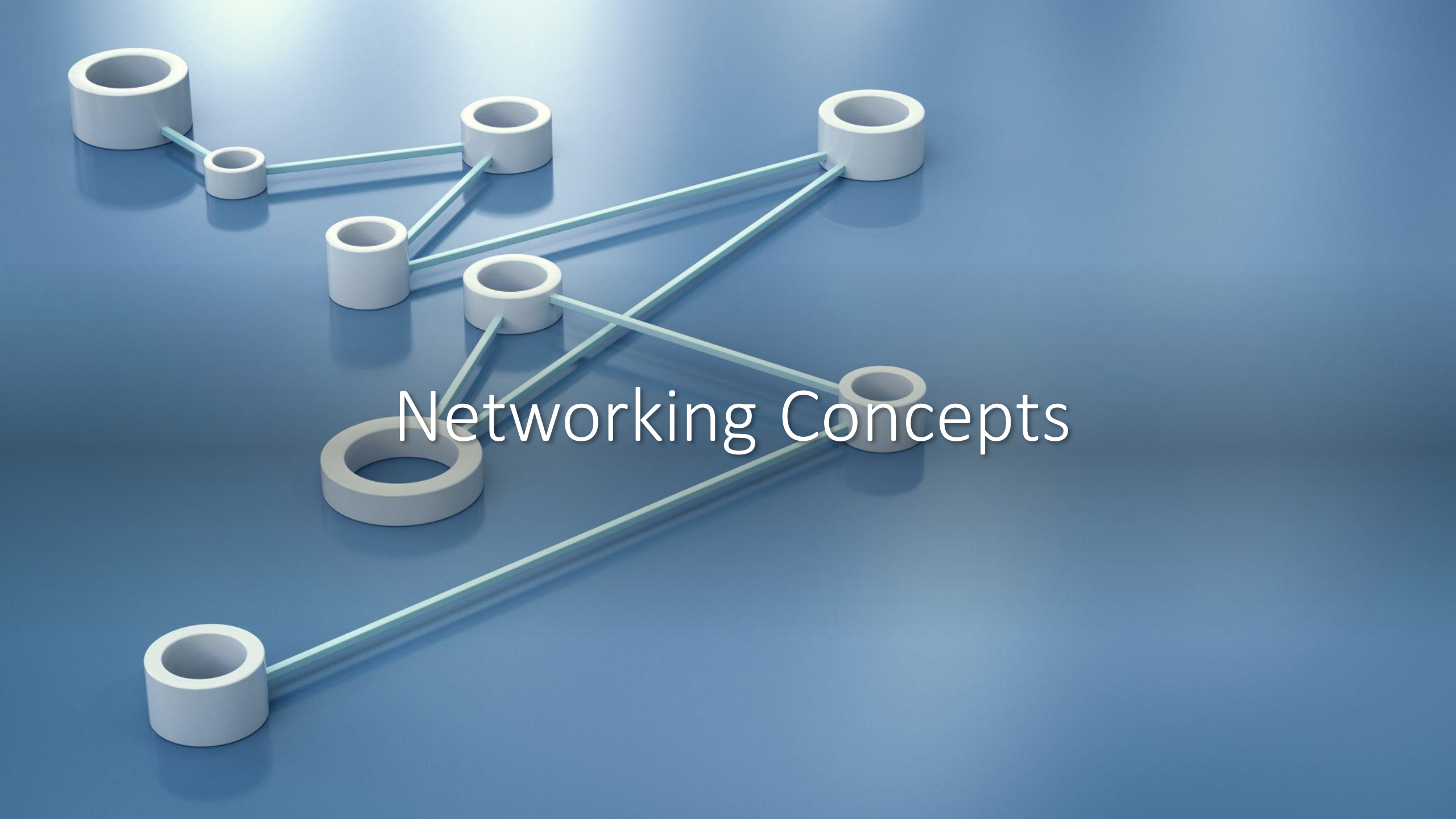

Networking Concepts

What is networking?

Computer networking refers to connecting multiple computers and other devices to share resources, exchange information, and communicate with each other. It enables the transfer of data and the sharing of resources such as files, printers, and internet connections among connected devices.

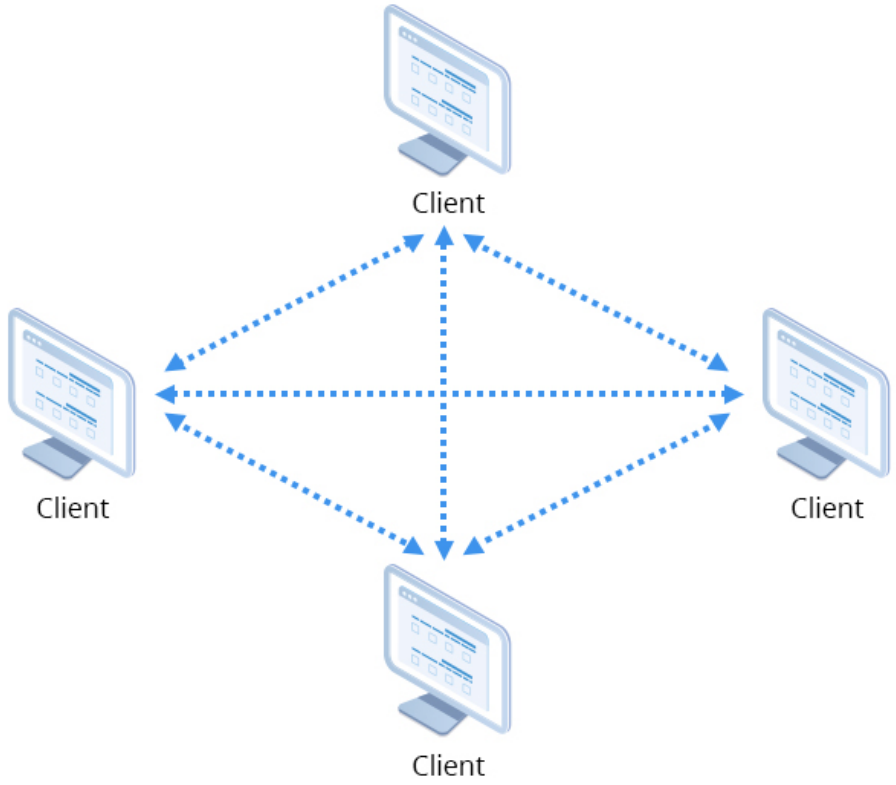
Types of Networks

Peer-to-Peer

In a *peer-to-peer* network, each host can provide network resources to other hosts or use resources located on other hosts. Each host providing resources controls access to the resources.

Advantages of peer-to-peer networks include:

- Easy implementation
- Inexpensive
- Disadvantages of peer-to-peer networks include:
- Difficult to expand (not scalable)
- Difficult to support
- Lack centralized control
- No centralized storage



Types of Networks Continued

Client Server

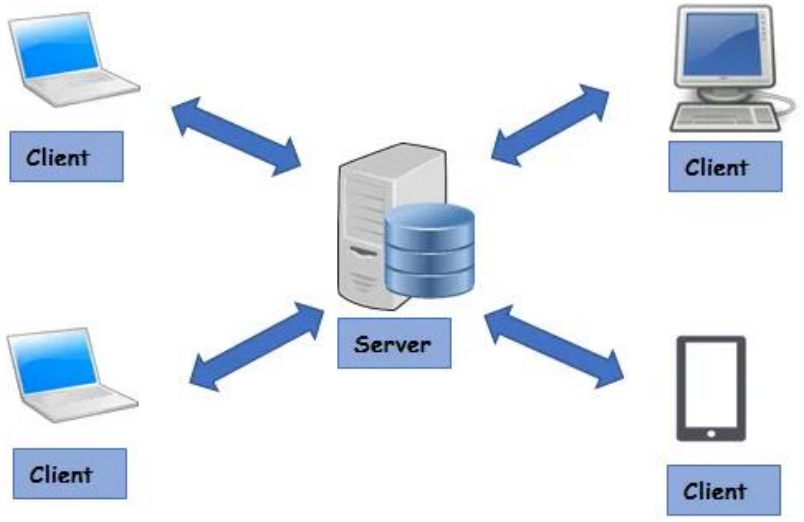
In a *client-server* network, hosts have specific roles. For example, some hosts are assigned server roles that allow them to provide network resources to other hosts. Other hosts are assigned client roles that allow them to consume network resources.

Advantages of client-server networks include the following:

- Easy to expand (scalable)
- Easy to support
- Centralized services
- Easy to back up

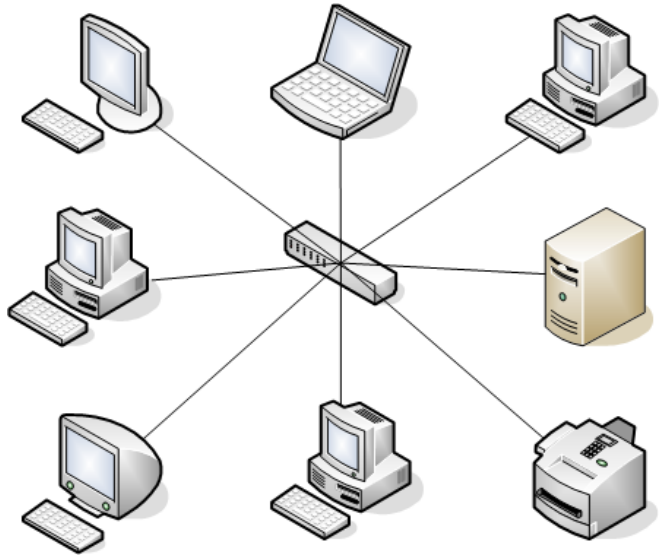
Disadvantages of client-server networks include the following:

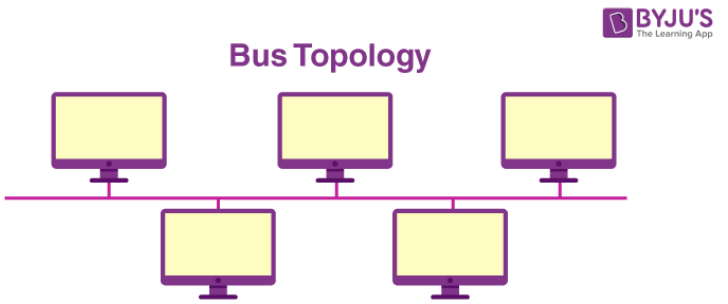
- Expensive server operating systems
- Extensive advanced planning required

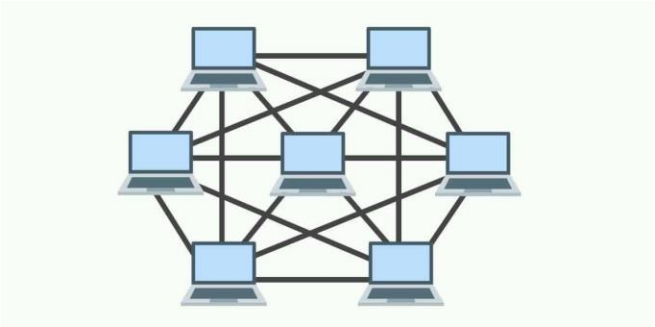


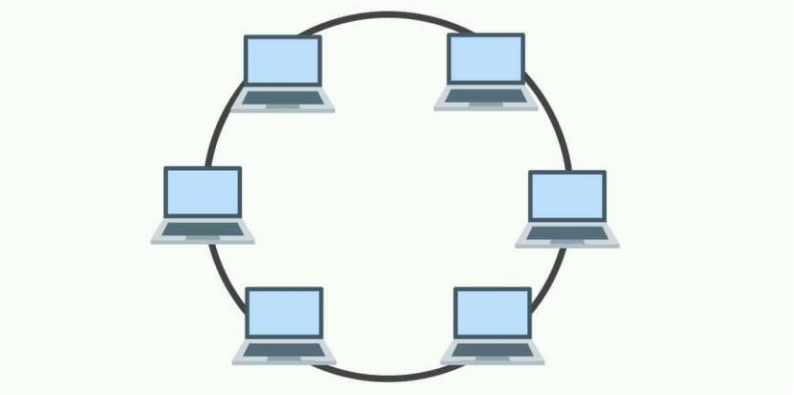
Network Topologies

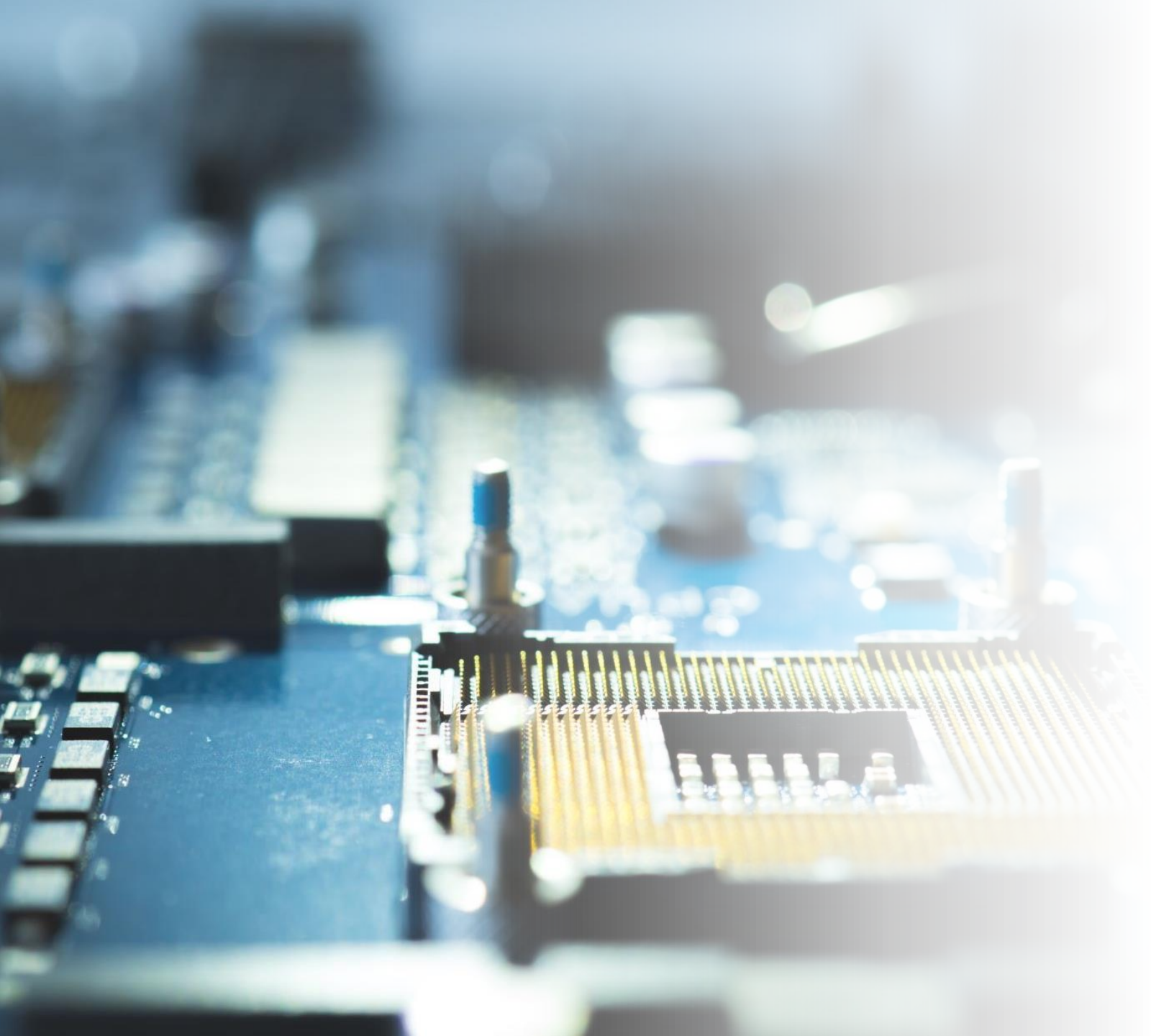
- Bus Topology: Devices are connected to a central bus or backbone.
- Star Topology: Devices are connected to a central hub or switch.
- Ring Topology: Devices are connected in a closed loop.
- Mesh Topology: Devices are interconnected, providing redundancy and fault tolerance.











Network Components

A computer network consists of various components that work together to enable communication and data exchange between devices.

Devices

Routers: Routers are responsible for routing data between different networks. They connect multiple networks and direct traffic between them.

Switches: Switches are used to create a network infrastructure within a local area network (LAN). They forward data only to the specific devices that need it.

Modems: Modems connect the network to the internet service provider (ISP) and are essential for internet access.

Network Infrastructure

Hubs: While less common today, hubs were used to connect multiple devices in a LAN. Unlike switches, hubs do not intelligently forward data and broadcast it to all connected devices.

Bridges: Bridges connect and filter traffic between two or more network segments to improve network performance.

Gateways: Gateways act as translators between different network protocols or data formats, allowing communication between networks with different architectures.

Network Security

Firewalls: As mentioned earlier, firewalls protect the network from unauthorized access and threats.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS): These systems monitor network traffic for suspicious activity and can take action to block or mitigate threats.

Encryption: Secure communication is achieved through encryption methods such as SSL/TLS for web traffic and VPNs for secure remote access.

IP Addresses

- An IP address, which stands for Internet Protocol address, is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.

<u>These addresses serve two main purposes:</u>

- Host or Network Identification: IP addresses are used to identify and locate devices on a network. They can pinpoint a specific device or a network segment, depending on the type of IP address being used.
- Routing of Data: IP addresses play a crucial role in routing data packets across the internet and other computer networks. Routers and other networking equipment use IP addresses to determine where to send data packets so that they reach their intended destination.

<u>There are two primary versions of IP addresses in use today:</u>

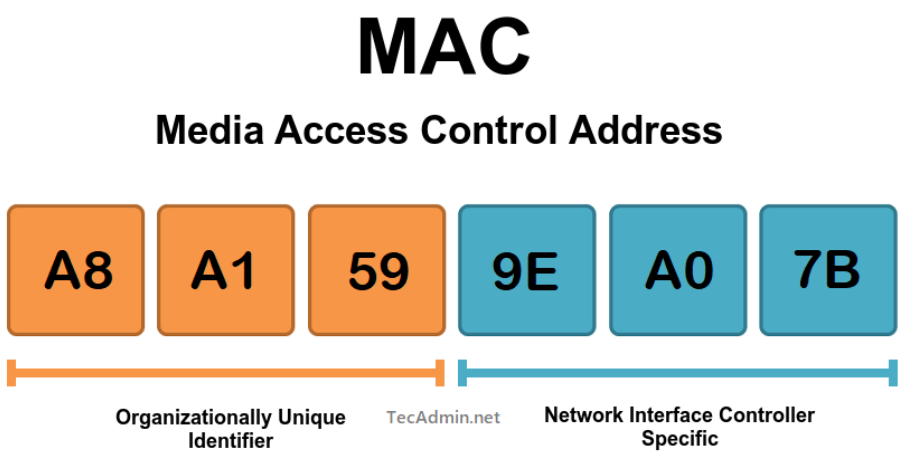
- IPv4 - example 192.168.1.1
- IPv6 - example 2001:0db8:85a3:0000:0000:8a2e:0370:7334

<u>IP addresses can be further categorized into two main types:</u>

- Public IP Address: This is the address that is assigned to a device by an Internet Service Provider (ISP) and is used to identify it on the wider internet. Public IP addresses are unique and routable across the internet.
- Private IP Address: These addresses are used within private networks, such as a home or business network. They are not directly routable on the internet and are used for local network communication. Common ranges for private IP addresses include 192.168.x.x and 10.x.x.x.

MAC Addresses

- MAC (Media Access Control) addressing is a method used in networking to uniquely identify and address individual devices on a local area network (LAN). Unlike IP addresses, which are used for routing data across networks, MAC addresses are used for communication within a single network segment, such as a Wi-Fi network or an Ethernet LAN.



Subnetting and networking

- NetworkChuck: what is an IP Address?

  NetworkChuck: Subnetting

Networking Protocols

- Mental Outlaw: Common Network Ports and Protocols