جامعة المستقبل
AL MUSTAQBAL UNIVERSITY

كلية العلوم

قسم التقنيات الاحيائية الطبية

Lecture: (1)

Security and Networking

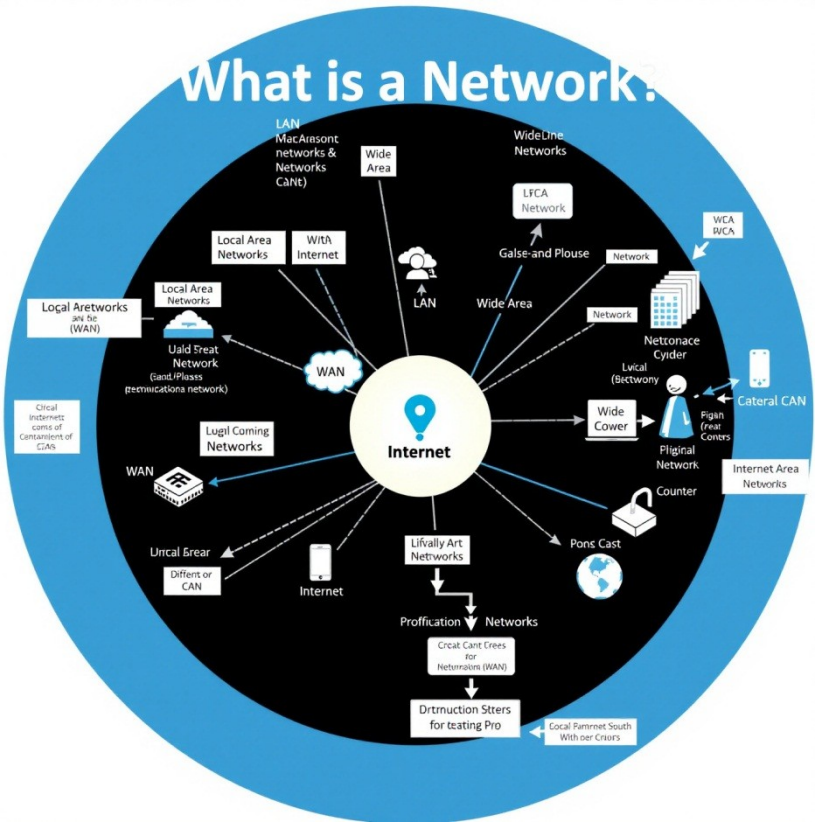
Subject: Computer Science (II)
Level: Second
Lecturer: Dr. Maytham N. Meqdad

Security and Networking:

- What is a network?
- Types of networks.
- Basic Network components.
- Network security basics
- Understanding network threats
- network troubleshooting

What is a Network?

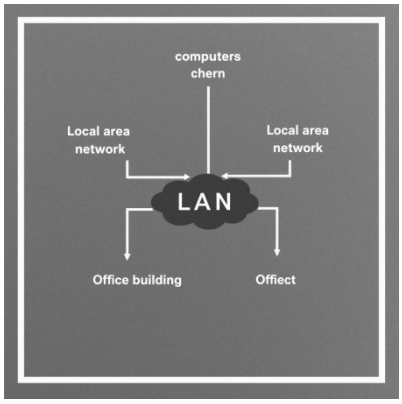
In the simplest terms, a network is a group of interconnected devices that can communicate with each other. These devices can be computers, smartphones, servers, printers, or even home appliances. They share data, resources, and services through a common communication channel, such as cables, wireless signals, or the internet. Networks enable us to work collaboratively, access information quickly, and connect with people across the globe.



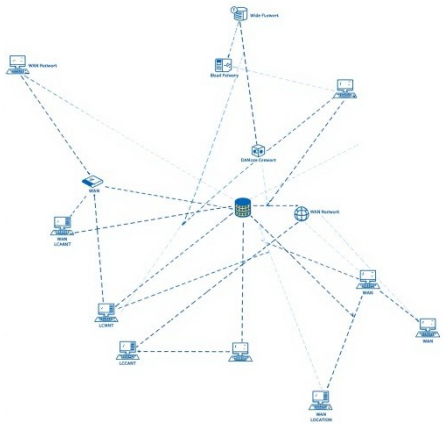
Types of Networks

Networks come in various sizes and configurations, depending on their purpose and scale. Here are some common types:

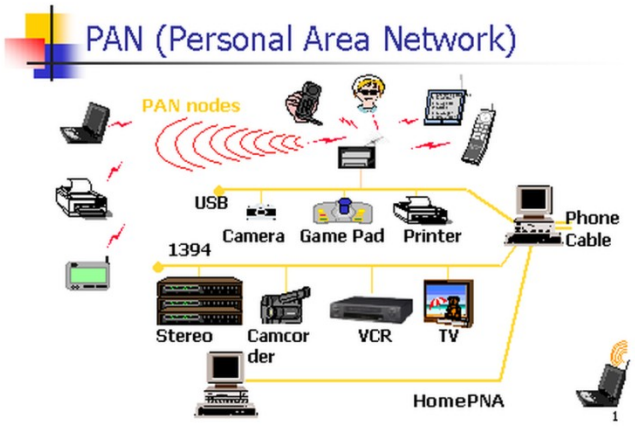
- LAN (Local Area Network): A network that connects devices within a limited geographical area, typically a single building or office.



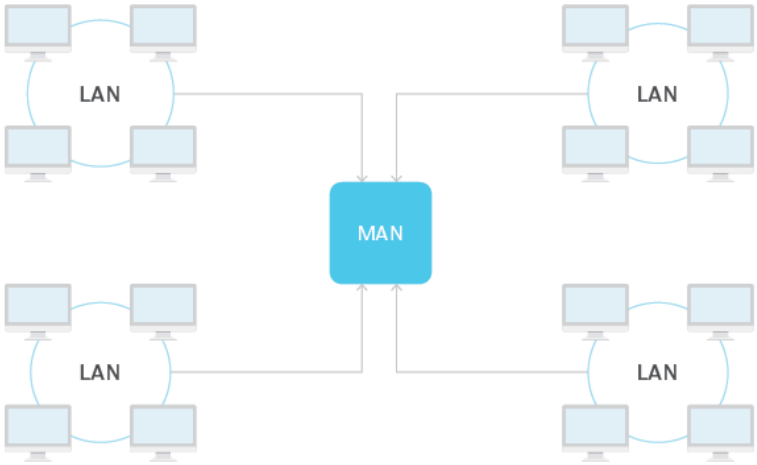
- WAN (Wide Area Network): A network that spans across a wide geographical area, connecting multiple LANs or other networks over long distances.



- PAN (Personal Area Network): A network that connects devices within a personal space, such as a smartphone and a wireless headset.



- MAN (Metropolitan Area Network): A network that connects devices within a city or metropolitan area, providing connectivity for businesses and residents.

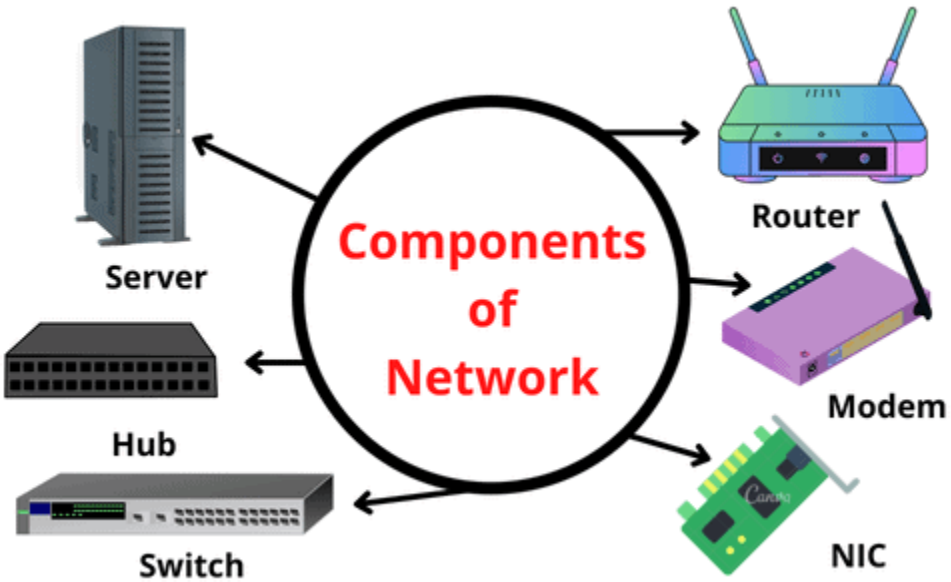


These networks are essential for communication, data sharing, and resource access in modern society.

Basic Network Components

A network is composed of several fundamental components that work together to enable communication. These include:

- Nodes: Any device connected to the network, such as computers, servers, printers, or smartphones.
- Links: The physical or logical connections between nodes, allowing data transmission.
- Protocols: Sets of rules that govern communication between devices on the network, ensuring data is sent and received correctly.
- Network Interface Card (NIC): A device that connects a node to the network and manages data transmission.
- Routers: Devices that connect networks, forwarding data packets between networks and managing network traffic.
- Switches: Devices that connect devices within a LAN, creating a dedicated connection between two nodes.
- Hubs: Devices that connect multiple devices on a LAN, but do not offer a dedicated connection.



Network Security Basics

Network security is essential to protect your network from unauthorized access, data breaches, and other malicious activities. It encompasses various practices and technologies aimed at maintaining the confidentiality, integrity, and availability of your network data and resources. Here are some key concepts:

- Authentication: Verifying the identity of users and devices before granting access to the network.
- Authorization: Determining the level of access granted to authenticated users and devices.
- Encryption: Converting data into an unreadable format to protect it during transmission and storage.
- Firewalls: Network security devices that block unauthorized access to your network by filtering incoming and outgoing traffic.
- Intrusion Detection and Prevention Systems (IDS/IPS): Tools that monitor network traffic for suspicious activity and either alert administrators or block malicious traffic.

Understanding Network Threats

Network threats pose a constant risk to organizations and individuals, potentially causing data breaches, system failures, and financial losses. Some common network threats include:

Malware: Malicious software designed to harm or steal data from your network.

Phishing: Attempts to trick users into revealing sensitive information through fraudulent emails, websites, or messages.

Denial-of-Service (DoS) Attacks: Attempts to overload a network or server, making it unavailable to legitimate users.

Man-in-the-Middle (MitM) Attacks: Attacks where an attacker intercepts communication between two parties, stealing or modifying data.

Social Engineering: Attempts to manipulate users into divulging sensitive information or performing actions that compromise network security.

Securing Your Network

Securing your network requires a multi-layered approach that addresses various aspects of security. Here are some key steps you can take:

- Use Strong Passwords: Implement strong passwords for all user accounts and devices, ensuring they are long, complex, and unique for each account.
- Keep Software Up-to-Date: Regularly update software on all devices to patch security vulnerabilities and mitigate potential threats.
- Use Anti-Virus and Anti-Malware Software: Install and maintain robust anti-virus and anti-malware software to protect your network from malicious software.
- Implement a Firewall: Configure a firewall to block unauthorized access to your network and filter incoming and outgoing traffic.
- Educate Users: Train users about common network security threats and best practices to avoid falling prey to phishing attempts and other social engineering tactics.

Network Troubleshooting

Network issues can occur at any time, causing disruption to communication and data access. Identifying and resolving these issues efficiently requires a systematic approach to troubleshooting. Here are some common steps involved:

- Identify the Problem: Clearly define the symptoms and scope of the network issue, including affected devices, services, and network performance degradation.
- Check Basic Connections: Verify physical connections between devices, cables, and network devices, ensuring they are secure and functioning correctly.
- Test Network Connectivity: Use diagnostic tools to test network connectivity, pinging devices and websites to check for network reachability.
- Analyze Network Logs: Review network logs and event logs to identify any error messages, warning signs, or suspicious activity.
- Consult Documentation: Refer to relevant documentation for network devices, software, and protocols to understand configuration settings and troubleshooting guides.

- Seek Expert Assistance: If you're unable to resolve the issue independently, contact network professionals or technical support for assistance.