AQA Computer Science GCSE

3.5 Fundamentals of Computer Networks

Advanced Notes

What is a computer network?

A computer network is a group of connected devices, such as computers, printers, and smartphones, that share data and resources like files or internet access.

Advantages of computer networks

- Users can share hardware, meaning that several people can use the same printers and other similar devices
- Users can share data/files, making it easier to work collaboratively
- Machines can be managed centrally, for instance network administrators can deploy software centrally or back up everyone's files to prevent data loss

Disadvantages of computer networks

- Network failures can result in a loss of files or services
- Setting up and maintaining networks can be expensive (e.g., hardware and cabling)

Types of networks

PAN (Personal Area Network)

- Covers a very small geographical area (e.g., around a single person or desk)
- Typically connects personal devices like smartphones, headphones, and wearables
- Uses a technology such as Bluetooth
- Common examples include connecting a phone to wireless headphones or a laptop to a wireless mouse

LAN (Local Area Network)

- Covers a relatively small geographical area (e.g., a school, home, office)
- Often owned and managed by a single person or organisation
- Only connected to a small number of devices and users

WAN (Wide Area Network)

- Covers a wide geographical area (e.g., the internet)
- Usually made up of several LANs connected together
- Often under collective ownership
- Usually slower than LANs
- Cost per byte for transmission is much higher on WANs than on PANs and LANs

Wired and wireless networks

Networks can be wired, meaning that devices are connected with cables, or wireless, meaning that devices connect using radio signals.

Feature	Wired	Wireless
Speed	Faster	Slower
Security	More secure	Less secure (as signal can be intercepted)
Convenience	Less convenient as cables are required, meaning users can't move around with their devices and it is more difficult to add new devices, such as for guests.	More convenient, as users can move freely with their devices, and there is no need to drill holes, install cabling, or any possibility of trip hazards.
Versatility	Less versatility, as only some devices have wired connections	More versatility, as modern devices are more likely to be designed to connect wirelessly
Reliability	Very reliable, doesn't suffer interference	Can suffer interference

Wired network cabling

Wired networks can use different types of cable such as fibre and copper:

- Copper cables are generally cheaper than fibre cables. They can only reliably transmit data over short distances, are susceptible to interference and are slower than fibre cables.

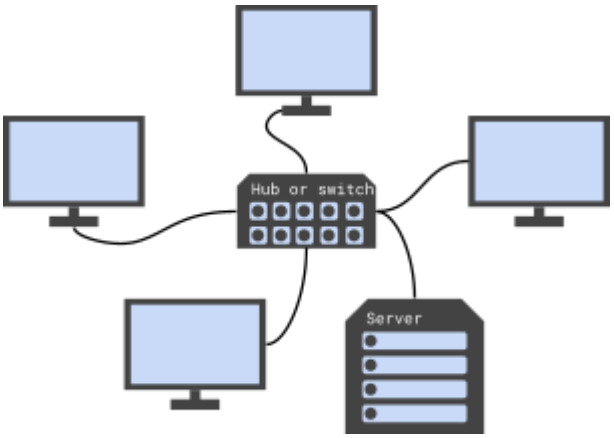
- Fibre cables are more expensive than copper cables and they use light to transmit data. They are much faster, less susceptible to interference, as well as being able to transmit data over longer distances.

LAN topologies

The topology of a network is the way that the devices are connected. Two common network topologies are the star topology and bus topology.

Star topology

Each client (that is, a device connected to the hub/switch) has its own direct connection to the central hub or switch. The hub/switch receives data packets for all of the clients connected to it and is responsible for delivering them to the correct recipient. Whilst a switch sends data packets only to the intended device, a hub sends data to all devices.

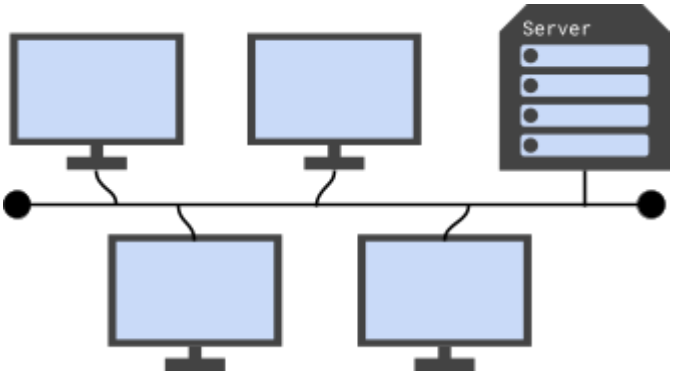


A server or shared device such as a printer can be added to the network in the same way that clients are connected to the central hub/switch.

Advantages	Disadvantages
Assuming a switch is used, packets are sent directly to their recipient, over a cable that is connected only to the recipient. Other clients on the network cannot see packets that aren't intended for them.	Should the central hub/switch fail, all communication over the network is stopped.
It is easy to add and remove clients to and from the network.	Expensive to install due to the amount of cable required.
Each cable has just one device communicating over it, eliminating the possibility of collisions.	
The failure of one cable does not affect the performance of the rest of the network.	

Bus topology

A bus topology connects clients to a single cable called a backbone. A device called a terminator is placed at either end of the backbone. There is no need for a central hub/switch like in star networks and a server can be connected to the backbone just like a client.



Advantages	Disadvantages
There is no central hub, reducing the chances of a network failure and decreasing the cost of installation.	Packets are sent through the shared backbone, allowing every client on the network to see packets that aren't intended for them.
Inexpensive to install as a minimum length of cable is required.	The backbone is used for communication by multiple clients, introducing the risk of collisions.
	Should the backbone fail, the entire network becomes unusable.

Network protocols

A network protocol is a set of rules that allow devices to communicate.

Protocol	Purpose
Ethernet	Ethernet is a common method for connecting devices in a local area network (LAN) using wired connections. It allows computers, printers, and other devices to communicate and share data quickly and reliably over physical cables.
Wi-Fi (Wireless Fidelity)	Wi-Fi is a wireless technology that allows devices to connect to a local area network (LAN) and access the internet without using cables. It uses radio waves to transmit data between devices and a router.
TCP (Transmission Control Protocol)	TCP ensures that data sent over a network arrives completely and in the correct order. It breaks data into packets and checks that all packets are received properly, requesting any missing ones to be resent.
UDP (User Datagram Protocol)	UDP is a fast, lightweight protocol for sending data over a network without checking if it arrives correctly. Unlike TCP, it doesn't confirm delivery or order of data packets, and it is connectionless, meaning that it sends data packets without establishing a prior connection.
IP (Internet Protocol)	IP is responsible for addressing and routing data packets across networks. It ensures that data packets can find their way from the sender to the correct destination computer using IP addresses.
HTTP (Hypertext Transfer Protocol)	HTTP is the protocol used for transferring web pages and other content between web servers and browsers. It defines how web browsers request pages and how web servers respond with the requested content.

HTTPS (Hypertext Transfer Protocol Secure)	HTTPS is the secure version of HTTP that encrypts data being transferred between web browsers and servers. It protects sensitive information like passwords and credit card details from being understood if it is intercepted by hackers.
FTP (File Transfer Protocol)	FTP is used to transfer files between computers over a network, such as the internet. It allows users to upload or download files to and from a remote server, often used for managing files on websites.
SMTP (Simple Mail Transfer Protocol)	SMTP is used for sending emails from one email server to another across the internet. It handles the delivery of outgoing emails from your email client to the recipient's email server.
IMAP (Internet Message Access Protocol)	IMAP allows users to access and manage their emails stored on a remote email server. It enables emails to be read and organised from multiple devices whilst keeping them synchronised on the server.

Network security

Many organisations rely on networks to store and transfer sensitive information, such as personal details, financial records, and business secrets. Without proper security, this data could be stolen, deleted, or altered by hackers, leading to serious consequences like identity theft, fraud, or disruption of services.

Methods of network security include authentication, encryption, firewalls and MAC address filtering. These methods can work together to provide a greater level of security.

Authentication

Authentication is the process of verifying the identity of a user or device before allowing access to a system or network. A common example is entering a username and password to log in to an account. More secure systems might use two-factor authentication (2FA), which combines something the user knows (like a password) with something they have (like a code sent to their phone). Authentication is used in almost all online services (such as email, banking, or school systems) to make sure only authorised users can access private information.

Encryption

Encryption is a method of converting data into a coded format so that only authorised users with the correct decryption key can understand it. For example, when you shop online, your payment details are encrypted so that if the data is intercepted, it cannot be read by hackers.

Firewalls

A firewall is a network security device that monitors incoming and outgoing traffic and blocks or allows data based on a set of security rules. For example, it might block traffic from suspicious IP addresses or stop certain types of data from entering a network.

MAC address filtering

Every device has a unique MAC (Media Access Control) address built into its physical network adaptor. MAC address filtering uses these addresses to only permit an allow list of MAC addresses to access the network. For example, a school might allow only school-owned laptops to access the Wi-Fi by adding their MAC addresses to the allow list. Devices not on the allow list will be blocked.

The 4 layer TCP/IP model

The TCP/IP model is used to transmit data over a network. It's made up of four ordered layers, each with specific functions.

1. **Application layer:** this is where the network applications, such as web browsers or email programs, operate.
2. **Transport layer:** this layer sets up the communication between the two hosts and they agree settings such as the size of packets.
3. **Internet layer:** addresses and packages data for transmission. Routes the packets across the network.
4. **Link layer:** this is where the network hardware such as the NIC (network interface card) is located. OS device drivers also sit here.

Different protocols operate at each layer:

- The HTTP, HTTPS, SMTP, IMAP and FTP protocols operate at the application layer.
- The TCP and UDP protocols operate at the transport layer.
- The IP protocol operates at the internet layer.