4 Networks and the effects of using them

In this chapter you will learn about:

- networks:
  - routers
  - common network devices – NICs, hubs, switches, bridges and
  - Wi-Fi and Bluetooth
  - cloud computing
  - intranets, extranets and the internet
  - LANs, WLANs and WANs
- network issues and communication:
  - security (including passwords, types of authentication)
  - anti-malware
  - electronic conferencing.

Most computer systems are now connected in some way to form a network. This ranges from a basic home network of only a few devices to very large networks, often set up to share resources, such as printers or software. The largest network is the internet itself.

4.1 Networks

4.1.1 Common network devices and terms

We will begin this section by defining four important terms you will often come across in this chapter:

- network interface card (NIC)
- media access control (MAC) address
- internet protocol (IP) address
- data packet.

Network interface card (NIC)

A **network interface card (NIC)** is needed to allow a device to connect to a network. An NIC turns binary data into an electrical signal that allows access to a network. The NIC is usually integrated into the motherboard on most modern computers.

Each NIC is given a unique hardwired (or hard-coded) media access control (MAC) address at the manufacturing stage. When installed in a device, this uniquely identifies that device.

Wireless network interface cards (WNICs) are the same as NICs in that they are used to connect devices to the internet or other networks. However, they use wireless connectivity, utilising an antenna to communicate with networks via microwaves. They would normally plug into the USB port or be part of an internal integrated circuit.

Media access control (MAC) address

The **media access control (MAC) address** is a number which uniquely identifies a device when it is connected to a network. The MAC address is made up of 48 bits which are shown as six groups of hexadecimal digits with the general format:

NN – NN – NN – DD – DD – DD
manufacturer's code device serial number

For example, 00 – 1C – B3 – 4F – 25 – FF, where the first six hex digits identify a device made by Apple and the second set of six hex digits are the unique serial number of the device itself. If the NIC card is replaced, the MAC address will also change. The MAC address is sometimes referred to as the **physical address** because it uniquely identifies a device. MAC addresses are useful when trying to identify network faults because they never change, which makes it a more reliable method of identifying data senders and data receivers on a network.

Internet protocol (IP) addresses

Whenever a computer connects to the internet it is given an **internet protocol (IP) address**. This is usually assigned to the computer by the internet service provider (ISP). Because the operation of the internet is based on a set of protocols (rules), it is necessary to supply an IP address. Internet protocols define the rules that must be agreed by senders and receivers of data communicating through the internet. An IP address essentially identifies the location of a device on a network.

This means that if you are using your laptop at home, it will have been given an IP address when it connected to the internet. If you now take your laptop to a coffee shop, and log into the internet again, it will be assigned a new IP address. Unlike the MAC address which remains constant, the IP address changes each time you log in at different locations.

There are two versions of IP: IPv4 and IPv6. IPv4 is based on 32 bits and the address is written as four groups of eight bits (shown in denary format); for example:

254.25.28.77

Because there are now so many devices connected to the internet, and this number is growing, in the future 32 bits will no longer be enough to give each of them a unique address. Therefore, a newer version called IPv6 is now being used. This uses a 128-bit address, which take the form of eight groups of hex digits; for example:

A8FB:7A88:FFF0:0FFF:3D21:2085:66FB:F0FA

Note the use of colons (:) and hexadecimal numbering. IPv6 has been designed to allow the internet to grow in terms of the number of hosts and potential increase in the amount of data traffic.

Data packets

Data is moved around networks in the form of data packets. Whenever a user sends some data, it is split up into a number of packets and each packet is transmitted separately. Packets of data will usually have a header which contains:

- the sender's IP address
- the receiver's IP address
- the sequence/identity number of the packet (this is to ensure that all the packets can be reassembled into the correct order once they reach the destination)
- the packet size (this is to ensure the receiving station can check if all of the packets have arrived intact)
- how many data packets make up the whole message.

When a router (see later) receives a packet of data, it checks the destination IP address against the stored routing table, which allows the router to determine the packet's next step in the path. A data packet will pass through a number of routers before it reaches its final destination. All the information in the data packet headers allows the data packets to be reassembled in their correct order, according to the sequence/identity number, by the receiving station.

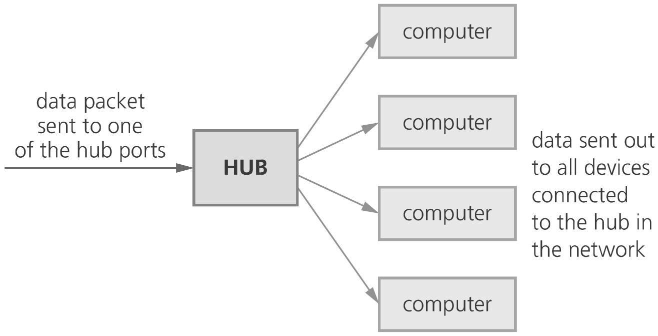
Exercise 4a

Try finding and running a program called 'tracert' which shows the 'hops' data packets take from sender to receiver. The screen printout will show the routers used in the path and the 'hop' numbers. (You can find 'tracert' utilities using a search engine.)

Hubs

Hubs are hardware devices that can have a number of other devices connected to them. They are used primarily to connect devices together to form a **local area network (LAN)**, often in the same building. A hub will take a data packet received at one of its ports and broadcast it to **every** device connected to it.

▲ **Figure 4.1** Hub


data packet sent to one of the hub ports
HUB
computer
computer
computer
computer
data sent out to all devices connected to the hub in the network

▲ **Figure 4.2** Hub network connections

Because data packets are delivered to every device on the network:

- hubs are not very secure because every device will receive every data packet
- there will be unnecessary traffic on the network, which results in reduced bandwidth.

Switches

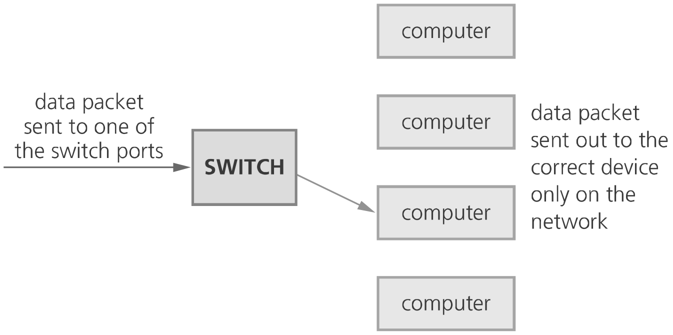
Switches are 'intelligent' versions of hubs. As with hubs, they connect a number of devices together to form a LAN. However, unlike a hub, a switch stores the MAC addresses of all devices on the network. Each port on the switch connected to a device will have a matching MAC address (called a look-up table) as shown in Table 4.1.

▲ **Figure 4.3** Switch

▼ **Table 4.1** Switch MAC address table

Port number	MAC address
1	a4-00-22-a4-fe-d1
2	00-1c-b3-4f-25-ff
3	33-11-ad-6f-f1-00
4	a4-00-22-b2-24-11
5	00-1c-b3-44-ff-02
6	0d-3e-4f-1a-22-00

Using the look-up table, a switch matches the MAC address of an incoming data packet arriving at one of its ports, and directs it to the correct device. None of the other devices will see this data packet. Thus, if a data packet arrives at port 2, and the MAC address in the data packet is a4-00-22-b2-24-11, then the switch will connect the data packet to port 4 only.


computer
data packet sent to one of the switch ports
computer
data packet sent out to the correct device only on the network
SWITCH
computer
computer

▲ **Figure 4.4** Switch network connections

Consequently, switches are more secure than hubs (because only the intended device is sent the data) and do not waste bandwidth (because network traffic is reduced).

In conclusion, hubs and switches are used to exchange data **within** their own local area networks. They are unable to exchange data with outside networks (such as the internet). To exchange data outside their own LAN, a device needs to be able to read an IP address. Therefore, we need another device to allow communication with external networks.

In summary:

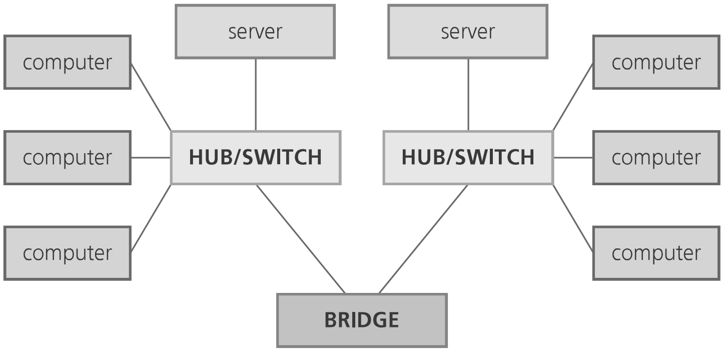
- both a hub and a switch are used to connect devices in a LAN
- both hubs and switches use data packets
- hubs send data packets to every device on the network; whereas switches send data packets to a specific device only

- security is lower with hubs than with switches
- a switch uses a look-up table to determine the destination device
- switches use MAC addresses to locate the destination device.

Bridges

Bridges are devices that connect one LAN to another LAN that uses the same protocol (communication rules). They are often used to connect together different parts of a LAN so that they can function as a single LAN.

▲ **Figure 4.5** Bridge



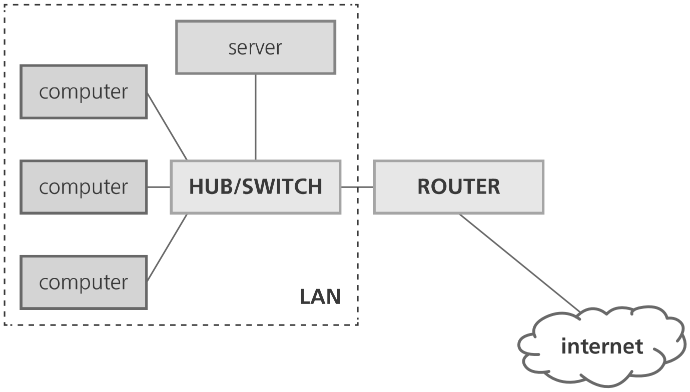
▲ **Figure 4.6** Use of a bridge to connect two LANs together

Unlike routers, bridges cannot communicate with other external networks, such as the internet.

4.1.2 Routers

Routers are used to route data packets from one network to another network, based on IP addresses. It can do this because each router has its own IP address. Routers are used to join a LAN to the internet.

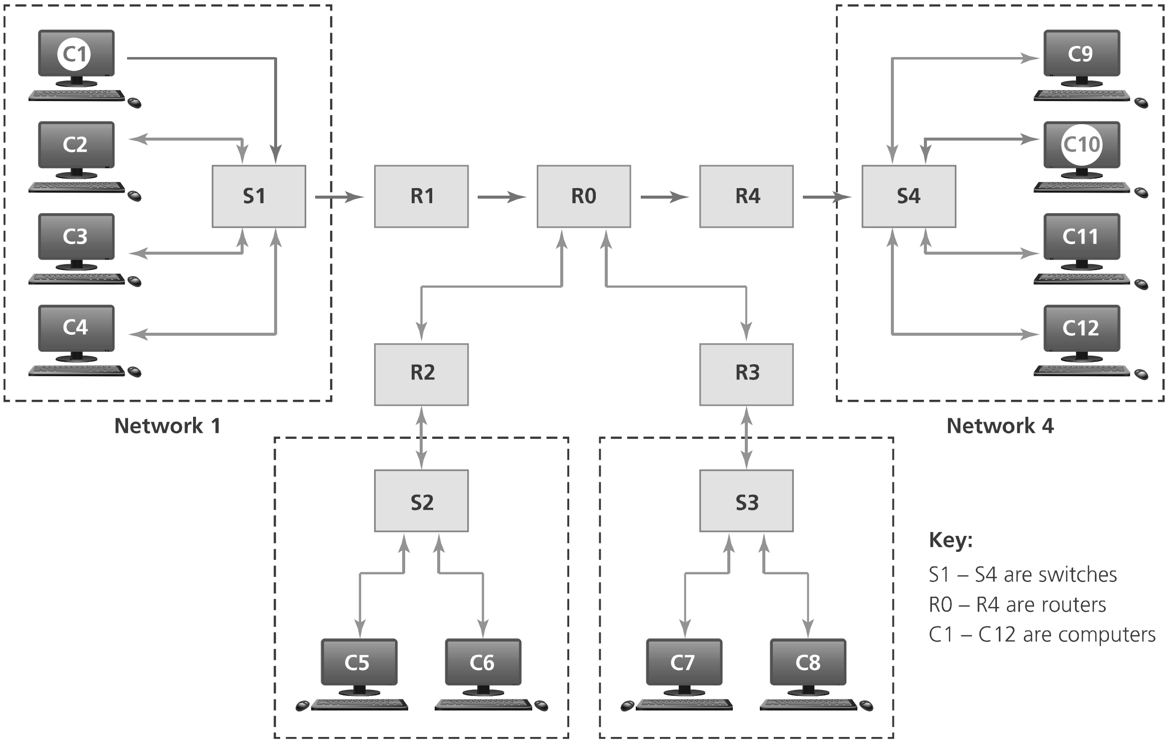
▲ **Figure 4.7** Router



▲ **Figure 4.8** Router used to connect a LAN to the internet

When a data packet is received at one of its ports, the router inspects the IP address and determines whether the data packet is meant for its own network or for another, external network. If the data packet is meant for its own network, then the data packet is routed to the local switch or hub. Otherwise, the data packet is transmitted to a different router (and therefore to an external network).

Routers know where to send data packets by consulting a routing table (stored on the router's RAM). The routing table will contain information about the router's immediate network (such as computer addresses) and information about other routers in its immediate vicinity. When a data packet reaches a router, it examines the IP address. Because the routing table contains computer addresses of all the computers/devices on its network, it will be able to work out that the data packet is intended for a computer on its network. Routers however, do not store the MAC addresses of devices (only IP addresses of all computers and devices are stored). The router does not need the MAC address because the data packet will be sent by the router to the switch on the recipient local network. The switch can then use its look-up table to send the data packet to the correct device.



▲ **Figure 4.9** Routing of data from **C1** to **C10**

Suppose, in Figure 4.9, computer **C1** wishes to send data to computer **C10**:

- Data packets are sent from C1 to R1.
- R1 checks the IP addresses and notes the data packets are not intended for any devices on Network 1.
- The data packets are then forwarded onto the internet (R0).
- The IP address (in the header of the data packet) matches that of R4; this ensures that each data packet is eventually forwarded to R4.
- R4 recognises that the IP address of each data packet refers to Network 4, and forwards them to S4 which then directs each data packet to C10.

Many modern broadband 'routers' actually combine the functions of a router and a switch – this means that they store MAC addresses and IP addresses to enable data packets to be sent to the correct network and then to the correct device on the network.

Table 4.2 summarises the differences between bridges and routers.

▼ **Table 4.2** Comparison of routers and bridges

Router	Bridge
The main objective of a router is to connect various types of network together	The main objective of a bridge is to connect LANs together
Routers scan a device's IP address	Bridges scan a device's MAC address
Data is sent out using data packets	Data is sent out using data packets
Connected networks will use different protocols	Connects networks together that use the same protocols
A routing table is used to direct data packets to the correct device	Bridges do not make use of routing tables
A router has more than two ports	A bridge has only two ports

4.1.3 Wi-Fi and Bluetooth

Both **Wi-Fi** and **Bluetooth** offer wireless communication between devices. They both use electromagnetic radiation as the carrier of data transmission.

Bluetooth sends and receives radio waves in a band of 79 different frequencies (known as channels). These are all centred on a frequency of 2.45 GHz. Devices using Bluetooth automatically detect and connect to each other, but they do not interfere with other devices because each communicating pair uses a different channel (from the 79 options).

When a device wants to communicate, it picks one of the 79 channels at random to pair with another device. If the channel is already being used, it randomly picks another channel. Once paired, to minimise the risks of interference with other devices, the devices constantly change the channels they are using (several times a second). This is known as **spread-spectrum frequency hopping**. Bluetooth uses key encryption to create a secure **wireless personal area network (WPAN)**.

Bluetooth is useful:

- when transferring data between two or more devices which are very close together (less than 30 metres distance)
- when the speed of data transmission is not critical
- for low-bandwidth applications (for example, when sending music files from a mobile phone to a headset).

Wi-Fi sends and receives radio waves in several different frequency bands – 2.4 GHz and 5 GHz are the most common at the moment. Like Bluetooth, each band is also further split into channels. The 5GHz band has a faster data transfer rate but a shorter signal range.

Wi-Fi is best suited to operating full-scale networks because it offers much faster data transfer rates, better range and better security than Bluetooth. A Wi-Fi-enabled device (such as a computer or smartphone) can access, for example, the internet wirelessly at any **access point (AP)** or **'hot spot'** up to 100 metres away. Table 4.3 summarises some of the differences between Wi-Fi and Bluetooth.

▼ **Table 4.3** Comparison of Wi-Fi and Bluetooth connectivity

Feature	Bluetooth	Wi-Fi
Transmission frequency used	2.4 GHz	2.4, 3.6, 5.0 GHz
Data transfer rate (maximum)	25 Mbits/second (~3.1 Mbytes/second)	250 Mbits/second (~31 Mbytes/second)
Maximum effective range (metres)	30 metres	100 metres (but can be obstructed by walls, etc. reducing effective range to only a few metres)
Maximum number of devices connected	Up to 7	Depends on the router used (can be one device or many devices)
Type of data transmission security	Key matching encryption	WEP (wireless equivalent privacy) and WPA (Wi-Fi protected access) are the most common security systems)

4.1.4 Cloud computing (storage)

Cloud computing is a method of data storage where data is stored on remote servers – there may be thousands of servers in many different locations. The same data is stored on more than one server in case of maintenance or repair, allowing clients to access data at any time. This is known as **data redundancy**. The physical environment of the cloud servers is owned and managed by a hosting company.

There are three common cloud storage systems:

- Public cloud – this is a storage environment where the customer/client and cloud storage provider are different companies.
- Private cloud – this is storage provided by a dedicated environment behind a company firewall; customer/client and cloud storage provider are integrated and operate as a single entity.
- Hybrid cloud – this is a combination of the two previous environments; some data resides in the private cloud and less-sensitive/less-commercial data can be accessed from a public cloud storage provider.

Instead of, or in addition to, saving data on a local hard disk or other storage device, a user can save their data 'in the cloud'.

Advantages of cloud computing (storage)

- Customer/client files stored in the cloud can be accessed at any time, from any device, anywhere in the world, as long as internet access is available.
- There is no need for a customer/client to carry an external storage device with them, or even use the same computer, to store and retrieve information.
- The cloud provides the user with remote backup of data, with obvious advantages in the event of data loss/disaster recovery on their own computer.
- If a customer/client has a failure of their hard disk or backup device, cloud storage will allow recovery of their data.
- The cloud system offers almost unlimited storage capacity (at a price!).

Disadvantages of cloud computing (storage)

- Security aspects of storing data in the cloud (see comments later on).
- If the customer/client has a slow or unstable internet connection, they could have many problems accessing or downloading their data/files.

- Costs can be high if a large storage capacity or high download/upload data transfer is required.
- The potential failure of the cloud storage company is always possible – this poses a risk of loss of all backup data.

Several computer manufacturers (especially tablets and laptops) and mobile phone manufacturers are encouraging customers to store or backup all their files on to cloud storage. Users purchase cloud storage and can then access all their files (for example, photos, videos, music or e-books) from any device anywhere in the world. This has obvious advantages:

- You do not need to carry memory sticks around with you if you want to access your files away from home.
- You do not have to pay for large storage capacity on your computer/tablet or mobile phone.
- Because the cloud is controlled by external companies, they will ensure that your files are backed up and therefore reduce the possibility of losing irreplaceable data.
- The ability to synchronise (sync) files ensures they are automatically updated across all devices; this means that the latest version of a file saved on a desktop computer, for example, is also available on other devices, such as a smartphone.
- Cloud storage is also ideal for collaboration purposes; it allows several users to edit and collaborate on a single file or document – there is no need to worry about tracking the latest version or which user made the changes.

In spite of all these obvious advantages, there are still security worries about using cloud storage. The main fears are data security and data loss.

Data security using cloud storage/computing

Companies that transfer vast amounts of confidential data from their own systems to a cloud service provider are potentially relinquishing control of their own data security. This raises a number of questions:

- What physical security exists regarding the building where the data is housed?
- How good is the cloud service provider's resistance to natural disasters or power cuts?
- What safeguards exist regarding personnel who work for the cloud service company? Can they use their authorisation codes to access confidential data for monetary purposes?

Data loss

There is a risk that important and irreplaceable data could be lost from cloud storage facilities. Actions from hackers (gaining access to accounts or pharming attacks, for example) could lead to loss or corruption of data. Users need to be certain that sufficient safeguards exist to overcome these potentially very harmful risks.

In 2019, there were a number of breaches of cloud security. We will briefly mention two of these breaches:

- On 2 April, a Mexican digital media company (called Cultura Colectiva) exposed 540 million Facebook accounts stored on one of their cloud servers; the data included user profiles, user IDs, account names, likes and comments.

- On 29 July, Capital One Bank (in the USA) had some of their cloud-based data hacked exposing 80,000 bank account numbers, 140,000 social security numbers and over one million government ID numbers.

4.1.5 Common network environments

Extranets, intranets and the internet

Extranets, intranets and the internet are all common types of network environment. You will find these types of network covered in some depth in Chapter 10.

Link

See Section 10.2 for more on extranets, intranets and the internet.

4.1.6 Network types

This section will cover the following types of network:

- local area network (LAN)
- wireless local area network (WLAN)
- wide area network (WAN).

Local area network (LAN)

Local area networks (LANs) are usually within one building or geographically near each other. A typical LAN will consist of a number of computers and devices (for example, printers) which will be connected to hubs or switches. One of the hubs or switches will usually be connected to a router to allow the LAN to connect to external networks, such as the internet.

There are advantages of networking computers together using LANs:

- they allow the sharing of resources such as hardware (e.g. printers and scanners) and software (e.g. word processors and photo editing software)
- they permit easy communication between users of the LAN (e.g. by using simple text messaging between computers on the network)
- they use a network administrator that ensures security and use of the LAN is constantly monitored (e.g. the administrator can maintain passwords and also monitor data traffic within the network).

There are also disadvantages of networking computers using LANs:

- easier spread of viruses throughout the whole network
- queues for shared resources (such as a printer) which can be frustrating
- slower access to external networks
- increased security risk when compared to stand-alone computers
- if the main server breaks down, in many types of network structures, the network will no longer function properly.

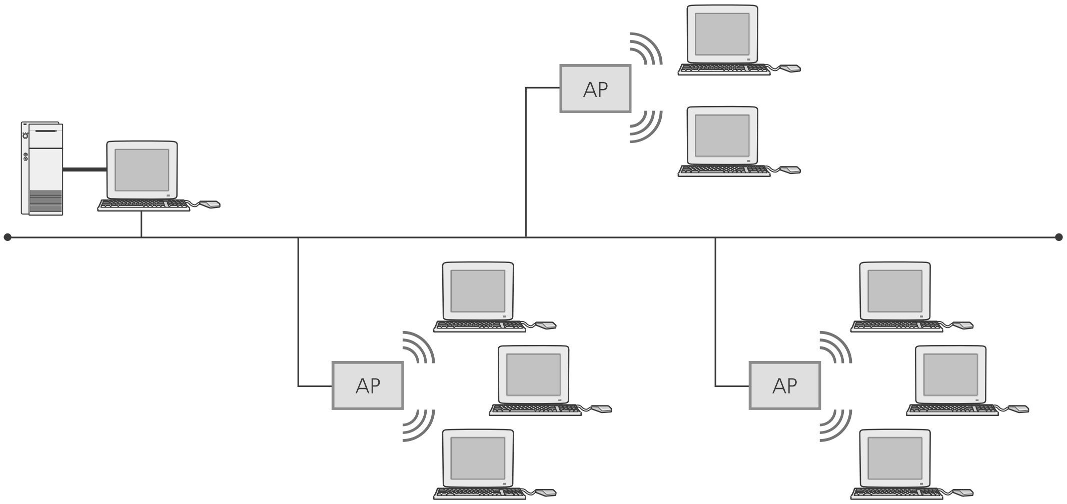
Wireless local area network (WLAN)

Wireless LANs (WLANs) are similar to LANs, but there are no wires or cables. In other words, they provide wireless network communications over fairly short distances using radio or infrared signals instead of using cables.

Devices, known as **access points (APs)**, are connected into a wired network at fixed locations. Because of the limited range, most commercial LANs (for example, a college campus or an airport) need several APs to permit uninterrupted wireless communications. The APs use either **spread-spectrum**

technology (which is a wideband radio frequency with a range of about 30 to 50 metres) or **infrared**, but this has a very short range (about 1–2 metres) and is easily blocked, and therefore infrared has limited use.

The AP receives and transmits data between the WLAN and the wired network structure. End-users access the WLAN through wireless LAN adapters which are built into their devices.



▲ **Figure 4.10** Wireless LAN set-up

Wired versus wireless

Table 4.4 compares wired LANs and wireless LANs.

▼ **Table 4.4** Wired versus wired LAN

Wireless networking	Wired networking
It is easier to expand the networks and it is not necessary to connect the devices using cables	Using cables produces a more reliable and stable network; wireless connectivity is often subject to interference
This gives devices increased mobility, as long as they are within range of the APs	Data transfer rates tend to be faster and there will not be any 'dead spots'
No cabling, so there is a safety improvement and increased flexibility	
There is an increased chance of interference from external sources	Setting up cabled networks tends to be cheaper overall in spite of the need to buy and install cable
Data is less secure than with wired systems; it is easier to intercept radio waves and microwaves than cables; it is essential to protect data transmissions using encryption	However, cabled networks lose the ability for devices to be mobile; they must be close enough to allow for cable connections
Data transmission rate is still slower than for cabled networks although it continues to improve	Having lots of wires can lead to a number of hazards, such as tripping hazards, overheating of connections (leading to potential fire risk) and disconnection of cables during routine office cleaning
It is possible for signals to be stopped by thick walls (for example, in old houses) and there may be areas of variable signal strength leading to 'drop out'	

Advice

Wi-Fi is a series of protocols that enable a WLAN to be set up.

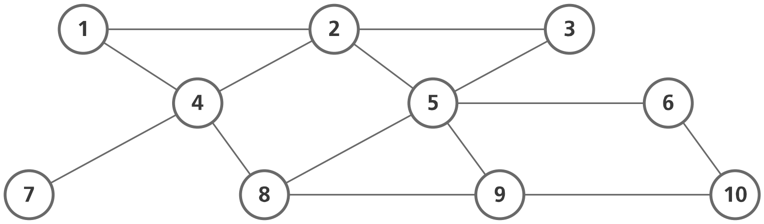
Wide area networks (WANs)

Wide area networks (WANs) are used where computers or networks are situated a long distance from each other geographically (for example, in a different city or country). As mentioned earlier, if a number of LANs are joined together using a router, then they can form a WAN. The network of ATMs (automated teller machines) used by banks is one of the most common examples of the use of a WAN.

Because of the long distances between devices, WANs usually make use of some public communications network (such as telephone lines or satellites), but they can use dedicated or leased communication lines, which can be less expensive and also more secure (less risk of hacking, for example).

A typical WAN will consist of end systems and intermediate systems (Figure 4.11).

In Figure 4.11, **1**, **3**, **7** and **10** are known as end systems and the remainder are known as intermediate systems. The distance between each system can be considerable, especially if the WAN is run by a multinational company.



▲ **Figure 4.11** WAN end systems and intermediate systems

The following is used as a guide for deciding the 'size' of a network:

- WAN: 100 km to over 1000 km
- MAN: 1 km to 100 km
- LAN: 10 m to 1000 m (1 km)

Advice

Metropolitan area networks (MANs) is outside the syllabus; this is included here for comparison purposes only.

4.2 Network issues and communication

4.2.1 Security issues regarding data transfer

Many aspects of security (such as hacking, phishing, pharming and viruses) are covered in depth in Chapter 8 (Section 8.3). This section covers some of the more general aspects of internet security, together with how we use networks to communicate.

4.2.2 Passwords

Passwords are used in many instances when accessing the internet. For example:

- when accessing your email account
- when carrying out online banking
- accessing social networking sites.

There are many more instances when you might need to type in a password and, in many cases, a user ID. It is important that passwords are protected. Some ways of doing this are described below:

- Run anti-spyware software to make sure that your passwords are not being relayed back to whoever put the spyware on your computer
- Change passwords on a regular basis in case it has come into the possession of another user illegally or accidentally.
- Passwords should not be easy to crack (e.g. your favourite colour, name of a pet or favourite rock group); passwords are grouped as either strong (hard to crack or guess) or weak (relatively easy to crack or guess).
- Strong passwords should contain:
  - at least one capital letter
  - at least one numerical value
  - at least one other keyboard character (such as @, *, & etc.).

An example of a strong password is: Sy12@#TT90kj=0

An example of a weak password is: GREEN1

Exercise 4b

Which of the following are weak passwords and which are strong passwords?

Explain your decision in each case.

i 25-May-2000
ii Pas5word
iii ChapTer@15
iv AbC*N55!
v 12345X

4.2.3 Other authentication methods

Passwords are one of the most common types of authentication (that is, a way of proving your identity). This section will look at a number of other types of authentication:

- zero login
- biometrics
- magnetic stripes
- smart cards
- physical tokens
- electronic tokens.

Zero login and biometrics

The Fast ID online (FIDO) Alliance and WWW Consortium (W3C) announced a new technology standard that allows users to login to computer systems without the need to type in a password. The mishandling of personal data over the years now means we can no longer regard data, such as passwords, as being secret or protected.

Exam-style questions

1 A company is setting up a video conference.

a Name **three** computer hardware devices they would need. [3]

b The company could have set up a web-conference rather than a video-conference.
Describe what is meant by a web-conference. [4]

Cambridge IGCSE Information and Communication Technology (0417) Paper 11 Q8, May/June 2017

2 Both Wi-Fi and Bluetooth can be used to enable devices to communicate wirelessly.
Describe the differences in how Bluetooth and Wi-Fi both operate. [6]

3 Hubs and switches are both used to enable devices to communicate with each other in a network.

a Describe the differences and similarities in the use of hubs and switches in a network. [4]

b A bridge is another device used in network connectivity.
Describe the function of a bridge. [2]

c Routers are used to allow local area networks to connect to external networks. Local area network 'A' is in Europe and local area network 'B' is in India.
Describe how routers are used to enable a computer on network 'A' to send data to a computer on network 'B'. [3]

d Describe the main differences between routers and bridges. [3]

4 Authentication is an important part of network security.
Explain the meaning of the following three types of authentication.
In each case, also give an example of its use.

a Zero login

b Physical token

c Electronic token [9]

5 Six features of network devices are given in the table below.
For each feature, tick (✓) the appropriate box to indicate whether it refers to a router, hub or switch. [6]

Feature	Router (✓)	Switch (✓)	Hub (✓)
Used to connect devices together to form a local area network (LAN)			
The destination MAC address is looked up before the data packet is sent to the correct device			
Used to connect LANs to other, external networks			
Uses both MAC and IP addresses to enable data packets to be sent to the correct device on another network			
All data packets are sent to all the devices on the network			
Data packets are sent only to a specific device on the same network			

6 **a** Describe what is meant by a virus. [2]
b Describe **three** of the features you would expect to find in any anti-virus software. [3]

7 **a** Explain how magnetic stripe cards could be used to control the entry and exit to a security building. [4]
b Describe how these magnetic stripe cards could be improved to increase the security of the building. [3]

8 Seven descriptions are shown on the left and ten computer terms are shown on the right.
By drawing arrows, connect each description to the correct computer term. [7]

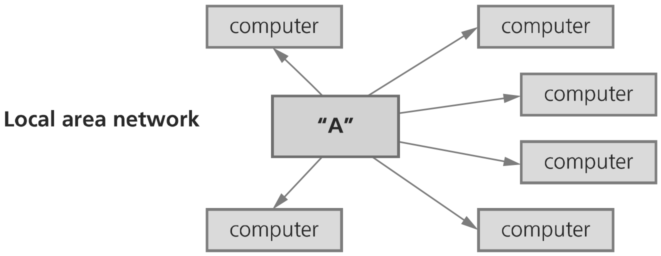
- Form of authentication in the form of hardware devices; uses periodically changing random numbers to log in to a secure system
- Type of network that covers a huge geographical area, such as a country or different continent
- Devices used to connect two LANs together that use the same protocols, but cannot communicate outside the two LANs
- Authentication software installed on a user's smartphone that generates a one-time password
- Type of login authentication that relies on biometrics and behavioural patterns
- Devices that connect computers together to form a LAN; directs data packets to a specific device or computer only
- Hardware needed to connect a device to a network; a MAC address is hardwired or hard-coded into the device at manufacture

- Password
- Zero login
- Physical token
- Wide area network
- Internet
- Network interface card
- Hub
- Bridge
- Electronic token
- Switch

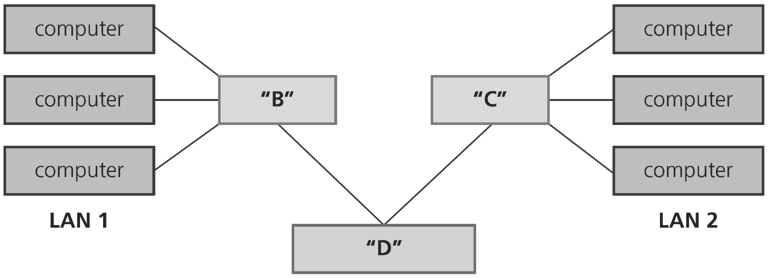
9 **a** Explain what is meant by cloud computing. [3]
b Give **three** advantages of storing data on the cloud. [3]
c Give **three** disadvantages of storing data on the cloud. [3]

10 Name each of the **six** network devices labelled 'A' to 'F' in the diagrams below: [6]

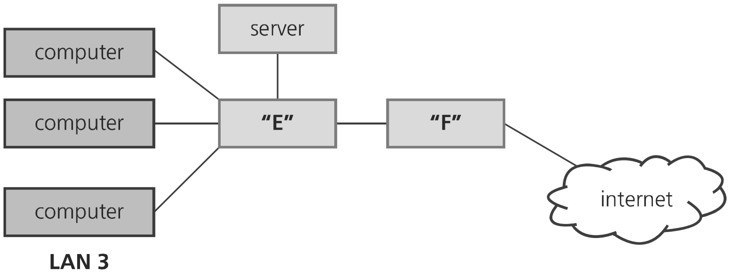
a



b



c


server
computer
computer
"E"
"F"
computer
internet
LAN 3