Edexcel

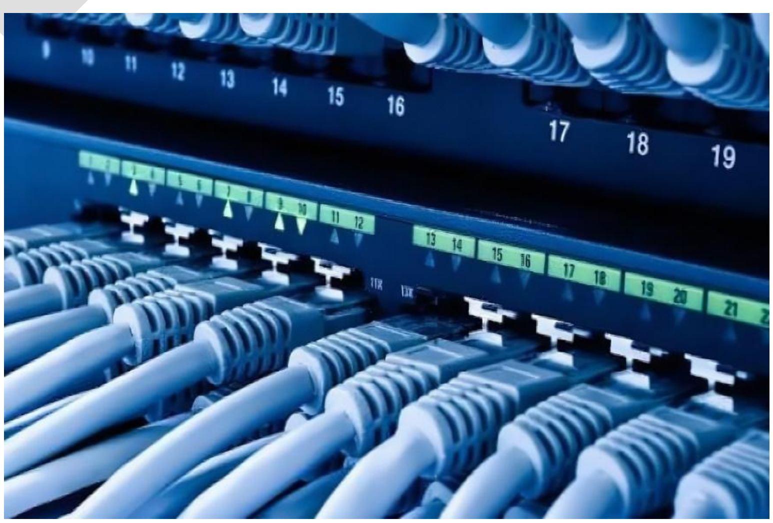
OL

ICT

CODE: (4IT1)

Unit 2

Connectivity



Chapter 04

Digital communication

SPEED AND VOLUME OF DATA TRANSFER

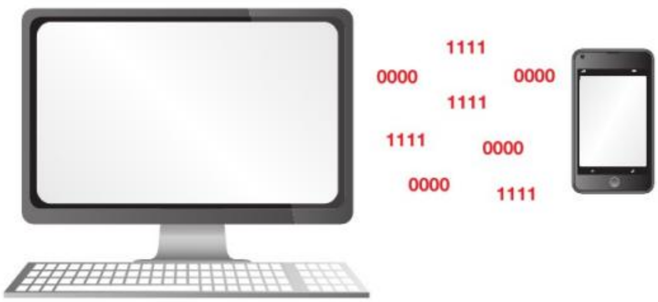
As we transfer more and more data, it becomes more important that we understand how to increase the **speed** at which we can transfer it.

Bandwidth

The speed at which devices can transfer data depends on the **bandwidth** of the connection.

IMPACT ON USER EXPERIENCE

Higher bandwidth enables faster data transfer, faster uploads and downloads, and faster tasks like multiplayer online gaming and high-definition video streaming.



▲ **Figure 4.1** Binary data is stored within and transferred between digital devices

SUBJECT VOCABULARY

buffer an area of memory used to temporarily store data, especially when streaming video

SUBJECT VOCABULARY

bandwidth the number of bits that can be carried by a connection in one second

SUBJECT VOCABULARY

latency the amount of time it takes to send data between devices

domain the name used to identify a web server

When streaming video, all of the data does not need to be downloaded before playback can start. Instead, a portion of the video data is stored temporarily in an area of memory called a **buffer**.

Latency

As well as bandwidth, the speed of data transfer also depends on **latency**. Latency is the delay in the time it takes to send data between devices.

You can identify latency by 'pinging' a **domain**. When you ping a domain, you send a packet of data to a server and the packet of data is immediately returned by the server to the originating device.

IMPACT ON USER EXPERIENCE

In online gaming, the game will play smoothly if the bandwidth is adequate. However, if the latency is high, events in the game will lag and the game will not seem responsive to the player's commands.

Factors that affect speed and volume of data transfer

When devices transfer data, they can be affected by many factors that stop bits from reaching their destination. These bits then have to be sent again, which slows the overall data transfer rate.

TRANSFER METHOD

Wireless methods operate on limited **frequencies**, while copper cable can carry more frequencies, providing more bandwidth for cabled methods.

INTERFERENCE
Electromagnetic signals from wireless devices and appliances can disrupt wired and wireless connections, which can be shielded by wrapping wires in a thin metal layer.

BLOCKAGES
Walls and furniture reduce the strength of wireless signals. This reduces the available bandwidth.

DISTANCE
The strength of a wired or wireless signal is reduced as the distance that it has to travel increases.

DEVICE-TO-DEVICE COMMUNICATION

Devices can connect directly to each other using wired or wireless methods. This is called **device-to-device communication**.
Table 4.1 shows some examples of device-to-device communication.

SUBJECT VOCABULARY
minijack a plug and socket widely used for analogue audio signals in portable devices
HDMI (High-Definition Multimedia Interface) used to transmit video and audio data

▼ **Table 4.1** Examples of device-to-device communication

DEVICE 1	DEVICE 2	CONNECTION BETWEEN DEVICES 1 AND 2	USE
Temperature sensor	Air conditioner	Wired	To turn on the air conditioning when the temperature is too high
Smartphone	Headphones	**Minijack**	To play music from the smartphone on the headphones
Laptop	External hard drive	USB	To transfer files
Camcorder	Monitor	**HDMI**	To operate as a security camera
Games controller	Games console	Bluetooth	To control a game

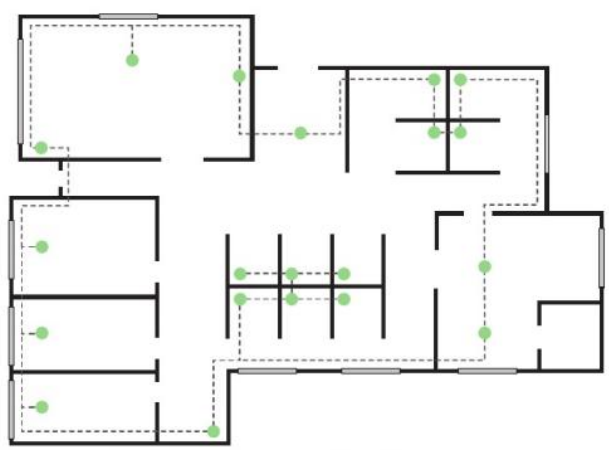

▲ **Figure 4.3** Device-to-device communication

NETWORK COMMUNICATION

When two or more computers are connected, a network is created. There are four major types of networks.

Local area network (LAN)

A LAN is a network that connects digital devices that are in a small geographical area, like a building or group of buildings that are close to each other.


▲ **Figure 4.4** LANs are found in homes, schools and office buildings

Wide area network (WAN)

A Wide Area Network (WAN) is a large network used to connect buildings owned by businesses, law enforcement, health, education, and government departments. WANs use third-party telecommunications but have slower transfer speeds.

Personal area network (PAN)

A PAN is a group of connected devices that are all near an individual user. When a PAN only uses wireless connectivity, it can also be referred to as a WPAN (Wireless Personal Area Network). However, the general term PAN is more commonly used to refer to all types of PAN.

Tethering

Tethering is the act of connecting a host device, like a smartphone or tablet, to another device using a mobile broadband connection, enabling sharing of the connection.

Mobile phone network providers can enable or disable tethering as part of the **service agreement**. Some network providers charge more for this feature to be enabled.

SUBJECT VOCABULARY

tethering connecting a host device that uses a mobile broadband connection with other devices so that they can use the host's broadband connection

SUBJECT VOCABULARY

service agreement contract

▲ Figure 4.6 Devices can be tethered using wired or wireless connectivity

THE WAYS IN WHICH DIGITAL DEVICES COMMUNICATE

The methods that digital devices use to share data and some common uses of these methods are shown in Table 4.2.

▼ Table 4.2 Ways in which digital devices communicate and their common uses

Method	Technology	Use
Satellite	Radio waves	GPS, television, telephone, military
Broadcast	Radio waves	Television shows, radio shows
Wired	Electrical signal	Networking, connecting peripherals
Wireless	Radio waves	Networking, connecting peripherals

Satellite communication

Satellites transmit and receive data from digital devices using antennae. They offer constant availability and immunity from power shortages. However, signals cannot pass through solid objects and can be affected by atmospheric weather conditions.

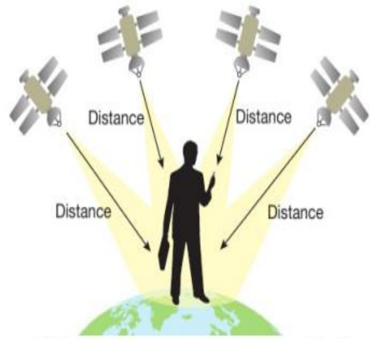
▲ Figure 4.7 A communication satellite

GPS

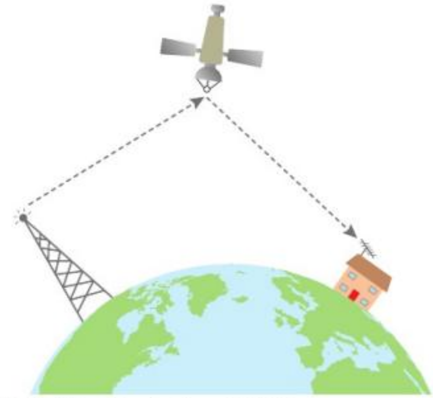
GPS signals are used in navigation aids to calculate device location, sent from a network of 24 Earth-orbiting satellites. To calculate accurate location, a device must view only four satellites.

Television

Digital Video Broadcasting (DVB) is the international standard for broadcasting digital television. It involves transmitting video signals from a broadcaster to satellites, which then broadcast the signal back to Earth. Satellite viewers have antennas that receive and decode the signal, with some televisions having decoders.



▲ Figure 4.8 Only four satellites need to be in view to get an accurate location of a device using a GPS signal


▲ Figure 4.9 DVB-S (Digital Video Broadcasting – Satellite)

TELEPHONE

Satellite communication is also used to allow people in remote areas to place voice calls using satellite telephones. (figure 4.11 and figure 4.12)

MILITARY

The military in many countries use satellites for communication systems, such as the Global Command and Control System.


▲ Figure 4.11 Satellite telephones use antennae to transmit data to (and receive data from) one or more satellites

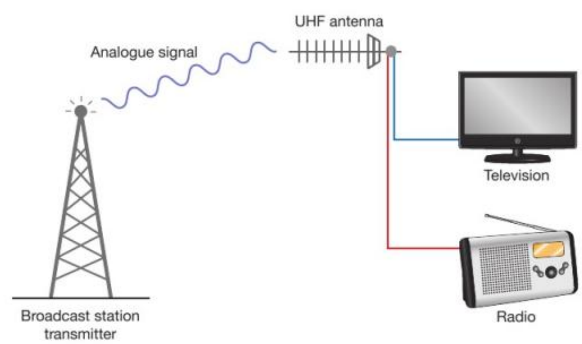

▲ Figure 4.12 Satellite phones are used in remote areas


▲ Figure 4.13 The Global Command and Control System provides military communication

Broadcast communication

ANALOGUE TELEVISION AND RADIO

Transmitters broadcast television and radio signals that are received by a viewer's antenna. This antenna sends a signal through a wire to the television or radio receiver, which converts it into images and audio. (figure 4.14)



▲ Figure 4.14 An analogue signal is received by an antenna and fed to different devices

Digital television

DVB-T is a terrestrial DVB method with Earth-based transmitters, allowing viewers to receive digital television without a special antenna. DVB-T2 offers HDTV and interactive services, providing more functionality.

Digital radio

DAB (Digital Audio Broadcasting) is used in Europe and the Asia Pacific region. It is broadcast in the same way as DVB. DAB provides more radio stations and can also carry text data that DAB receivers can display. The text data can include the time, name of the station and details of the music being played.

Wired communication

Devices utilize cables for communication, with various types like USB and **Ethernet** used for various purposes, as illustrated in Table 4.3.

USB and Ethernet are common connection types, with revisions enhancing data transfer speeds. USB adapts to complex digital devices, while Ethernet improves data transfer speed and quality, allowing cables to be 100 meters long.

▼ **Table 4.3** Common wired connection types and their uses

CONNECTION TYPE	USE
HDMI	Digital video connections
S/PDIF	Digital audio connections
Minijack	Personal headphones
USB	Storage transfer
Ethernet	Networking

SUBJECT VOCABULARY

Ethernet a network connectivity standard that provides a way for computers to communicate

Wireless communication

Devices can also use wireless connectivity to communicate with each other. Just as with wired communication, there are many different types of wireless connection.

Wi - fi

Wi-Fi is a wireless technology used in home and office networks, with some companies offering access in towns and cities. It uses the IEEE 802.11 specification, which is regularly revised to improve data transfer speed and device connection distance. The first version was IEEE 802.11a.

Bluetooth

BLUETOOTH Bluetooth is a type of wireless connectivity that lets devices connect over short distances. It cannot carry as much data as Wi-Fi. Bluetooth devices need to be **paired** with each other before they can communicate.

▼ **Table 4.4** Comparing Wi-Fi and Bluetooth

	WI-FI	BLUETOOTH
Range	Long ✓	Short ✗
Bandwidth	High ✓	Low ✗
Power	High ✗	Low ✓
Security	High ✓	Low ✗
Can connect multiple devices simultaneously	Yes ✓	Limited ✗ (usually have to be paired)

SUBJECT VOCABULARY

pair connect two devices (usually only with each other)

3G and 4G

3G and 4G are mobile broadband technologies that offer internet access to mobile devices when Wi-Fi is unavailable.
4G is the fourth generation, and future generations aim to enhance signal speed and availability.

INFRA-RED (IR)

Infra-red signals cannot carry much data and only have a short range. Transmitters must have a clear line of sight to receivers, because this allows the signal to travel in a straight line between them without being blocked by solid objects like walls. The signal is also affected by sunlight. It is often used in remote-control devices such as television remote controls.

NEAR-FIELD COMMUNICATION (NFC)

NFC uses close proximity RFID (Radio Frequency Identification) chips. NFC is used in smartphones, payment cards and travel cards.

BENEFITS AND DRAWBACKS OF WIRED vs WIRELESS

The World Health Organization (WHO) says that current research findings suggest that exposure to wireless signals does not cause health issues.

BROADBAND, MOBILE BROADBAND AND CELLULAR NETWORKS

Broadband networks provide fast access to the internet through a connection to an **Internet Service Provider** (**ISP**). They use the **fibre optic cable** or **copper cable network**. You will learn more about fibre optic cables. Mobile broadband provides high-speed wireless connectivity using 3G or 4G technology to connect to the mobile phone network, which acts as the user's ISP.

▼ **Table 4.6** Comparing wired and wireless connectivity

	WIRED	WIRELESS
COST	Cables are cheap if purchasing for a small number of devices	• No need to buy cables • May need a wireless access point for multiple connections
SAFETY	Risk of tripping over cables	None (though some people are worried about the effects of radiation)
SPEED	Faster than wireless	Slower than wired
STABILITY	Less affected by interference than wireless	Affected by interference and obstacles
PORTABILITY	• Not portable as limited by connecting cables • May need signal booster if connection is more than 100 metres long	Portable within signal range
MESS	Can look untidy if lots of cables are used	Tidy
SECURITY	Most secure	Less secure than wired connection because it is easier to intercept a wireless signal
MAINTENANCE	Using cables and ports continuously over a long period of time may damage them	None

SUBJECT VOCABULARY

Internet Service Provider (ISP) a company that provides customers with access to the internet

fibre optic cable a cable that sends data using light signals

copper cable a cable that sends data using electrical signals, which are conducted through copper wires

SUBJECT VOCABULARY

infra-red a type of electromagnetic radiation with a longer frequency than that of visible light

Chapter 05

Networks

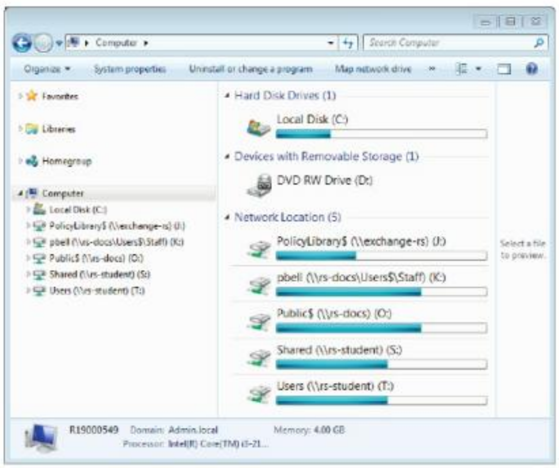
REQUIREMENTS FOR CONNECTING TO NETWORKS

In order to connect to a network, computers need to fulfil certain requirements so that they all operate using standard **protocols**.

Networking operating systems

A network operating system allows a computer to communicate on a network. It provides additional functionality to a stand-alone operating system,
including:

- Passing usernames and passwords to a server for checking when a user logs in
- Separating user accounts and ensuring that users cannot access each other's files
- Providing access to network storage and shared resources such as networked printers.



▲ **Figure 5.1** Network operating systems provide access to shared storage that is available on the network

SUBJECT VOCABULARY

protocols rules that allow the exchange and transmission of data between devices

SUBJECT VOCABULARY

hexadecimal a base-16 number system that uses the numbers 0–9 and the letters A–F

network administrator a person who manages an organisation's network

SUBJECT VOCABULARY

IP address a unique address that networked devices use to send data to each other

How are devices identified on a network?

There are three methods used to identify devices on a network:

■ Internet Protocol (IP)
■ MAC address
■ device name.

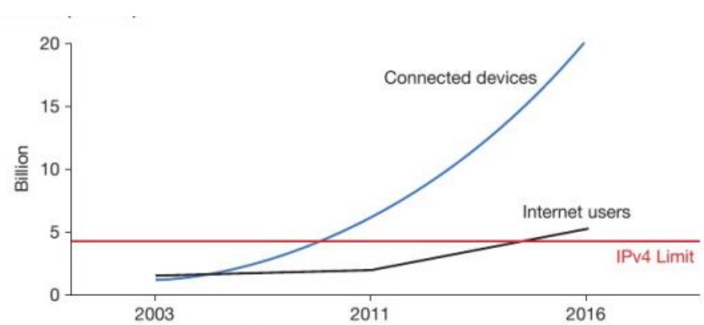
INTERNET PROTOCOL (IP)

An IP address is a unique address that networked devices use to send data to each other. Each piece of data that is sent across a network carries the IP address of the destination, so that each device in the network knows where to send it.

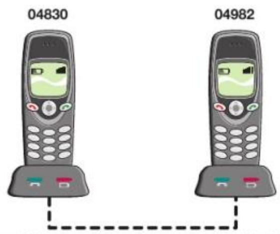
IP addresses are made up groups of numbers. There are two main versions of IP in use.

■ IPv4 uses four groups of up to three numbers separated by full stops
■ IPv6 uses eight groups of four **hexadecimal** numbers separated by colons

IP addresses can either be assigned by a **network administrator** or allocated dynamically by a server running Dynamic Host Configuration Protocol (DHCP).

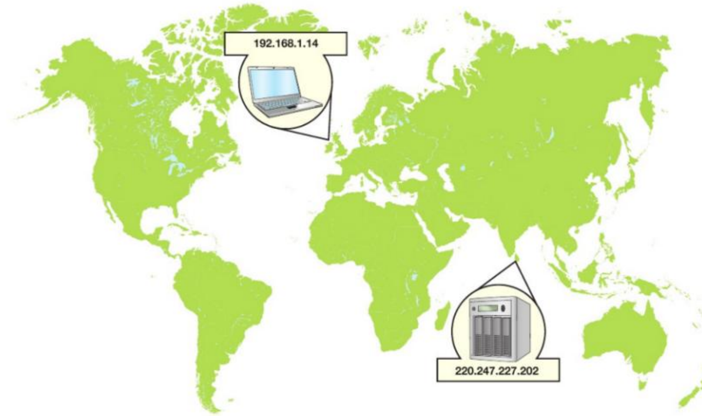


▲ **Figure 5.2** IPv4 can hold 4,294,967,296 possible addresses



▲ Figure 5.3 When you make a telephone call, you dial a number that identifies the destination telephone

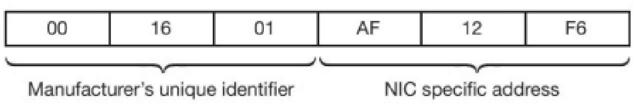
▲ Figure 5.4 When you post a letter, you write the address on the letter so that every part of the postal system knows where to send it



▲ Figure 5.5 When sending data, devices include the destination address of the data, just like in the telephone or postal system

MAC address

MAC addresses are universally unique **identifiers** assigned to the network interface card (NIC) by the manufacturer. They are used in devices connected to local area networks (LANS) using Ethernet, Bluetooth, or Wi-Fi. The first three pairs identify the manufacturer, while the remaining pairs uniquely identify the device. MAC addresses are generally considered fixed addresses.



▲ Figure 5.6 A MAC address

▼ Table 5.1 Uses of MAC addresses

USE	EXAMPLE
Restricting or allowing access to a network	MAC address filtering checks the MAC address of devices attempting to gain access to a network and only grants access to devices with specified MAC addresses
Identifying a device on a network	Some Wi-Fi hotspots only provide free access for a certain length of time, and they identify a device using its MAC address in order to work out whether it is trying to access the hotspot for longer than the permitted time
Tracking a device	Some companies and organisations track devices (and therefore their users) by checking which wireless access points have been accessed by specific MAC address
Assigning 'static' or 'fixed' IP addresses	Each time a device connects to a network, it is identified by a DHCP server (usually using its MAC) and given the same IP address as before

SUBJECT VOCABULARY

identifier a group of letters, numbers, or symbols that a computer has been programmed to recognise and uses to process information

SUBJECT VOCABULARY

hotspot a place in a public building where there is a computer system with an access point, which allows people in the building with a wireless computer or Bluetooth mobile phone to connect to a service such as the internet

SUBJECT VOCABULARY

Mbit/s the amount of data that can be transferred per second, measured in Megabits (1 Mb = 1 million bits)
Gbit/s the amount of data that can be transferred per second, measured in Gigabits (1 Gb = 1,000,000,000 bits)

DEVICE NAME

A device name is a descriptive name that helps users to identify computers on a network. Device names are not used by computers to communicate with each other as they are not always unique.

COMPONENTS OF WIRED AND WIRELESS SYSTEMS

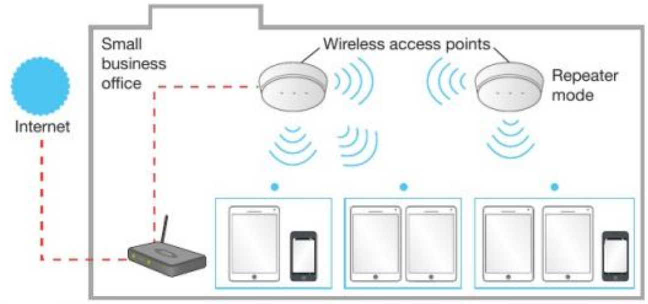
Wired and wireless systems can be made up of a variety of components.

Cables

Cables are used to connect devices in a wired network. In homes and small businesses, Cat5e cables are used for Ethernet connections. These cables are able to transfer data at 10 **Mbit**/s, 100 Mbit/s or 1 **Gbit**/s.

Wireless access point

A wireless access point connects Wi-Fi-enabled devices to a wired network, often integrated into routers or available as standalone devices that use Ethernet cables for connection.



▲ **Figure 5.9** Wireless access points can be used in a small business to provide Wi-Fi access to wireless devices in a network

Switch

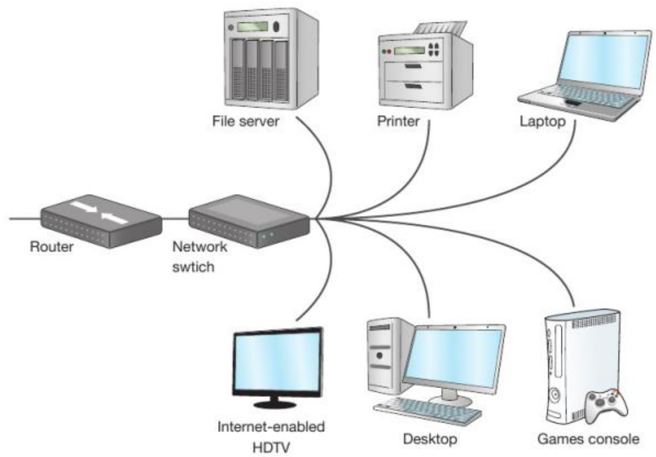
A switch connects devices on a network using **ports** connected via cables. It ensures data sent from any device reaches the correct device on the network, such as a printer, by sending the printer's IP address to the switch.

Gateway

A gateway connects two different types of network. For example, a LAN is connected to a WAN using a gateway.

Router

A router stores device addresses for forwarding network traffic, often used in homes as switches and wireless access points. They act as gateways connecting LANs to the internet.



▲ **Figure 5.10** A switch allows multiple devices to send data to each other

▲ **Figure 5.12** This router has a four-port switch; the last (grey) port on the right is used to connect the router to a WAN (in this case, the internet)

SUBJECT VOCABULARY

port a socket into which cables and devices can be plugged

▲ **Figure 5.11** A switch

Booster

A booster is used to amplify the signal in a network so that its range can be extended. For homes and offices, wired Ethernet connections often have a maximum range of 100 m. Wireless signals have limited range, too. Boosters can be used for both wired and wireless connections.

Wireless access points can be set to repeater mode in order to act as boosters for Wi-Fi signals, as shown in Figure 5.9.

Sever

A server is a computer that shares its resources with connected devices. Computers connected to a server are known as clients. Resources that can be shared by one or more servers include printers, storage and applications.

AUTHENTICATION SERVER

An authentication server checks usernames and passwords. When a user successfully logs in, the client receives an electronic certificate that it can then use to access various resources, including applications and storage.

PRINT SERVER

A print server manages multiple printers at a time, dealing with print requests from client computers and adding jobs to a queue so that individual printers are not overloaded with requests. Print servers can also monitor and process print requests, making sure that users or departments can be invoiced for the jobs that they send to the printers.

FILE SERVER

File servers allow users to access shared and private storage.

APPLICATION SERVER

Application servers provide clients with access to applications that can be run directly from the server.

WEB SERVER

Web servers process requests for data made via **Hypertext Transfer Protocol (HTTP)**. Together, all of the content stored on all web servers is known as the World Wide Web. Client computers often access web servers from outside the LAN to which the server is connected.

CONNECTING TO AND USING THE INTERNET

In order to access the online services provided by servers and data centres, users must have a connection to the internet.

Internet service provider (ISP)

Users also need software that allows them to use and work with the services effectively and safely.

To connect to the internet, users need to subscribe to an ISP. ISPs provide connections to the **telecommunications infrastructure** that forms the framework for the internet.

SUBJECT VOCABULARY

telecommunications infrastructure the networks of hardware facilities, owned by private and public organisations, that are used to transfer data

Web browser

A web browser is a type of software application used to request and display information stored on web servers. Examples of web browsers are Mozilla Firefox, Google Chrome, Internet Explorer® or Microsoft Edge, Opera[8], and Safari®[9].

▶ **Figure 5.14** Web browsers have versions available for mobile devices

Service
energy

A search engine provides users with a way to find information in web pages stored on web servers. Users enter keywords that describe the information they want to find. The search engine then compares the keywords with those in its database of web pages and returns the results that are the closest match to the given keywords.

▲ Figure 5.15 A search engine

Filter software

Filter software prevents users from accessing inappropriate information. When a user tries to access a web page, the address (URL) and/or the contents of the web page are compared against two lists of **URLs** and keywords stored in the filter software's database. The two lists are the **blacklist** and the **whitelist**.

- If the results match anything in the blacklist, the user will be prevented from viewing the web page.
- If the result matches anything in the whitelist, then the user will be allowed to view the web page.
- If the result does not match anything in either the blacklist or the whitelist, the user will be allowed to view the information.

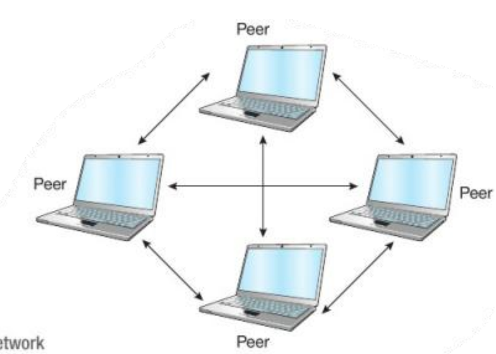
LOCAL AREA NETWORKS (LANS)

A LAN is a network contained to a small area, such as a home or office network (see page 69 for more information about LANs). Computers in a network can be connected using one of two different models:

- peer-to-peer
- client-server.

peer- to-peer networks

Computers in a peer- to-peer network share their resources with other computers in the network, but they do not access servers. Figure 5.16 is an example of a peer-to-peer network.



▶ Figure 5.16 A peer-to-peer network

client-server networks

Some networks use servers. A network that uses servers and clients is called a client-server network. Figure 5.17 is an example of a client- server network.

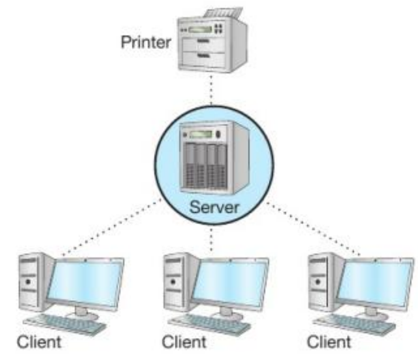


Figure 5.17 A client-server network

Benefits of using LANs

Connecting computers using a LAN provides a range of benefits. These include:
- ■ Access to shared peripherals
- ■ Access to shared storage and data
- ■ Flexible access (that is, being able to access peripherals, storage and data from any connected device)
- ■ Media streaming (including movies, music and gaming)
- ■ Communication (that is, being able to send messages and files to others on the network)
- ■ Shared access to the internet.

BENEFITS OF USING CLIENT-SERVER NETWORKS

There are several benefits of using client-server networks that are not available when using a peer-to-peer network.

■Control of user access rights: Users, or groups of users, can be given access to some resources (such as storage or printers) and restricted from accessing others.

■Centralised administration: Resources and user accounts can be managed by an individual, or individual group of servers and administrators.

■Centralised backup: User data is protected from loss because backups can be automated for all users. This makes it more likely that backups will happen than if individual users were asked to complete backups themselves.

■Shared software: Application servers can provide access to shared software. Some servers can provide access to operating systems.

■Shared storage and file access: The amount of storage available to users can be managed centrally. Sharing storage means that users can make files available to others.

■Roaming profiles: This is the ability to log into any computer in an office and see your settings and files. This allows users to access data, applications, mail and printers from any client, enabling them to work from anywhere where there is a client.

SECURING DATA ON NETWORKS

Security prevents unauthorised users from accessing network resources and data.

Loging and passwords

Users log in to computers on a network to access centrally managed resources. Without the correct **login** details, users cannot access the network or its resources.

Passwords are used to **authenticate** a user to the network. An authentication server can be used to manage the authentication of a user to a range of network resource and services.

SUBJECT VOCABULARY

login user or account information, such as a user name or account name
authenticate confirm that the user is who they say they are

Fire walls

A firewall is used at the gateway to a network. It controls the network traffic to and from a network, particularly the traffic from the internet. Firewalls prevent unauthorised users from accessing network devices and resources, such as storage.

SUBJECT VOCABULARY
cipher a code

Encryption

Encryption is the process of encoding, scrambling or jumbling data so that unauthorised users are prevented from being able to understand it.

One method used to encrypt text is called a Caesar **cipher**. This method shifts each letter to the left by a set number of places. The number of places by which the letters have been shifted is known as the key.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V

▲ Figure 5.18 Once you know the key, it is easy to decrypt the message

A Caesar cipher is quite easy to crack, but most modern encryption is much more secure. There are two types of encryptions:

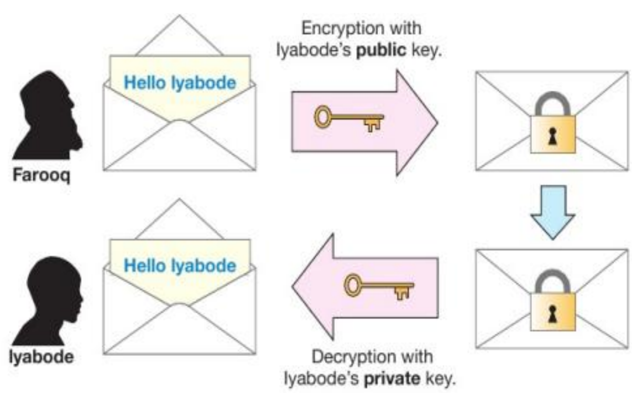
- Symmetric key encryption
- Public key encryption.

SYMMETRIC KEY ENCRYPTION

Symmetric key encryption uses the same key at both ends of the process, meaning that the same key is used to encrypt and decrypt the data.

PUBLIC KEY ENCRYPTION

Public key encryption uses two mathematically related keys, a public key and a private key, to encrypt and decrypt data. A computer shares a public key with others, while a private key is not shared. An example is shown in Figure 5.19.



▲ Figure 5.19 Farooq first sends Iyabode a request to send a secure message, then Iyabode shares her public key with Farooq

WIRELESS ENCRYPTION PROTOCOL (WEP)

Wireless Encryption Protocol (WEP) is used to secure the wireless transfer of data. It is the least secure wireless data encryption method. This is because every device on the wireless network uses the same key for every transfer. This means that if an **eavesdropper** studies enough **packets**, they can identify the key, and this provides them with unlimited access to all data from every device on the wireless network.

WI-FI PROTECTED ACCESS (WPA)

Wi-Fi Protected Access (WPA) is a security protocol designed to provide better encryption than WEP, WPA generates a new key for each device on the wireless network. New keys are also provided for each packet of data that is sent.

Virtual private network (vpn)

Data sent using a VPN is encrypted so that it is secure if it is intercepted. An individual might use a VPN to:

- ■ Access their employer's network when working from home
- ■ Access computers in a different geographical location, perhaps to avoid the local restrictions on access to web content (such as due to censorship or **geolocation rights management**)
- ■ Make secure payments
- ■Prevent surveillance of and access to their web activity.

SUBJECT VOCABULARY

geolocation rights management the use of a user's location to block access to services online; for example, a television channel might only allow users in their own country to watch their shows online

File access rights

File access rights are also known as file permissions. They can be set for individual files, folders or drives, and they ensure that users are either allowed to read only or allowed to read and write to the file, folder or drive.

Transaction logs

All network activity can be recorded in a **log** file. Although this does not directly secure network data, a **transaction** log can help to identify which computers and network devices have been accessed. This can allow administrators to identify any unusual activity that might be a threat to data security.

backups

A backup is a copy of one or more files. The backup or backups are usually stored on a different storage device to the original file.

Revision questions

(1)2023 November

Which **one** of these is a role of a server?

☐ **A** Handle requests from clients

☐ **B** Provide a wireless connection

☐ **C** Provide access to a WAN from a LAN

☐ **D** Store the client's operating system

2023 November 2).

(i) Gail uses different types of networks in her job.

(i) Draw **one** straight line from **each** type of network to the correct reason for its use.

Type of network	Reason for use
PAN	To connect Bluetooth headphones to a smartphone
LAN	To set up a home office network
WAN	To use cloud-based services
	To prevent viruses

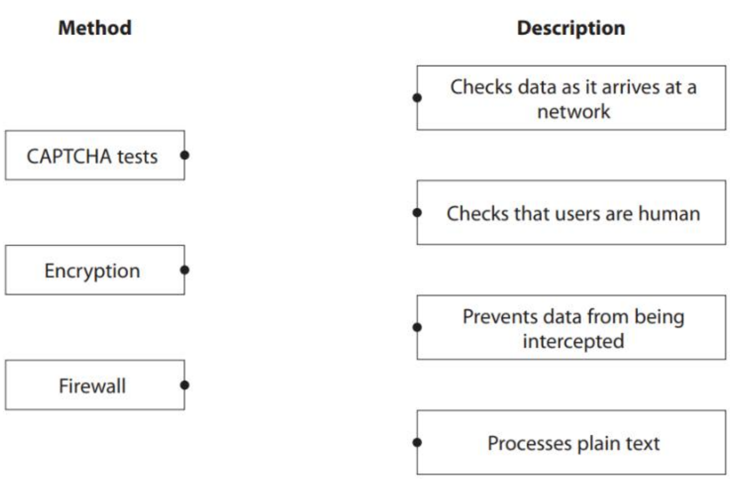
(ii) Define the term 'peer-to-peer!
(iii) Describe the function of Media Access Control.
Describe how a roaming profile allows Gail to hotdesk.

3). 2022 May
Letta uses the Internet for work.
(a) Letta can collaborate with others so expertise can be shared.
Explain one other way that the Internet could positively impact how Letta works.
(b) Letta's employer uses hosted applications and storage.
(i) Explain one benefit to Letta's employer of doing this.
(ii) State the type of computer used to store online software.
(c) Describe how filter software works.
(d) Give two features of a strong password.
2022 May
4).Nihal connects his laptop to the hotel's local area network.
(i) Explain one advantage of using Media Access Control (MAC) addresses rather than Internet Protocol (IP) addresses to identify devices on a local area network.
(ii) State two issues caused by not identifying devices correctly on a network.
(iii) Complete this sentence by adding the correct network devices.

A local area network uses a ……………………………………………. to connect devices
whereas a wide area network uses a ………………………………..to connect local area networks.

(iv) Explain one disadvantage of connecting a printer to a network.

(v) Draw **one** straight line from **each** method of protecting a network to the correct description.



(vi) Which **one** of these is an example of a device that connects using a personal area network?

- ☐ **A** Hard drive
- ☐ **B** Router
- ☐ **C** Server
- ☐ **D** Smartphone

2022 May

5).

Which **one** of these connectivity types is the fastest Letta could use to transfer files from her camcorder to her laptop?

- ☒ **A** 3G
- ☒ **B** GPS
- ☒ **C** NFC
- ☒ **D** USB

2022 May

6).Give one reason why WiFi is a better choice than Bluetooth for transferring files from her camera to her laptop.

7).Letta connects to the hotel's local area network.

(i) One way of identifying a device on a network is the device name.
State two other ways of identifying a device on a network.

(ii) State two reasons for identifying devices on a network.

(iii) State two ways a local area network (LAN) is different from a wide area network (WAN).

(iv) Explain one advantage of connecting a printer to a network.

(v) Draw one straight line from each method of protecting a network to the correct use.

Method	**Use**
Firewall	Blocks ports in a network
Encryption	Authenticates users
Biometric	Prevents data from being understood if intercepted
	Deletes viruses from infected networks

(vi) Which **one** of these connects to a local area network using a gateway?

- ☒ **A** Personal area network
- ☒ **B** Server
- ☒ **C** Smartphone
- ☒ **D** Wide area network