Chapter 4: Networks

In this chapter you will learn:

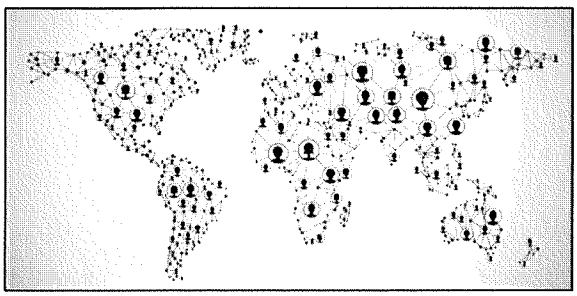
- what is meant by a network
- the different ways that a network can be structured
- the basic hardware that is required to build a network
- the role of each type of hardware in a network
- what factors can affect the performance of a network
- what is meant by a virtual network
- what is meant by the term 'Wi-Fi'
- what is meant by the Internet, and how websites and data are accessed and stored
- what is meant by the term 'packet switching'
- what is meant by a protocol
- how layers are used in a protocol
- the different protocols that are used for different applications

What is a network?

Up until the 1990s, most computers in both the home and in businesses were **stand-alone computers**. A stand-alone computer is one that is not connected to any other computers that it needs for regular use. When we connect computers together we create a **network**.

Stand-alone computer – a computer that is not connected to a network

Network – a collection of computers that are connected together



We network our computers together all over the world so that we can communicate with each other and share resources

One of the first networks to be created was back in 1969. This became known as the Advanced Research Projects Agency Network (ARPANET). Universities decided to connect their computers together so they could communicate with each other and share resources. This network was the predecessor to the Internet.

We still use networks today primarily for these two functions, to be able to share files and resources and to be able to communicate with each other.

There are a range of advantages and disadvantages of networking computers together; these include:

Advantages	Disadvantages
• Users can share files and resources with others. • Users can access their files and resources from another computer on the same network. • Servers can be created to centrally control a number of operations and services on a network, such as security and file backup. • Communications can be sent to any computer on the network. • **Peripherals** can be shared.	• Networks can be subject to security issues, allowing unauthorised access to users' files and resources. • Malware and viruses can be spread from computer to computer and it may be difficult to control and eradicate the issue. • Depending on the structure of the network, if an element of it fails, this could cause failure or issues for the rest of the network. • A high amount of **network traffic** can cause a network to run slowly.

Discussion point: Do you think that the widespread use of computer networks has changed the way we communicate with each other for better or worse?

Peripheral – a device that is attached to a computer system

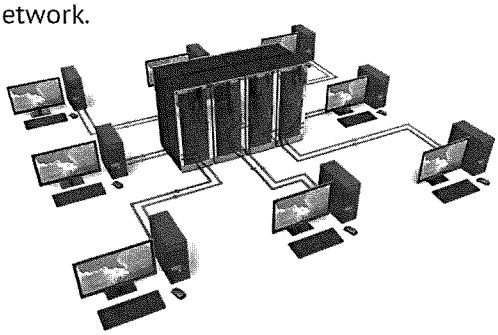
Network traffic – the amount of data that is travelling across a network at any one time

What are the different ways in which a network can be structured?

OCR specification point:

- ☑ Types of network:
  - LAN (Local Area Network)
  - WAN (Wide Area Network)
- ☑ The different roles of computers in a client–server and a peer-to-peer network
- ☑ Star and mesh network topologies

There are different ways in which networks can be structured and this will depend on their function and purpose. It will also depend on the resources available to create the network.

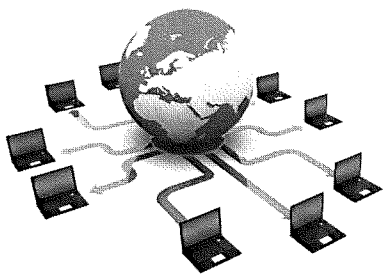


Local area network (LAN)

A LAN is a network that covers a small geographical area. They are normally contained within a single building or a small site of buildings. LANs are normally found in the home, schools and small businesses.

The key characteristics of a LAN include:

Characteristic	Description
Connection method	Can be copper cables, coaxial cables, twisted cables, fibre-optic cables or radio waves
Ownership	The structure is normally owned by the individual or the organisation
Transfer rate	High – often as much as 1 Gb per second (gigabits, not gigabytes!)
Transmission errors	Fewer errors as packets of data are being sent over a small distance
Security	Can be kept fairly high as security can be controlled and updated centrally and regularly



Wide area network (WAN)

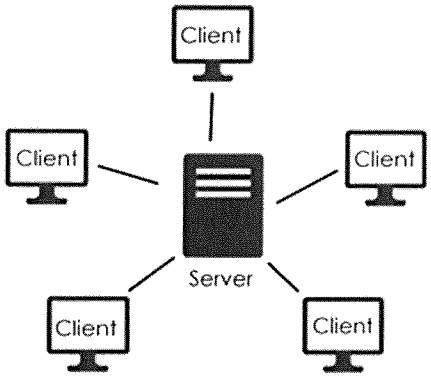
A WAN is a network that covers a large geographical area. A WAN could cover a city, several branches of an organisation, a country or even several countries. The Internet is the largest WAN that we have created. A WAN is often a collection of connected LANs.

The key characteristics of a WAN include:

Characteristic	Description
Connection method	Can be coaxial cables, twisted cables, fibre optic cables or radio waves. They will also make use of telephone network systems, leased lines and sometimes satellite communications.
Ownership	Parts of the structure will often be owned by other people, often quite a number
Transfer rate	Normally restricted to less than 200 Mb per second
Transmission errors	Greater chance of an error occurring as packets of data are being sent over longer distances
Security	Can be difficult to manage due to the high number of devices connected

Client-server network

A client–server network contains two main types of computer, a **client** and a **server**. Each computer that is connected to the network that is available for general use is called a client. Each of the clients is connected to a central computer in the network called a server. A client–server network may have a single central server or it may have several performing different functions.



The server allows a variety of functions to be performed on the network from a central computer, rather than having to carry each one out on the individual clients. These functions include:

- User access control
- Data storage
- Monitoring network traffic
- Managing Internet connections
- Centralised security
- Scheduling backups
- Providing email services
- Managing printing jobs

Client – a computer that requests data and services from a server

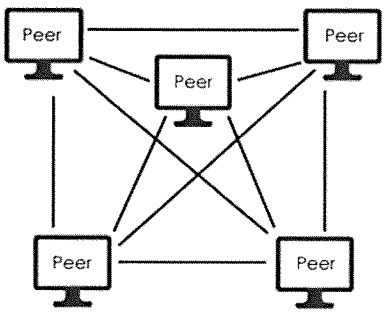
Server – a computer that provides services and data for other computers on a network

If a client–server network is particularly large, it will have a number of servers dedicated to performing each of the functions. This enables the network to run as efficiently as possible.

Advantages of a client–server network	Disadvantages of a client–server network
• Centralised process for security so the organisation can make sure all computers are up to date with their security • Centralised process for backup so users do not need to worry about needing to back up their data • Levels of access can be applied to stored data making sure the correct people see the correct data • Centralised process for updating software so this does not need to be done individually for each computer on the network	• Expensive to set up as lots of hardware will need to be purchased; servers in particular are expensive to purchase • Expensive to maintain as specialist staff will need to be hired to maintain the network • If a server fails, this may cause some functions of the network to be unavailable; for example, if the email server fails then it may not be possible to send emails

Peer-to-peer (P2P) network

Each computer in this network is known as a **peer**. A peer-to-peer network does not have a central server to manage the network; the management of all functions is down to the responsibility of each individual peer.



Peer – a computer that is part of a network that is not controlled by a server

Each computer on the network is able to share files and resources with other computers on the network. They can do this by making them available in a public area.

Advantages of a peer-to-peer network	Disadvantages of a peer-to-peer network
• Cheaper to set up as it does not require expensive servers • Cheaper to maintain as it does not require specialist staff to maintain • If any peer fails on the network, only the resources provided by that peer are unavailable	• There is no centralised process managing data and security, so this may make the network less secure as it is each peer's responsibility to maintain their own • Each user will need to make sure they run their own backup as this is not performed centrally • If a peer-to-peer network has many peers on it, this can cause a lot of network traffic and may make the network run more slowly

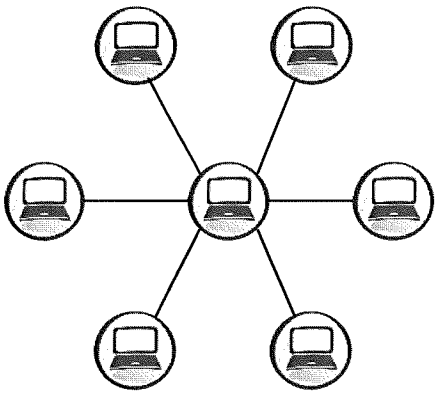
Network topologies

A **network topology** is essentially the structure of a network. It is the way in which all the computers and devices are connected together in a network. We need to know the structure of two main network topologies; these are the star and the mesh topologies.

Network topology – the physical structure of a network

Star topology

In a star network topology there is a central computer or server that all other computers are directly connected to. Each computer is also indirectly connected to every other computer via the central computer or server.



An example of a star network topology

If a computer fails in the star topology it has little effect on the other computers, unless it is the server in which case it is catastrophic! Also, the security of a star topology is generally quite high as the traffic from each computer goes through the central computer or server before interacting with another computer. **Data collisions** can be an issue on a computer depending on the structure of a network. This is not too much of a problem on a star network, though, as each computer has its own dedicated cable that connects it to the server.

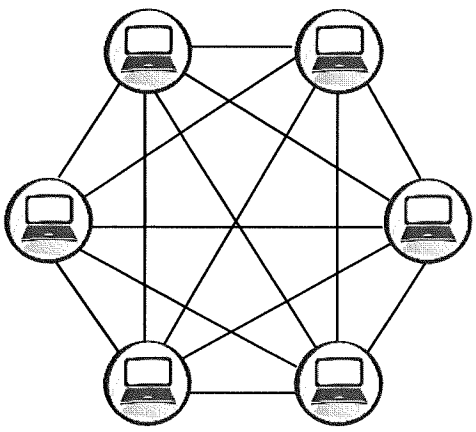
Data collision – the result of two devices on the same network attempting to transmit data at the same time down the same connection

However, this network structure can be expensive to set up as it needs a central controlling computer and a large amount of cabling to connect each computer.

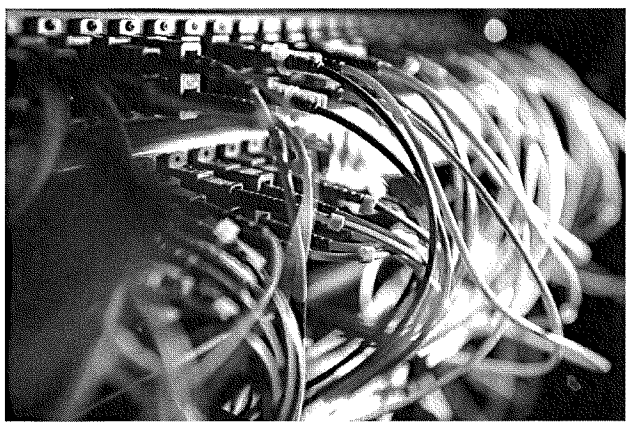
Mesh topology

A mesh topology can either be a full mesh or a partial mesh. In a full mesh topology each computer in the network is directly connected to every other computer in the network. In a partial mesh topology, computers that need to interact the most with each other, for example exchange data, are the ones that are connected together.

It is easy to add further computers into a mesh network, but this can often take quite a lot of cabling. The network structure itself needs a great deal of cabling to be set up; this can be an expensive setup cost. If one connection to a computer fails in this type of network, it has little effect on the network as the computer can find another working connection to use instead. There can sometimes be redundant connection in a mesh network; this is often why a partial mesh will be set up instead of a full mesh.



An example of a full mesh network topology



What hardware is required to build a network?

OCR specification point:

☑ The hardware needed to connect stand-alone computers into a local area network:

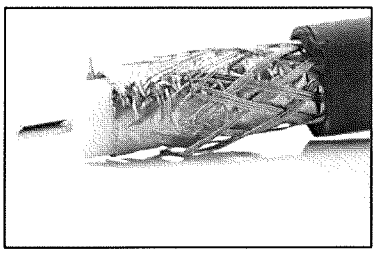
- wireless access points
- routers/switches
- NIC (Network Interface Controller/Card)
- transmission media

In order to create a physical network, we need certain **hardware**. There are some fundamental hardware devices that are required to create most networks. The most basic of these is the transmission media.

Hardware – the physical parts of a computer system

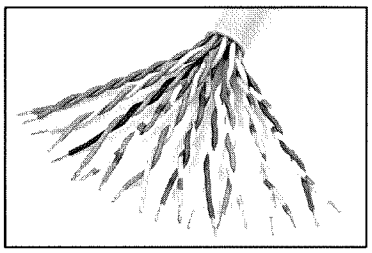
The transmission media is what will be used to carry the data around the network, effectively the cables. There are several different types of cables that can be used; these include:

- Coaxial cable
- Twisted pair cable
- Fibre-optic cable



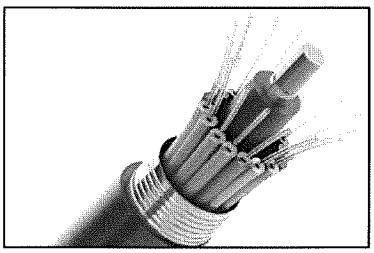
Coaxial cable

Coaxial cable is a type of cable that has a central wire that is surrounded by an insulating layer. Many coaxial cables then have a final outer layer that acts like a jacket.



Twisted pair cable

Twisted pair cable is a type of cable that has two separately insulated wires that are twisted around each other inside an outer layer. This is the most common type of cable that is used in a network.



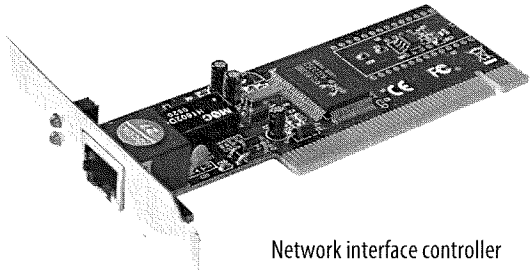
Fibre-optic cable

Fibre-optic cable is a type of cable that has lots of very fine glass threads inside an outer layer. Many networks are slowly replacing their cabling with fibre-optic cables as it carries data much faster than other media.

As well as transmission media, a computer will need some way of connecting the transmission media to the computer so that data can be transmitted around the network. The component that is required for this is called a network interface controller, or card (NIC). A NIC is a circuit board that is installed into a computer to allow it to be connected to a network.

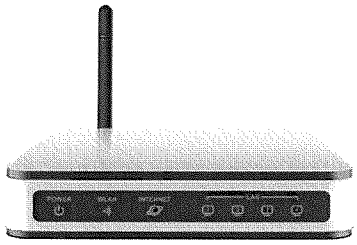
A computer can also be fitted with a wireless network interface controller (WNIC) to allow a computer to be connected wirelessly to a network.

In order for computers to connect wirelessly to a network, the network will need to have wireless access points (WAP). A WAP is a network hardware device that allows any device that has Wi-Fi capabilities to connect to the network. In many home networks the WAP is built into the router.



Network interface controller

A router is a hardware device that is essential for connecting computer networks together. It is the device that is used to connect our devices at home to the Internet. It is responsible for forwarding packets of data from one network to another network. A router will scan a packet of data that enters the device to see whether its destination is the network that it is currently travelling in or another network. It will then forward the packet on to its destination.



Router

A switch performs a very similar function to a router, except it only operates within a single network. It too scans a packet of data that enters the device to see what the destination of the package is. It will then forward the package on to its destination. Switches are often used to join together sections of a LAN network in larger networks.

What can affect the performance of a network?

OCR specification point:

☑ factors that affect the performance of networks

The performance of a network is something that is very important if we want it to be efficient. But what do we mean by the performance? We mean how well the network is operating and how free from errors it is; this includes how quickly data can be transmitted around the network.

There are a number of factors that can affect the performance of a network, including:

Interference – additional energy that appears in a network, that causes a signal to be disrupted

Bottleneck – data that is delayed in transmission through an overloaded section of a network

Factor	Description
Bandwidth	This is the rate at which data can be transmitted around a network. This means the time that it takes for the data to be sent from one device to another in the network. It is not a measure of how fast the data can travel. Bandwidth is commonly measured in megabits per second. The more bandwidth a network has, the higher the performance ability of the network. If a network has many users, it will require a high amount of bandwidth to operate efficiently. If it does not have a high amount of bandwidth, this may cause the performance of the network to be affected due to the high amount of network traffic. Bandwidth can also be referred to as the bit-rate.
Latency	Latency is the measure of any delay that it takes to transmit a data packet from one destination to another in a network. There are many things that can create latency on a network. This can range from the level of **interference** in the type of cables that are used, to the occurrence of any **bottlenecks** in a network. If the latency of a network increases, this will affect the performance of a network and cause it to run more slowly.
Error rate	The error rate of a network simply refers to the number of errors that occur in the transmission of data packets around a network. The higher the error rate of a network, the less reliable the data and the network connection will be.
Transmission media	The type of cables used in a network can affect the network performance. Fibre-optic cables are capable of transmitting data much more quickly than coaxial or twisted pair cables. The signal is also less likely to deteriorate in fibre-optic cable, making it more reliable. This can increase the performance of the network.

What is a virtual network?

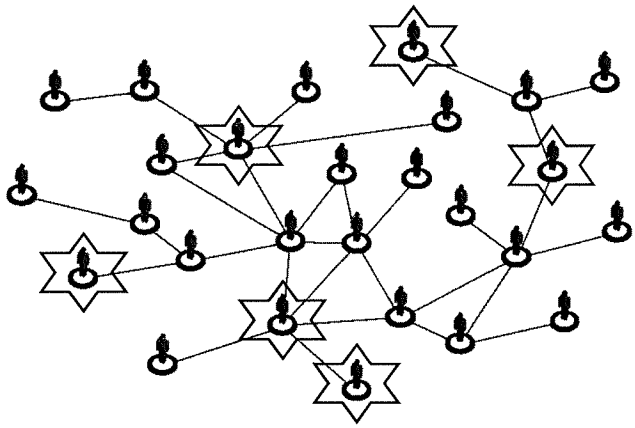
OCR specification point:

☑ the concept of virtual networks

A **virtual network** is one that is created using software. A business may choose to partition off its larger physical network into a number of virtual networks. The part of the network that has been partitioned off by the virtualisation software is referred to as a VLAN. By doing so it can provide each department with their own separate network by virtually partitioning off some of the physical network it has. This can have a number of benefits for a business; including:

Virtual network – a network created using software

- It only needs to have one large physical network in place.
- Each virtual network can have its own level of security and access. This can be set at different levels across each VLAN, depending on the sensitivity of the information for each department.
- Bandwidth can be distributed differently across each VLAN. This means that those departments that create more network traffic can be given more of the bandwidth available.



The computers used by these people are part of a large physical network. A virtual network has been created for all those people who are marked with a star. Only they can see the information available on the virtual network. The other people are not aware that the virtual network exists.

Users within a large physical network may not even be aware that a virtual network exists. It can be created so that they cannot see it and are not aware that it exists. This can be imperative to the security of some companies that hold highly confidential data.

We can make use of virtual networks to keep our own personal data safe. This type of virtual network is called a virtual private network (VPN). A VPN can be set up within a large WAN such as the Internet. A user can then log in to their VPN from anywhere in the world and use their own private network to communicate any of their personal data. The packets of data that are sent when using a VPN have an extra element to them. This element acts like an outer layer of protection that means that only the VPN can understand that packet of data. Special protocols and encryption are used to do this.

Discussion point: How could a business make use of a VPN?

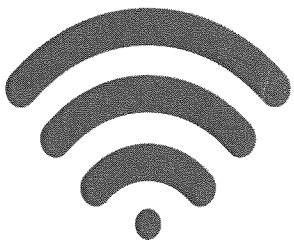
What is Wi-Fi?

OCR specification point:

☑ Wi-Fi:

- frequency and channels
- encryption

Wi-Fi is the name given to the wireless technology that we use to connect all our devices to the Internet. Unlike a hardwired connection, Wi-Fi uses radio waves to provide a connection to the Internet. The radio waves are transmitted by a WAP that normally has a wired connection to the Internet. Devices that have Wi-Fi capability will detect the radio waves and allow a connection to the network to be established.



Discussion point: Wi-Fi is something that you probably use on a daily basis, but do you know how it works? Do you think it is okay for people to use technology on a daily basis when they do not know how it works?

The radio waves of Wi-Fi are mainly in two different **frequency** bands:

- 2.4 GHz – ultra-high frequency
- 5 GHz – super-high frequency

The frequency of the band represents the number of radio waves per second that can be transmitted. Each frequency band is separated into a number of different channels. A device will use a certain channel to receive the radio waves. If two devices close together are using channels that are close together, this can cause interference. Therefore, it is possible for a user to choose the channel used by their Wi-Fi device.

Frequency – the rate per second at which vibration occurs, creating a wave

It is important when using a wireless network to have an **encryption** method in place. A username and password adds one level of security to our wireless network, but a wireless encryption method adds an extra level of security.

Encryption – scrambling data to make it unreadable, to add to security in transmitting the data

Most WAPs will have three methods of encryption to choose from; these are wired equivalent privacy (WEP), Wi-Fi protected access (WPA) and WPA2.6+89

Discussion point: To what extent do you think we should trust encryption? For example, WEP listed above is no longer thought to be very secure; passwords can be cracked really easily!

How are websites and data accessed and stored using the Internet?

OCR specification point:

☑ the Internet as a worldwide collection of computer networks:
- DNS (Domain Name Server)
- hosting
- the cloud

The **Internet** is the largest network that we use. It is a wide area network that is made up of a network of networks. The Internet is the name that we give to the infrastructure (all the hardware) that is required to create the network. It is not to be confused with the **World Wide Web**, which is the collection of web pages and protocols that we access using the Internet.

Internet – the largest WAN network

World Wide Web – the collection of web pages and protocols we access using the Internet

There are three key elements of the Internet that we need to be aware of; these are a domain name server (DNS), hosting and the cloud.

Domain name server (DNS)

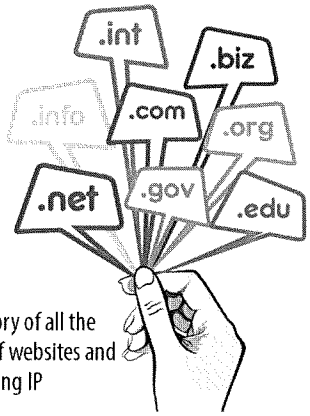
When computers use the Internet they are given an IP address. This is a unique address given to each device that is using the Internet Protocol (IP) to communicate over a network. We use the IP in the TCP/IP that we use when communicating using the Internet. Servers are created to store the IP addresses for each device. Computers and network components use an IP address to route the request to view a web page to the correct site that we are trying to reach.

A domain name is the name given to a collection of web pages that we may want to view, for example ocr.org.uk. A DNS keeps a directory of all the domain names along with their IP address.

This means that we do not need to remember the IP address to access the website, only the domain name of the website we want to access.

Each domain name ends with a set of letters that indicates which top-level domain it belongs to. These include:

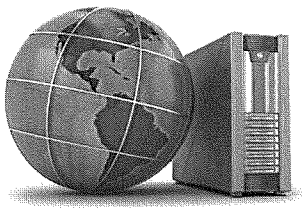
- .com – a commercial business
- .uk – a business based in the UK
- .org – a non-profit organisation
- .gov – a governmental agency



A DNS is a directory of all the domain names of websites and their corresponding IP

Hosting

When a company sets up a website it will need to find a way to host it so that it can be made available for access on the Internet. A host is a web server that hosts one or more websites. If a company has a number of web servers dedicated that hosts a number of different websites for other companies, this is called hosting.



It is quite difficult to host a website; there are a number of things that need to be considered. The host will need to be switched on at all times, it takes a great deal of technical knowledge to keep it operational, it takes a great deal to security to protect it against hackers, and if it fails, any websites it holds are no longer accessible. Therefore, there are whole businesses dedicated to hosting websites for other companies.

Discussion point: Why might you choose not to host a website on your personal computer?

The cloud

The cloud is an ever-growing feature of the Internet. More and more businesses and individuals are choosing to use it every day.

A cloud is the name given to the remote storage of data and software that we access using a device. The data and software that we want to use are not stored on our individual device or hardware, but stored in a remote location, normally by another company. We use the Internet to access the data and software whenever we need it.

The advantages and disadvantages of using the cloud include:

Advantages	Disadvantages
• We do not need to purchase additional hardware to store data and software • Companies do not need to employ technical staff that may be needed to maintain the hardware to store the data and the software • Companies and individuals do not need to worry about running a backup of their data when it is stored in a cloud • It is easy to access files and software from anywhere in the world as long as we have an Internet connection • If software is accessed remotely there is no need to update it	• We are relying on the responsibility of another to keep our data safe and secure as we do not control these measures • If we do not have an Internet connection, or have a poor one, we may not be able to access our data • If the cloud servers fail, we may not be able to access our data until they are made available again

What is packet switching?

OCR specification point:

☑ packet switching

To send data over a network we divide it into **packets**. The packets are created by software and normally contain three elements:

Packet – a unit of data that is transmitted across a network

1. A header – this contains the sender's IP address, the receiver's IP address, the packet number, the length of the packet and the protocol
2. The payload – this is the data itself
3. The trailer – this contains the end-of-packet marker and error checking

When the data has been divided into packets, it can be sent across a network. This act of sending the packets is called **switching**. There are two ways in which packets can be sent across a network: these are packet switching and circuit switching.

Packet switching – the process of sending data packets across a network

In a packet switching network, each packet finds its own route to its destination. All packets do not need to follow the same route. So if a problem occurs with a connection on a network, each packet can take a different route. The route they normally take is selected by a router. When all packets have arrived they can be reassembled.

In a circuit switching network a link is established first between the sender and the receiver. The packets of data are sent in a stream along the established connection until they have all been received.

What is a protocol and how are layers used in them?

OCR specification point:

☑ the uses of IP addressing, MAC addressing, and protocols including:

- TCP/IP
- HTTP and HTTPS
- FTP
- POP
- IMAP
- SMTP
- the concept of layers
- Ethernet

In order for us to use the Internet to communicate effectively using a network, we need to have in place a number of **protocols**. These are rules that govern how the network functions and how communication is carried out. If protocols did not exist it would be like a group of people trying to communicate with each other and share resources that are all in a different language. This would make the process very difficult! A protocol makes it possible for all devices to effectively be speaking the same language when communicating with each other on a network.

Protocol – a set of rules that govern network operations

Different protocols are used for different applications on a network. This what the following protocols are used for:

Protocol	Application
Transmission Control Protocol / Internet Protocol (TCP/IP)	This sets rules for how devices on a network are connected. The TCP part manages the separation of a file into data packets to be sent across a network. It then manages the process of reassembling the data packets. The IP part gives each packet and address to allow it to reach its destination.
Hypertext Transfer Protocol (HTTP)	This is used by web browsers to access websites. It allows the browser to communicate with a web server.

Protocol	Application
Hypertext Transfer Protocol Secure (HTTPS)	This is a more secure version of HTTP. It encrypts and decrypts web pages and data as it is sent using this protocol. It is used by banks and online shopping sites to keep personal data secure.
File Transfer Protocol (FTP)	Used in conjunction with the TCP/IP protocol to transmit files across a network.
Post Office Protocol (POP)	The POP3 protocol is used to retrieve emails from a server. An email server receives a user's emails and they are then held on the server. Periodically, the user or the user's email client checks the user's mailbox on the server and downloads any mail using the POP3 protocol. When the email is downloaded, it is then deleted from the server by the protocol.
Internet Message Access Protocol (IMAP)	IMAP works in a very similar way to POP3. One difference, though, is that the email is not deleted from the server when the email is downloaded, until the user chooses to delete it.
Simple Mail Transfer Protocol (SMTP)	POP3 and IMAP are concerned with the downloading and reading of emails, but SMTP governs the sending of emails using a network.

A protocol is normally separated into different **layers**. The layers in a protocol are responsible for different parts of the process. The process is broken down into layers to make it less complex. The main things that need to be considered when using a network to communicate data are: What is it that is being communicated? Who is the data being sent to? How will the data get there?

Layer – an individual section of a protocol that is responsible for one part of the operation

Firstly, one way to send information across LANs at least is through Ethernet cables: implemented using twisted pair cables, capable of data transfer speeds up to 100 Gb per second. In order to transfer data across larger networks, a communication protocol is needed. Not using a communication protocol would be like asking someone who doesn't speak English to understand a question in English; while what you want to say will be heard by the non-English speaker, they will not understand what you are communicating, so will not reply to your question.

We can look at the layering of one of the protocols, the TCP/IP protocol. It manages the separation of data into packets and provides the packet with an address for its destination. TCP/IP has four layers:

The Application Layer
This layer is concerned with collecting and distributing data. It makes sure data is in a suitable format for transmission.

The Transport Layer
This layer is concerned with establishing and terminating connections between devices on a network. It does this via the use of a router. This layer also performs any error detection and correction functions, and establishes the speed at which the data can be sent and received.

The Internet Layer / network layer
This layer allows the exchange of data between lots of different networks. It is at this layer where the IP part of the protocol is used to establish a route to the destination of the data packet.

The Data Link Layer
This is concerned with the transmission media that is used to send data over a local network. It ensures the network hardware can be used to transmit the data and that any transmission media can be used.

Chapter Summary

- A network is a collection of devices that are connected together.
- We mainly use networks to communicate and share resources.
- A network can be a LAN or a WAN. A LAN is a network that covers a small geographic area; a WAN is a network that covers a large geographic area.
- A network can be structured as a client–server or a peer-to-peer format. A client–server network has a central computer that controls the operations of the network. A peer-to-peer network does not have a central computer; all the computers are equal.
- A network topology is the way in which the network is wired and structured. The two most common network topologies are star and mesh.
- To build a network we need a range of hardware including transmission media, routers, switches, NIC and, if it is a wireless network, WAPs.
- There are four main factors that can affect the performance of a network: bandwidth, latency, error rate and transmission media.
- A virtual network is one that is created using software.
- Wi-Fi is the wireless technology that we use to connect devices to the Internet. Wi-Fi uses radio waves to provide the connection.
- A DNS is a server that holds a directory of domain names and their corresponding IP addresses.
- Hosting is when a company stores the websites for companies of a web server to make them available for access using the Internet.
- For data to be transmitted over a network, it needs to be divided into packets. The act of sending the packets of data over a network is called packet switching.
- A protocol is a set of rules that govern how a network operates. Different protocols are used for different applications; they are also made up of a number of different layers.

Practice Questions

1. Explain two benefits of networking computers together. [2]
2. Explain the difference between a LAN and a WAN. [4]
3. Explain two factors that can affect the performance of a network. [4]
4. Describe the role of a client in a client–server network. [2]
5. Describe the operation of two different layers in the TCP/IP protocol. [4]

