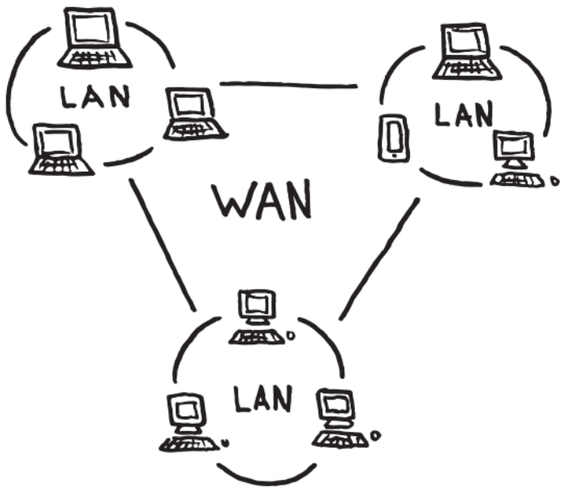
Benefits of Networking computers

- Can share files/data
- Can share applications/software
- Can collaborate
- Can share peripherals (printers, speakers)
- Can share connectivity (Internet connection, hotspot)
- Can access files from any computer / hot desk
- Central control/management (security, software updates, backup, remote support, users, remote monitoring)
- Allows communication (email, social media, video conferencing, online meeting, collaborative games)



LAN vs WAN

LAN (Local Area Network): A network that covers a small geographical area, typically within a single building or campus.

WAN (Wide Area Network): A network that covers a large geographical area, often connecting multiple LANs or other networks.

What is the difference between a LAN and WAN?

A LAN covers a small geographic area whereas a WAN covers a large geographic area

A LAN uses infrastructure owned by one company whereas a WAN uses third-party infrastructure

A LAN connects individual devices whereas a WAN connects LANs

A LAN connects using switches whereas a WAN connects using gateways

Wired vs Wireless

Computers can be connected using wired or wireless methods

Wired transmission methods use cables to communicate

Wireless transmission use radio waves communicate on 2 **frequency bands** 2.4 GHz & 5 GHz. Within each frequency band there are **Channels.**

Advantages of wireless	*Advantages of wired*
✓ Can use computer anywhere and not constrained by cables	✓ Allows more control, security and reliability. Can restrict who has access to the network. ✓ Wired methods have greater speeds than wireless methods.
Disadvantages of wireless	*Disadvantages of wired*
✓ Packets can be intercepted more easily than wired connections ✓ Security is a much more difficult challenge, as the network can be accessed from outside the confines of a building. ✓ Slower than wired methods ✓ Signal can be interfered with by other electronic devices.	✓ Cables can be difficult to maintain in big organisations

Wireless Access Points (WAP)- Converts network signals into radio waves allowing devices to connect wirelessly.

Switches - Connects devices on a LAN together by transmitting data between devices.

Router – connects networks.

NIC (Network Interface Card) -A piece of hardware within a device which allows it to connect to the network. Transmission Media

Connects the NIC to the router or switch. Could be:

- **Wireless** - using radio waves
- **Ethernet** – twisted pair coper cables
- **Fibre Optic** – data transmitted as light through glass or plastic cable

IP/ MAC Addressing

Addressing allows us to identify devices on a network

Every device has a MAC address which never changes. MAC addresses are used on a LAN network to transfer data and communicate with other devices on the network.

Each device on a network has an IP address but this can change. IP Addresses are used to route traffic across networks, for example sending data across the internet.

Explain two ways that the performance of a wireless network can be affected by its environment.

- Wireless networks have a short range because walls and floors can block the signal.
- Wireless/radio signals may not go very far because solid structures (thick walls, steel beams) block the signal.
- Wireless networks can have high latency because they suffer from interference from other wireless networks or devices.
- The performance of a wireless network can be adversely affected by interference from other devices because they can operate on the same frequency band/they are high voltage, such as a microwave.
- Wireless networks have low speed because all the devices must share the available bandwidth.
- The more devices that are connected to the network, the more likely bottlenecks are to occur because they all want a share of the available bandwidth.

Network speed

Latency

The delay/amount of time between data/signal being sent and it being received

Bandwidth

- The **maximum** volume/amount of data that can be transmitted (in one second/unit of time)
- The **full capacity** of data that can be transmitted (in one second)

The following units are used to measure network speeds.

Units	Abbrev	bits per second
bits per second	bps	1
kilobits per cond	Kbps	1000 bps
megabits per cond	Mbps	1 000 000 bps (1000 pps)
gigabits per cond	Gbps	1 000 000 000 bps (1000 bps)

Edexcel require you to measure file size using the following:

Unit		*Bytes*	*Equivalent to*
bit			*1 bit*
nibble			*4 bits*
byte		*2^0 bytes*	*8 bits or 2 nibbles*
kibibyte	*KiB*	*2^{10} bytes*	*1024 bytes*
mebibyte	*MiB*	*2^{20} bytes*	*1024 kibibytes*
gibibyte	*GiB*	*2^{30} bytes*	*1024 mebibytes*
tebibyte	*TiB*	*2^{40} bytes*	*1024 gibibytes*

$$time = \frac{file\ size\ (in\ bits)}{network\ speed\ (in\ bps)}$$

Worked Example:

How long will it take to download a **20MiB file** over a **12 Mbps connection?**

1. Convert the file size to bits

$$20 \times 8 \times 1024 \times 1024$$

2. Convert the speed to bits per second

$$12 \times 1000 \times 1000$$

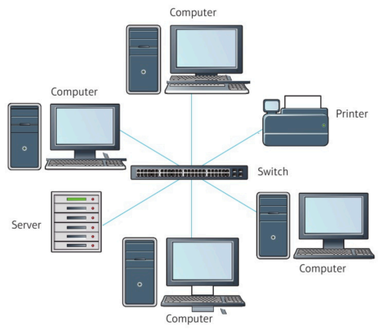
3. Arrange the size and speed expressions

$$time = \frac{20 \times 8 \times 1024 \times 1024}{12 \times 1000 \times 1000}$$

Topologies

A network topology describes how a set of computers are arranged within a network.

Star network topology all devices including clients, servers, printers and so on are connected to a central hub or switch. All communication is via the hub



Star Network Advantages

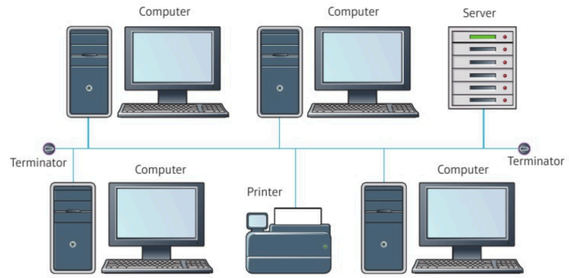
- ✓ Greater security as data are only sent to the intended recipient.
- ✓ If any of the connections fail only a single node will be affected.
- ✓ Fewer collisions between data packets

Star Network Disadvantages

- ☒ If the central hub fails then every computer on the network is affected.
- ☒ Expensive as extra cable and hardware (hubs) are needed.

Bus network

The bus topology is an older arrangement of devices, although it is still used in some places including cars and aircraft.
It includes a cable known as a backbone.
Each device connects to the backbone cable.
At each end of the backbone is a **terminator** (T).
The terminator prevents data from being sent back along the cable which prevents data collisions



Bus Advantages

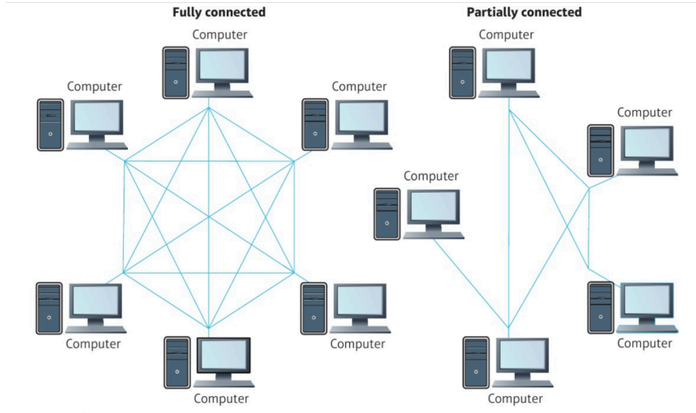
- ✓ Less cable is required than a star network making it cheaper to install.
- ✓ It works well for a small network.
- ✓ New nodes can be added anywhere on the bus.

Bus Disadvantages

- ☒ If the backbone breaks, the whole network goes down.
- ☒ If there is a problem with a terminator, the whole network goes down.
- ☒ Collisions slow down the performance of the network.
- ☒ More devices on the network will mean more collisions so it's not good for larger networks.
- ☒ Only one device can send data at a time.

Mesh network

- Mesh networks connect devices directly to each other
- No central switch
- Each device is a node in the network.
- Data can flow in any direction.
- Every device on a mesh network has to be able to send/receive data
- Data packets are sent by hopping from one node to another until they reach their destination.



Mesh Advantages:

- ✓ If a link breaks another route is available.
- ✓ The fastest route can be chosen.
- ✓ Can be quite cheap if wireless.

Mesh Disadvantages

- ☒ Expensive if wired.
- ☒ More complicated to maintain
- ☒ Set-up and maintenance can be costly

Internet

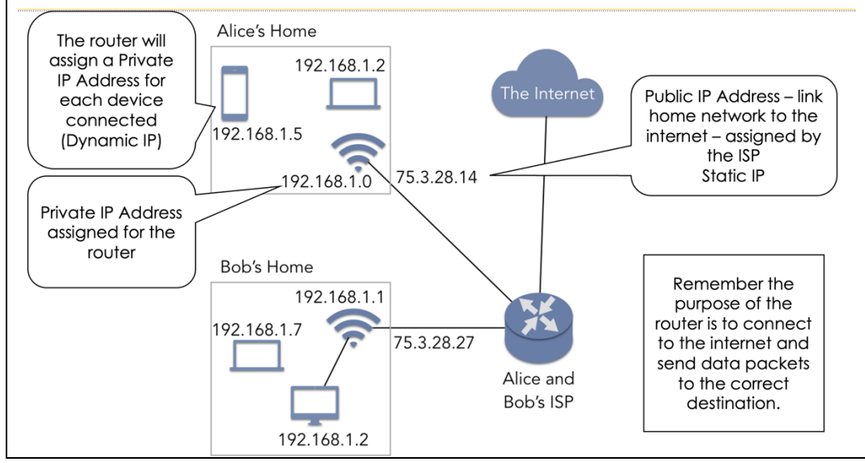
Internet Backbone – the multiple cables, fibre optic cables and satellite connections connect countries and continents to each other.

Local networks connect to the internet via a **Point of Presence** (POP) provided by an Internet service provider (ISP)

Network Access Points (NAP's) interconnect the internet backbones to form a worldwide mesh network

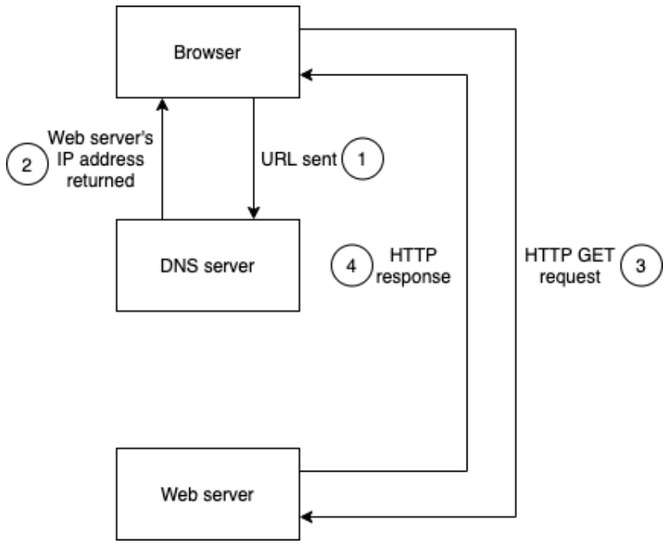
Routers forward data from one network to another across the internet from source to destination.

Every device connected to the internet is allocated an **IP address**.



DNS (Domain Name System)

A system for converting host names and web addresses into IP addresses



Routers

Routers send packets that contain data around the internet.

Describe how a router enables data to arrive at its destination.

Read the destination/recipient's IP address in each packet

Uses a routing table

Sends the data packet **to the next router**

Uses the fastest/least congested route/pathway

Keeps track / informs other routers of traffic conditions

Packet switching

Sending packets of data across the internet

Data is split into packets.

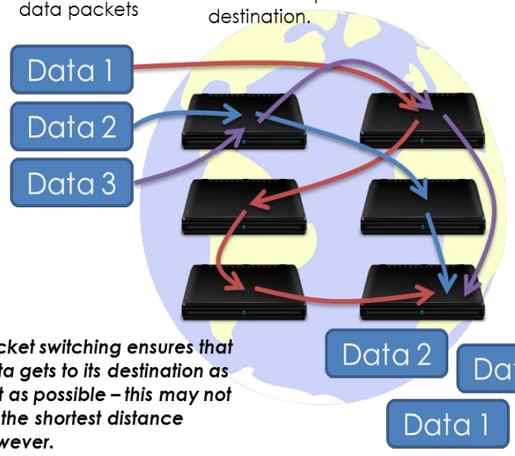
Each packets contain the following information:

Header	IP address of source IP address of destination Sequence number of packet Total number of packets Checksum
Body	Data
Footer	End of packet flag

1. A file is split into data packets

2. Routers follow the IP rules and direct data packets towards their destination.

3. Due to network traffic, packet switching may occur where the packets may take different routes and be directed to other routers before arriving at the destination.



4. If the packets are in the wrong order, the packet number can be used to reorder them back into the original file.

Packet switching ensures that data gets to its destination as fast as possible – this may not be the shortest distance however.

State one reason for splitting data into packets.

- Speeds up data transfer
- Reduces the reliability on a single pathway
- Reduces the impact of data corruption

Describe the process that ensures the data received matches the original.

Each packet has a sequence number (added at the sending end)
The packets are put back into (sequence) order (at the destination)

State two other items found in a packet

- Destination address
- Source address
- Error checking field / check sum
- Time stamp
- Sequence number

Check sum

Describe how a checksum is used to identify packets that have been corrupted during transmission.

A checksum formula is applied to the packet before it leaves the source computer

↓

The source calculated checksum is added to the packet header

↓

At the receiving end, the same checksum formula is reapplied

↓

The new checksum is compared to the received checksum in the packet header

↓

If the received checksum and the newly calculated checksum do not match, a resend request is issued

4-layer TCP/IP model

Layer	Example Protocols	Layer Purpose
Application Layer	FTP, HTTP, SMTP	Selects the correct protocol depending application, e.g. sending an email or viewing a web page.
Transport Layer	TCP	Provides transport of data between devices by splitting files into data packets and checking that they have been sent and received correctly.
Internet Layer	IP	Provides the routing of data across the network by making use of IP addressing. Adds the source and destination IP's to the packets.
Data Link Layer	Ethernet, WiFi	Provides the physical transport of data, such as the NIC and Cabling

	Computer A	Computer B
Application layer	FTP defines how the file must be requested.	FTP defines how the file will be provided.
Transport layer	TCP establishes a channel between the sending and receiving devices and splits the data into packets.	TCP reassembles the packets and checks that they are correct.
Internet layer	IP adds a packet header with the source and destination IP addresses.	IP removes the packet headers.
Link layer	Ethernet/Wi-Fi convert outgoing data packets into electric/radio signals for transmission to the network router. The packets are routed across the internet until they reach, and are received by, the link layer on Computer B.	Ethernet/Wi-Fi protocols specify how incoming signals should be converted back into data packets.

Protocols

Email Protocols:

- POP3 / IMAP – receiving emails
- SMTP – sending emails

Difference between the POP3 and IMAP email protocols.

POP3 deletes messages from the server when downloaded whereas IMAP leaves them on the server when downloaded.

Benefits to a user of using IMAP to access emails.

- Emails can be accessed from multiple devices because IMAP does not remove/delete emails (from the server)
- Emails can be accessed through a browser because IMAP doesn't need a client application to download messages

Network protocol used to request a webpage.

- HTTP
- HTTPS - secure

FTP (File Transfer Protocol) - Allows the transfer of files between computers

Methods of Network Security

Access levels

Access control determines the facilities a user has access to, such as:

- software
- email
- internet
- documents and data
- the ability to install and/or remove software
- the ability to maintain other users' accounts
- File permissions – read only, read/write, execute a program file, delete
- A *network manager* should restrict most users to allow them to access only the facilities they need.

Authentication

Allows us to confirm the identity an individual.

There are lots of ways of confirming the identity of an individual that come under one of three factors:

- ✓ Knowledge factor: Something the user knows, eg a password
- ✓ Possession factor: Something the user owns eg a mobile phone
- ✓ Biometric factor: eg Fingerprint, iris scan

Physical security

- Physical security can be used to only allow authorised people to enter critical areas, such as server rooms.
- Doors could be fitted with an electronic lock system
- Electronic lock systems can read cards/fobs/biometrics of employees and check them against details stored on a database to determine if an employee has special permission to enter.
- Movement sensors to activate an alarm/ a light
- Security lights / alarms, so that intruders would be scared off / identified
- Alarms / alerts could trigger because there is unauthorised access

Firewalls

- A firewall acts as a barrier between the local area network and the internet.
- Firewalls use a set of rules to determine which packets of data are allowed in and out, so unauthorised access
- attempts to the network will be denied.
- Rules can be customised to suit the company's particular needs.
- They can flag up suspicious activity by employees such as downloading viruses or sending confidential data.

Encryption

A method of scrambling data with a key. Anyone can join an open Wi-Fi network and see traffic from other users. If encrypted data is intercepted, it will have no meaning. To read the data, the user must decrypt it using the key. The encryption method used is called 'SSL' (Secure Socket Layer).

Pen testing

- **Ethical hacking** is 'good' hacking by looking for weaknesses in the software and systems. They work on behalf of an organisation, simulating the actions of a hacker, known as **Pen testing**
- Penetration testing is the process of attempting to gain unauthorized access to a network in order to find and fix vulnerabilities.
- There are two types of penetration testing: white box and black-box testing.
- **White box testing** simulates a scenario where an insider with knowledge of basic credentials and login information attempts to breach security.
- **Black-box testing**, on the other hand, simulates an external hacking attempt on an organization or company, similar to what is often portrayed in the media.