UNIT 2 CONNECTIVITY

Assessment Objective 1

Demonstrate knowledge and understanding of Information and Communication Technology (ICT)

Assessment Objective 2

Apply knowledge, understanding and skills to produce ICT based solutions

Assessment Objective 3

Analyse, evaluate, make reasoned judgments and present conclusions

In this unit, you will learn about the ways in which digital devices exchange data and communicate with each other and with larger systems supporting online organisations. Understanding which technology to use in a particular context, and knowing how to do so securely, are increasingly important because of people's growing need to connect from everywhere.

4 DIGITAL COMMUNICATION

Our world is connected by wired and wireless digital communication systems. Data flows around these systems, carrying information about our personal and work lives and providing us with entertainment and news. Digital devices exchange data and communicate with each other and with larger systems.

Understanding the way in which devices communicate will help you to understand why things do not work as expected and will enable you to stay connected to the streams of data that drive our world.

By the end of this chapter, you should be able to select the most appropriate digital communication for a particular situation, after considering how each option would affect the quality of a connection.

LEARNING OBJECTIVES

- Know the range of ways that digital devices communicate: satellite, broadcast (TV, radio), wired (cable), wireless
- Know that digital devices can communicate device to device and by using networks: local area network (LAN), wide area network (WAN), personal area network (PAN), tethering
- Know the types of wireless communication: Wi-Fi, Bluetooth, GPS, 3G, 4G, infra-red (IR), near-field communication (NFC)
- Know the differences between Wi-Fi and Bluetooth and when each is best used
- Understand factors influencing the speed and volume of data transfer
- Understand the benefits and drawbacks of wired versus wireless communication in local networks
- Understand the significance of bandwidth and latency, and their impact on the 'user experience'
- Understand the features of broadband, mobile broadband and cellular networks

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. If we do not, transferring more data will mean that transfer times will increase.

BANDWIDTH

SUBJECT VOCABULARY

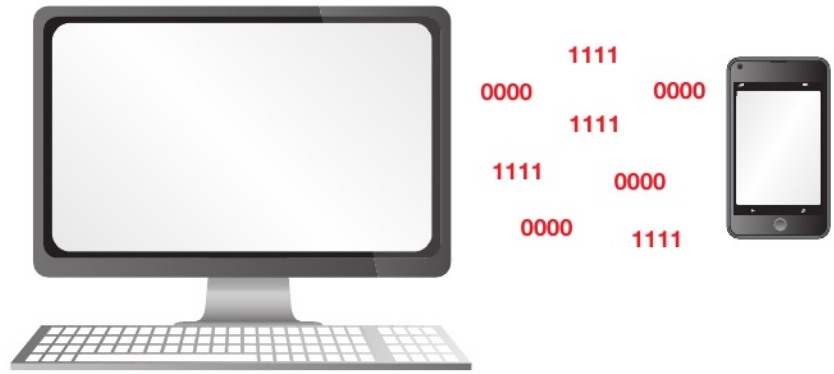
bandwidth the number of bits that can be carried by a connection in one second

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

You can think about a data connection as being like a water pipe. In the same way that a large water pipe can carry a large amount of water, a connection with a large bandwidth can carry a large amount of data.

IMPACT ON USER EXPERIENCE

A higher bandwidth means that more data can be transferred every second. This makes uploads and downloads faster. It also makes it possible to do things that require lots of data to be transferred in short amounts of time, such as multiplayer online gaming or 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

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**. The video will not start until there is enough data in the buffer to play a few seconds of video. While those few seconds are playing, more data is downloaded to fill up the buffer. If the buffer is empty, there is no more video to play and it will pause until more data is downloaded. To avoid the buffer becoming empty, data must be constantly downloaded into the buffer, filling it up at a rate faster than it is emptied.

Imagine a glass of water being repeatedly filled up from a big bottle. The bottle is like the full video data file and the glass is like the buffer that holds the data ready to be used.

▲ **Figure 4.2** A visual representation of streaming

LATENCY

SUBJECT VOCABULARY

latency the amount of time it takes to send data between devices
domain the name used to identify a web server

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. If you think again about a data connection acting like a water pipe, latency is the average time that it takes for a drop of water to flow through the pipe.

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. The 'ping time' is the amount of time it takes for the packet of data to make the return trip.

SKILLS INTELLECTUAL INTEREST AND CURIOSITY
EXECUTIVE FUNCTION
REASONING
PROBLEM SOLVING

ACTIVITY

▼ PINGING DOMAINS

Using a command line interface (Terminal in MacOS and Linux or Command Prompt in Windows), type 'ping [domain]' to ping the following domains:

- gov.au (by typing 'ping gov.au')
- newsfirst.lk
- gov.uk

Note the ping time for each domain. Why are they different?

SKILLS INTELLECTUAL INTEREST AND CURIOSITY

ACTIVITY

▼ SPEED TESTING

Carry out a speed test on the internet connections of a fixed line broadband device, such as a laptop or PC, and a mobile broadband device, such as a smartphone.

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. When watching live television, high latency will result in a delay between the real-time events and the video being received for playback.

GENERAL VOCABULARY

lag move slowly or fail to keep up

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 have to work on a limited number of **frequencies**. In comparison, copper cable can carry more frequencies than wireless methods. This means that cabled methods can have more bandwidth available to them than wireless methods.

SUBJECT VOCABULARY

frequency the waveband at which a radio signal is transmitted

HINT

Some older wired methods have less bandwidth than newer wireless methods.

INTERFERENCE

Other electromagnetic signals disrupt or interfere with wired and wireless signals. For example, interference can be caused by signals from wireless devices, wireless routers and appliances emitting electromagnetic fields like fridges and microwave ovens. Cabled connections can be **shielded** from this interference by having the wires wrapped in a thin layer of metal.

GENERAL VOCABULARY

shielded protected

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

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

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

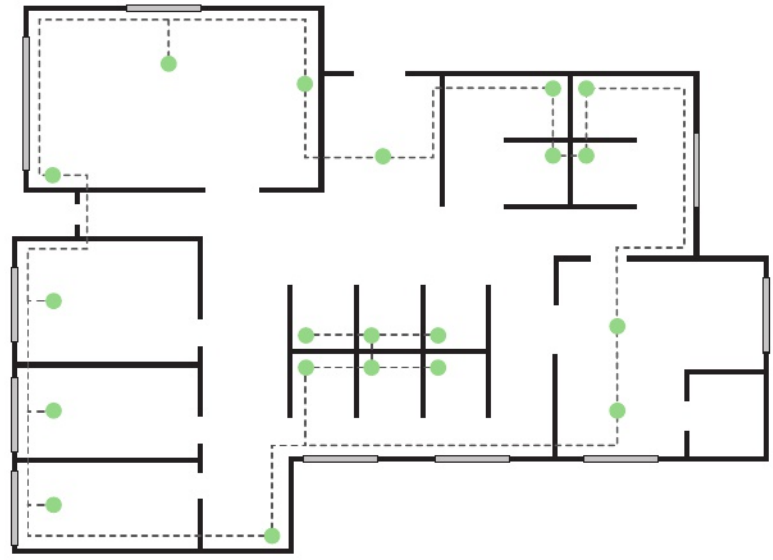
DEVICE 1	DEVICE 2	CONNECTION BETWEEN DEVICES 1 AND 2	USE
Temperature sensor	Air conditioner	Wired	To turn on the air conditioning when the temperature is too high
Smartphone	Headphones	**Minijack**	To play music from the smartphone on the headphones
Laptop	External hard drive	USB	To transfer files
Camcorder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

NETWORK COMMUNICATION

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

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 WAN is a network that is spread over a large geographical area. WANs are often used to connect different buildings owned by national and international businesses, law enforcement agencies, health and education organisations and government departments. Some organisations launch their own satellites to provide connectivity for their own global WANs.

WANs often use connectivity provided by a third-party telecommunications company, often linking LANs together through the internet. Because of their wider reach, WANs often have slower transfer speeds than LANs.

DID YOU KNOW?
The internet is the largest example of a WAN.

▲ **Figure 4.5** The internet is the largest example of a WAN

PERSONAL AREA NETWORK (PAN)

A PAN is a group of connected devices that are all near an individual user. For example, a user could connect their smartwatch to their smartphone, which is connected to their laptop and home cinema speaker system. Devices in a PAN can either be connected to each other directly or connected through access points (see page 84 for more information about access points).

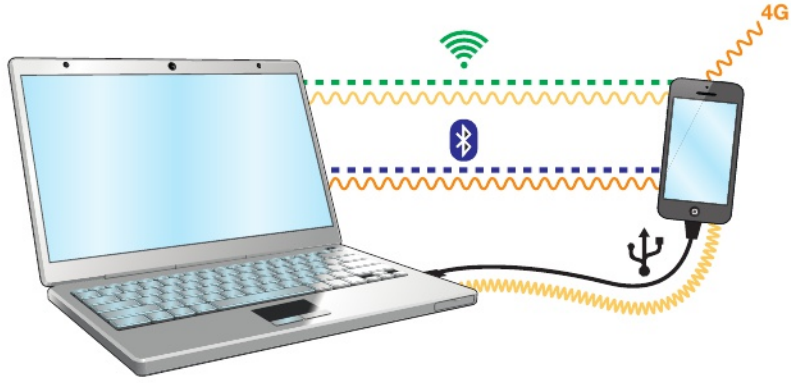
When a PAN only uses wireless connectivity, it can also be referred to as a WPAN (**W**ireless **P**ersonal **A**rea **N**etwork). However, the general term PAN is more commonly used to refer to all types of PAN.

TETHERING

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

Tethering is the process of connecting a host device, such as a smartphone or a tablet device, that uses a mobile broadband connection with one or more other devices. This enables the other device or devices to share the host device's broadband connection.



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

SUBJECT VOCABULARY

service agreement contract

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.

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

▲ **Figure 4.7** A communication satellite

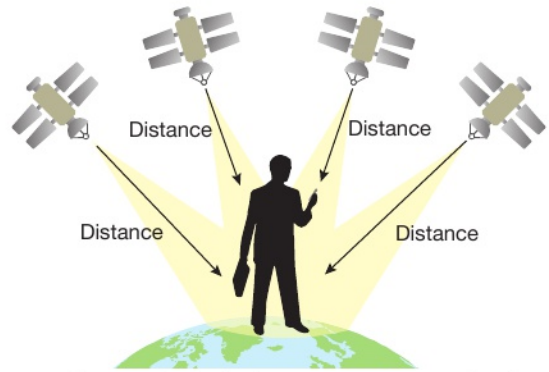
Satellites transmit data to and receive data from digital devices. Digital devices use antennae to receive the radio signals that satellites transmit.

The benefit of satellite communication is that the number of satellites means that the system is always available. It also cannot be affected by power shortages.The drawback is that satellite signals do not pass through solid objects. This means that they will not work in areas with tall buildings or in tunnels. Signals can also be affected by atmospheric weather conditions such as heavy snow or rain.

GPS

Satellite communications are used for GPS. Navigation aids make use of GPS signals to calculate the exact location of a device. GPS signals are sent from a network of 24 satellites orbiting the Earth. At any one time, a device will be within view of approximately 12 of these satellites. However, a view of only four satellites is required to calculate an accurate location, as illustrated in Figure 4.8.

For more information about navigation aids, see *Unit 1 Digital devices* (page 14)

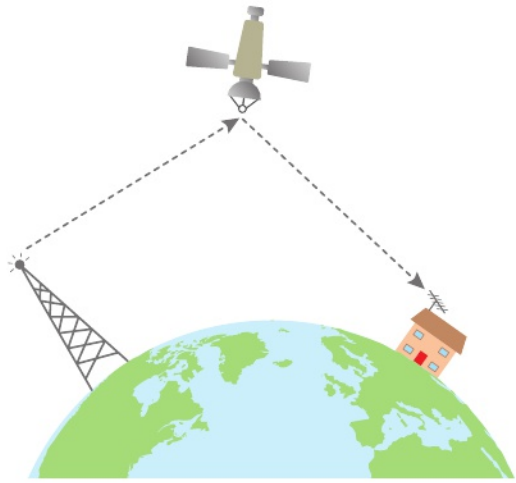


▲ **Figure 4.8** Only four satellites need to be in view to get an accurate location of a device using a GPS signal

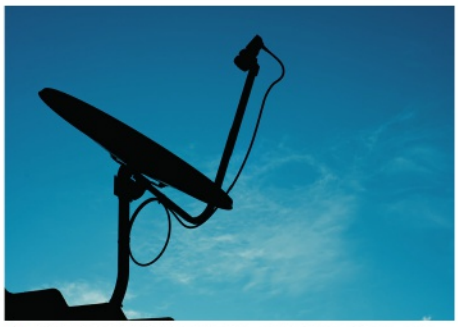
TELEVISION

Digital Video Broadcasting (DVB) is the internationally accepted standard method of broadcasting digital television. DVB-S (Digital Video Broadcasting – Satellite) is one example of DVB. A video signal from the broadcaster is transmitted using a large antenna on Earth to one or more satellites, which

then broadcast the signal back down to Earth. A satellite television viewer will have an antenna installed, and this receives the signal and sends it to a set-top box. The set-top box decodes the signal and converts it so that it is ready to be sent to a television. Some televisions have decoders installed, so the antenna can be connected directly to the television rather than requiring a set-top box to decode the signal first.



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



▲ **Figure 4.10** A receiving antenna with a set-top box

DVB-S2 and DVB-S2X are newer digital broadcasting standards. They provide more functionality, such as High Definition Television (HDTV), interactive services and internet access.

TELEPHONE

Satellite communication is also used to allow people in remote areas to place voice calls using satellite telephones.

▲ **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

MILITARY

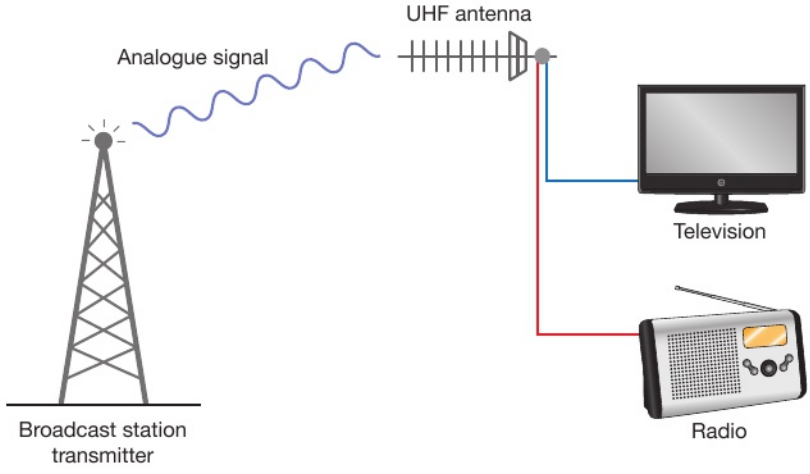
The military in many countries use satellites for communication systems, such as the Global Command and Control System.

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

DID YOU KNOW?

In some countries, analogue signals have been switched off and only digital signals are now broadcast. In January 2017, Norway became the first country to begin switching off the transmissions from its national FM radio stations.

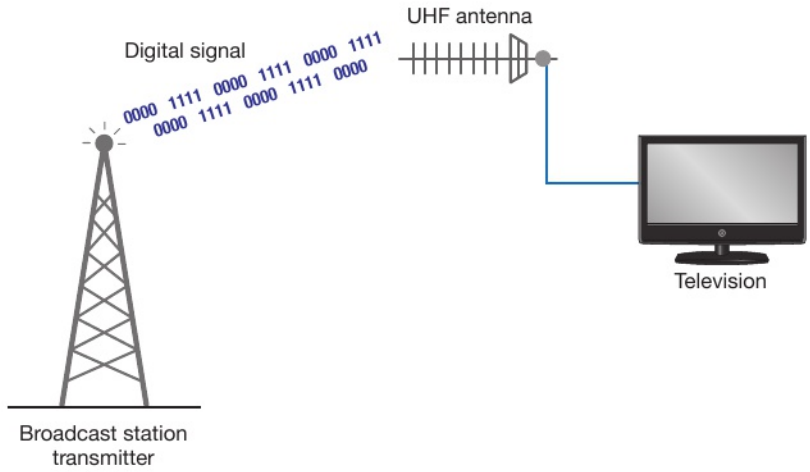
DIGITAL TELEVISION

GENERAL VOCABULARY

terrestrial on the Earth

DVB-T (Digital Video Broadcasting – **Terrestrial**) is a method of DVB where the transmitters are based on Earth, rather than in orbit as they are in DVB-S. To receive digital television broadcasts transmitted by DVB-T, viewers can use the same antenna that they use to receive analogue broadcasts. They do not need a special antenna.

DVB-T2 is a newer standard that provides more functionality, such as High Definition Television (HDTV) and interactive services.



▲ **Figure 4.15** Some televisions have decoders installed, so the antenna can be connected directly to the television rather than requiring a set-top box to decode the signal first

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

SUBJECT VOCABULARY

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

Devices can use cables to communicate with each other via a wired connection. There are many different types of wired connection. Some are used for many different purposes, such as USB. Others are only used to meet one particular need, such as **Ethernet**.

Some of the uses for different wired connection types are given in Table 4.3.

▼ **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

▲ **Figure 4.16** An Ethernet connection

USB is a very common connection type. USB has been through a number of revisions, and each revision allows faster data transfer speeds. This development of standards is common with all types of connectivity. This progress is made necessary as digital devices become more complex in their features and functionality.

Ethernet allows a user to connect to wired networks. As Ethernet technology develops, the speed at which data can be transferred between devices is improved. Ethernet cables can be 100 metres long before the signals they carry start to lose quality.

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.

HINT

The terms 'Wi-Fi' and 'internet access' are often used incorrectly to mean the same thing. Wi-Fi allows you to wirelessly connect to a network. That network may or may not be connected to the internet. For more information about networks, see pages 79–93.

DID YOU KNOW?

A laser transmitter in New Mexico, USA is used to beam a wireless signal 384,400 km to a satellite orbiting the moon. It can carry 19.44 megabits of data per second, which is more than enough to stream live television.

WI-FI

Wi-Fi is used in home and office networks. Some companies provide Wi-Fi access in towns and cities. Wi-Fi is a wireless technology used to connect devices to a network. That network can itself then be connected to the internet, so that devices connected to the Wi-Fi network can connect to the internet.

Wi-Fi uses the IEEE 802.11 specification of standards for wireless communication. The specification is revised regularly to take account of improvements in technology. Each revision to the specification is given a different letter or pair of letters at the end. The first version was IEEE 802.11**a**. Each revision of the technology improves the speed at which data can be transferred and increases the distance over which devices can connect.

SKILLS SELF-DIRECTION

ACTIVITY

▼ DIFFERENT REVISIONS OF WI-FI

Do some research to compare the different revisions of Wi-Fi. How do their speeds and range differ?

BLUETOOTH

SUBJECT VOCABULARY

pair connect two devices (usually only with each other)

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.

Bluetooth can be used to transfer small files between devices. It is used to connect devices such as smartphones and laptops to peripherals such as portable speakers, headphones, earphones, keyboards and mice.

▼ 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)

DID YOU KNOW?

Wi-Fi Direct is an alternative to Bluetooth. It is a low-power version of Wi-Fi that can connect two devices directly over a short range.

3G AND 4G

3G and 4G are sometimes referred to as mobile broadband. They are used to provide internet access to mobile devices such as smartphones and tablet devices when a Wi-Fi signal is not available. The G stands for 'generation', meaning that 4G is the fourth generation of mobile broadband technology. Future generations of the technology are planned to improve the speed and availability of the signal.

SKILLS SELF-DIRECTION
INTELLECTUAL INTEREST AND CURIOSITY

ACTIVITY

▼ 3G AND 4G

1 Compare the speeds, costs and availability of 3G and 4G in your location.

2 Research the next generation of this technology.

HINT

3G or 4G is **not** the same as Wi-Fi. 3G and 4G connectivity is provided by mobile phone companies. Some people say they 'have Wi-Fi' when they mean that they have a mobile broadband connection.

INFRA-RED (IR)

SUBJECT VOCABULARY

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

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.

For more information about NFC and RFID chips, see *Unit 1 Digital devices* (page 30).

SKILLS SELF-DIRECTION

ACTIVITY

▼ COMPARING WIRELESS CONNECTIONS

Complete Table 4.5 by identifying the technology used by each type of wireless connection and some common uses for that type of connection.

▼ **Table 4.5** Wireless connections: technology and uses

METHOD	TECHNOLOGY	USE
Wi-Fi	Radio waves	Home and office networks
Bluetooth		
3G and 4G		
Infra-red		
NFC		

▲ **Figure 4.17** Infra-red is commonly used by remote controls to transmit signals

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. However, it also says that further long-term research about the effects on children using mobile phones for more than 10 years is necessary. This is because symptoms may take a long time to appear and young people are most vulnerable to radiation.

DID YOU KNOW?

The wavelength of Wi-Fi (12 cm) is at least 300,000 times longer than the wavelength of light (400–700 nanometres). The WHO generally considers anything above the wavelength of light to be harmless to humans.

▼ **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

KEY POINT

The International Agency for Research on Cancer is part of the WHO. It classifies Wi-Fi as a possible human **carcinogen**. However, many things are possibly carcinogenic. For example, Wi-Fi shares this classification with coffee, carpentry, foam cups and pickled vegetables.

GENERAL VOCABULARY

carcinogen a substance that can cause cancer

HINT

Cellular network is another name for a mobile phone network.

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

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 on page 84.

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.

CHAPTER QUESTIONS

SKILLS REASONING

1 a Explain **one** reason why some games console controllers use Bluetooth rather than infra-red to connect to the console. **(1)**

b State **one** way in which using infra-red in games console controllers could affect the experience of the person playing the game. **(1)**

SKILLS INTERPRETATION

2 Describe how video streaming works. **(3)**

SKILLS REASONING

3 Explain why streaming is more convenient for the user than downloading. **(3)**

SKILLS PROBLEM SOLVING

4 State **three** types of wired connection. **(3)**

SKILLS INTERPRETATION

5 Which **one** of these best describes the internet? **(1)**

A LAN
B WAN
C PAN
D VLAN

SKILLS REASONING

6 Explain why global games companies use games servers in multiple countries to ensure that the experience of users is not negatively affected when playing online games. **(3)**

5 NETWORKS

A network is created when two or more computers are connected together. Using a network, a computer can communicate with others and share resources such as hardware, software and data. It does this by sending data in a packet, which is a unit of data packaged together so that it can travel across a network.

The first network was created in 1960 by a commercial airline when it connected two mainframe computers together in order to speed up its reservation system. In 1962, researchers at the Advanced Research Projects Agency (ARPA) developed a project called the 'Intergalactic Computer Network'. In 1969, computers at four universities in the USA were connected, which created the ARPANET. This is considered to have been the predecessor of the internet.

LEARNING OBJECTIVES

- Know about network operating systems and how devices are identified on a network: device name, internet protocol (IP) and machine address code (MAC)
- Understand the function of components of wired and wireless systems: cable, wireless access point, router, gateway, booster, server
- Know the role of these for connecting to and using the internet:
  - web browser
  - ISP
  - search engine
  - filter software
- Know about peer-to-peer and client-server networks
- Know about the role of servers in a client-server network
- Understand the benefits of using local area network:
  - shared peripherals
  - shared data
  - flexible access
  - media streaming
  - communication
  - shared access to the internet
- Understand the benefits of using a client-server network:
  - control of user access rights
  - centralised administration
  - centralised backup
  - shared software
  - shared storage and file access
  - roaming profiles (hotdesk)
- Know about and understand the use of logins and passwords, firewalls, WEP/WPA, encryption, VPN, file access rights, transaction logs and backups
- Be able to select suitable methods of securing data for a particular context

SUBJECT VOCABULARY

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

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**.

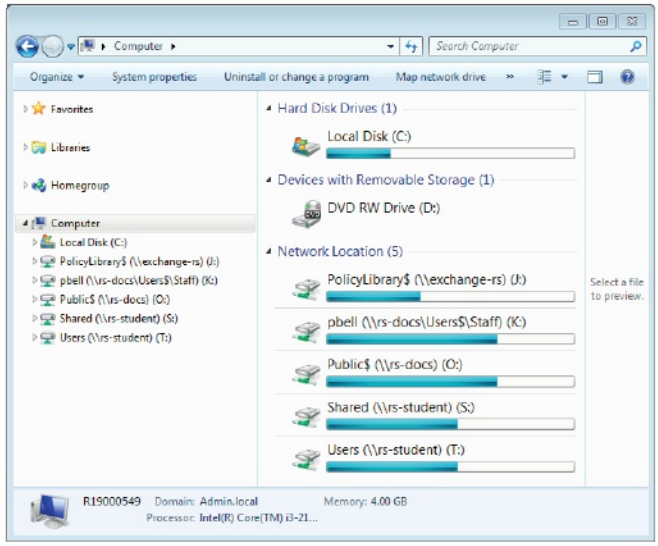
NETWORK OPERATING SYSTEMS

GENERAL VOCABULARY

stand-alone capable of functioning on its own, such as a stand-alone computer working on its own without being part of a network

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

SKILLS CRITICAL THINKING EXECUTIVE FUNCTION

ACTIVITY

▼ COMPARING OPERATING SYSTEMS

Create a table to compare the features of a network operating system to a stand-alone operating system.

HOW DEVICES ARE IDENTIFIED ON A NETWORK

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

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

SUBJECT VOCABULARY

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

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.

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

DID YOU KNOW?

IPv4 can store over 4 billion addresses. It was developed because of the huge growth in the number of devices that were being connected.

GENERAL VOCABULARY

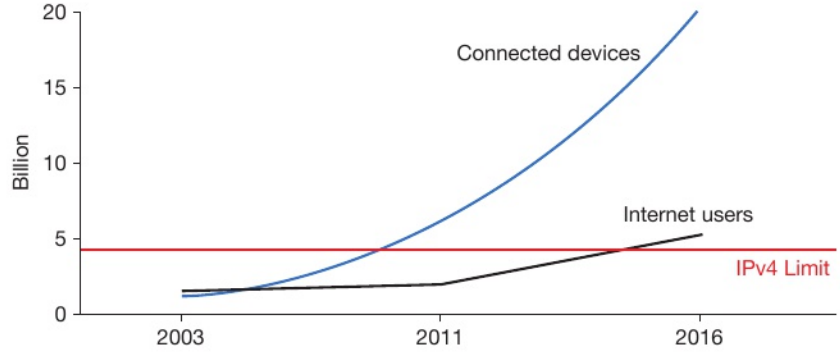
dynamically in a way that is open to change
Dynamic Host Configuration Protocol (DHCP) server a networked computer that automatically assigns an IP address to other computers when they join the network

SKILLS
INTELLECTUAL INTEREST AND CURIOSITY
CRITICAL THINKING
REASONING
COMMUNICATION
INTERPERSONAL SKILLS

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 (for example, 192.168.1.1).
- **IPv6** uses eight groups of four **hexadecimal** numbers separated by colons (for example, 2001:0db8:0000:0042:0000:8a2e:0370:7334).

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

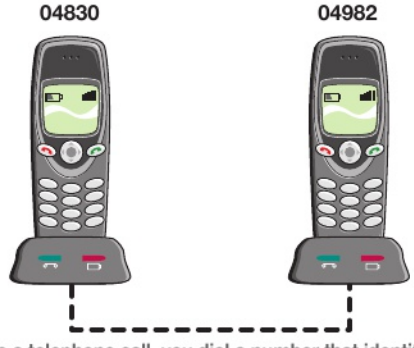


▲ **Figure 5.2** IPv4 can hold 4,294,967,296 possible addresses

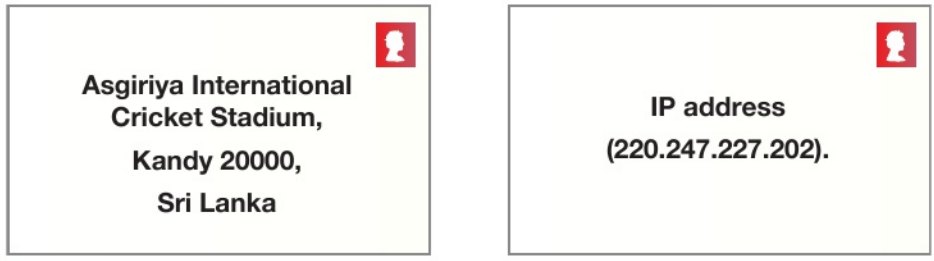
ACTIVITY

▼ IP ADDRESSES

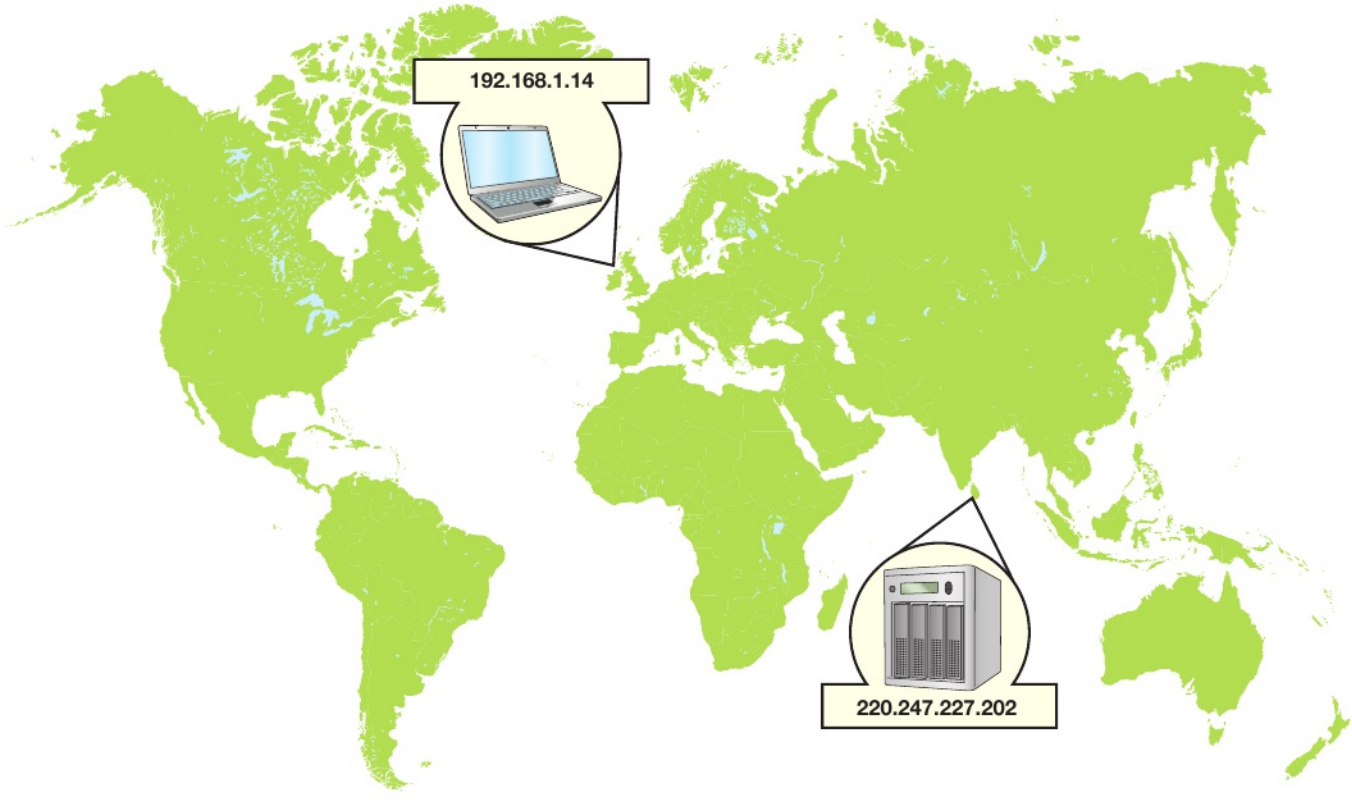
1 Research the maximum number of addresses that can be provided by IPv6.
2 Discuss why the number of connected devices is growing at a faster rate than the number of internet users.



▲ **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

GENERAL VOCABULARY

universally unique the only one of its kind in the world

SUBJECT VOCABULARY

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

MAC ADDRESS

Unlike IP addresses, which can be dynamically allocated by users or servers, media access control (MAC) addresses are **universally unique identifiers** given to the network interface card (NIC). MAC addresses are used in devices connected to local area networks (LANs) using Ethernet, Bluetooth or Wi-Fi.

MAC addresses are assigned by the NIC manufacturer and are generally considered to be fixed addresses.

A MAC address is usually made up of six pairs of characters. The first three pairs identify the manufacturer and the remaining pairs are assigned by the manufacturer to uniquely identify the device. Figure 5.6 is an example of a MAC address.

▲ **Figure 5.6** A MAC address

SKILLS SELF-DIRECTION PROBLEM SOLVING

ACTIVITY

▼ USING MAC ADDRESSES

Using the internet and other resources, find out which manufacturer made the device with the MAC address in Figure 5.6.

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

▼ **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

SKILLS INTELLECTUAL INTEREST AND CURIOSITY, CRITICAL THINKING, REASONING, COMMUNICATION, INTERPERSONAL SKILLS, PERSONAL AND SOCIAL RESPONSIBILITY

ACTIVITY

▼ SPOOFING

MAC addresses can be changed through a process called spoofing, which means using the MAC address of another device. Discuss how spoofing would affect each of the uses listed in Table 5.1.

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. This means that they could cause conflicts if data was sent to more than one device with the same name for processing.

You can change a device name using tools in the device's operating system.

SKILLS ADAPTABILITY

ACTIVITY

▼ IDENTIFYING DEVICES ON YOUR NETWORK

Identify the name, an IP address and the MAC address of a device on a network that you use.

COMPONENTS OF WIRED AND WIRELESS SYSTEMS

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

CABLE

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)

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**. Cat5e cable connects devices through their NICs. The device's NIC allows the computer to exchange data with other networked computers and contains LEDs that signal network activity.

Cat6 cables can be used to transfer data at 10 Gbit/s. These are more expensive than Cat5e cables and are usually only used by businesses.

▲ **Figure 5.7** Cat5e cable is used to connect devices through their NICs

DID YOU KNOW?

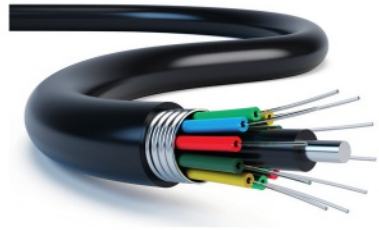
400 Gbit/s Ethernet is expected to be available by late 2017.

DID YOU KNOW?

The speed of a network is limited by its slowest part. For example, if a network uses 10 Gbit/s cables and its internet connection speed is 100Mbit/s, then the internet connection is the slowest part of the network. This means that the 10 Gbit/s cables will not speed up the internet download speeds. The cables will only be transferring data at 1/100 of their maximum.

Fibre optic cables are flexible fibres. Each fibre optic cable contains a glass thread that bounces light signals between two devices faster and further than is possible with wire cables. Fibre optic cables can now carry data at 40 Gbit/s over many kilometres without affecting signal quality.

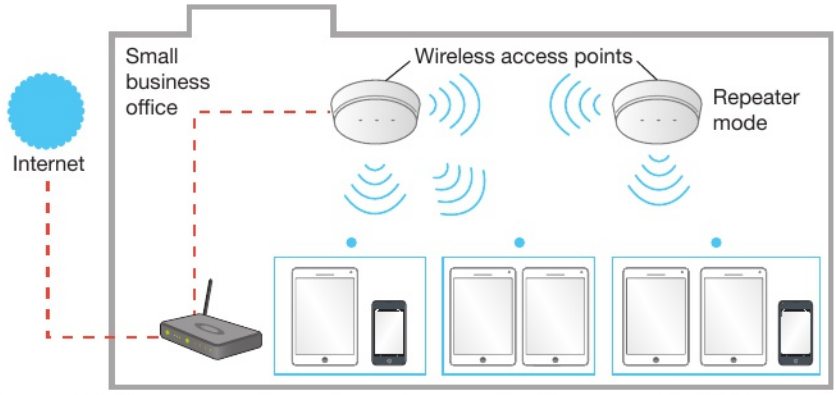
Fibre optic cables are expensive. This means that they are used by telecommunications companies and by organisations that need very fast data transfer speeds, such as science and engineering laboratories, hospitals, banks, schools and universities.



▲ **Figure 5.8** Fibre optic cable is capable of very high transfer speeds

WIRELESS ACCESS POINT

A wireless access point allows devices with Wi-Fi connectivity to connect to a wired network. They are often built into other hardware, such as routers (see page 85), but they are also available as stand-alone devices that connect to a wired network using Ethernet cables.



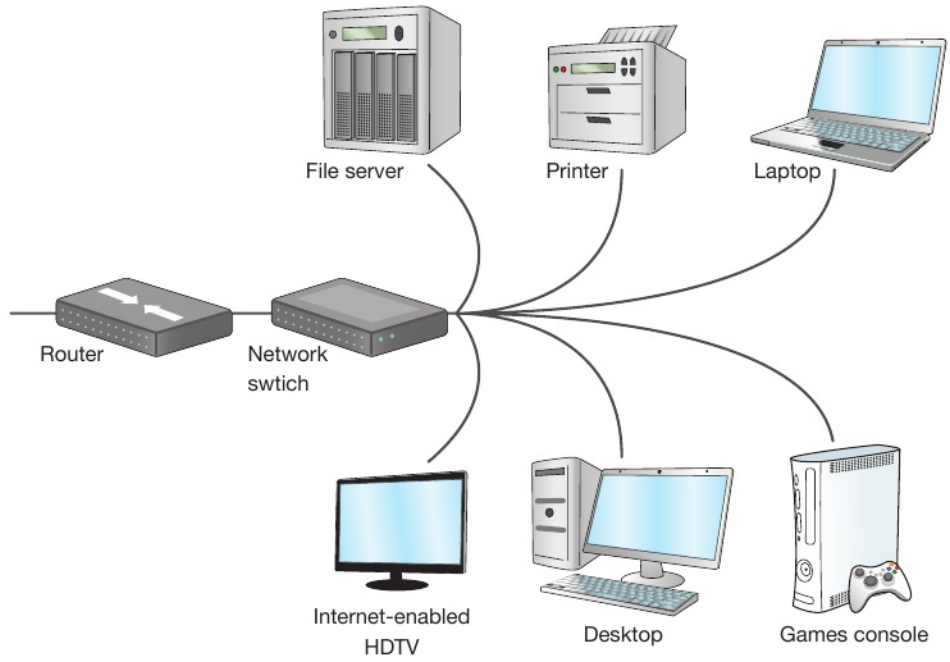
▲ **Figure 5.9** Wireless access points can be used in a small business to provide Wi-Fi access to wireless devices in a network

SWITCH

SUBJECT VOCABULARY

port a socket into which cables and devices can be plugged

A switch connects devices on a network. It has **ports**, each of which can be connected to a device using a cable. Connecting a wireless access point to a switch via a cable gives wireless devices access to the wired network. The switch makes sure that data sent from any device gets to the correct device on the network. For example, when printing a document, a laptop will send data that includes the printer's IP address to the switch and the switch then sends the data to the connected printer.



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

▲ **Figure 5.11** A 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 the addresses of all devices that are connected to it so that it can forward network traffic to its destination using the quickest route.

Most routers used in homes include a switch and a wireless access point. They also act as gateways, connecting the LAN to the internet, which is a type of WAN. Home routers are dynamically allocated an IP address by the internet service provider (ISP).

▲ **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)

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.

SERVER

SUBJECT VOCABULARY

client a computer connected to a server

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.

▲ **Figure 5.13** Servers are often more powerful than clients, with lots of memory and fast processors to enable them to process multiple requests for their resources

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.

HINT

A single computer can be used to perform multiple server functions. Performing multiple roles will affect a computer's performance. Its ability to perform multiple roles will depend on its resources, especially its memory and processor.

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.

You will learn more about the difference between the internet and the World Wide Web in *Unit 3 Operating online* (page 110).

SUBJECT VOCABULARY

Hypertext Transfer Protocol (HTTP) a set of standards that control how computer documents that are written in HTML connect to each other

DID YOU KNOW?

HTTP was developed in 1989 by Sir Tim Berners-Lee as a way of sharing information with colleagues. He is credited with inventing the World Wide Web.

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

INTERNET SERVICE PROVIDER (ISP)

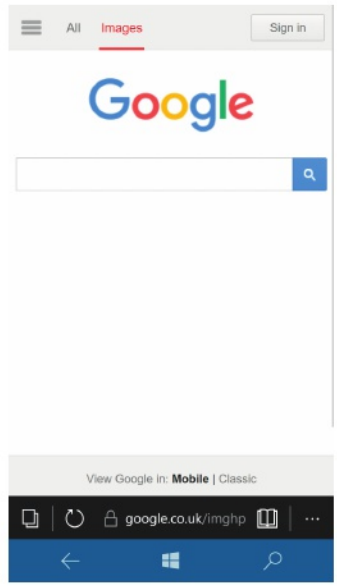
SUBJECT VOCABULARY

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

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. ISPs provide access via mobile telephone networks and landline telephone networks. Commercial ISPs charge subscription fees for access to the internet. Some ISPs provide free access as part of community schemes, which aim to provide internet access to groups of residents who either do not have or do not want access to commercial ISPs.

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

SEARCH ENGINE

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

8 OPERA IS A TRADEMARK OF OPERA SOFTWARE A

9 SAFARI® IS A TRADEMARK OF APPLE INC., REGISTERED IN THE U.S. AND OTHER COUNTRIES

HINT

Many people confuse search engines with web browsers. A search engine allows users to search and find information using keywords. A web browser is an application that users can use to view online content. Users can use a web browser to access a search engine.

DID YOU KNOW?

Some search engines allow users to search for information by uploading an image that represents the information they are looking for. The web browser then compares the image against a database of pages that include similar images and returns the results that are the closest matches.

You will learn more about search engines in *Unit 3 Operating online* (page 160–163).

FILTER SOFTWARE

SUBJECT VOCABULARY

URL (uniform resource locator) a website address
blacklist a list of unacceptable URLs
whitelist a list of acceptable URLs

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.

Administrators can add URLs to the blacklist and whitelist. The blacklist can be updated during software updates.

Filter software can help schools and parents to protect children from accessing disturbing or age-inappropriate content.

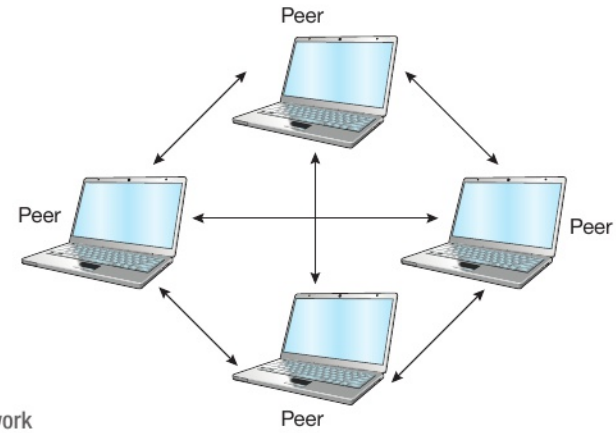
LOCAL AREA NETWORKS (LANS)

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

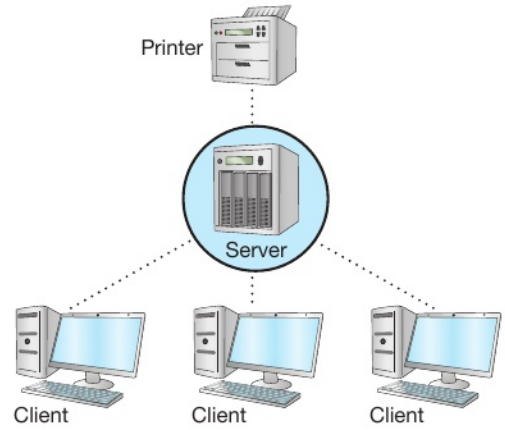
Computers in a peer-to-peer network share their resources with other computers in the network, but they do not access servers. Figure 5.16 is an example of a peer-to-peer network.



▶ **Figure 5.16** A peer-to-peer network

CLIENT-SERVER NETWORKS

Some networks use servers (see page 86). 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.

SKILLS INTELLECTUAL INTEREST AND CURIOSITY
ADAPTABILITY
SELF-DIRECTION

ACTIVITY

▼ LAN PARTIES

What is a 'LAN party'? Use the internet to find out and write your own definition of the term.

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. This ensures that support can be provided by people who have an overview of the network and avoids inexperienced users creating problems for themselves or others.
- **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 (see page 86) 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. File permissions can be set for individual files, folders or drives, allowing users to either read only or read and write to different files.
- **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.

HINT

You learned about sharing software, storage and file access in *Unit 1 Digital devices* (pages 4–63).

SECURING DATA ON NETWORKS

Security prevents unauthorised users from accessing network resources and data.

LOGINS AND PASSWORDS

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

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. This means that, once a user has been authenticated, they do not have to log in each time they access a resource or service.

See page 86 for more information about authentication servers. You will learn more about passwords in *Unit 3 Operating online* (page 100).

FIREWALLS

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. Firewalls are available as hardware and software, which can be installed on computers to prevent attacks from within a network.

ENCRYPTION

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

SKILLS INTELLECTUAL INTEREST AND CURIOSITY
CREATIVITY
ADAPTABILITY
SELF-DIRECTION
COMMUNICATION

ACTIVITY

▼ ANCIENT ENCRYPTION

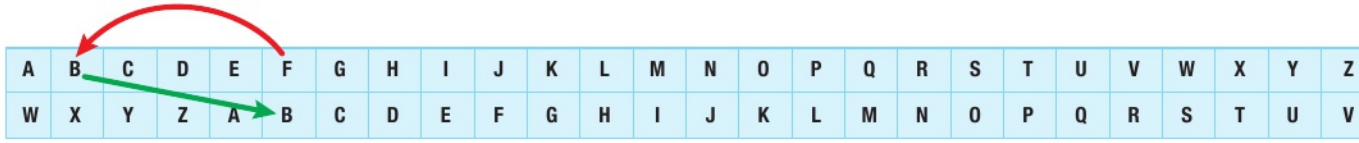
Research how a tool called a scytale was used by Spartans to encrypt messages. Create your own scytale and then use it to produce an encrypted message.

SUBJECT VOCABULARY

cipher a code

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.

Figure 5.18 shows an example of using a Caesar cipher. The top row is the original alphabet. The bottom row shows the alphabet after applying a Caesar cipher with a shift of four places. The example shows how the original letter F is encrypted to B.



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

SKILLS
PROBLEM SOLVING
INTELLECTUAL INTEREST AND CURIOSITY

ACTIVITY

▼ DECRYPTING A MESSAGE

Using Figure 5.18, decrypt this message: WHWJ PQNEJC. When you have decrypted it, you will find that it is a person's name. Research the importance of this person's work during the Second World War.

SKILLS
PROBLEM SOLVING
INTELLECTUAL INTEREST AND CURIOSITY
ADAPTABILITY
CO-OPERATION
RESPONSIBILITY

ACTIVITY

▼ ENCRYPTING A MESSAGE

1 The following is a message encrypted with a Caesar cipher. The shift is 16.
CEIJBO XQHCBUII
Decipher the message to give the original text.

2 Use a new Caesar cipher key to create an encoded message for a classmate. Do not include spaces between words, because this makes it harder to decrypt the message. Give them the encrypted message and see whether they can decrypt it and tell you the key.

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

- symmetric key encryption
- public key encryption.

SYMMETRIC KEY ENCRYPTION

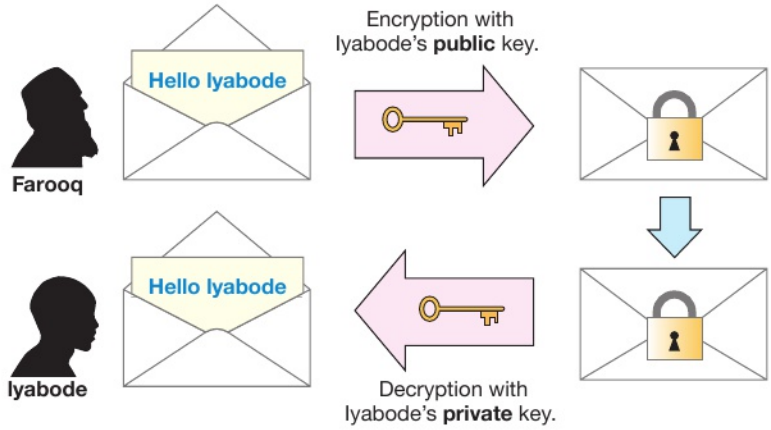
Symmetric key encryption uses the same key at both ends of the process, meaning that the same key is used to encrypt and decrypt the data.

PUBLIC KEY ENCRYPTION

Public key encryption uses two mathematically related keys called a key pair. One key is used to encrypt the data and a different key is used to decrypt it.

A computer shares a public key with other computers that want to send it encrypted data. This public key is mathematically related to a private key, which is not shared.

Figure 5.19 shows an example of public key encryption. If Farooq wants to send Iyabode an encrypted message, Farooq uses Iyabode's public key to encrypt the data. The data is then sent to Iyabode, who uses her private key to decrypt the message.



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

HINT

A key is not the same as a password.

Although Farooq's message won't be secure, because the public key is published, anyone who receives the message will not be able to understand it without Iyabode's private key.

SUBJECT VOCABULARY

eavesdropper an unauthorised person or piece of software that intercepts data from a private communication
packet a unit of data packaged to travel across a network

WIRELESS ENCRYPTION PROTOCOL (WEP)

It is easier to intercept data in a wireless network than in a wired network. 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.

DID YOU KNOW?

Experts tested the strength of WEP by examining 10,000 packets in less than a minute. Having done this, they then took less than 3 seconds to identify the WEP encryption key used to encrypt the packets.

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)

A VPN provides access to a private LAN from a remote location. The connection to the LAN is created using the infrastructure of a public network like the internet. 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

DID YOU KNOW?

Mobile, desktop and browser apps are available to make it easy for users to change their network settings so that they can use VPNs.

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

SUBJECT VOCABULARY

log a record of events
transaction the exchange of data

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.

For more information about backups, see *Unit 1 Digital devices* (page 42) and *Unit 3 Operating online* (pages 104–105).

CHAPTER QUESTIONS

SKILLS PROBLEM SOLVING

1 Which **one** of these connects a LAN to a WAN? **(1)**

A Switch
B Gateway
C Modem
D Server

SKILLS DECISION MAKING

2 Explain why public key encryption is more secure than symmetric key encryption. **(2)**

SKILLS PROBLEM SOLVING

3 State which security device controls the traffic entering a network. **(1)**

SKILLS PROBLEM SOLVING

4 State **two** methods by which devices are identified to each other on a network. **(2)**

SKILLS REASONING

5 Explain why IPv6 was used to replace IPv4. **(2)**

SKILLS PROBLEM SOLVING

6 State **two** uses for a VPN. **(2)**

SKILLS REASONING PROBLEM SOLVING

7 State the reason why a booster is used in a network. **(1)**

SKILLS INTERPRETATION

8 Describe how encryption secures data. **(3)**

SKILLS PROBLEM SOLVING

9 List **three** methods of securing data on networks. **(3)**

SKILLS DECISION MAKING

10 State **three** benefits to users of using a local area network. **(3)**

SKILLS ADAPTIVE LEARNING EXECUTIVE FUNCTION ADAPTABILITY COMMUNICATION

11 Draw and label a network diagram for a home that includes:

- two smartphones
- one tablet device
- two desktop PCs
- internet access. **(8)**