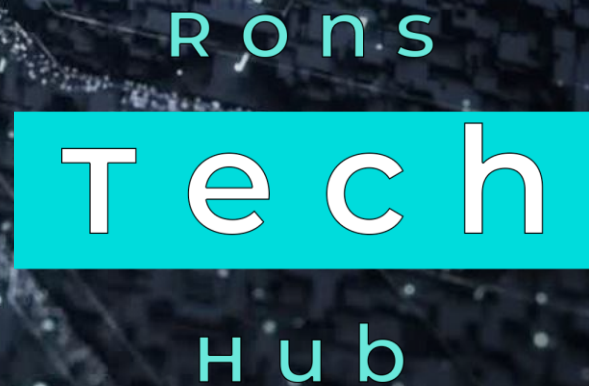


AAQ IT Unit 2: Cyber Security and Incident Management



B1: Network Types



Network Architectures and Vulnerabilities



Organisations use different network architectures to connect devices.



The way a network is designed affects its security and performance.



Poor network design can create vulnerabilities.



Understanding network architectures helps improve security.

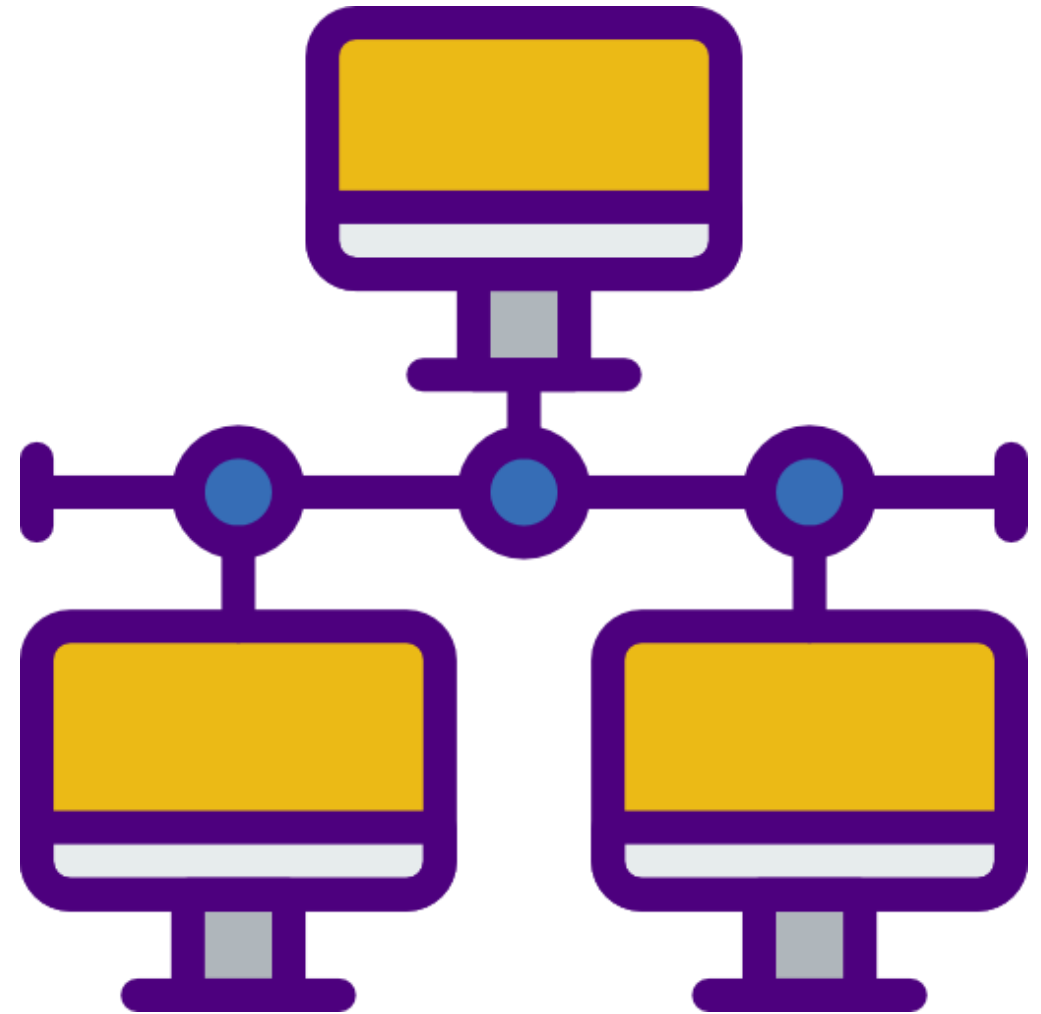
RONS

Tech

Hub

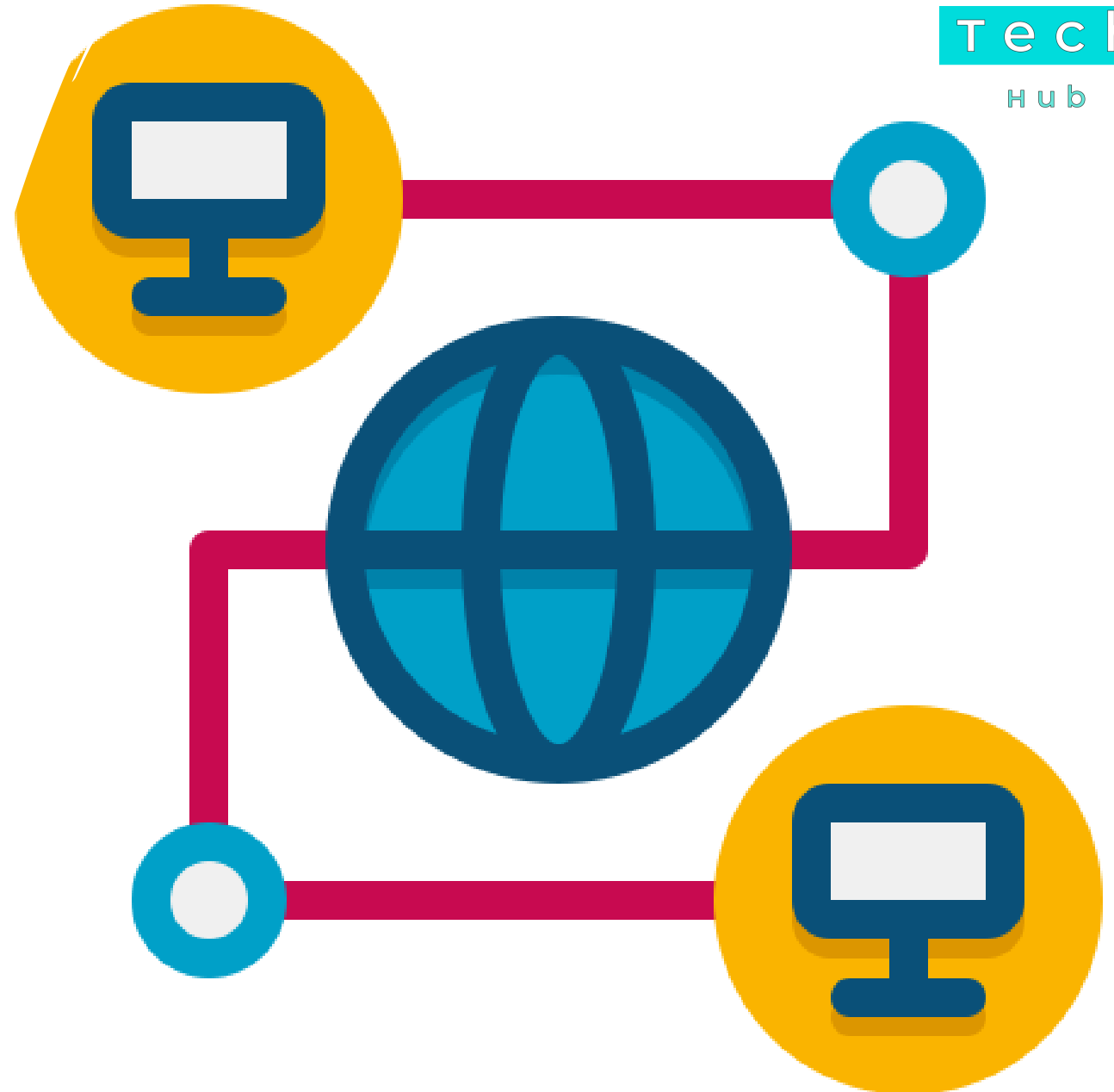
Local Area Network (LAN)

- A Local Area Network (LAN) connects devices within a small area.
- LANs are commonly found in schools, homes, and offices.
- Devices usually connect using Ethernet cables or Wi-Fi.
- LANs are normally owned and managed by one organisation.



Wide Area Network (WAN)

- A Wide Area Network (WAN) connects networks across large distances.
- The internet is the largest example of a WAN.
- WANs often connect multiple offices or locations together.
- Data usually travels through telecommunications providers.

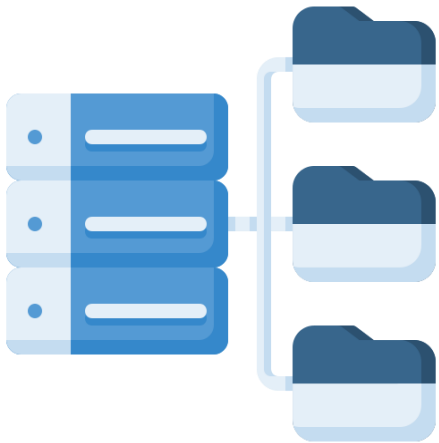


Wireless Local Area Network (WLAN)

- A WLAN is a LAN that uses wireless connections.
- Devices connect using Wi-Fi instead of network cables.
- WLANs provide flexibility and mobility for users.
- Poorly secured WLANs can be vulnerable to attack.



Storage Area Network (SAN)



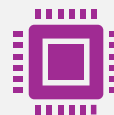
A Storage Area Network (SAN) provides shared storage to servers.



SANs are commonly used in data centres.



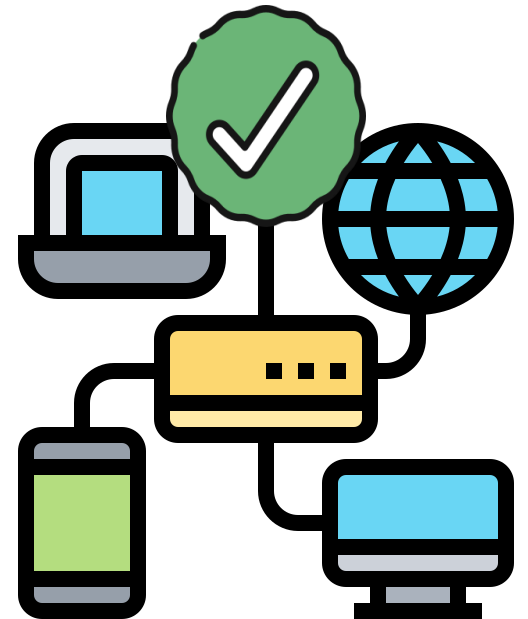
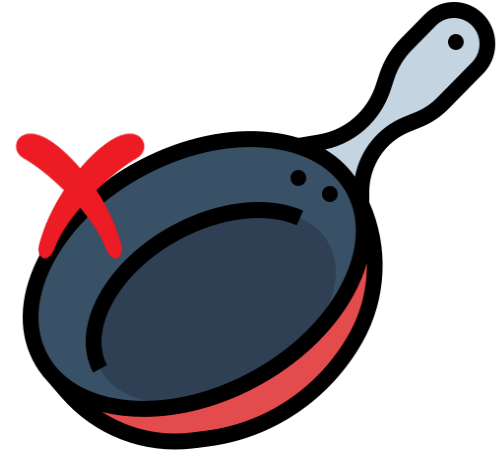
They allow large amounts of data to be stored efficiently.



SANs improve data availability and performance.

Personal Area Network (PAN)

- A Personal Area Network (PAN) connects devices over a short distance.
- **"Bluetooth"** is a common PAN technology.
- Examples include wireless headphones and smartwatches.
- PANs are usually used by a single person.



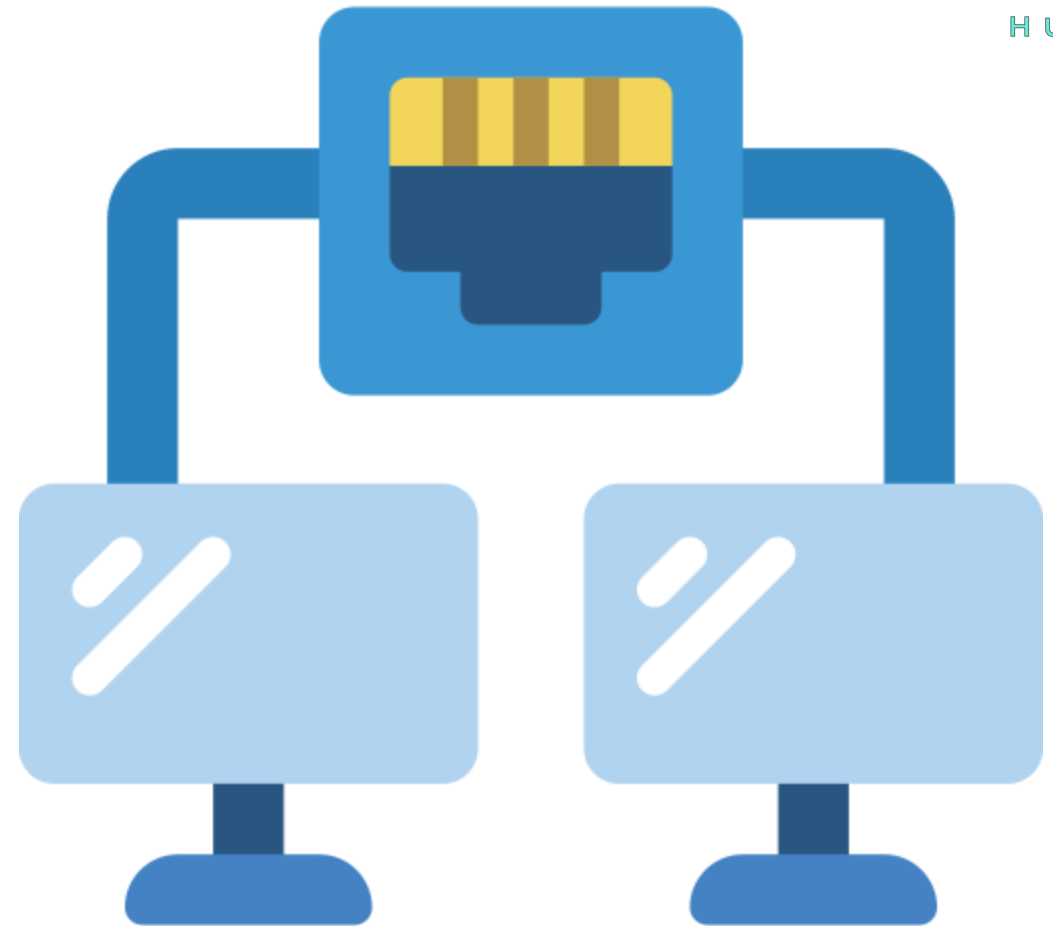
Metropolitan Area Network (MAN)

- A Metropolitan Area Network (MAN) covers a city or large town.
- It is larger than a LAN but smaller than a WAN.
- Universities and local authorities may use MANs.
- MANs connect multiple buildings within a region.



Virtual Local Area Network (VLAN)

- A VLAN creates separate logical networks on the same physical network.
- Devices can be grouped based on their role or department.
- VLANs improve network management and security.
- Traffic between VLANs can be controlled and monitored.





Virtual Private Network (VPN)

- A VPN creates a secure connection over a public network.
- VPNs encrypt data travelling between locations.
- They are often used for remote working.
- VPNs help protect data from interception.

RONS

Tech

Hub

Network Topologies



A topology describes how devices are connected in a network.



Different topologies have different strengths and weaknesses.



The choice of topology affects reliability and security.

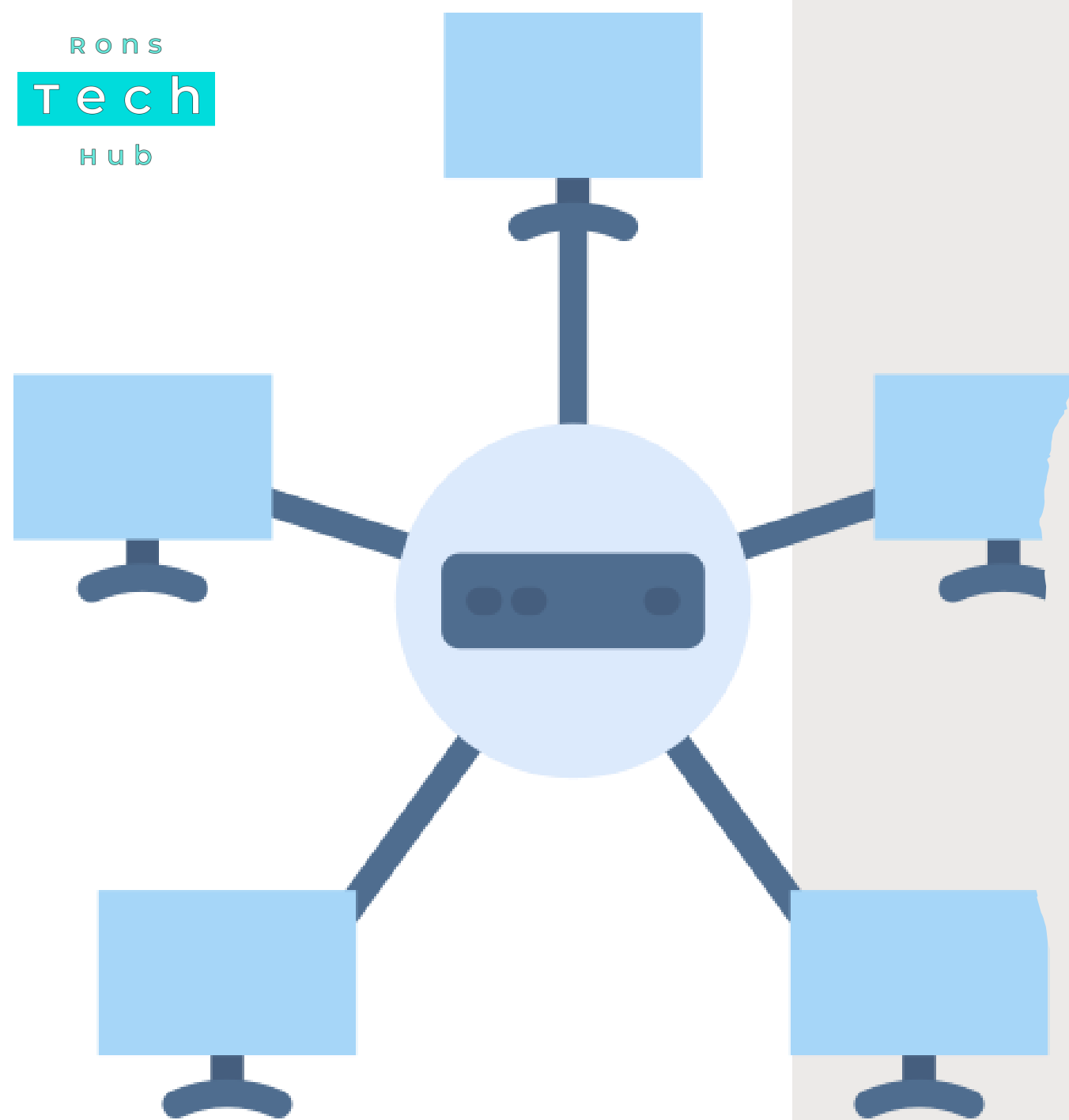


Organisations select topologies based on their requirements.

RONS

Tech

Hub

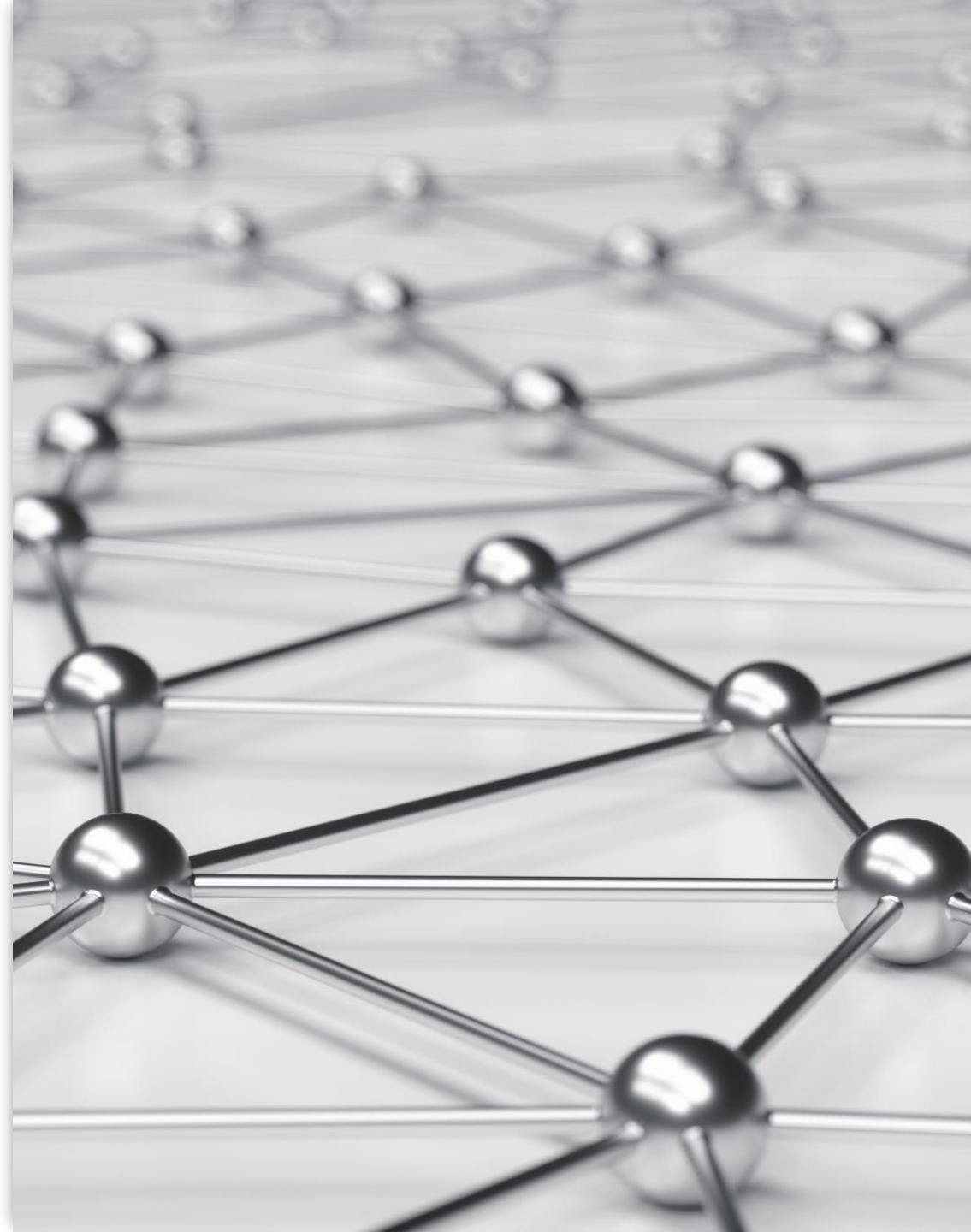


Star Topology

- In a star topology, all devices connect to a central switch.
- This is the most common topology used today.
- If one cable fails, only one device is affected.
- If the central switch fails, the entire network is affected.

Mesh Topology

- In a mesh topology, devices have multiple connections.
- Data can travel through different paths if one path fails.
- Mesh networks provide high reliability and redundancy.
- They are usually more expensive to implement.



Bus Topology



A bus topology uses a single shared communication cable.



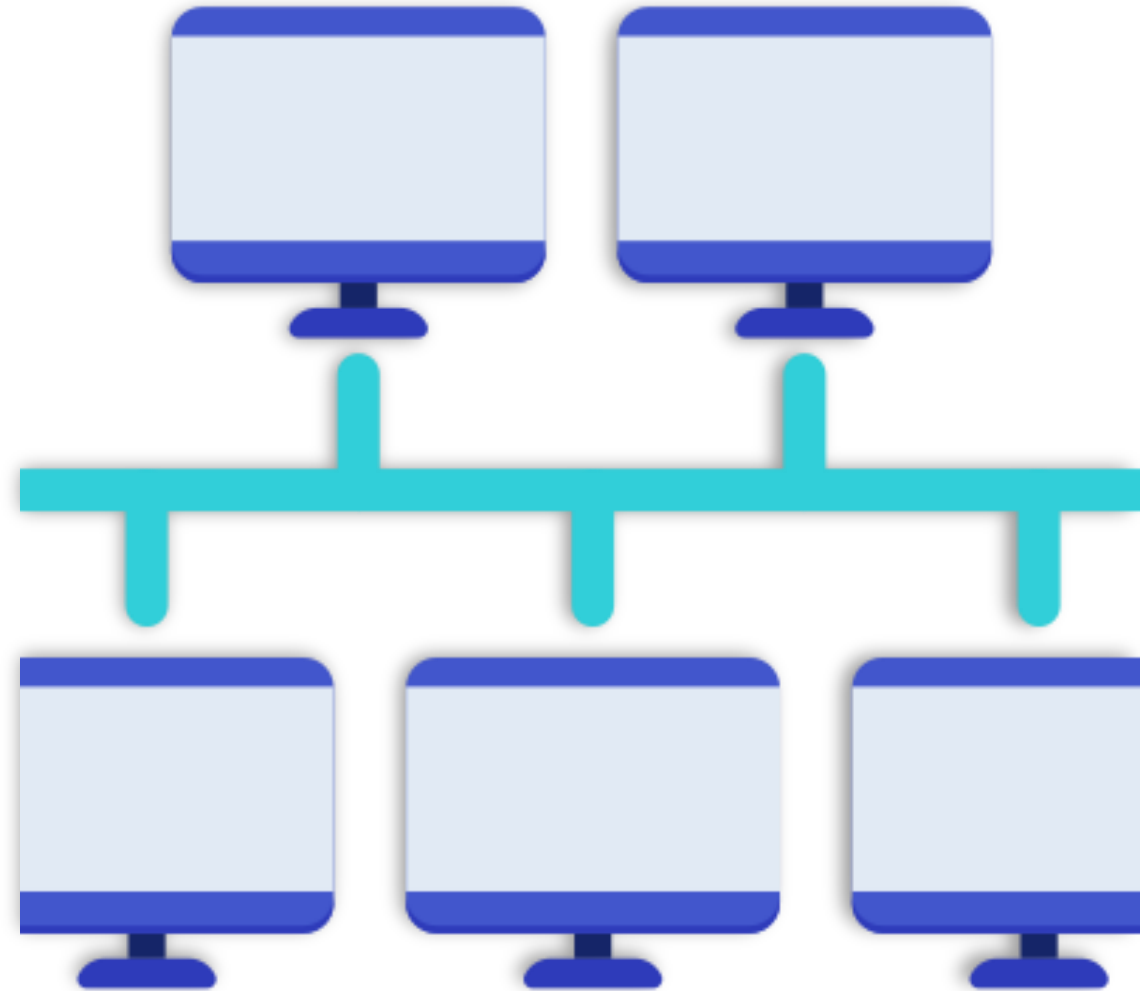
All devices send and receive data through the same cable.



Bus networks are simple and inexpensive.

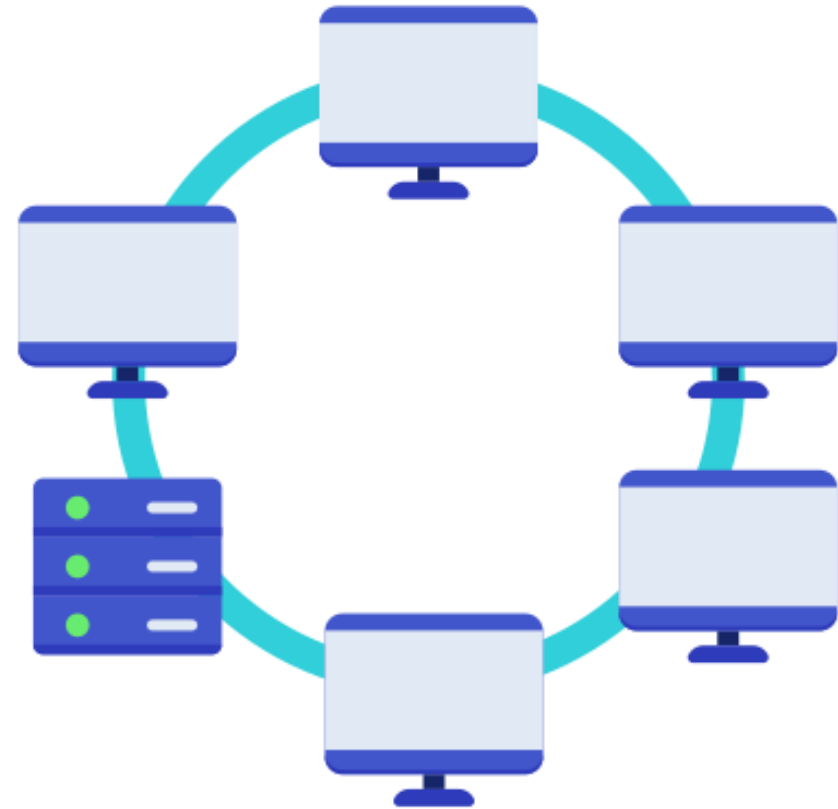


Failure of the main cable can stop the entire network.



Ring Topology

- A ring topology connects devices in a circular arrangement.
- Data travels around the ring between devices.
- Each device acts as a link in the chain.
- A break in the ring can disrupt communication.



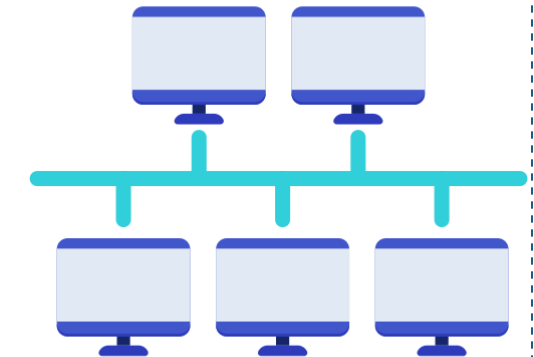
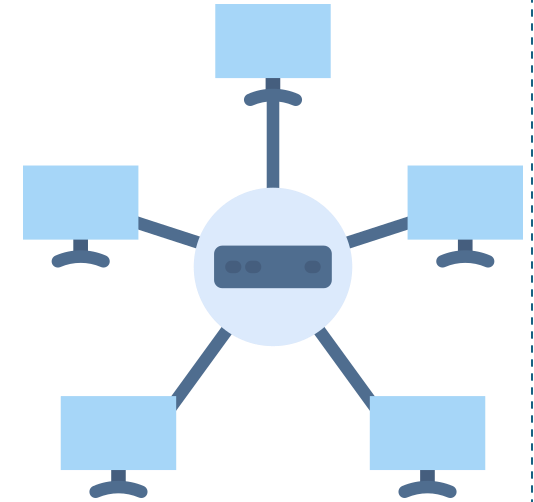
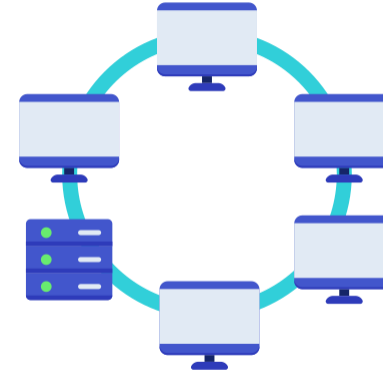
Hybrid Topology

A hybrid topology combines two or more topology types.

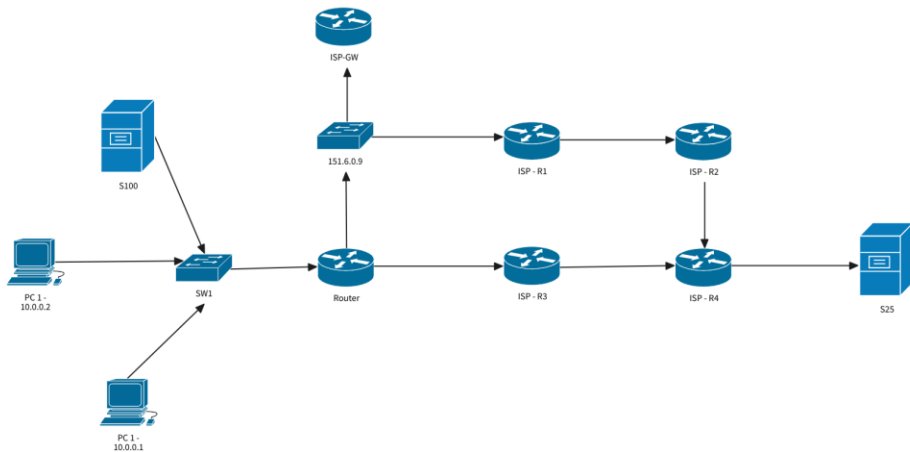
Many modern networks use hybrid designs.

Hybrid networks offer flexibility and scalability.

They can be more complex to manage.



Understanding Network Diagrams



Network diagrams show how devices and systems are connected.



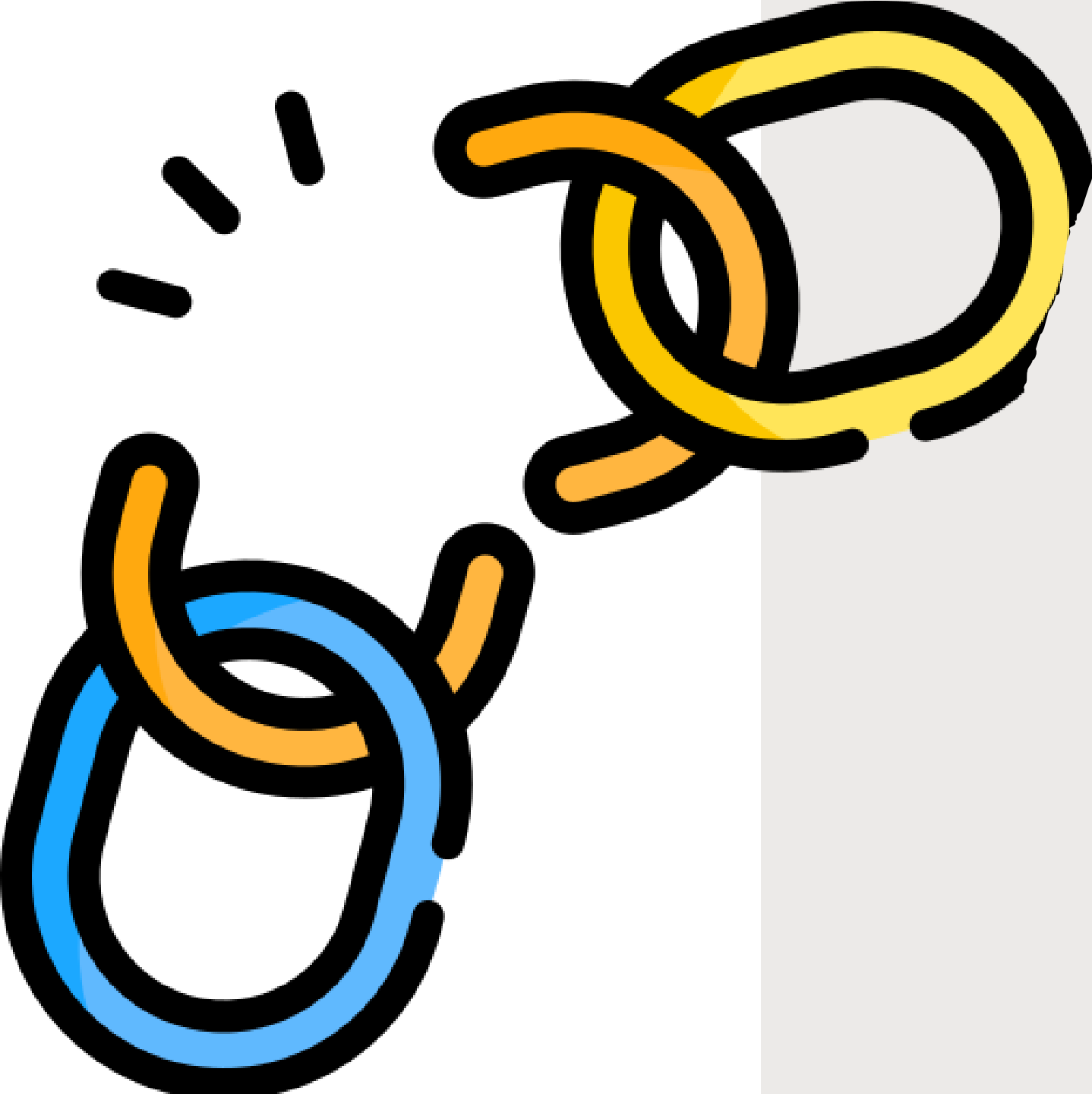
Physical diagrams show actual hardware and cabling.



Logical diagrams show how data flows through the network.

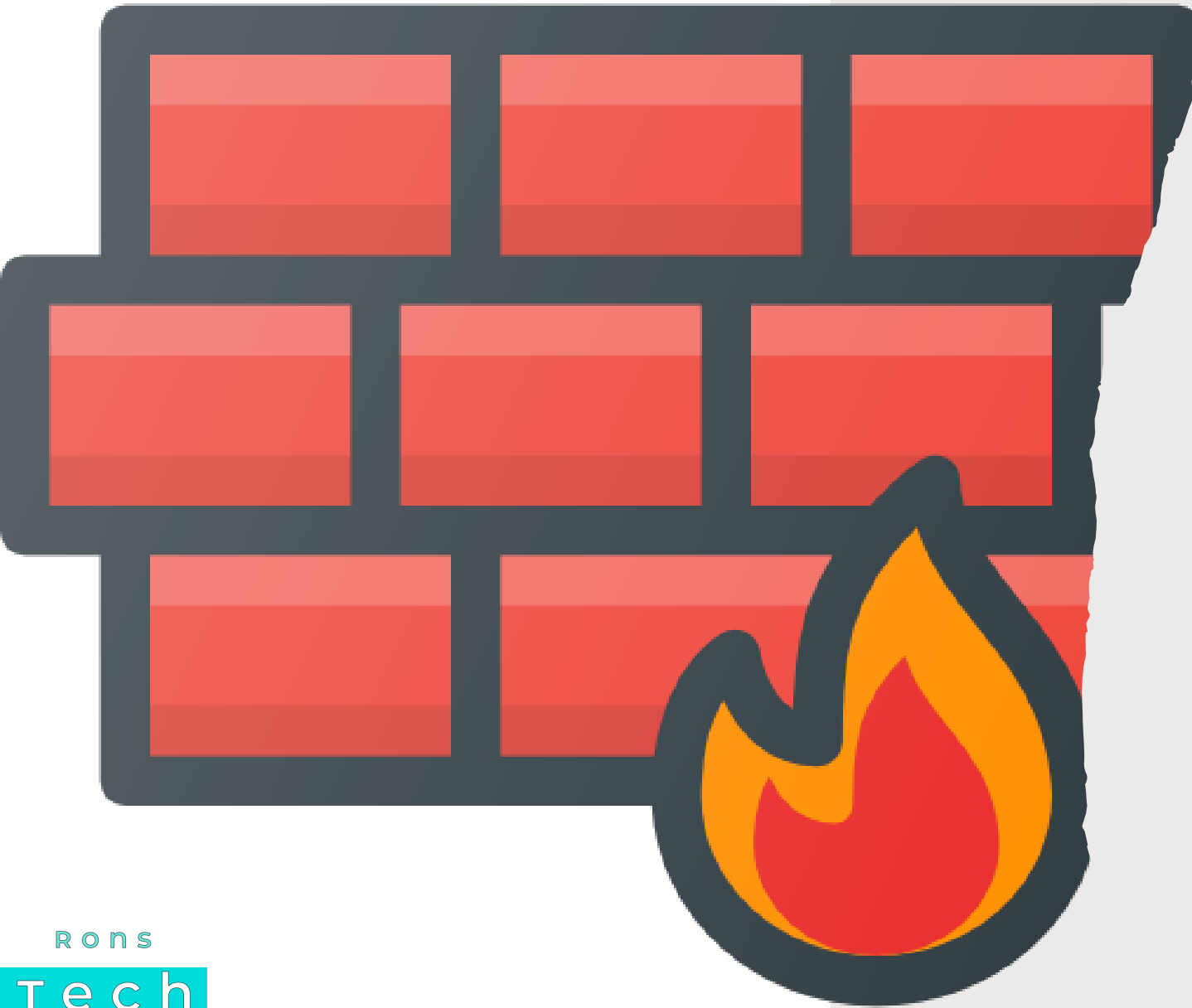


Diagrams help technicians understand network structures.



Identifying Weaknesses

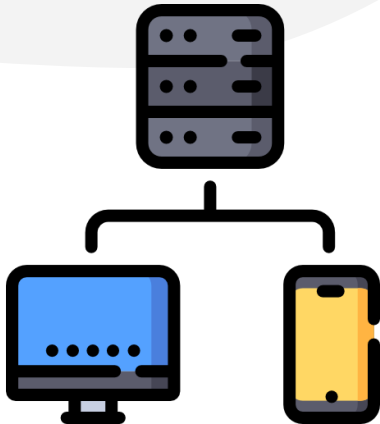
- Network diagrams can reveal security weaknesses.
- Single points of failure can reduce reliability.
- Unprotected devices may create vulnerabilities.
- Weaknesses should be identified and improved.



Improving Network Security

- Firewalls can help protect networks from threats.
- Redundant devices improve reliability.
- Secure configurations reduce vulnerabilities.
- Security should be considered during network design.

Client-Server Networks



Servers provide services to client devices.



Security and permissions are usually managed centrally.



Central management makes administration easier.



Client-server networks are common in organisations.

Peer-to-Peer Networks



Devices share resources directly with each other.



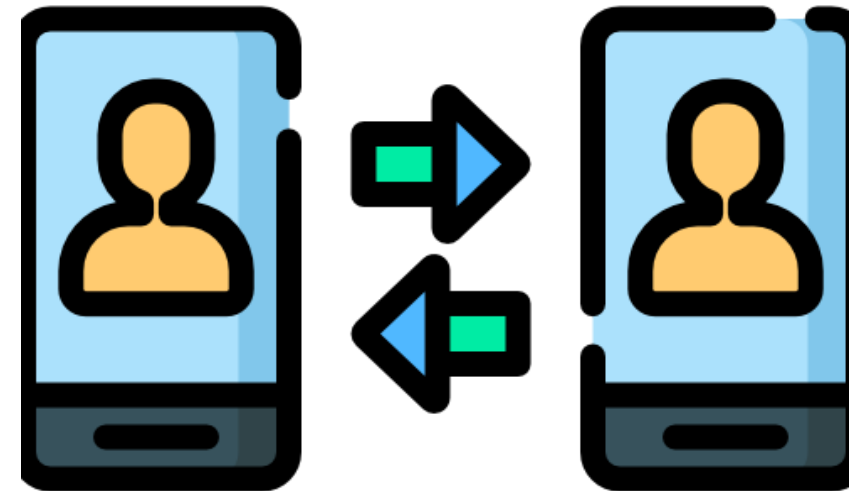
There is usually no central server.



Security management can be more difficult.



Malware can spread more easily between devices.



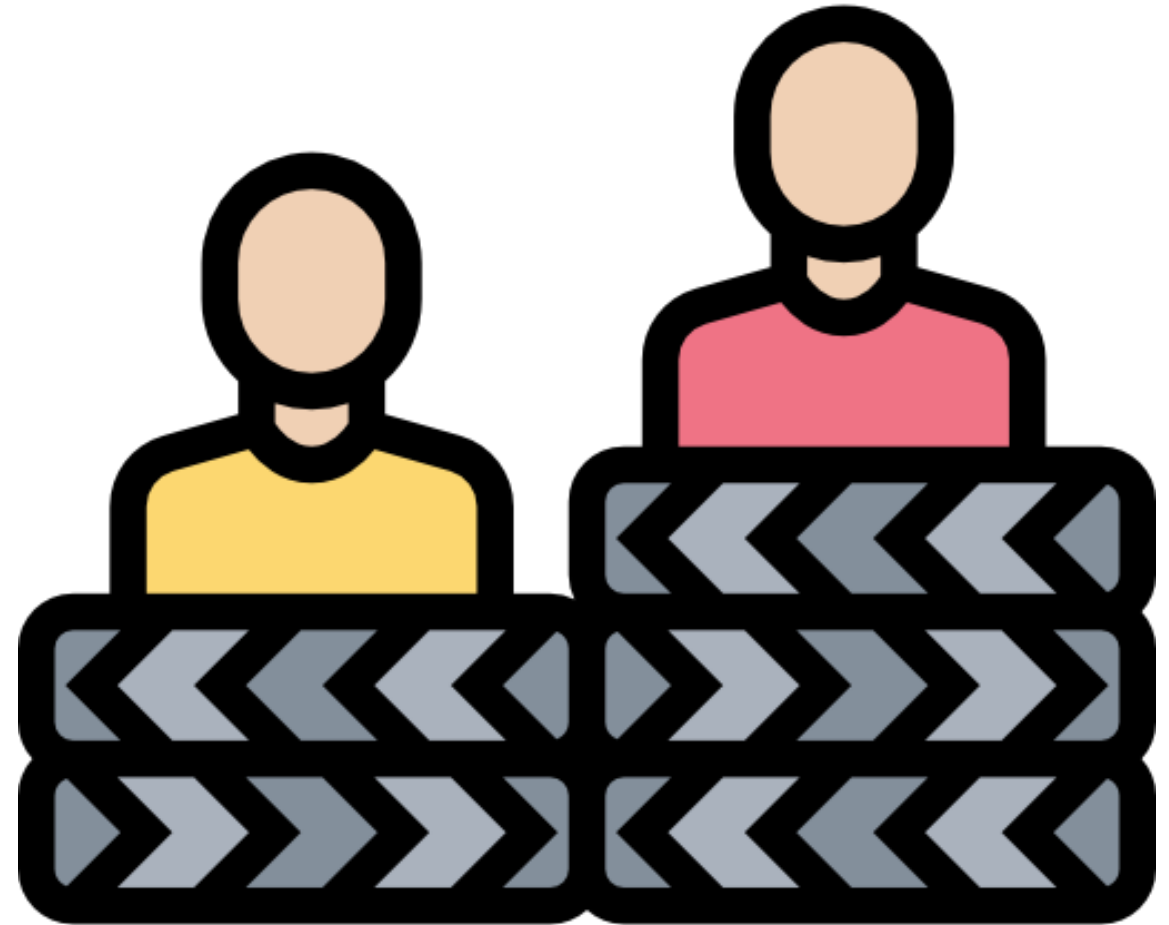
Security Issues in Network Models

- Client-server networks provide centralised security control.
- Peer-to-peer networks use distributed security control.
- Data duplication can make information harder to manage.
- Access permissions should be carefully controlled.



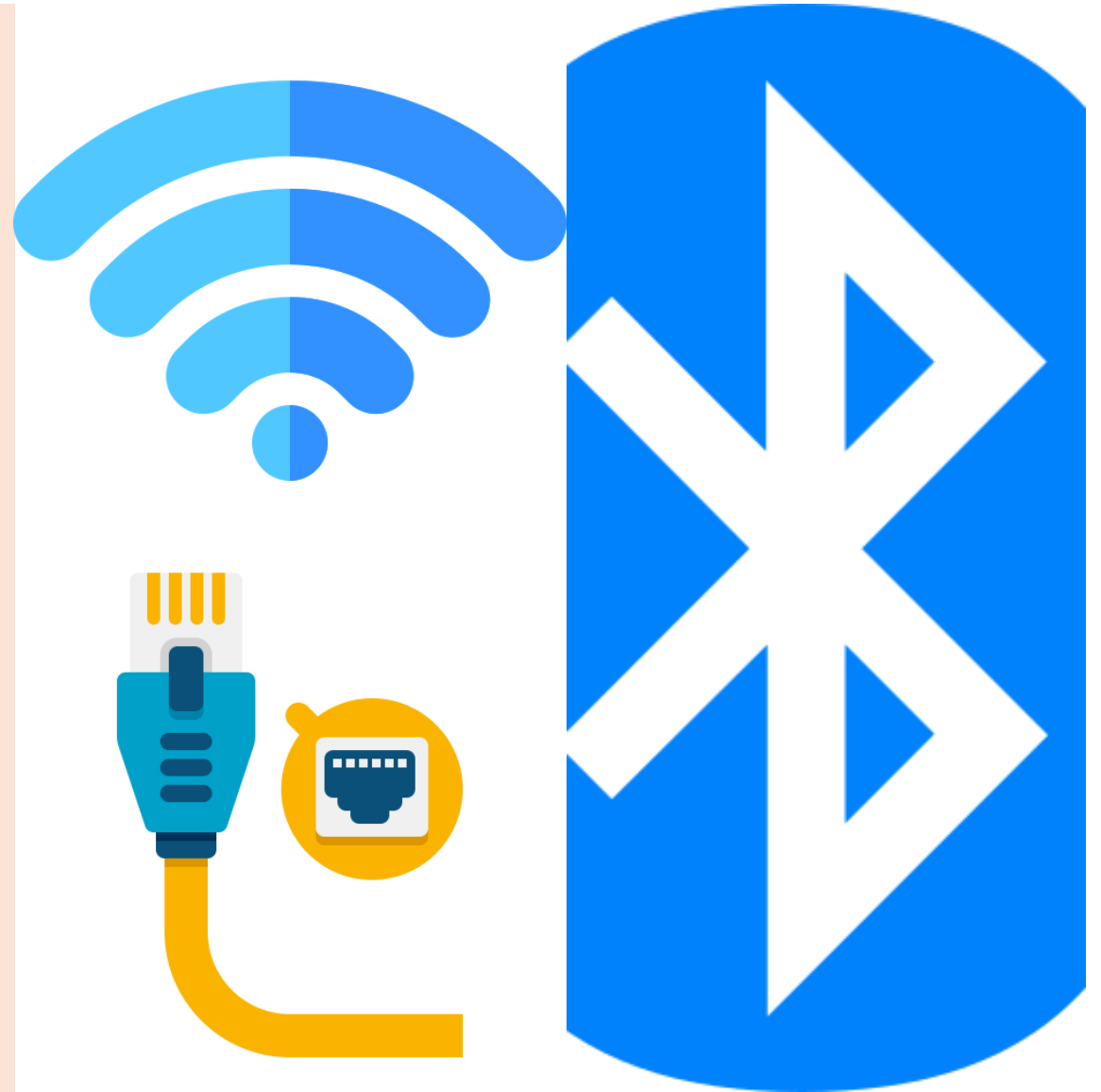
Administrative Boundaries and Trust

- Administrative boundaries define who manages systems.
- Trust relationships allow systems to share resources.
- Trust should only be given where necessary.
- Poor trust management can increase security risks.



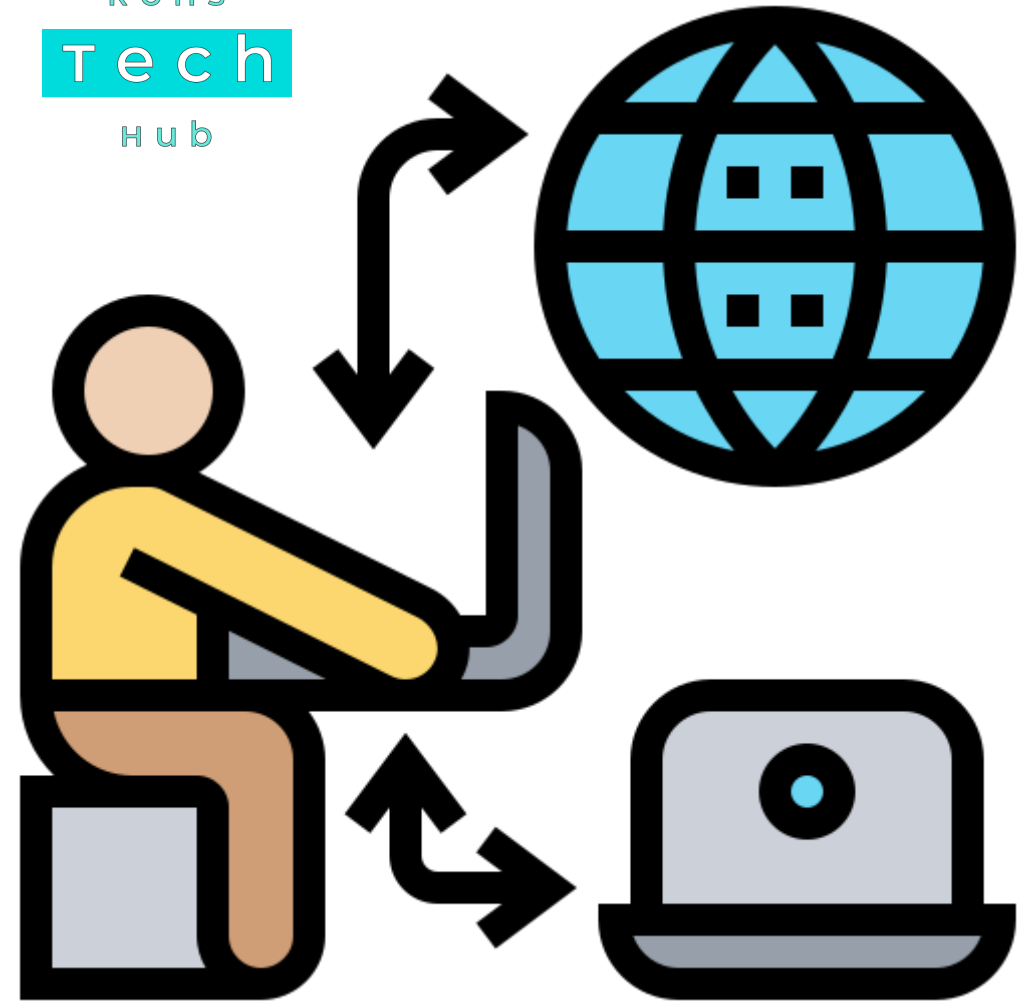
Local Network Connections

- Ethernet provides wired network connectivity.
- Wi-Fi provides wireless network connectivity.
- Bluetooth supports short-range device communication.
- Each connection method has different security risks.



Remote Network Connections

- Virtual Private Network: VPNs provide secure remote access.
- Remote Desktop: RDP allows remote control of computers.
- Virtual network Computing: VNC is another remote desktop technology.
- Remote access should always be secured.



Secure File Transfer



SFTP transfers files securely using encryption.

HTTPS secures communication between websites and users.

Encryption protects data during transmission.

Secure protocols help prevent interception.



Cloud and Third-Party Access

- Organisations often use cloud-based services.
- Vendors may require access to organisational systems.
- Third-party access should be carefully controlled.
- Poorly managed access can create security vulnerabilities.

R O N S

T e c h

H u b

Summary



Organisations use different network types for different purposes.



Topologies affect network reliability and security.



Secure access methods help protect data and systems.



Good network design reduces vulnerabilities.