Lecture 1

SECURITY AND NETWORKING

What is a network?

A network is simply two or more devices that are connected via software and hardware so they can communicate with each other. Each device connected to a network is referred to as a node. A node can be a computer, a peripheral such as a printer or a game console, or a network device such as a router.

Importance of networks

- Resource Sharing: Allows users to share printers, files, and internet connections.
- Data Management: Facilitates centralized data storage and access (e.g., cloud services).
- Improved Communication: Supports communication tools like email, instant messaging, and video conferencing.

Benefits of networks

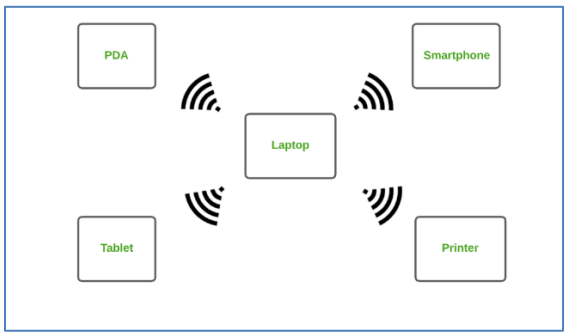
There are several benefits to having computers networked:

- Sharing an Internet connection.
- Sharing printers and other peripherals.
- Sharing files.
- Online gaming and home entertainment.
- Telephone.
- Common communications: Devices running different operating systems can communicate on the same network.

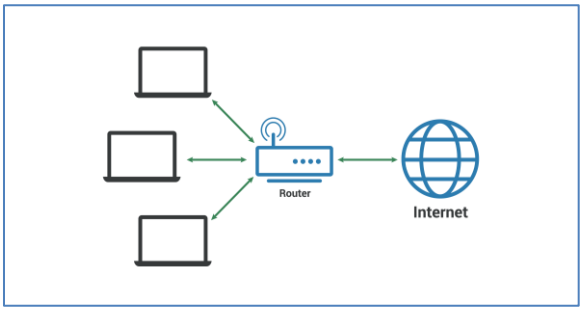
Types of networks

Networks can range from the smallest network of just one person, in one room with multiple connected devices, to the largest network that spans between cities and even the world. Below are common types of networks based on size and range:

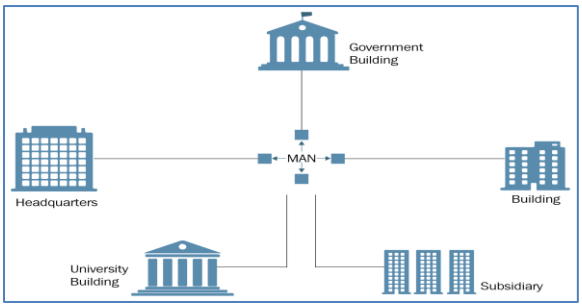
- A personal area network (PAN) is a network used for communication among devices close to one person, such as smartphones and tablets using wireless technologies such as Bluetooth and Wi-Fi.



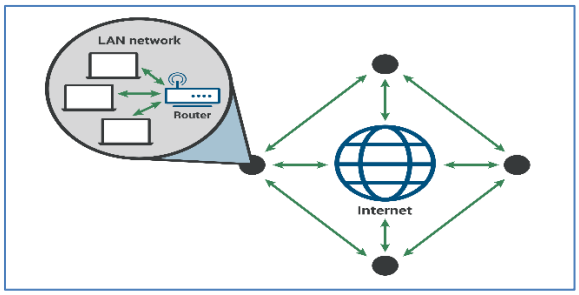
- A local area network (LAN) is a network in which the nodes are located within a small geographical area. Examples include a network in a computer lab at college.



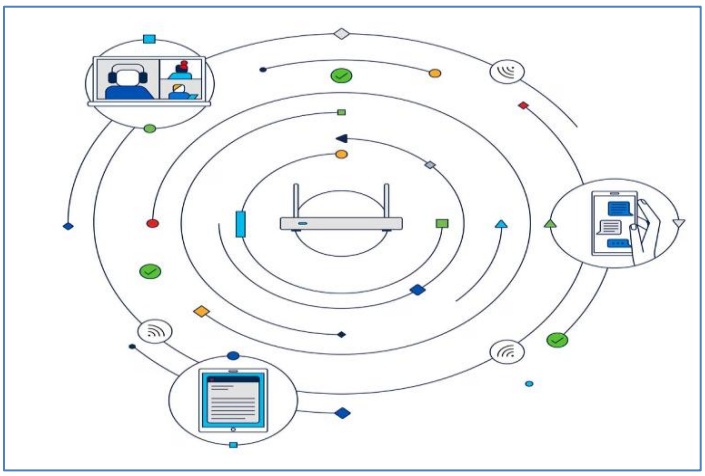
- A metropolitan area network (MAN) is a large network designed to provide access to a specific geographical area, such as an entire city.



- A wide area network (WAN) spans a large physical distance, interconnecting cities or countries.



- Wireless local area network (WLAN) is a group of computers or other devices that form a network based on radio transmissions. A WLAN allows users to move around the coverage area – such as a home, office, or campus while maintaining a network connection.

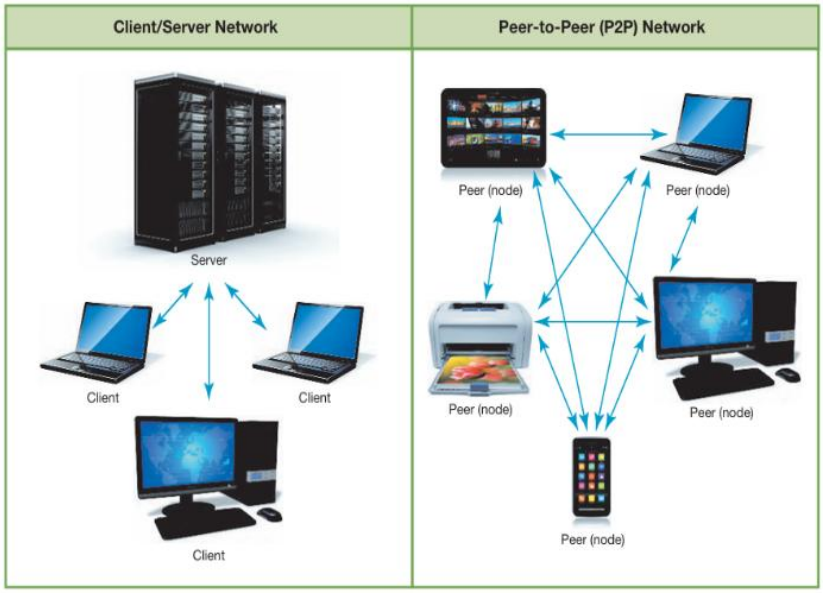


Levels of administration network

A network can be administered in two main ways — centrally or locally:

- Central administration *(Client/Server Network)*: In a centrally administered network, tasks performed from one computer can affect the other computers on the network.

- Local administration *(Peer-to-Peer (P2P) Network)*: In a locally administered network, the configuration and maintenance of the network must be performed on each computer attached to the network.



Ethernet protocols

The vast majority of home and corporate networks are Ethernet networks. An Ethernet network is so named because it uses the Ethernet protocol as the means (or standard) by which the nodes on the network communicate.

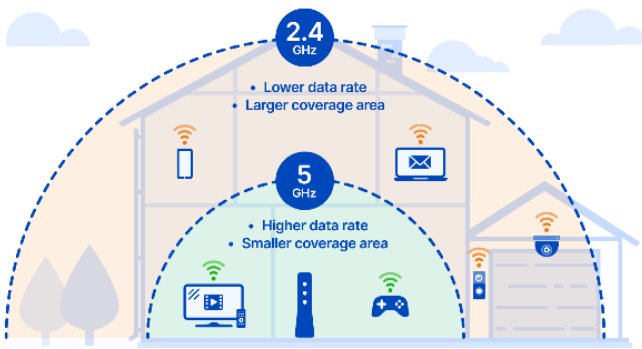
The Ethernet protocol was developed by the Institute of Electrical and Electronics Engineers (IEEE), which develops many standard specifications for electronic data transmission that are adopted throughout the world.

There are different standards for wired and wireless Ethernet networks:

- Standard for wired Ethernet networks:
  The standard for wired Ethernet networks is IEEE 802.3, or gigabit Ethernet (GbE), which supports data transfer rates up to 1 Gbps. Faster versions, such as 10, 40, and 100 GbE, offer speeds of 10, 40, and 100 Gbps, respectively.

- Standard for wireless Ethernet networks:
  Wireless networks (Wi-Fi), based on the IEEE 802.11 standard, were previously named using letter-based versions (e.g., 802.11n, 802.11ac). To simplify naming, the Wi-Fi Alliance now uses generation numbers: 802.11ac is Wi-Fi 5, and 802.11n is Wi-Fi 4.

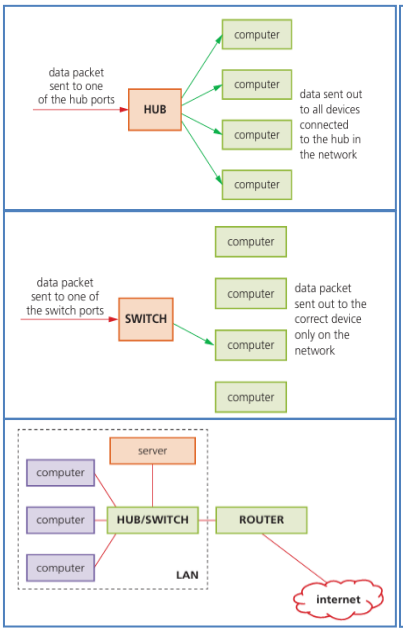
  Wi-Fi 5 is faster and has a better range than Wi-Fi 4. While Wi-Fi 4 operates on both 2.4 GHz and 5 GHz.
  Earlier standards used only 2.4 GHz, causing interference with other devices. Wi-Fi 5 operates at 5 GHz, reducing signal interference.

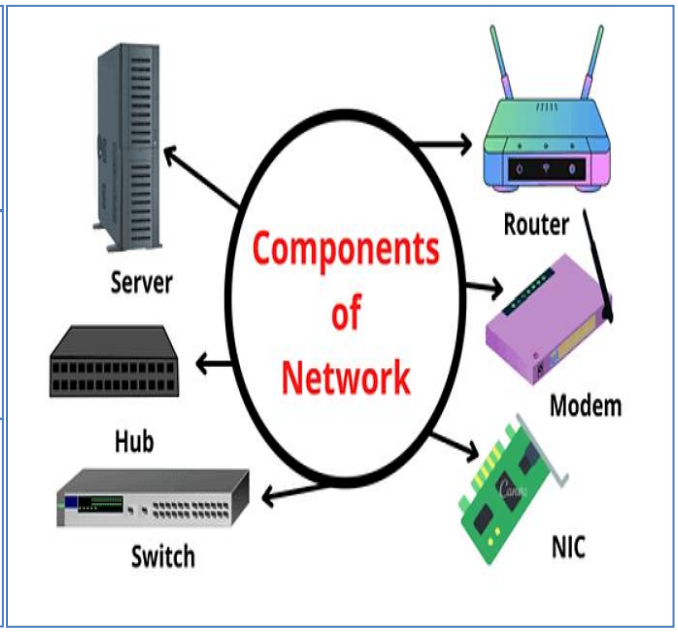


Basic network components

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.

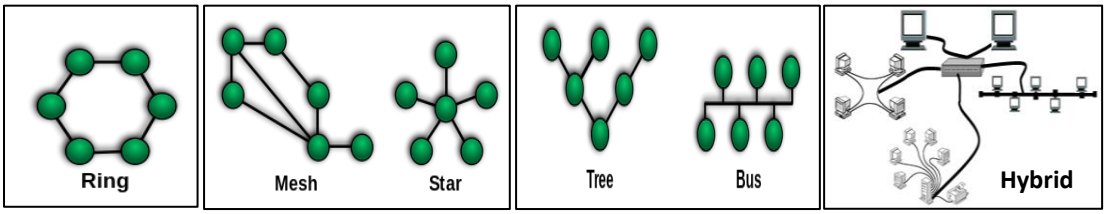




Network topologies

Common Topologies:

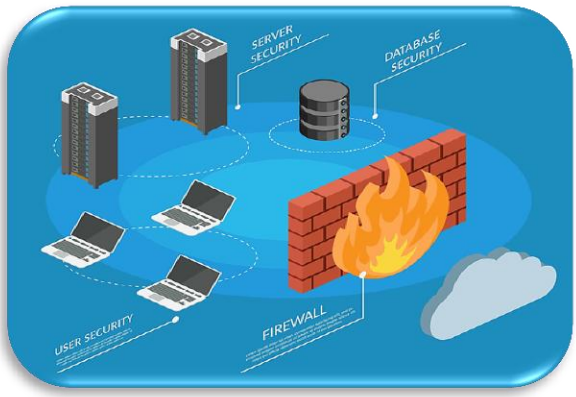
- Star: All devices are connected to a central hub/switch. Most common in LANs.
- Bus: All devices share a single communication line. Simple but can be slow.
- Ring: Devices are connected in a circular format. Data travels in one direction.
- Mesh: Devices are interconnected. Highly reliable but complex and expensive.
- Tree: A mix of star and bus topology; devices connect in a hierarchical manner.
- Hybrid: A combination of two or more topologies.



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:*

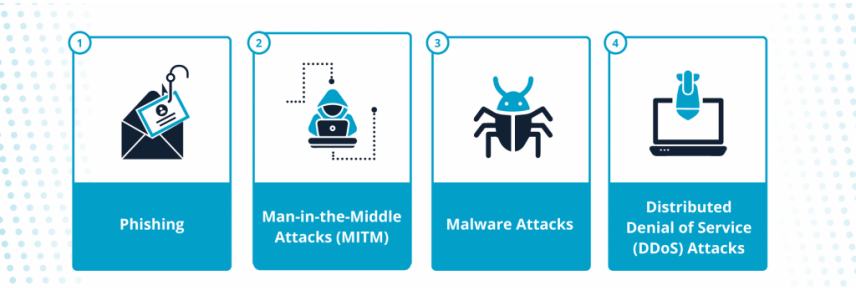
- Authentication: Verifying the identity of users and devices before granting access to the network.
- Authorization: Determining the level of access granted to authenticated users and devices.
- Encryption: Converting data into an unreadable format to protect it during transmission and storage.
- Firewalls: 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:*

- Phishing: Attempts to trick users into revealing sensitive information through fraudulent emails, websites, or messages.
- Man-in-the-Middle (MitM) Attacks: Attacks where an attacker intercepts communication between two parties, stealing or modifying data.
- Malware: Malicious software designed to harm or steal data from your network.
- Distributed Denial-of-Service (DDoS) Attacks: Attempts to overload a network or server, making it unavailable to legitimate users.
- 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*:

- 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.