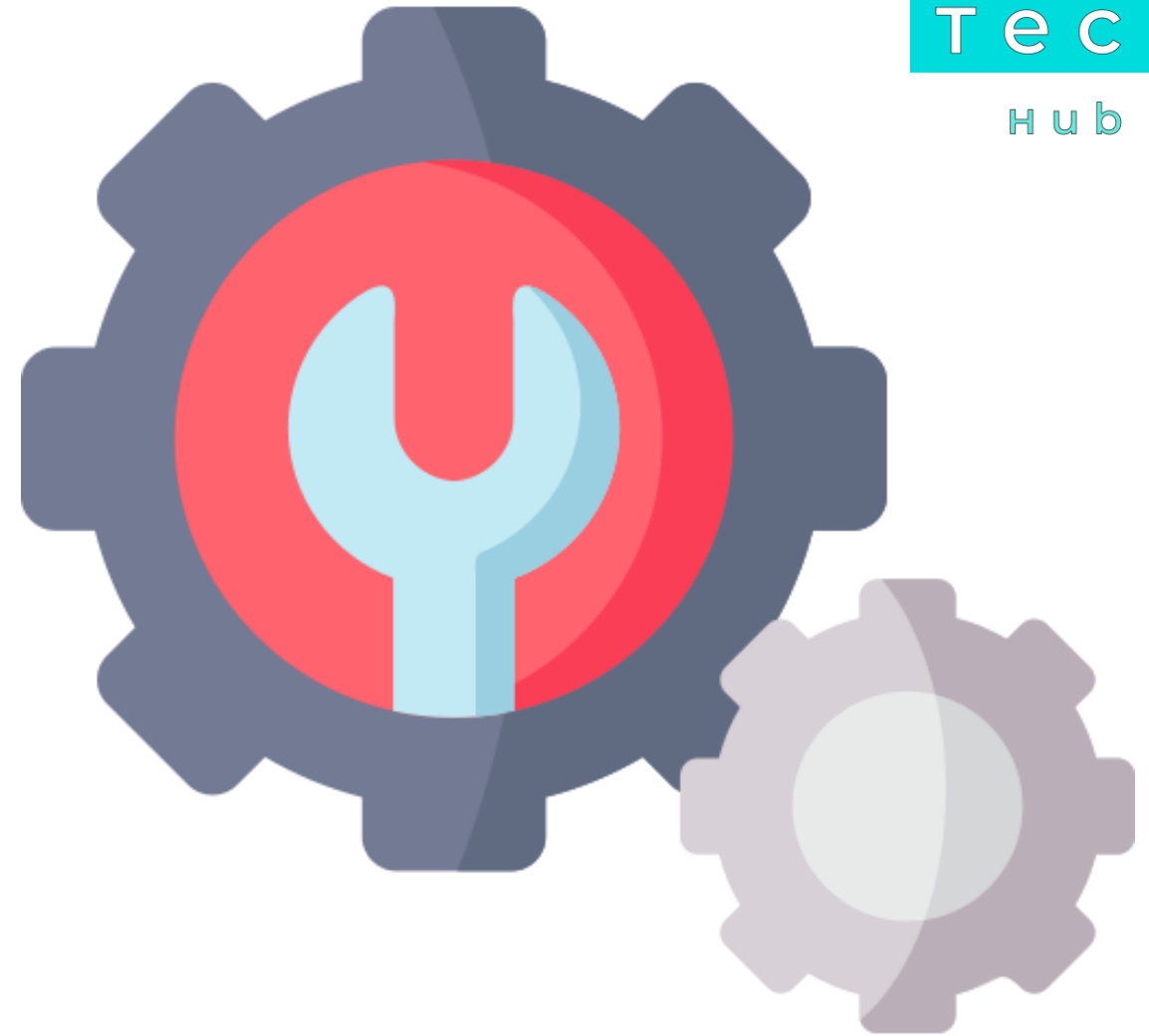


AAQ IT Unit 2 Cyber Security

B2: Network Components

Network Components

- Network components are the hardware and software used to build and manage networks.
- Understanding these components helps organisations operate securely and efficiently.



End-User Devices

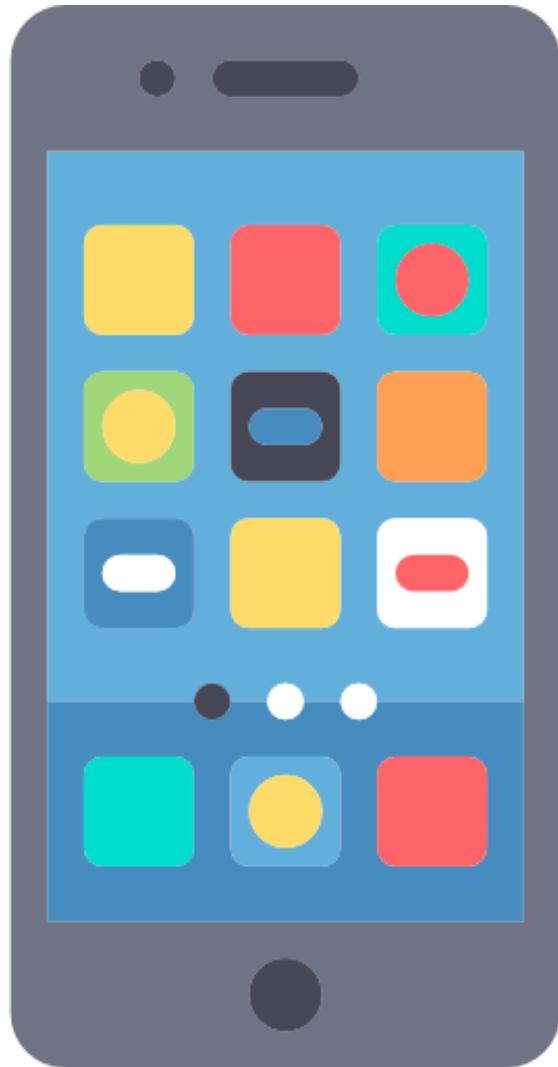
- End-user devices are the devices people use to access network services.
- Examples include smartphones, tablets, smartwatches, PCs, printers, and scanners.

RONS

Tech

Hub



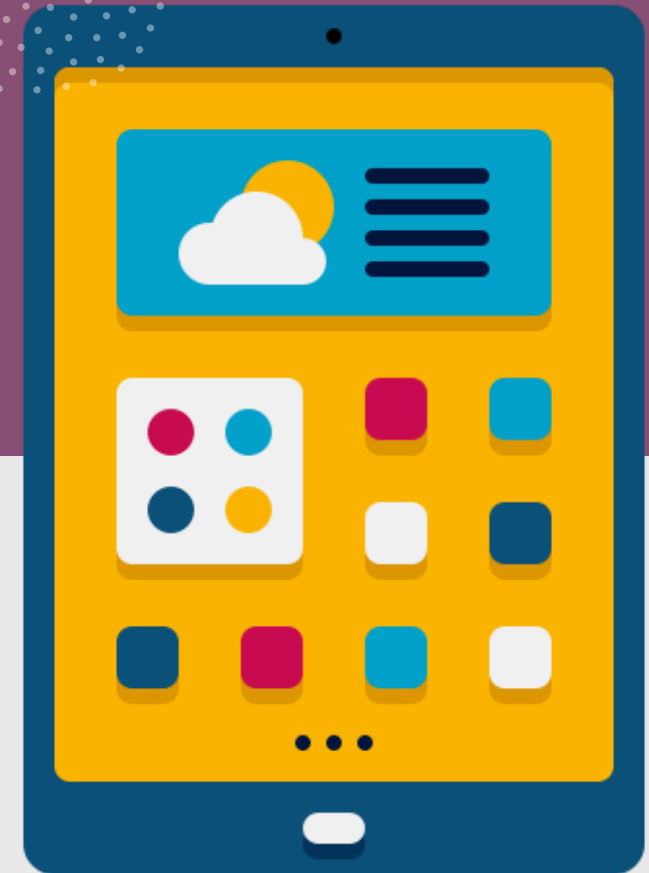


Smartphones

- Smartphones provide access to applications, email, cloud services, and the internet.
- They often contain sensitive personal and business information.

Tablets

- Tablets provide many of the same functions as a laptop but in a more portable form.
- They are commonly used in education, healthcare, and business.



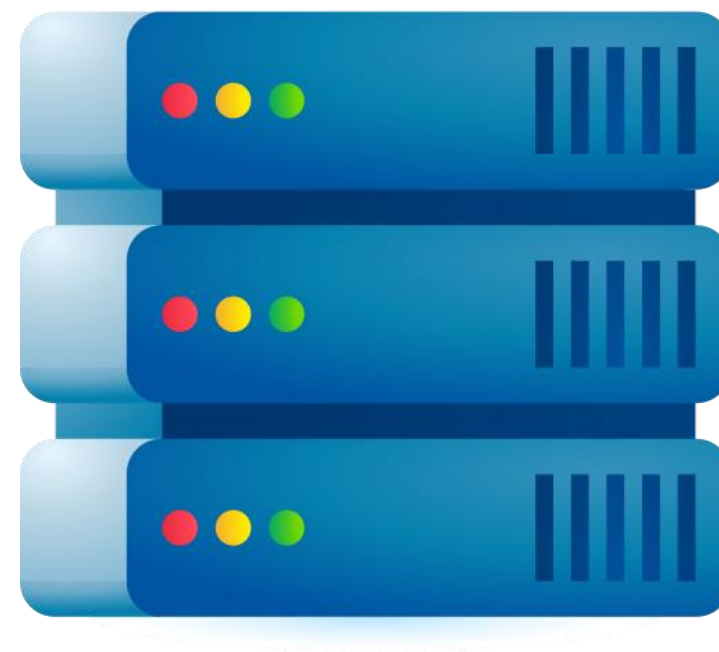
Smartwatches

- Smartwatches connect to phones and networks to exchange information.
- They can store personal and health-related data.



Servers

- Servers provide services and resources to other devices on a network.
- Examples include file servers, web servers, and database servers.



PCs/Personal Computers

- Personal computers are used to access applications, files, and network resources.
- They are one of the most common devices found in organisations.



Printers

- Network printers can be shared by multiple users.
- Security settings help prevent unauthorised use.



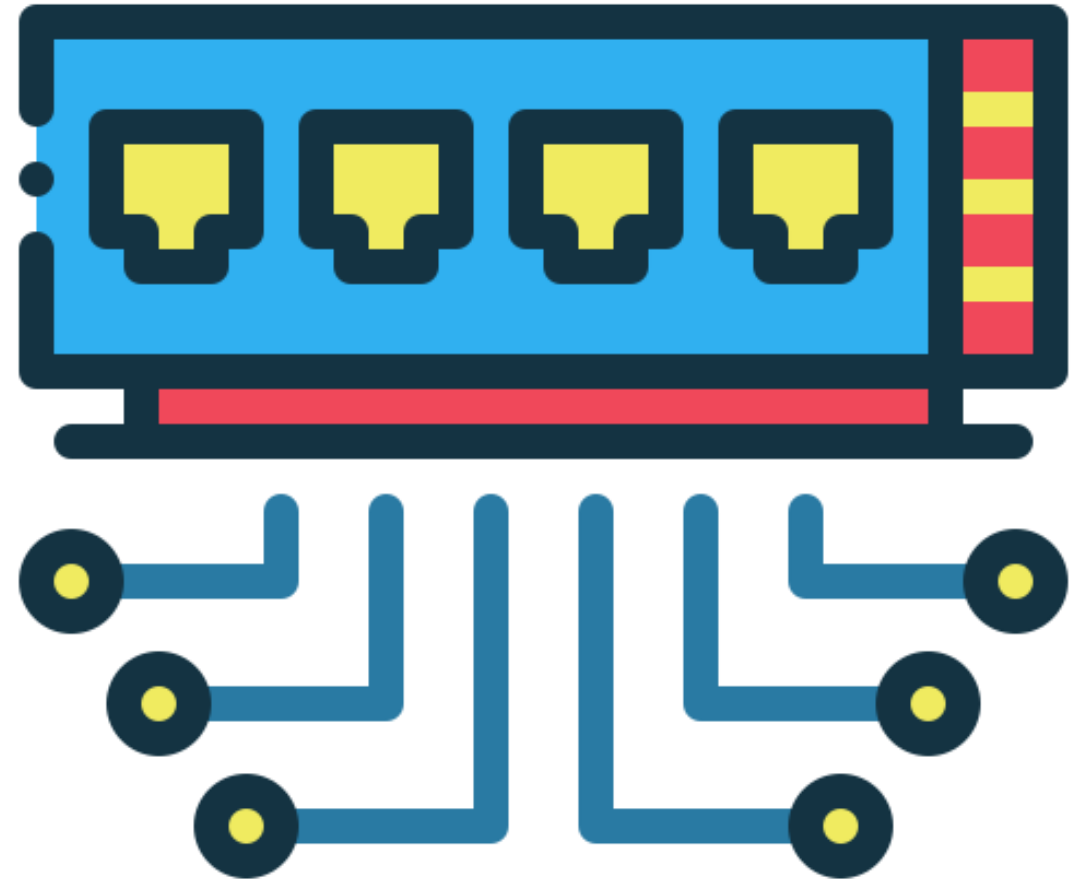
Scanners

- Scanners convert physical documents into digital files.
- They help organisations store information electronically.



Connectivity Hardware

- Connectivity hardware allows devices and networks to communicate.
- Different devices perform different networking functions.
- Example: Network switches, routers, and wireless access points installed in a server room.



Managed Switches



1

Managed switches allow administrators to configure and monitor network traffic.



2

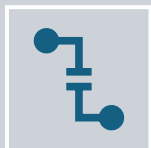
Security features can be used to control access and improve network performance.



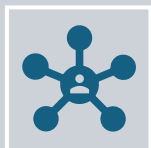
3

Example: A high-end switch configured by a technician to separate student traffic from staff traffic.

Unmanaged Switches



Unmanaged switches require little or no configuration.



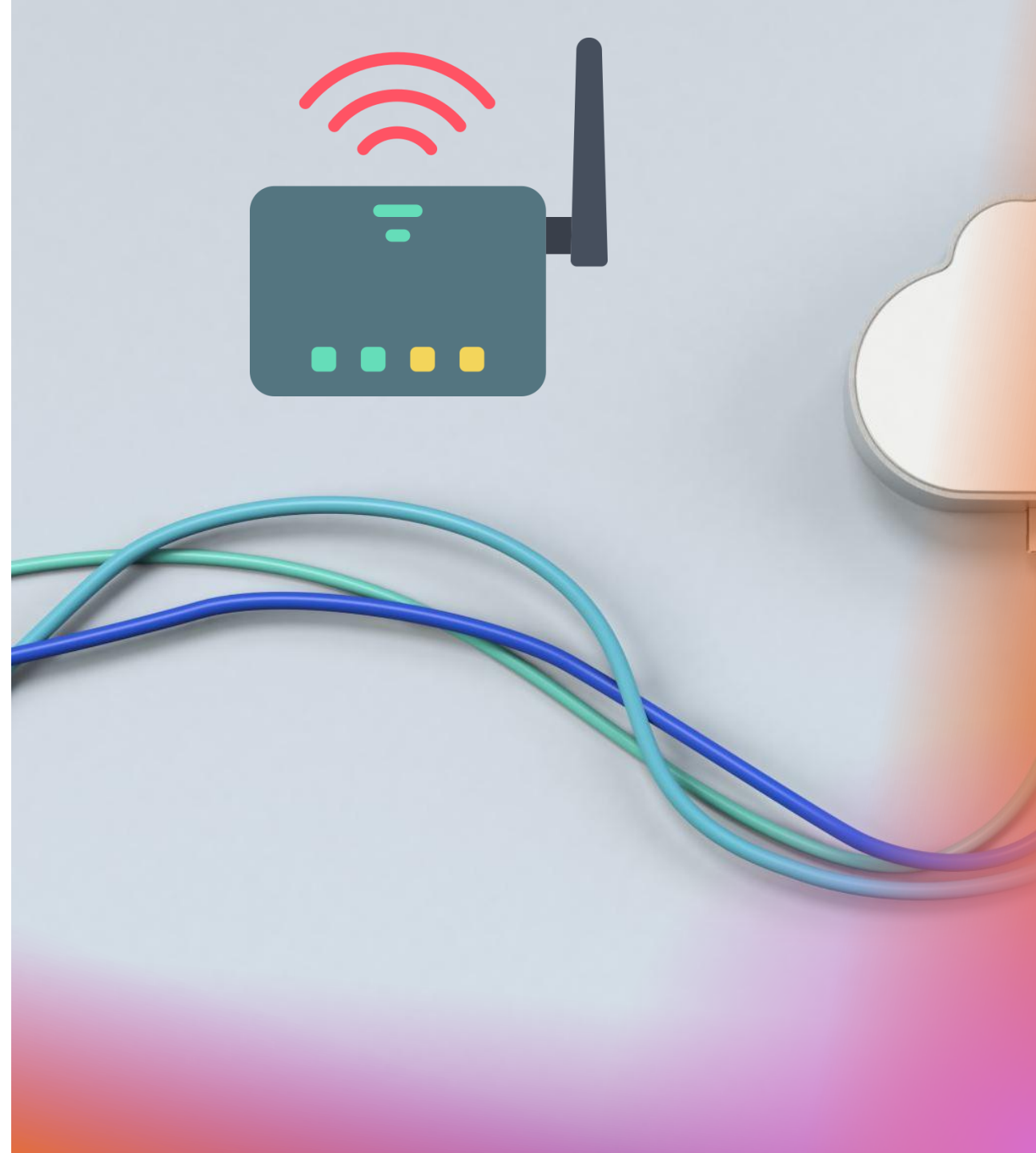
They are commonly used in small networks.

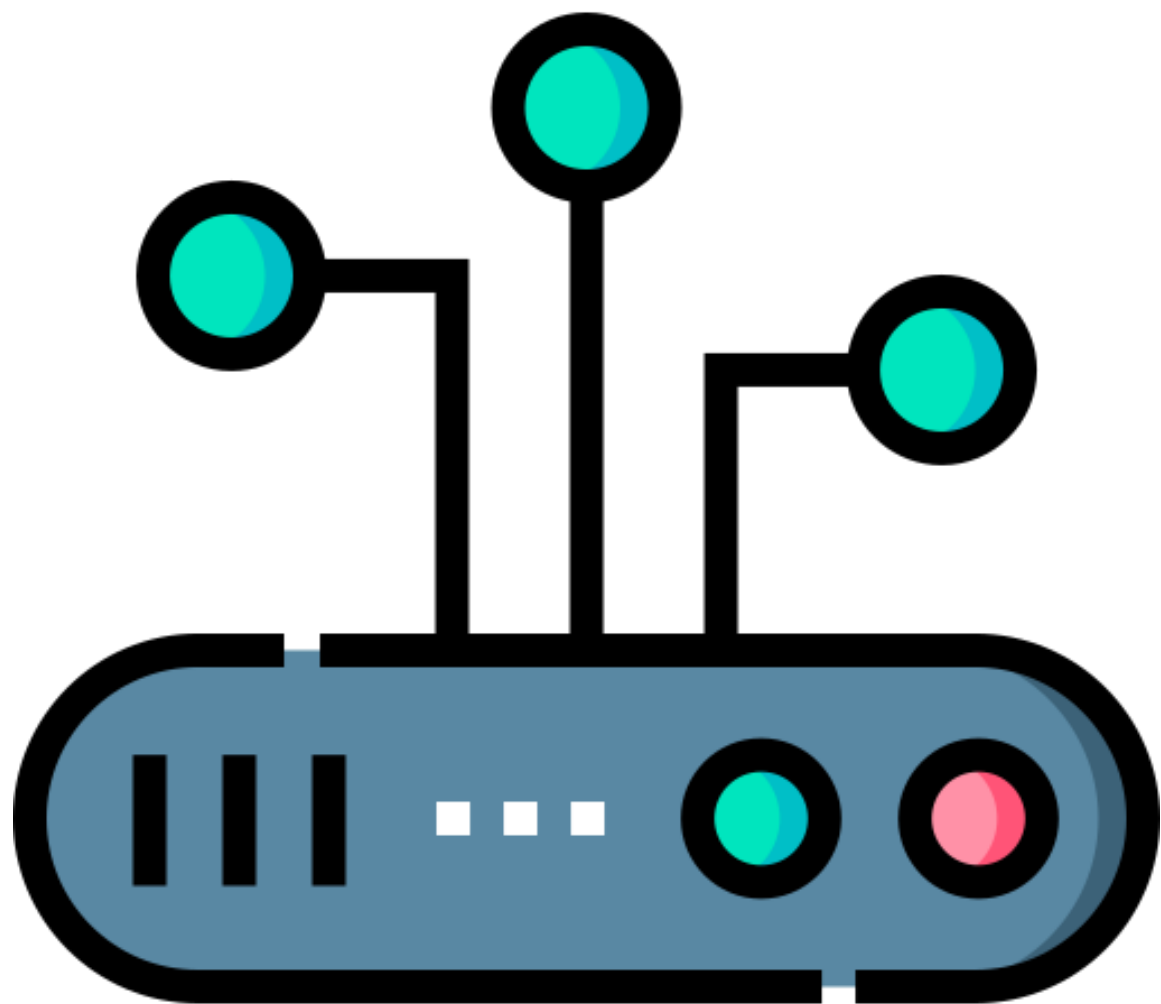


Example: A small plug-and-play desktop switch used to connect a few computers in a tiny home office.

Routers

- Routers connect different networks together.
- Most routers connect a local network to the internet.
- Example: A home broadband box connecting your local devices to your Internet Service Provider (ISP).



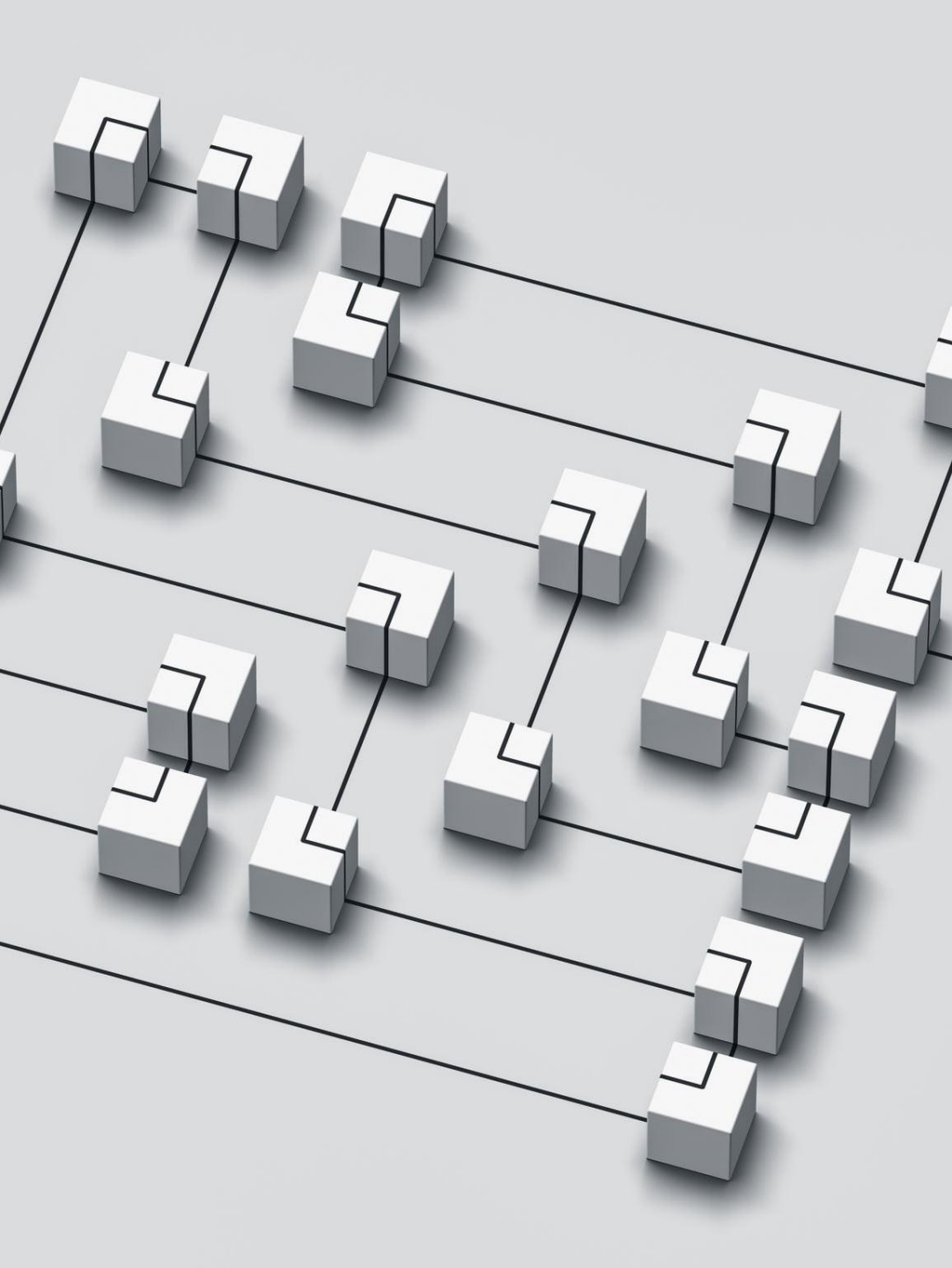


Gateways

- Gateways allow communication between systems that use different protocols or technologies.
- Example: A device connecting an old corporate telephone setup to a modern cloud network.

Bridges

- Bridges connect network segments together.
- They can help reduce unnecessary traffic.
- Example: Connecting a separate science block network directly to a main school block network.



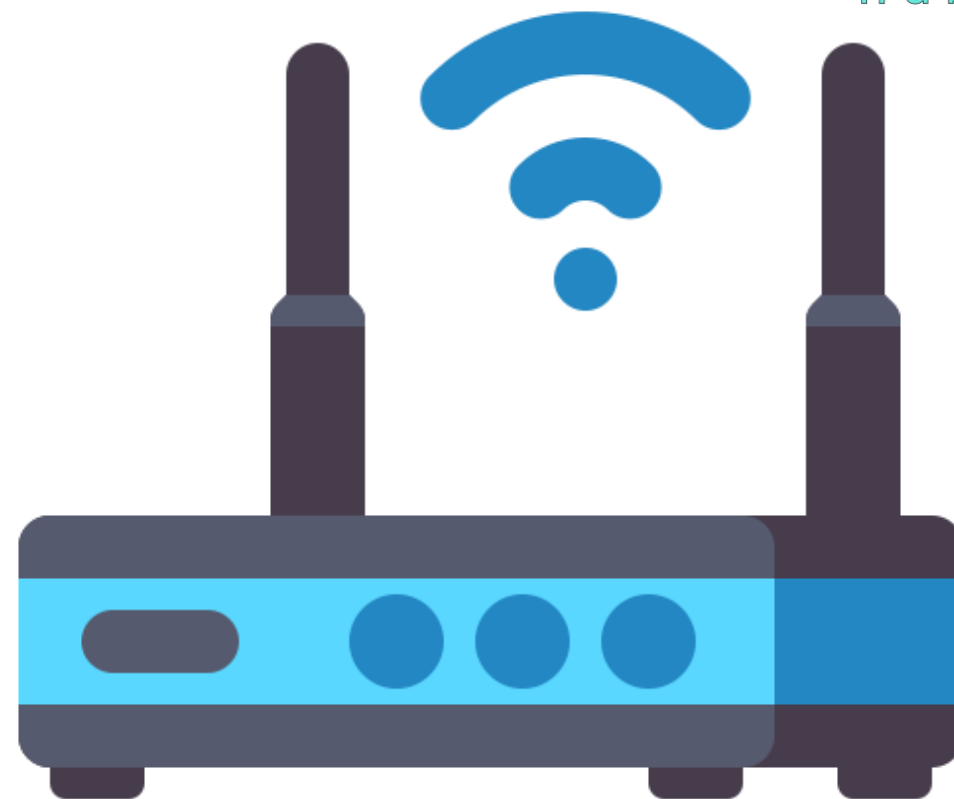
Repeaters

- Repeaters regenerate signals so that data can travel further across a network.
- Example: A device boosting a copper network cable signal down a hallway that is longer than 100 metres.



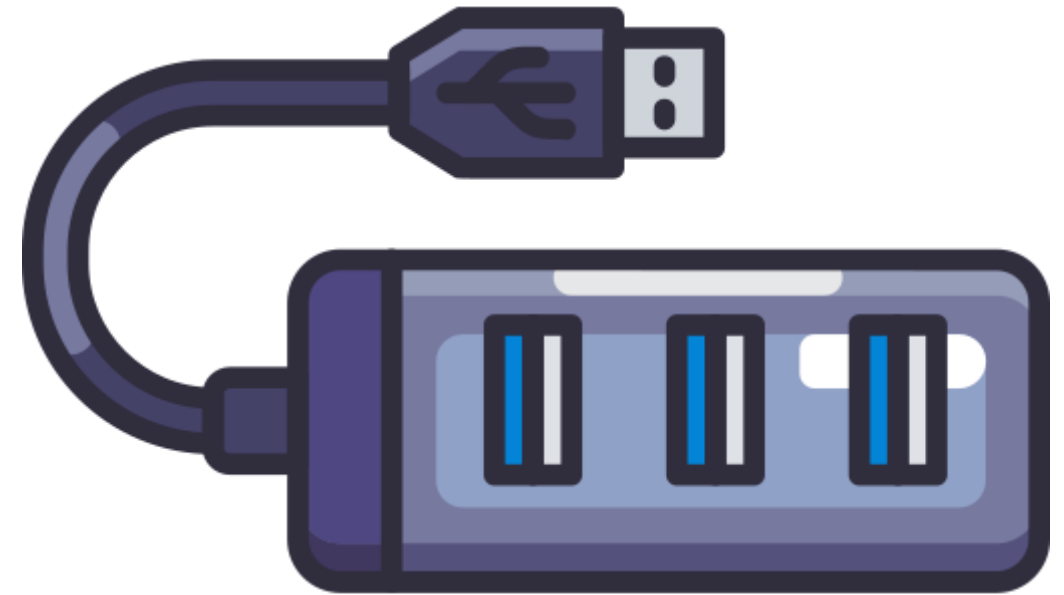
Wireless Access Points

- Access points provide Wi-Fi connectivity to wireless devices.
- Example: A Wi-Fi box mounted on a classroom ceiling to give students wireless internet access.



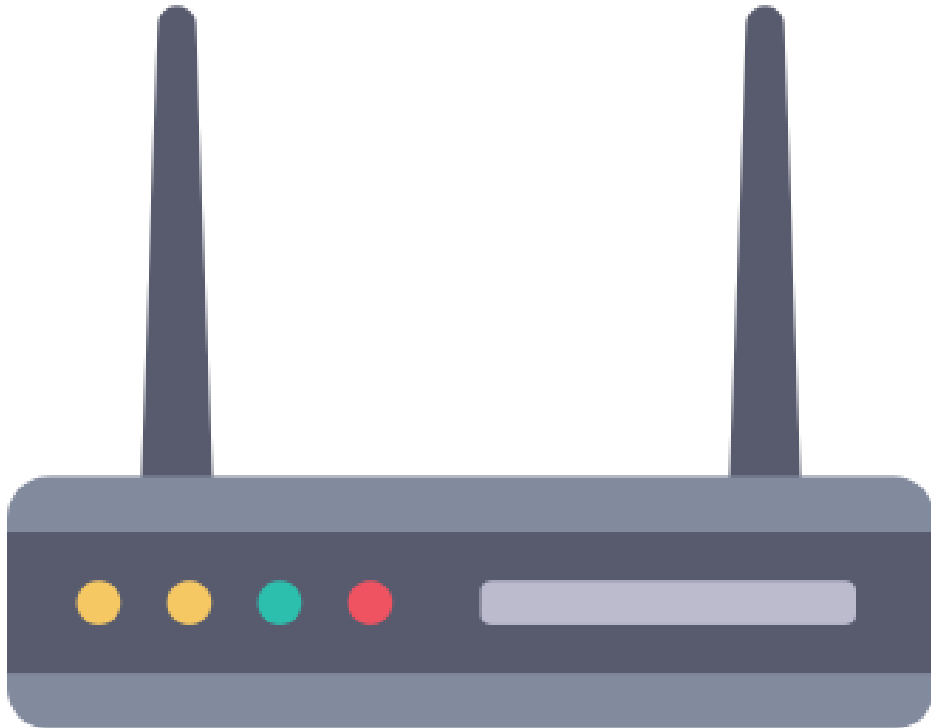
USB Hubs

- USB hubs allow multiple USB devices to connect through a single USB port.
- Example: A desktop adapter block that lets you plug four USB memory sticks into one laptop port.



DSL Modems

- DSL modems provide internet access using telephone lines.
- Example: A broadband box connected into a standard copper telephone wall socket.



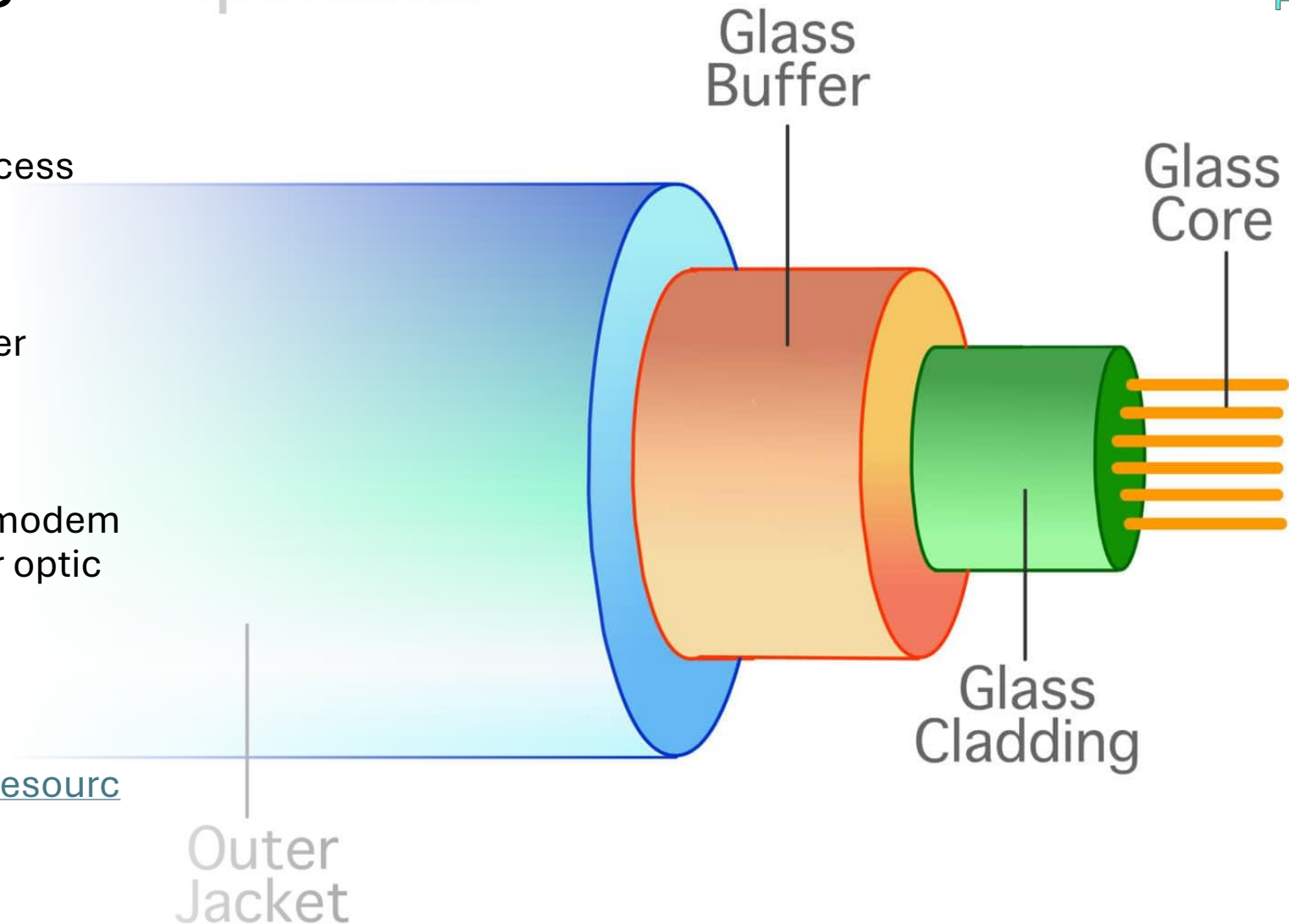
R O N S
Tech
H u b

- <https://www.amazon.co.uk/iMBPrice-Imbaprice-Line-Splitter-Filter-DSL/dp/B01258GUCQ>

Fibre Optic Components

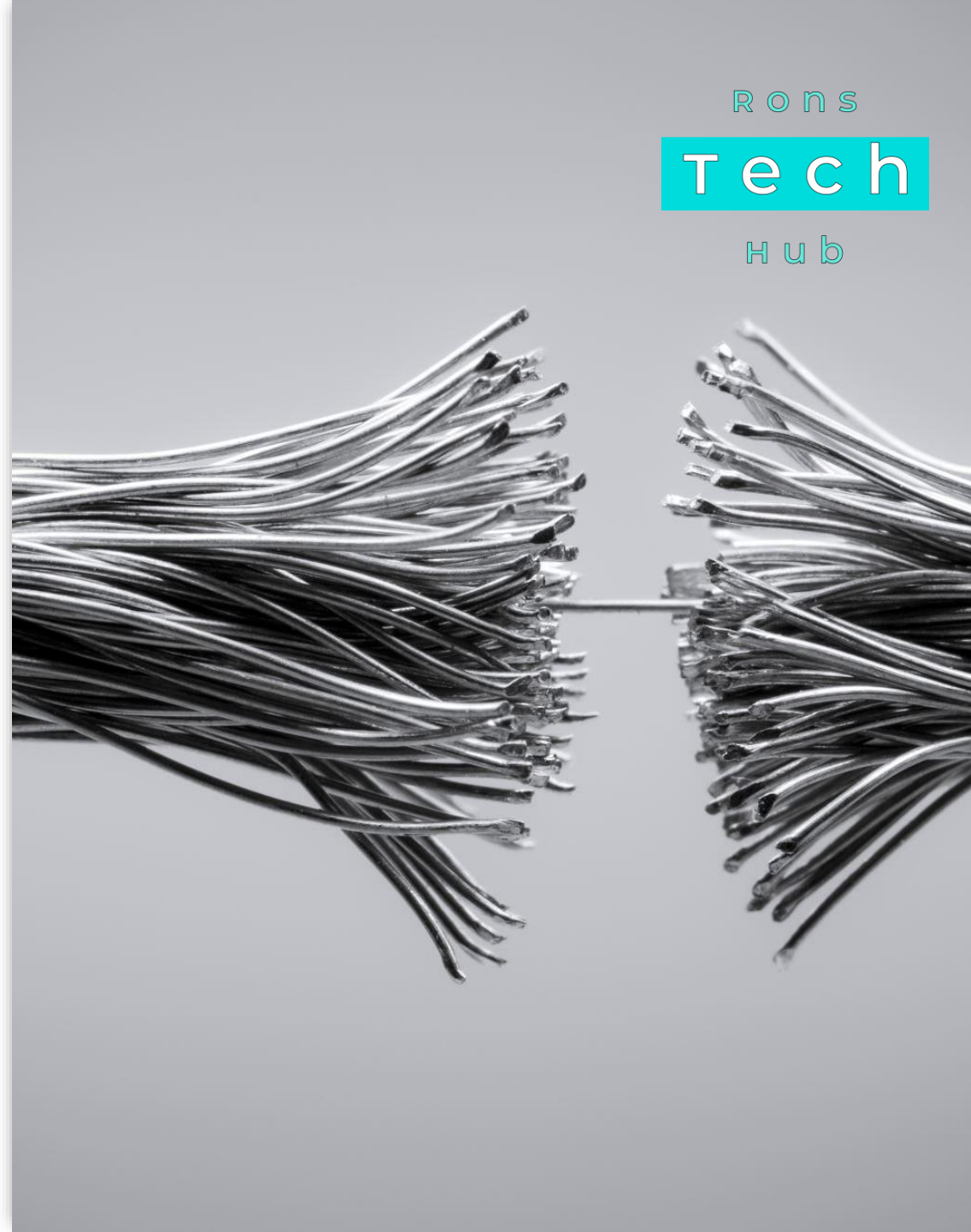
Fibre Modems

- Fibre modems provide internet access using optical fibre connections.
- They support very high data transfer speeds.
- Example: A superfast broadband modem connected directly to a street fiber optic line.
- Image Location: <https://www.zayo.com/resources/fiber-optic-networks-a-comprehensive-guide/>



Wired Connection Methods

- **Ethernet Cables:** The standard copper wire for high-speed LAN connections.
- **USB Cables:** Used to connect peripherals (like mice or external drives) to a PC.
- **Optical Fibre:** Uses light to send data.
 - Extremely fast.
 - Harder to "tap" into, making it more secure than copper.





Wireless Connection Methods



Wi-Fi: High-speed local wireless networking.



NFC (Near Field Communication): Very short range (e.g., contactless payments).



Bluetooth: Short range, used for connecting headsets or keyboards.



5G Cellular: High-speed mobile data for smartphones.



Li-Fi: Uses light waves to transmit data instead of radio waves.

External Storage Security

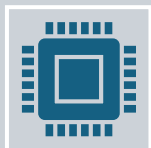
Encryption: Scrambles data on the drive so only those with a key can read it.

Secure Disposal: Completely wiping or physically destroying old drives.

Data Loss Prevention (DLP): Rules that stop users from copying sensitive data to USB sticks.

Propagation Vectors: How malware (viruses) spreads from a USB drive to the whole network.

Operating System Interfaces



GUI (Graphical User Interface): Using icons, windows, and a mouse (e.g., Windows 11).



CLI (Command Line Interface): Typing text commands (used by experts for speed and control).



Web-based Interfaces: Configuring devices (like routers) through a web browser.

Monitoring & Management Tools



Remote Administration: Managing a computer from a different location.



Vulnerability Scanners: Tools that look for "holes" in your security.



Performance Monitors: Check if the network is slow or overloaded.



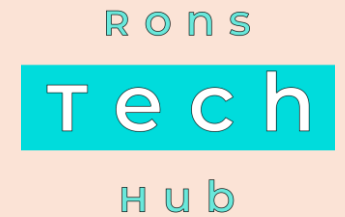
Event Log Viewers: A "diary" of everything that has happened on the system.

Security Tools

- **Packet Sniffers:** Intercept and look inside data moving across the network.
- **Why use them?** To find suspicious activity or fix technical errors.
- **Danger:** If a hacker uses a sniffer, they can steal unencrypted passwords.



Network Applications



- **Database Management:** Software used to store, find, and edit large amounts of data.
- **Document Management:** Systems used to track, manage, and store digital documents.
- **Security Focus:** Access to these applications must be restricted to "Authorised Users Only."

