Bluetooth.

Basic Network Components

1- Router:

- A device that forwards data packets between different networks, such as between a home LAN and the internet. Routers direct traffic to the right destination.

2- Switch:

- A device used within a network to connect multiple devices and allow them to communicate with each other.

3- Hub:

- A basic device that connects multiple devices on a network but without the intelligence of a switch. It broadcasts data to all devices.

4- Modem:

- A modem converts digital data from a computer into an analog signal that can be transmitted over telephone lines and vice versa.

5- Access Points:

- These are used in wireless networks to allow wireless devices to connect to a wired network.

6- Cables:

- Cables, such as Ethernet cables, are used to physically connect devices within a network.



Network Security

Network security refers to the policies, procedures, and technical measures used to protect the integrity, confidentiality, and availability of the data and resources in a network. The goal of network security is to prevent unauthorized access, or destruction of data and to ensure the reliability and performance of the network.



1- Firewalls:

- A firewall is a network security system that monitors and controls incoming and outgoing traffic based on predetermined security rules.

2- Intrusion Detection Systems (IDS):

- These systems monitor network traffic for suspicious activity or known threats, alerting administrators if any issues are found.

3- Encryption:

- Encrypting data ensures that even if data is intercepted, it cannot be read by unauthorized parties. Common protocols like SSL/TLS and IPsec are used to encrypt data.

4- Virtual Private Networks (VPNs):

- A VPN provides a secure and private connection over a less-secure network, such as the internet. It encrypts data between a user's device and the destination server.

5- Access Control:

- Access control mechanisms ensure that only authorized users can access certain resources within a network. This can include multi-factor authentication (MFA) and passwords.

Key areas in network security include:



Common Network Threats

- **Malware:**

Malicious software like viruses, worms, and Trojans that can damage systems, steal data, or take control of a network.

- **Phishing:**

A technique where attackers impersonate a trusted entity to trick users into revealing personal information like passwords or credit card numbers.

- **Man-in-the-Middle (MitM) Attacks:**

In a MitM attack, the attacker intercepts communication between two parties, often to steal sensitive data or inject malicious content.

- **DDoS (Distributed Denial of Service) Attacks:**

In a DDoS attack, an attacker floods a network or server with traffic from multiple sources, causing it to become overwhelmed and unavailable.

- **Social Engineering:**

This involves manipulating individuals into revealing confidential information or performing actions that compromise security. It can include tactics like pretexting, baiting, or tailgating.

- **Ransomware:**

A type of malware that locks users out of their systems or encrypts their data, demanding payment in exchange for the decryption key.



Thank You

Mortada Haider 

@mortada213 

www.mortada.h213@gmail.com 