Edexcel

OL IGCSE

Communication and the internet

CODE: (4CP0)

Unit 05

Chapter 21 – Networks

Computer networks and their use

A **network** is a collection of two or more computers that are connected for the purpose of sharing resources and data. All types of computers (e.g. desktops, laptops, tablets, e-readers, gaming systems, shop tills and even Internet-enabled fridges) can be linked in networks.

Many networks include servers. A server is a powerful computer that provides the network with **services**, such as storing files or sending/receiving emails. A small network might have one server, whereas a large business network could have tens or hundreds of servers.

WHY ARE NETWORKS USED?

A network can support multiple users accessing multiple services at the same time.
Almost all organisations (small or large), including schools, have a computer network that provides multiple services to its users.

The network allows multiple users:

■to read/write personal files on a central server - this provides extra storage space to that on a single computer and also gives a back-up facility
■to access shared files among several users
■to download data or updates to computer programs
■to send data to a shared printer
■to access the Internet
■to communicate with each other - perhaps through email or video, or to play interactive games.

Different types of networks

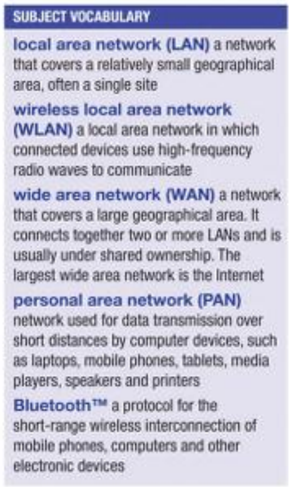
LAN, WAN AND PAN

A **local area network (LAN)** is a network that covers a relatively small geographical area. This is often a single site, such as a home, a hospital or a factory. The hardware (e.g. cables, routers, etc.) that connects the computers, servers and other hardware devices are usually owned by the organisation that the network belongs to.

Many people have a **wireless local area network (WLAN)** at home. A wireless router allows all the computer devices in a household to access the Internet and share devices such as printers and external hard drives.

A **wide area network (WAN)** covers a large geographical area, usually across several sites of an organisation. Each site has one or more LANS, and they are all connected together to make a WAN. The WAN allows employees on different sites to communicate and share data.

A **personal area network (PAN)** is a network communicating between computer devices, such as laptops, mobile phones, tablets, media players, speakers and printers. They may be devices belonging to one person or to several.



SUBJECT VOCABULARY

local area network (LAN) a network that covers a relatively small geographical area, often a single site

wireless local area network (WLAN) a local area network in which connected devices use high-frequency radio waves to communicate

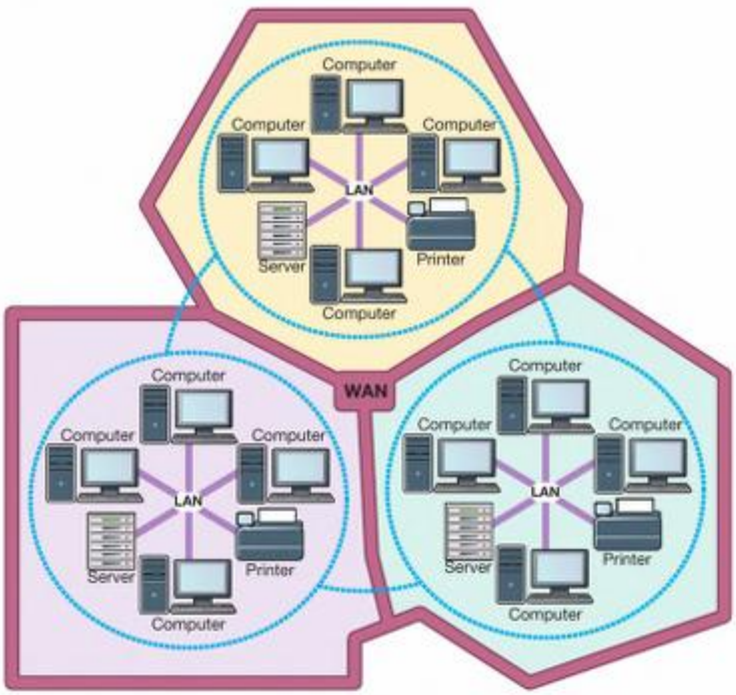
wide area network (WAN) a network that covers a large geographical area. It connects together two or more LANs and is usually under shared ownership. The largest wide area network is the Internet

personal area network (PAN) network used for data transmission over short distances by computer devices, such as laptops, mobile phones, tablets, media players, speakers and printers

Bluetooth™ a protocol for the short-range wireless interconnection of mobile phones, computers and other electronic devices

The PAN may just connect the local devices or allow them to connect to higher-type networks such as the Internet. The devices usually communicate wirelessly over distances of up to 10 metres by radio waves using a technology called **BluetoothTMM**

▶ **Figure 5.1** LANs may be connected together to form a WAN



CLIENT-SERVER AND PEER-TO-PEER NETWORKS

There are two main models relating to computer networks: client-server and peer-to-peer.

CLIENT-SERVER

In a client-server network there is at least one server, which is a powerful computer that provides a service or services to the network. The server provides services to the clients as required. A client accesses data or files from a server using the following process:

SUBJECT VOCABULARY

peer-to-peer network a network that doesn't have any dedicated servers. Each computer in the network can act as client and server

network topology describes how the devices on a network are connected together

1. A client will make a connection to the server using its address. The server will know the address of the client because this will be included in the request for a connection.
2. Once the connection has been made, the client will make a service request to the server.
3. If the request is valid, the server will send the requested data to the client using the address identified in step 1.

PEER-TO-PEER

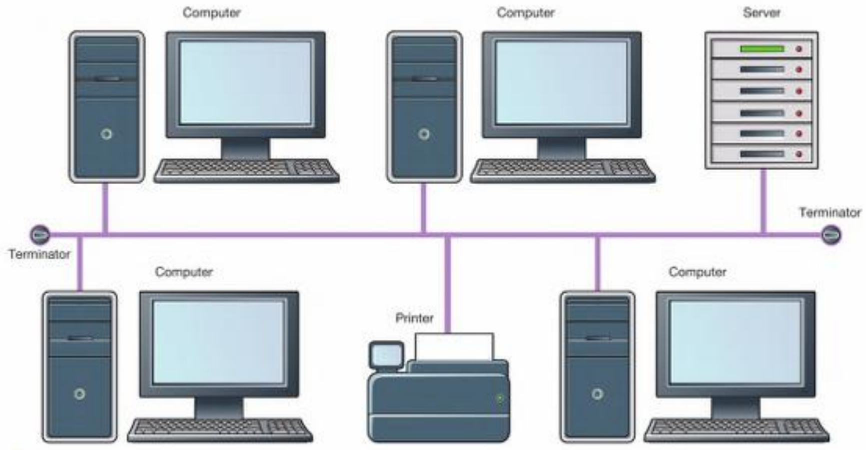
Unlike in a client-server network, there aren't any dedicated servers in a **peer-to-peer network**. Each computer can act as both a client and a server. Each computer in a peer-to-peer network can provide a service, such as share some files or provide access to a printer. Each computer can also request services from any other computer that has been configured to provide that service.

Network topologies

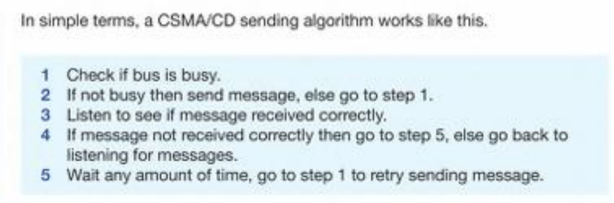
There are several different ways that the connections between networked devices can be arranged. The arrangement of these connections is referred to as the network topology.
There are four main network topologies - bus, ring, star and mesh.

BUS

A bus network consists of a single cable to which each networked device is connected. Messages are sent along the cable in the form of electronic signals. At each end of the cable is a terminator.

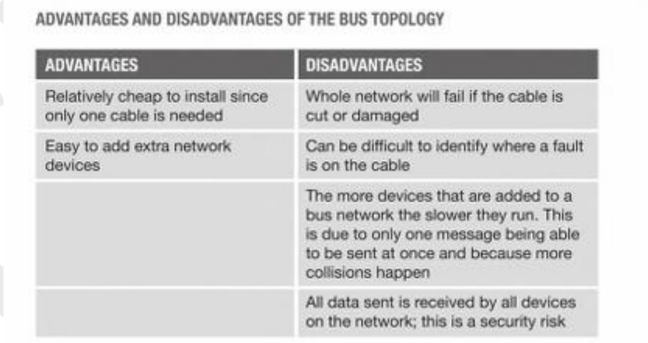


▲ Figure 5.2 Bus network topology



In simple terms, a CSMA/CD sending algorithm works like this.

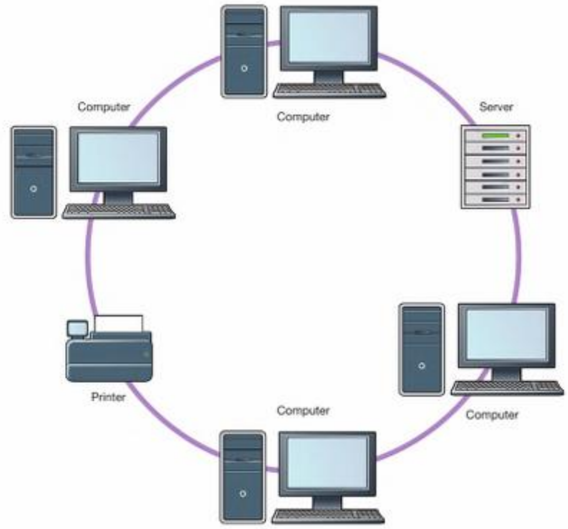
1. Check if bus is busy.
2. If not busy then send message, else go to step 1.
3. Listen to see if message received correctly.
4. If message not received correctly then go to step 5, else go back to listening for messages.
5. Wait any amount of time, go to step 1 to retry sending message.



ADVANTAGES AND DISADVANTAGES OF THE BUS TOPOLOGY

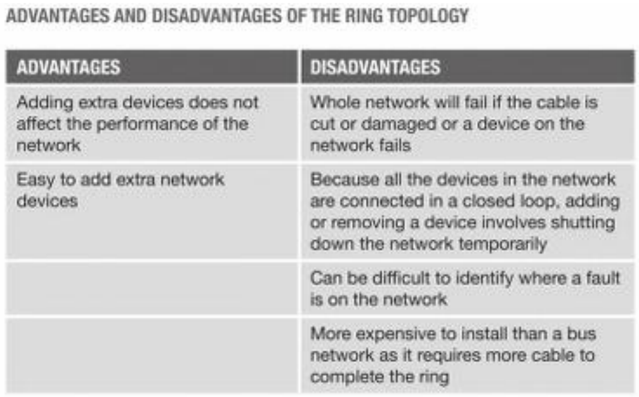
ADVANTAGES	DISADVANTAGES
Relatively cheap to install since only one cable is needed	Whole network will fail if the cable is cut or damaged
Easy to add extra network devices	Can be difficult to identify where a fault is on the cable
	The more devices that are added to a bus network the slower they run. This is due to only one message being able to be sent at once and because more collisions happen
	All data sent is received by all devices on the network; this is a security risk

RING



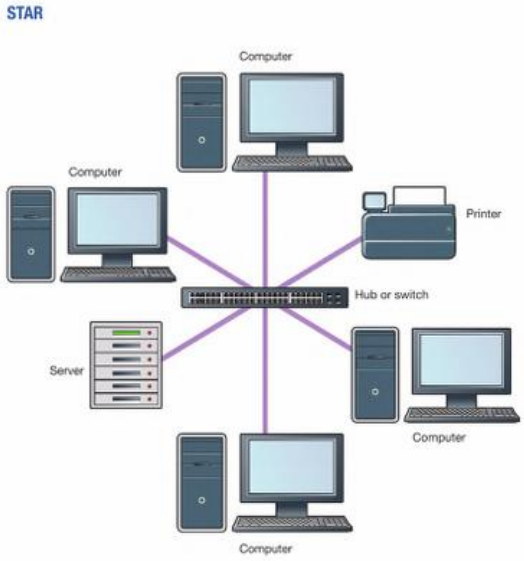
▶ Figure 5.3 Ring network topology

A ring network is a network in which the cable connects one network device to another in a closed loop, or ring. Each network device has what can be thought of as an 'in' and an 'out' connection.

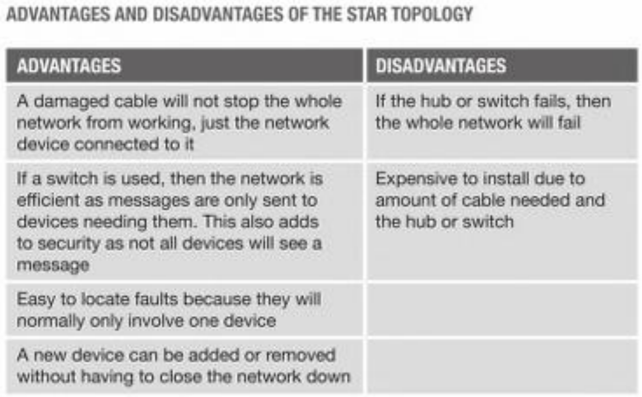


ADVANTAGES AND DISADVANTAGES OF THE RING TOPOLOGY

ADVANTAGES	DISADVANTAGES
Adding extra devices does not affect the performance of the network	Whole network will fail if the cable is cut or damaged or a device on the network fails
Easy to add extra network devices	Because all the devices in the network are connected in a closed loop, adding or removing a device involves shutting down the network temporarily
	Can be difficult to identify where a fault is on the network
	More expensive to install than a bus network as it requires more cable to complete the ring

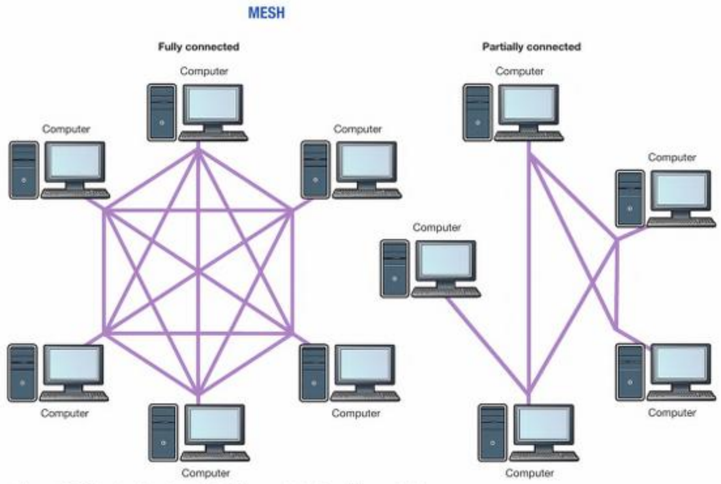


▶ Figure 5.4 Star network topology

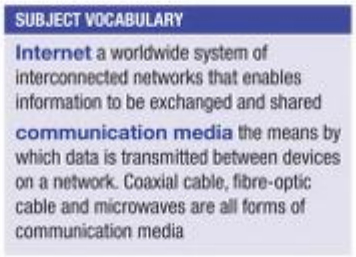


ADVANTAGES AND DISADVANTAGES OF THE STAR TOPOLOGY

ADVANTAGES	DISADVANTAGES
A damaged cable will not stop the whole network from working, just the network device connected to it	If the hub or switch fails, then the whole network will fail
If a switch is used, then the network is efficient as messages are only sent to devices needing them. This also adds to security as not all devices will see a message	Expensive to install due to amount of cable needed and the hub or switch
Easy to locate faults because they will normally only involve one device	
A new device can be added or removed without having to close the network down	



▲ Figure 5.5 Mesh network topology showing fully connected and partially connected types

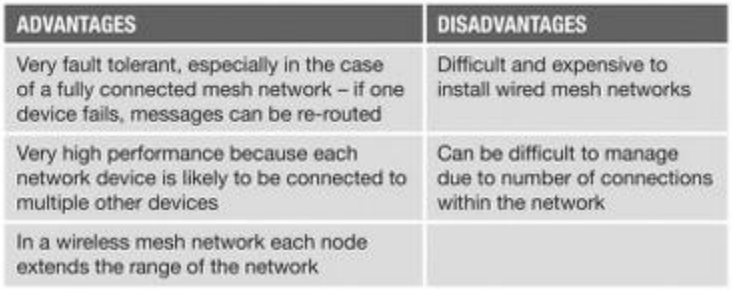


SUBJECT VOCABULARY

Internet a worldwide system of interconnected networks that enables information to be exchanged and shared

communication media the means by which data is transmitted between devices on a network. Coaxial cable, fibre-optic cable and microwaves are all forms of communication media

Mesh topology consists of fully connected and partially connected networks. Fully connected networks connect every device to every other, while partially connected networks have some devices connected to multiple devices. Mesh networks can be wired or wireless and are fault-tolerant. The **Internet** is the largest mesh network, used for communication between mobile sensors, as optimum network paths can be used regardless of the location of the sensor. Wireless mesh networks are less expensive and easier to implement.



ADVANTAGES	DISADVANTAGES
Very fault tolerant, especially in the case of a fully connected mesh network – if one device fails, messages can be re-routed	Difficult and expensive to install wired mesh networks
Very high performance because each network device is likely to be connected to multiple other devices	Can be difficult to manage due to number of connections within the network
In a wireless mesh network each node extends the range of the network	

Communication media

There are many different ways that computers can be connected together to form a network. Networks are either wired or wireless according to the transmission or **communication media** used.

WIRED

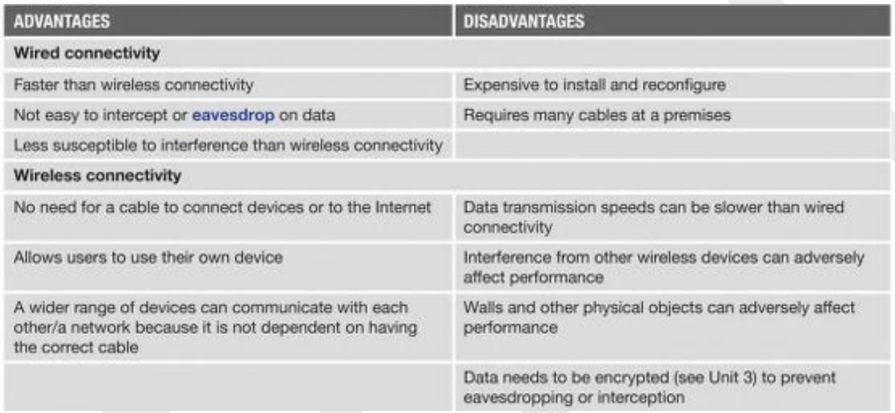
Wired connection methods involve a physical connection between the computer and the network. Most wired connections are made of copper wire. They could also be fibre-optic cable, which is made of either glass or plastic. Copper wire carries electrical signals, while fibre-optic cable carries light signals.

WIRELESS

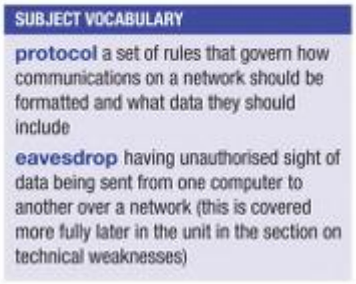
Wireless connectivity does not require a physical connection between devices. Most wireless connections transmit and receive radio signals, but other connection methods such as infra-red light can be used over limited distances.

WIRED OR WIRELESS CONNECTIVITY?

There are advantages and disadvantages to wired and wireless connection methods.



ADVANTAGES	DISADVANTAGES
Wired connectivity	
Faster than wireless connectivity	Expensive to install and reconfigure
Not easy to intercept or **eavesdrop** on data	Requires many cables at a premises
Less susceptible to interference than wireless connectivity	
Wireless connectivity	
No need for a cable to connect devices or to the Internet	Data transmission speeds can be slower than wired connectivity
Allows users to use their own device	Interference from other wireless devices can adversely affect performance
A wider range of devices can communicate with each other/a network because it is not dependent on having the correct cable	Walls and other physical objects can adversely affect performance
	Data needs to be encrypted (see Unit 3) to prevent eavesdropping or interception



SUBJECT VOCABULARY

protocol a set of rules that govern how communications on a network should be formatted and what data they should include

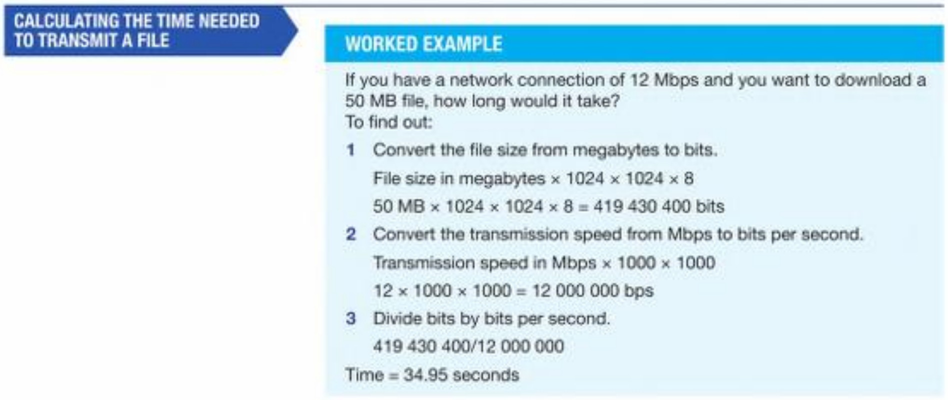
eavesdrop having unauthorised sight of data being sent from one computer to another over a network (this is covered more fully later in the unit in the section on technical weaknesses)

Networks data speed

Being able to measure the speed of a network allows you to:

- discover whether an equipment upgrade is necessary
- estimate how long it will take to download a file
- discover whether actual performance lives up to the promises made by the service provider.

The speed that data can be transmitted through a communications medium is measured in bits per second (this can shorten to bps, b/s or bit/s). Modern high-speed networks can transmit billions of bits per second.



CALCULATING THE TIME NEEDED TO TRANSMIT A FILE

WORKED EXAMPLE

If you have a network connection of 12 Mbps and you want to download a 50 MB file, how long would it take?

To find out:

1 Convert the file size from megabytes to bits.

File size in megabytes × 1024 × 1024 × 8

50 MB × 1024 × 1024 × 8 = 419 430 400 bits

2 Convert the transmission speed from Mbps to bits per second.

Transmission speed in Mbps × 1000 × 1000

12 × 1000 × 1000 = 12 000 000 bps

3 Divide bits by bits per second.

419 430 400/12 000 000

Time = 34.95 seconds

The amount of data that can be carried from one point to another on a network in a given period of time is referred to as its bandwidth. Bandwidth is usually expressed as bits per second (bps). Another important factor is the latency of the network connection. **Latency** refers to any kind of delay that data travelling through a network might encounter.

Protocols

In relation to computer systems and networks, a protocol is a set of rules that control how communications between devices are formatted and how these communications will be sent/received. Without protocols, different computers and other hardware wouldn't be able to communicate with each other because they would essentially be speaking different languages.

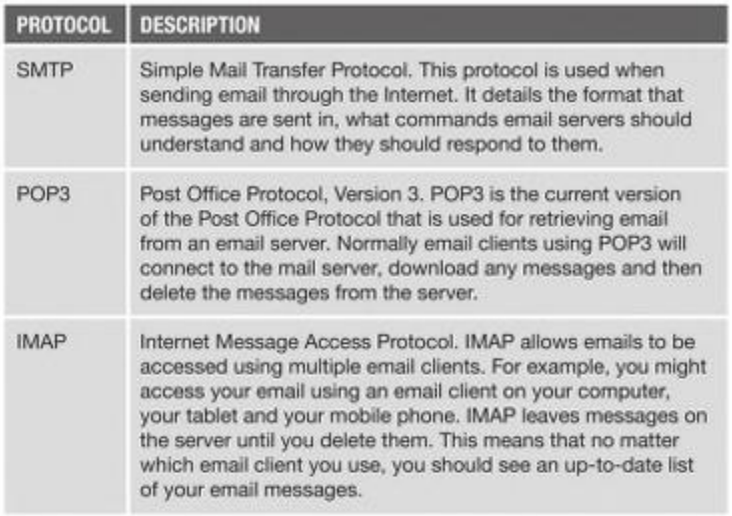
A protocol might contain details of:

- how each computer will be identified (its address)
- what route the data will take to get to its destination (routing information)
- how errors will be found and dealt with (error checking)
- whether each part of a message should be acknowledged as received correctly
- what to do if data isn't received correctly
- how the data is to be formatted
- how the data is to be sequenced (i.e. does it need to be sent in order or
- can it be put in its correct order later?)
- how the speed of the sender and receiver can be synchronised.

There are many different protocols for different purposes. The main ones in use relating to networks and the Internet are detailed below.

EMAIL PROTOCOLS

Emails are sent and received using a set of standard protocols. This means that when you send an email it doesn't matter what email provider the recipient uses or what type of computer system they have.
There are three main email protocols in use.



PROTOCOL	DESCRIPTION
SMTP	Simple Mail Transfer Protocol. This protocol is used when sending email through the Internet. It details the format that messages are sent in, what commands email servers should understand and how they should respond to them.
POP3	Post Office Protocol, Version 3. POP3 is the current version of the Post Office Protocol that is used for retrieving email from an email server. Normally email clients using POP3 will connect to the mail server, download any messages and then delete the messages from the server.
IMAP	Internet Message Access Protocol. IMAP allows emails to be accessed using multiple email clients. For example, you might access your email using an email client on your computer, your tablet and your mobile phone. IMAP leaves messages on the server until you delete them. This means that no matter which email client you use, you should see an up-to-date list of your email messages.

NETWORK PROTOCOLS

ETHERNET

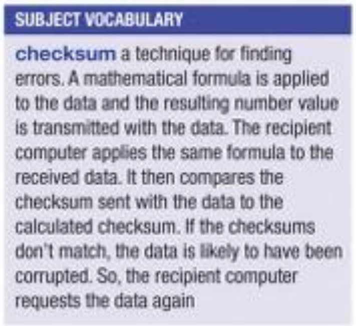
Ethernet is a family of protocols that are used in wired LANs. They cover everything from the physical parts of a network, such as type of cable or optical fibre and type of connector to be used, to the logical parts, such as how data is sent and checked for errors and the speed that data can be transmitted.

WI-FI

Wi-Fi is a digital communications protocol that sets out how data is transmitted on wireless LANs. Wi-Fi is a trademarked term that is owned by Wi-Fi Alliance.

TCP

The Transmission Control Protocol provides a reliable connection between computers. Here, 'reliable' means that the receiving computer can be certain that it has received all the data it should have (none of it is missing) and the data received is identical to the data sent (the data is correct).



SUBJECT VOCABULARY

checksum a technique for finding errors. A mathematical formula is applied to the data and the resulting number value is transmitted with the data. The recipient computer applies the same formula to the received data. It then compares the checksum sent with the data to the calculated checksum. If the checksums don't match, the data is likely to have been corrupted. So, the recipient computer requests the data again

TCP does this by:

■specifying that the receiving computer sends acknowledgements that each section of the data sent has been received

■using checksums to ensure that the data received is accurate

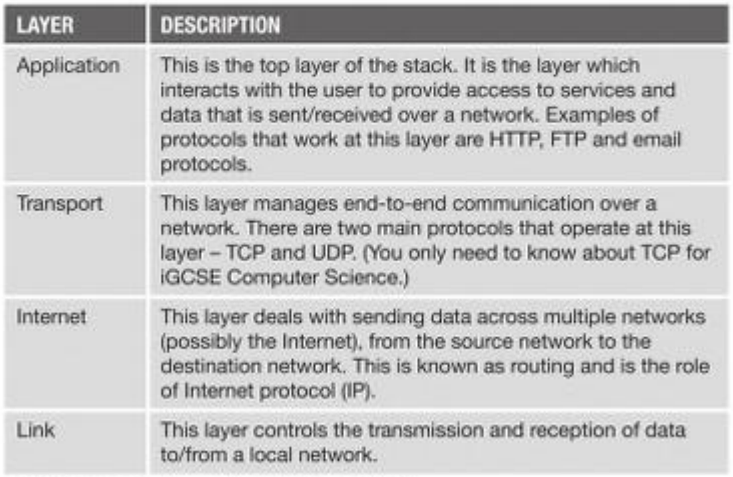
■allowing the receiving computer to tell the sending computer to slow down transmission. This means the receiving computer has time to process the received data (this is called flow control)

■ensuring that data sent up to the application layer contains no duplicates and is in the correct order.

TCP is used when you access web pages, send/receive email or upload/ download files.

TCP/IP

TCP/IP stands for Transmission Control Protocol/Internet Protocol. TCP/IP is a protocol stack, which means that it is a collection of protocols that work together. It is named after the two most important protocols used in the stack.



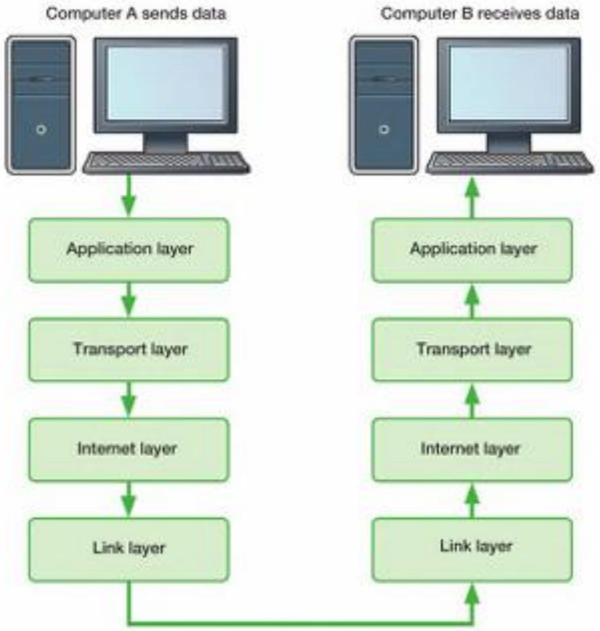
LAYER	DESCRIPTION
Application	This is the top layer of the stack. It is the layer which interacts with the user to provide access to services and data that is sent/received over a network. Examples of protocols that work at this layer are HTTP, FTP and email protocols.
Transport	This layer manages end-to-end communication over a network. There are two main protocols that operate at this layer – TCP and UDP. (You only need to know about TCP for iGCSE Computer Science.)
Internet	This layer deals with sending data across multiple networks (possibly the Internet), from the source network to the destination network. This is known as routing and is the role of Internet protocol (IP).
Link	This layer controls the transmission and reception of data to/from a local network.

▲ Table 5.1 The four layers of the TCP/IP protocol stack

Data sent using TCP/IP is broken up into packets. Each packet of data consists of a small section of the data being sent along with a packet header. A packet header contains details of:

- the sending computer
- the recipient computer
- how many packets the data has been split into
- the number of this particular packet.

Once the recipient computer receives all the packets, it will use the information in the header to reconstruct the data into its original format.



▶ Figure 5.6 Layers within the TCP/IP suite pass data down the stack when sending and back up the stack when receiving

DID YOU KNOW?
You will sometimes see TCP/IP described as a 'protocol suite' rather than a 'protocol stack'. These two terms are often used as if they are the same. However, some sources state that the suite is the definition of the protocols and that stack is the software implementation of the protocols.

HTTP

The HyperText Transfer Protocol (HTTP) is used when sending and receiving data between web browsers and web servers. The HTTP protocol covers how data should be formatted, what commands the web server and web browser should understand and how they should react to each command.

HTTPS

The HyperText Transfer Protocol Secure (HTTPS) is the secure version of HTTP. This means that the data sent between your web browser and the web server is encrypted. It should prevent the data being sent/received from being read by a third party. HTTPS also helps the web browser and user know that they are communicating with the intended web server rather than a fake that is trying to steal sensitive data, such as passwords or bank details.

FTP

File Transfer Protocol is used to transfer files over a network that uses the TCP protocol (see above), such as the Internet.

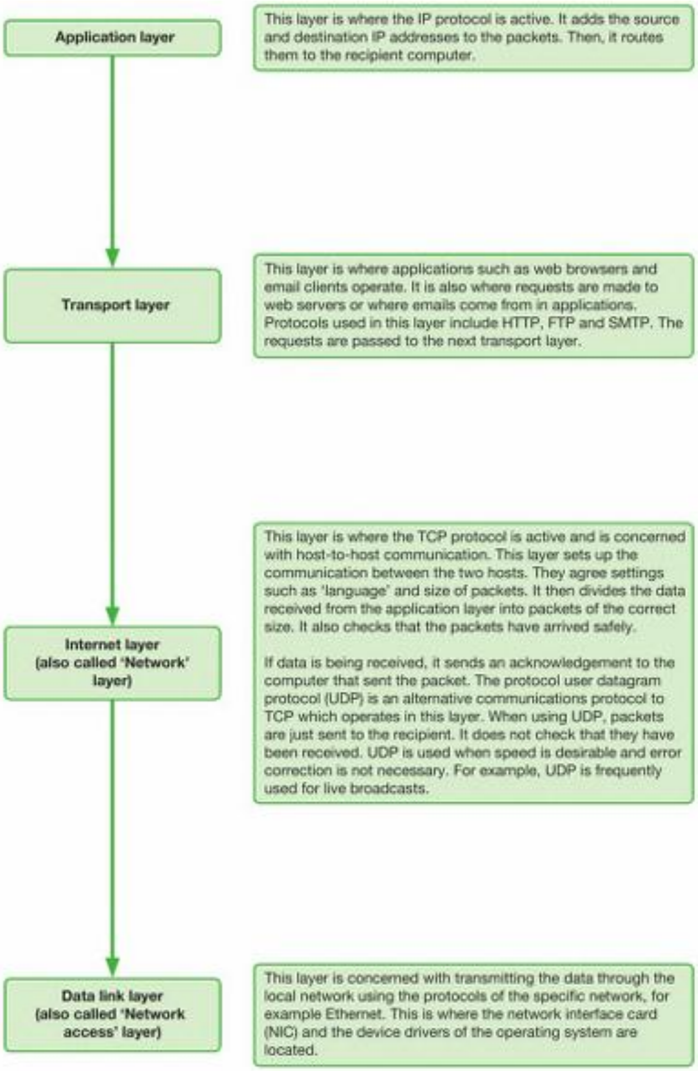
FTP is often used when sending web pages and other associated files that have been created on a web developer's computer to the web server. Once the files are on the web server, other computers connected to the Internet will be able to view them.

INTERNET PROTOCOLS

At the Internet layer, the Internet Protocol (IP) deals with:

- the addressing system to identify individual computers/servers on the network (usually the Internet)
- splitting data into packets and adding the packet header with details such as the sender/receiver addresses.

Each device linked directly to the Internet has a unique IP address assigned to it to allow data to be routed to it.



Application layer

This layer is where the IP protocol is active. It adds the source and destination IP addresses to the packets. Then, it routes them to the recipient computer.

Transport layer

This layer is where applications such as web browsers and email clients operate. It is also where requests are made to web servers or where emails come from in applications. Protocols used in this layer include HTTP, FTP and SMTP. The requests are passed to the next transport layer.

Internet layer (also called 'Network' layer)

This layer is where the TCP protocol is active and is concerned with host-to-host communication. This layer sets up the communication between the two hosts. They agree settings such as 'language' and size of packets. It then divides the data received from the application layer into packets of the correct size. It also checks that the packets have arrived safely.

If data is being received, it sends an acknowledgement to the computer that sent the packet. The protocol user datagram protocol (UDP) is an alternative communications protocol to TCP which operates in this layer. When using UDP, packets are just sent to the recipient. It does not check that they have been received. UDP is used when speed is desirable and error correction is not necessary. For example, UDP is frequently used for live broadcasts.

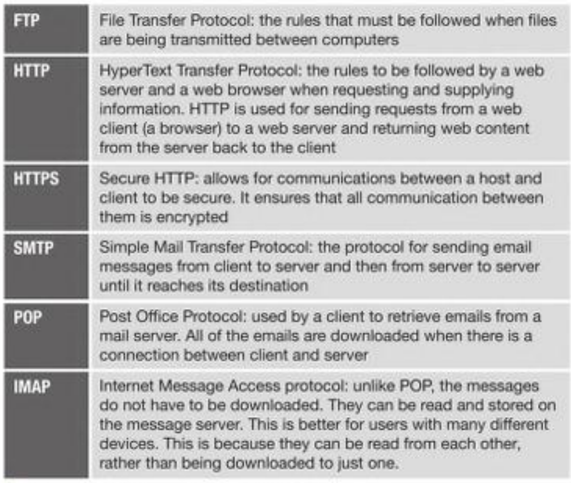
Data link layer (also called 'Network access' layer)

This layer is concerned with transmitting the data through the local network using the protocols of the specific network, for example Ethernet. This is where the network interface card (NIC) and the device drivers of the operating system are located.

▲ Figure 5.7 The 4-layer TCP/IP model

PROTOCOLS OF THE APPLICATION LAYER

Table 5.2 shows some of the protocols of the application layer.



FTP	File Transfer Protocol: the rules that must be followed when files are being transmitted between computers
HTTP	HyperText Transfer Protocol: the rules to be followed by a web server and a web browser when requesting and supplying information. HTTP is used for sending requests from a web client (a browser) to a web server and returning web content from the server back to the client
HTTPS	Secure HTTP: allows for communications between a host and client to be secure. It ensures that all communication between them is encrypted
SMTP	Simple Mail Transfer Protocol: the protocol for sending email messages from client to server and then from server to server until it reaches its destination
POP	Post Office Protocol: used by a client to retrieve emails from a mail server. All of the emails are downloaded when there is a connection between client and server
IMAP	Internet Message Access protocol: unlike POP, the messages do not have to be downloaded. They can be read and stored on the message server. This is better for users with many different devices. This is because they can be read from each other, rather than being downloaded to just one.

▲ Table 5.2 Some of the protocols of the application layer

Benefits of using networking layers

Networking technologies are separated into layers, each one containing specific hardware and software protocols. Each layer performs specific tasks and interacts with the adjacent layers in the 'network model'.
The benefits of this approach are:

■It makes the overall model easier to understand by dividing it into functional parts.
■Each layer is specialised to perform a particular function.
■The different layers can be combined in different ways.
■One layer can be developed or changed without affecting the other layers.
■It makes it easier to identify and correct networking errors and problems.
■It provides a universal standard for hardware and software manufacturers to follow. This is so that they will be able to communicate with each other.

Mobile communication

A mobile network is a wireless network distributed through cells with base stations, providing coverage over 9-21 miles. Handover occurs when a user moves out of range, and the European Telecommunications Standards Institute developed the Global System for Mobile Communications (GSM) to describe protocols. Generations include 2G, 3G, 4G, and 5G.

■2G was the first to use digital communications. It enabled text messages to be sent and introduced a multimedia messaging service (MMS).

■3G increased data transmission speeds to 2mbit/s. This gave wireless access to the Internet, so it enabled video calls and downloading and streaming. □ 4G provided much higher speeds and gave rise to the popularity of mobile gaming. A film that would have taken more than five hours to download on 3G could take less than eight minutes!

■4G has a much higher capacity, meaning it can support a greater number of users at the same time. It also gives a more immediate response to a user's commands, useful when playing online games.

■3G and 4G both use IP-based protocols for data but 4G also uses IP, even for voice calls.

■The new generation, 5G, is smarter, faster and more efficient than 4G. It achieves peak speeds of 100 Gbps, 100 times faster than 4G and faster than most home broadband networks. It also has a far lower latency than 4G. 5G will be able to handle current devices and emerging technologies, such as driverless cars and connected home products.

Chapter 22 – network security

Network security and its importance

Network security covers a wide range of activities that protect data from threats to its confidentiality, correctness (integrity) and availability.

CONFIDENTIALITY

An organisation's computer system often holds data about its people (employees and customers), It is important (and in the case of personal data, the law) that the network is not hacked so data is not intercepted or stolen by criminals or competitors who might use the data for illegal purposes or business advantage.

Some ways to protect data confidentiality include:

- ensuring only authorised users can access the parts of a network and its resources that they have a reason to require, such as its storage (data), printers or Internet connection.
- stopping misuse - even users who have been given permission to access a network might deliberately or accidentally access data they have not been given permission to read
- encrypting data - if a criminal or other unauthorised person gains access to data and it is encrypted, they won't be able to read it without the encryption key.

CORRECTNESS

Data is useless unless it is correct. Use of the network to communicate and store data must not change the data or allow the data to be changed without authorisation. Imagine the seriousness of an error on your health records or in a manufacturing control system.

AVAILABILITY

A network is useless if data cannot be accessed when it is needed. Complex systems are likely to fail at some time (e.g. a piece of hardware might stop working and have to be replaced, or program code might become corrupted), but it is also important that protection is put in place to prevent failures caused by criminals. Virus or **denial of service (DoS)** attacks can, for example:

- slow down network performance or stop it working altogether
- delete data
- allow data to be stolen or eavesdropped on
- alter data or program code.

Reasons why security is important?

Here are some more specific examples of the importance of network security. The data stored on the network could be:

■required for the running of the organisation - The business might have details of its customers, stock and outstanding orders saved on the network. If the data were lost and the business failed to fulfil any remaining

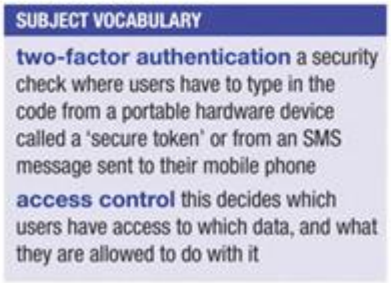
orders, this could mean losing the trust of customers who then go elsewhere. This could lead to the business going bankrupt. This has happened to a number of businesses, some of them very large.
Even a school would struggle to run effectively without its network and the data stored on it

■private and confidential - There are many types of private and confidential data that people or businesses wouldn't want to make public.

■financially valuable - Many types of data stored on business networks might be financially valuable. For example, imagine a business was planning a huge sale to increase its revenue and attract new customers. If a competitor obtained the details of the planned price reductions before the sale started, it could launch its own sale beforehand. It would undercut the business. This tactic would reduce the chance of the sale increasing revenue or attracting new customers.

Authentication and validation

Authentication is the process of checking the identity of a user of a computer system or network. This is often done by validating a username and password against details stored on a central server.



SUBJECT VOCABULARY

two-factor authentication a security check where users have to type in the code from a portable hardware device called a 'secure token' or from an SMS message sent to their mobile phone

access control this decides which users have access to which data, and what they are allowed to do with it

Other ways to secure a networks

ACCESS CONTROL

Once a user has been authenticated, they gain access to the network; however, you wouldn't want every user on a network to have access to every file. **Access control** is the method that controls whether a particular user will gain access to a particular file. Access control also decides if that user gets:

■read-only access-in this case, the user can open the file and read its contents, but not modify the contents or delete the file

■read and write access (modify access) - in this case, the user can read the file, alter the contents and then save the changes.

In some network systems you might need further permission if you want to delete a file - this is sometimes referred to as full control of the file.

FIREWALL

A firewall is a network security system that monitors and controls data that is moving from one network to another. Often one of these networks is the Internet, in which case the firewall sits between the Internet and the local internal network.

The organisation that owns the firewall can customise the rules so that the firewall is suitable for their particular circumstances. Some examples of what the rules can do:

- stop certain protocols from being used (for example FTP) to prevent the organisation's data from being potentially copied to an external server block data coming from or going to certain network addresses.

- The blocked addresses could be of particular computers, servers or websites, or even a range of network addresses that belong to particular countries or organisations

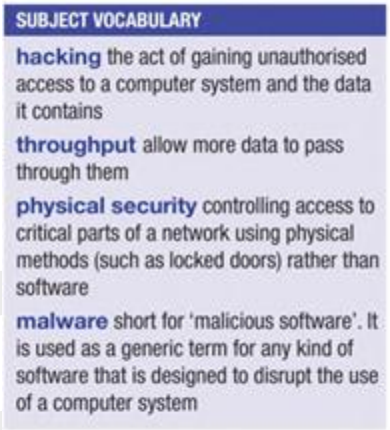
- stop attempts at **hacking** the internal network's servers by disallowing data that matches the pattern an attacker would use.

A business with a LAN and Internet connection is likely to have a hardware- based firewall. This is because these have much more flexibility in terms of the rules that can be applied and allow faster **throughput** of data.

PHYSICAL SECURITY

Physical security ensures that critical parts of the network can only be physically accessed by authorised people, such as the network technicians or a systems administrator. It also includes protecting against theft of equipment. It might involve installing a burglar alarm, security tagging and physically locking down equipment, etc.

Having done so they could copy, modify or delete any data on the network, or install **malware** that would allow them to gain remote access whenever they wanted.



SUBJECT VOCABULARY

hacking the act of gaining unauthorised access to a computer system and the data it contains

throughput allow more data to pass through them

physical security controlling access to critical parts of a network using physical methods (such as locked doors) rather than software

malware short for 'malicious software'. It is used as a generic term for any kind of software that is designed to disrupt the use of a computer system

Cloud storage and security

Many of the advantages of cloud storage relate to securing the availability of data.

■The cloud storage provider is responsible for the hardware your data is stored on. They will need to ensure that the data is accessible and that they maintain the hardware and software needed to make the data available.

■The amount of storage available to an organisation can easily be changed as and when required - the cloud storage provider can normally make extra storage available in minutes. Doing this physically would mean ordering more hard drives and employing technicians to install them and set them up. This would take a lot longer than a few minutes.

■ Having data stored off-site (not on the organisation's premises) means that it is protected from loss due to fire, theft of computers/servers, electrical failure, and so on. As the data is still available the business may be carried on from elsewhere. This could be the difference between staying in business or going bankrupt.

■Many cloud storage systems also manage the back-up of your data. They may take hourly or daily snapshots of your data and be able to restore from these in the case of hardware failure or accidental deletion of files.

However, cloud storage also has a number of security disadvantages.

■You are relying on a third-party storage provider to keep your organisation running.

■Data stored anywhere accessible via the Internet carries the risk of other people gaining access to it. This might happen through a deliberate attack by hackers, or as a result of an accidental error in the way it is set up that results in the data becoming available to the public.

■ Users of cloud storage have to assume that the people providing the service are trustworthy and that their data is being held safely and securely.

■The cloud storage provider might have its servers located in a different country (or countries) to your organisation. Some types of data can only legally be stored in countries that have similar data protection laws to our own.

■ Access to cloud storage is dependent on having a reliable, high-speed Internet connection available. How will a business operate if the Internet becomes unavailable for some reason?

The decision to use cloud storage involves carefully weighing up the advantages against the disadvantages. Many of the disadvantages present risks to the operations of an organisation, but the impact of some of these risks can be reduced.

Contemporary storage and security

NAS devices often include a wide range of additional features, such as allowing access over the Internet, and specialist apps to allow smartphones and tablets to access the files stored on the NAS easily.

Often NAS devices are designed for ease of use rather than being secure. Once a NAS is connected to the Internet it becomes possible for it to be hacked remotely. Home users often make mistakes such as:

- not changing a device's default password. This gives access to the stored files to anyone who looks up the default password on the Internet

- not updating the software running on the NAS. Manufacturers tend to release updated software to fix security weaknesses as they are found. If the software isn't kept up to date, these weaknesses might be used to gain access to the stored data. The security weaknesses are often published on the Internet for criminals to read.

Another widely used storage device is the **USB** flash drive. USB flash drives are easy to transport, relatively cheap for the amount of storage available and very convenient to use.

The disadvantage is that people can carry large amounts of possibly sensitive information around with them on a small drive that is easily lost. Anyone can find a lost flash drive and access the information. To overcome this, encrypted USB flash drives are available.

Cyber-attack

A cyber-attack is any kind of electronic attack on a computer system, server, network or other IT device. These attacks might be designed to:

■gain access to data contained within the system
■delete or modify information
■make the system unavailable for use
■physically damage a device connected to the network (usually by overriding safety limits).

TYPES OF CYBER ATTACK

There are many different forms of cyber attack and these are constantly changing as technology evolves. Most cyber attacks can be classed as exploiting either human behaviour or technical weaknesses.

SOCIAL ENGINEERING

Attacks that rely on exploiting human behaviour are often referred to as social engineering. This is because the attacker will 'engineer' a situation where the target person (or group of people) gives away confidential information or gives access to the confidential information.
Three common forms of social engineering are phishing, shoulder surfing and pharming.

PHISHING

A phishing attack is an attempt to get sensitive, confidential information from the user of a computer system or service. Often the phishing attack is targeting usernames and passwords or financial details such as bank account or credit card details.

There are various forms of phishing. The most common types are through email or fake websites that look legitimate, but phishing can also happen via phone calls or instant messaging.

A typical phishing attack might start with an email that asks the user to update details at a bank, online payment system, online auction website or social network. Sometimes the reason given for this request is that there has been a fraud attempt on the user's account.

SHOULDER SURFING

Shoulder surfing means gaining access to confidential information by directly observing a user, possibly literally looking over their shoulder, as they complete a task. Often shoulder surfing is used to get a person's username/password or PIN..

PHARMING

To make it easier for us to use the Internet, domain names are used to represent IP addresses. These are translated back into the IP address by the domain name service (DNS) when we enter the name into a browser. If we have visited the site before, then this IP address will be stored on our computer (in the DNS cache).
To prevent pharming, users should:

- check that the http address of the site is the one you intended to visit check that there is a secure connection (https) if you have to enter
- sensitive information
- check the site's security certificate
- install the latest security updates install antivirus software.

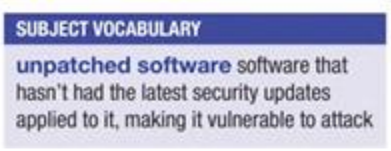
TECHNICAL WEAKNESSES

Other forms of cyber attack rely on technical weaknesses (vulnerabilities) in the system being attacked. Some common examples are described below.

UNPATCHED SOFTWARE

Software is very complicated and usually security issues are only found as it is used in the real world. The maker of the software will normally provide updates (referred to as patches) to fix security issues as they are found.

Often these security issues are discussed on the Internet. Some people will use this knowledge to attack **unpatched software** to gain unauthorised access to information.



SUBJECT VOCABULARY

unpatched software software that hasn't had the latest security updates applied to it, making it vulnerable to attack

USB DEVICES

You read earlier about the weaknesses associated with USB flash drives, but any USB device can potentially be a security threat because it might contain malware that could be transferred to your system or copy data to the attacker via the Internet.

EAVESDROPPING

One form of attack mentioned earlier is an eavesdropping attack. In computer security terminology, eavesdropping means intercepting data being sent to/from another computer system. In a similar way that a person can eavesdrop on a conversation without the speakers knowing about it, eavesdropping on a network is simply reading data without actually copying or stealing it. The owner of the data might not know that the data has been read until it is used by the criminal. Security weaknesses such as unpatched software or a USB device might allow malware to be installed on the network that allows an eavesdropping attack to be carried out, but specialised hardware might also be used.

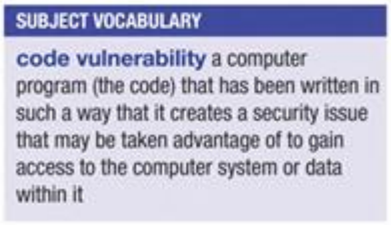
Protecting against security weakness

There are many ways to strengthen computer systems and networks from attacks, starting from when software is designed and written, to deciding on what kind of operating system should be used and how network security provision will be implemented.

DESIGN AND IMPLEMENTATION OF SOFTWARE

Security must be considered at the system and software or application design stage if a piece of software is to be as safe as possible against cyber attack. It should be a key concern when the system is being set up.

Another major issue is that some methods used in programming might lead to **code vulnerabilities**. A code vulnerability is when the code does the task intended but has been written in such a way that it creates a potential security issue.



SUBJECT VOCABULARY

code vulnerability a computer program (the code) that has been written in such a way that it creates a security issue that may be taken advantage of to gain access to the computer system or data within it

Issues like these can be minimised by having regular code reviews. There are two main types of code review.

■Review by another programmer, usually someone who is more senior and has more experience of writing secure code. The reviewer will look at the code produced. They will check to see if any bad programming practices have been used or if any code vulnerabilities are present. This is fairly labour intensive and therefore expensive.

■An automated review. Here, a specialist piece of software is used to examine the code. The software will highlight potential issues such as common vulnerabilities in the programming language or obvious bad programming practice. This software can't find every issue and is also fairly expensive.

Sometimes a combination of both types will be used. If issues are found, then the original programmer will be asked to improve the code and another code review will be scheduled.

■Modular testing is important to security because if small problems remain, they might be used by hackers to gain access to the system or the data it contains. For example, failing to validate input correctly could lead to a hacker being able to crash the program. They could then gain access to the whole system, which could allow valuable data to be obtained.

Other security measure to protect from cyber attacks

Here are some other methods to reduce the chance of cyber attacks succeeding.

- Use an audit trail. An audit trail is a record of activities that have taken place on a computer system, and which cannot be changed. The audit trail is automatically generated and likely to be in chronological order. Ordinary users of a system shouldn't be able to read an audit trail.

- Use secure operating systems. Different operating systems are designed for different purposes. Some are designed with security in mind and these are likely to be much harder to attack successfully. This is due to the way they have been written and the features they offer.

- Provide effective network security. Keeping a network secure requires effective management, monitoring and training of its users.

Identifying vulnerabilities

Ethical hacking is the branch of computer science that relates to cybersecurity and preventing cyber attacks from being successful. Ethical hacking is essentially 'good' hacking - it is looking for weaknesses in software and systems so that they can be improved - while hacking is seen as 'bad' if someone is trying to gain access to a system to steal data or cause damage.

PENETRATION TESTING

Penetration testing (often shortened to 'pen testing') is where the IT systems of an organisation are deliberately attacked to find any weaknesses. These attacks are authorised by the organisation and are therefore legal. The attacks might be run by employees of the organisation or by a business that has been contracted to run the tests.

COMMERCIAL ANALYSIS TOOLS

It is possible to use software tools to scan a system for vulnerabilities. These commercial analysis tools or vulnerability scanners can be either purchased or hired. The tools look for common issues and alert the user to them.
These tools can only identify already known vulnerabilities and must be kept up to date to be effective. They can be used to scan the network from within (internally) or from outside (externally). Both of these scans can be valuable.

REVIEWS OF NETWORK AND USER POLICIES

All networks should have written policies that document:

- who is authorised to carry out various activities on the network
- how and when patches to software should be applied
- access controls
- password requirements, including how complex passwords should be and how often they should be changed
- how security is set up and maintained on the network
- what data audit trails should collect and how long they should be kept for
- anything else relevant to the security and maintenance of the network.

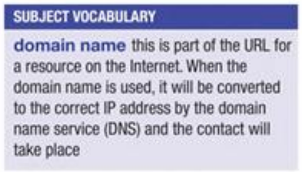
This user policy is likely to contain details of:

■what use of the network is allowed or not allowed

■what will happen to the user if they do something unacceptable (depending on the severity of what they do wrong, this could include losing their job)

■how to report faults, problems and security issues

■security information, such as good practice when choosing and using passwords.



SUBJECT VOCABULARY

domain name this is part of the URL for a resource on the Internet. When the domain name is used, it will be converted to the correct IP address by the domain name service (DNS) and the contact will take place

Chapter 23- The internet

The internet

The word 'Internet' is a shortened form of the words 'inter' and 'network', which together means 'interconnected networks'. It's a good idea to think of the Internet as a network of networks (i.e. the biggest WAN of all). Your school, many organisations and many people's homes all have a network that is a part of the Internet.

HOW THE INTERNET WORKS

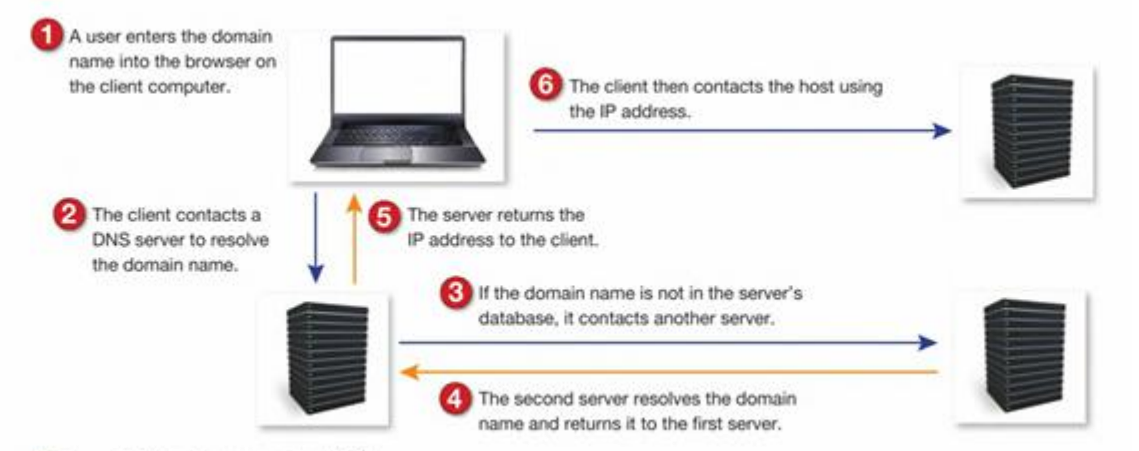
DOMAIN NAMES

Domain names are used to identify one or more IP addresses. They are more convenient to use and easier to remember than the four octets of binary numbers. For example, the IP address of bbc.co.uk is 212.58.244.27.

DOMAIN NAME SERVICE (DNS)

This is an Internet service that translates domain names into IP addresses. Because domain names are alphabetical, they're easier to remember. The Internet, however, is based on IP addresses.

Every time a user enters a domain name, a domain name service (DNS) must translate the name into the corresponding IP address. The DNS system is a network of servers. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned to the user.


1 A user enters the domain name into the browser on the client computer.
6 The client then contacts the host using the IP address.
2 The client contacts a DNS server to resolve the domain name.
5 The server returns the IP address to the client.
3 If the domain name is not in the server's database, it contacts another server.
4 The second server resolves the domain name and returns it to the first server.

▲ Figure 5.8 Domain name service (DNS)

Your computer or network is likely to be connected to the Internet using an **Internet service provider (ISP**). An ISP is an organisation that provides Internet connections. This connection to the Internet can be provided in a number of ways, but the most common is through telephone lines.

A **router** is a piece of networking hardware that forwards packets between networks. A router has a routing table that is essentially a list of rules stating where to send packets for different destinations.

When an Internet-connected computer wants to send data to another whose IP address it already knows the following happens.

1 The sending computer splits the data into packets.

2 Each packet has a header that contains the sender's address, the destination address, the current packet number and the total number of packets that make up the data.

3 Each packet is sent to your ISP.

4 Your ISP will have a router. This router will inspect the packet header and decide where to send the packet depending on its destination IP address.

5 The packet is likely to end up at another router, which will again look at the destination IP address and forward it on. This can happen many times before the packet reaches its destination network and intended recipient.

6 Once a packet reaches its destination, the receiving computer will put the data back together from the packets. Depending on the protocol being used, the packets might arrive in the wrong order and have to be put back in order using the information in the packet header.

The world wide web

ACCESSING THE WORLD WIDE WEB

You access the World Wide Web using a program called a web browser. There are many different web browsers to choose from, but they all use the same protocols and use the Internet to transfer information. The web browser's job is to convert the data received from a web server to a human-readable format.

HOW THE WORLD WIDE WEB WORKS

The World Wide Web uses the Internet to transfer data from one computer system to another. The computer being used to access the World Wide Web connects to the Internet using an ISP and will be running a web browser. Getting a web page or other file using the World Wide Web involves a large number of steps that use different protocols and standards:

1. The user of a computer enters the web address of the information he or she wants to look at. A web address is also known as a URL (uniform resource locator). A URL may be for a web page or an individual file. For example, a URL could be just for a particular picture file rather than a web page.

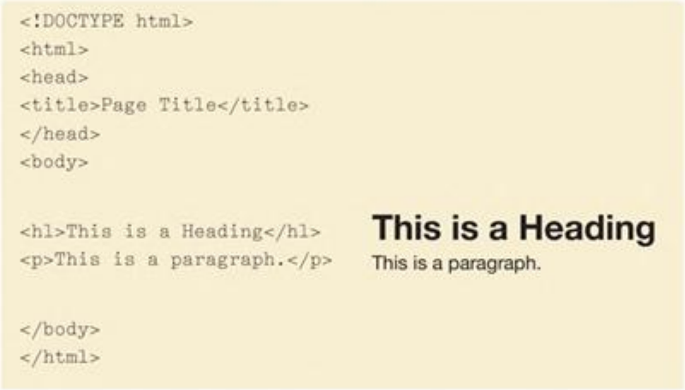
2. The computer uses a system called the domain name service (DNS) to find the IP address of the required web server.

3. The web browser connects to the web server using the IP address and requests the relevant web page or other object (picture, sound or video file).

4. A web page is transferred from one computer (normally a web server) to another using HTTP or HTTPS, which were covered in 'Network protocols' earlier in the unit.

5. Data sent from a web server to a web browser is in HyperText Markup Language (HTML) format. The web browser displays the web page as described by the HTML.

▶ **Figure 5.9** How a web browser display of a web page is generated from HTML



```
<!DOCTYPE html>
<html>
<head>
<title>Page Title</title>
</head>
<body>

<h1>This is a Heading</h1>
<p>This is a paragraph.</p>

</body>
</html>
```

This is a Heading

This is a paragraph.

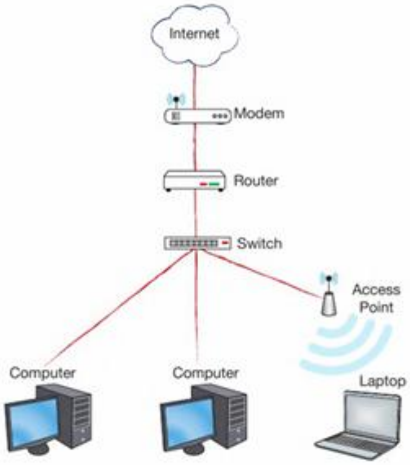
The need for IP addressing starts

An IP address is a set of numbers that are used to identify one particular computer.
The IP address is like a postal address. It allows Internet data and messages to be sent to the correct computer. It is therefore essential that they all conform to the same standard.

Components need to access the internet

Devices are needed to connect to a local area network (LAN) and that LAN to a wide area network (WAN) such as the Internet. As mentioned previously, devices can connect to a LAN using either cables or wirelessly, using radio waves.

▶ **Figure 5.10** Devices allowing network users to connect to the Internet



SWITCH

A switch is used to link the computers. Cables from each computer feed into it and so messages can be transmitted from one to the other. Switches are 'intelligent. They can read the destination addresses and send them to only the intended computers rather than to all of them. They can do this because they build up a table of all of the addresses on the network. This cuts down on network traffic.

▶ **Figure 5.11** A switch

WIRELESS ACCESS POINT (WAP)

Wireless access points allow wireless devices to connect to a wired network using Wi-Fi. They convert data they receive through cables into a wireless signal and vice versa.

They are commonly used in public buildings to provide 'Internet hotspots". They are similar to switches but cannot direct messages to particular devices: they transmit them to all.

SUBJECT VOCABULARY

Wireless access point (WAP) a device that is used to connect one or more computers wirelessly to an existing physical wired network

modem short for 'modulator–demodulator'. It modulates and demodulates signals (i.e. converts them from digital to analogue and vice versa) sent from and received by a computer over a communications network

▶ **Figure 5.12** A wireless access point (WAP)

ROUTER

Routers are similar to switches because they read the address information, but they transmit the messages between networks.

A switch does this within a single network, but a router does this across several networks. When you view a web page on a server in the United States, the data is transferred from router to router, until it reaches your network. All in less than a second!

▶ **Figure 5.13** A router

MODEM

A modem is needed to convert the signals in a LAN, such as a home network, into signals that can be transmitted along the cables provided by the Internet Service Provider (ISP).
The type of modem required will depend on the type of cable to the ISP, Le. it could be a copper telephone line or cable, carrying electrical signals, or a fibre-optic cable which carries the signals as light.

Revision questions

2023June
1). People use networks in all aspects of their lives.
(a) An office building has desktop computers connected in a network.
One reason for networking computers is to enable technicians to maintain them remotely.
State two other reasons for connecting computers in a network. (2)

(b) Access to data must be controlled.

(i) Identify one reason that encryption is used. (1)

- A To compress the file so it takes up less storage space
- B To make sure both sender and receiver use the same key
- C To make sure data is only understood by the intended receiver
- D To stop malicious hackers getting into a computer network

(ii) File servers are in a small room at the back of an office.
The office has a burglar alarm.
Give two other ways that the servers can be secured using physical methods. (2)

(iii) Phishing is a type of social engineering.
State what is meant by the term social engineering.(1)

(c) 5G is a communication standard.
Identify the characteristic that is true for the 5G communication standard. (1)

- A It has a high transmission latency
- B It has built-in security
- C It has a lower bandwidth than 3G and 4G
- D It uses wireless communication

2). Data packets travel across networks from one device to another.
(a) Identify the measurement of network speeds. (1)

- A Mebibits per second
- B Mebibytes per second
- C Megabits per second
- D Megabytes per second

(b) Data packets contain the addresses of the sender and the receiver.
Complete the table to give the number of bits that make up each type of network address. (2)

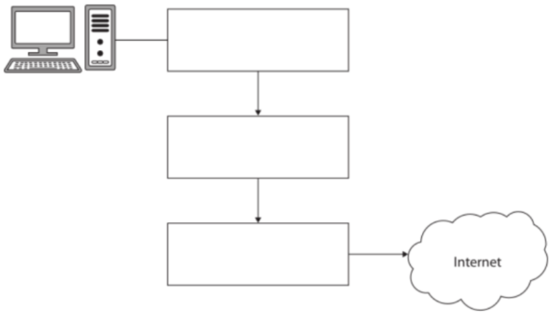
Type	Example	Number of bits
IPv4	192.169.0.3	
IPv6	1050:a500:00c0:0440:0006:0300:700d:436f	

(c) Data packets travel over physical media.

(i) Describe one difference between the media used by a wired network and a wireless network. (2)

(ii) Some people confuse Ethernet® and Wi-Fi.
Describe what is meant by the term Ethernet®. (2)

(d) A single physical box connects a desktop computer to the Internet.
The box incorporates three different components.
Complete the diagram to show the names of the components in the correct order. (3)



(e) Users enter passwords when logging onto a network and when creating accounts using a web page.
Describe one difference between validation and authentication. (2)

2022June

3).
(b) Alyssa uploads music files to her cloud storage.

(i) She compresses the files before she uploads them using a lossless algorithm.
Give **one** disadvantage of using a lossless rather than a lossy algorithm for this purpose. (1)

(ii) Explain **one** benefit to Alyssa of storing her music files in the cloud. (2)

(iii) Give **one** possible security issue associated with storing music files in the cloud. (1)

(iv) One of Alyssa's music files is stored at https://www.cloudisfab.com/re12/ru2.mp3
Complete the table by adding a description of each URL component. (4)

4). The health centre has clinics in two buildings: Cleveland and Stockton.
The network server is in the Cleveland building.

(i) Name the type of network used to access the server from within the Cleveland building. (1)

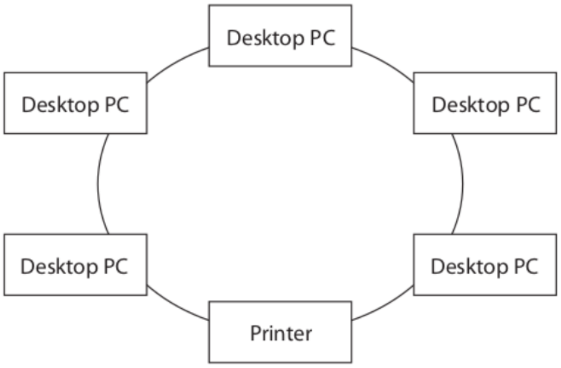
(ii) Name the type of network used to access the server from the Stockton building. (1)

(c) The network is at risk of an eavesdropping attack.

Identify the description of eavesdropping. (1)

- A Tricking people into giving information by sending emails pretending to be from someone in authority
- B Spying on someone using a computer
- C Intercepting information as it is transmitted over a network
- D Redirecting a user from a genuine website to a fake one

5). Santiago manages a computer network for a small business.
(a) Networks are based on a topology.
Figure 3 shows a network topology.



(i) Explain one benefit of this network topology. (2)

(ii) The internet is the world's largest mesh network.
Explain one reason why a mesh topology is essential for the internet. (2)

(b) Santiago works on his laptop whilst travelling by train.
There is a free Wi-Fi connection on the train, but Santiago doesn't use it.
He prefers to set up a network between his smartphone and his laptop to connect to the internet.

(i) Name this type of network. (1)

(ii) Explain one advantage for Santiago of using the network he has set up to connect to the internet, rather than the free Wi-Fi connection. (2)

(c) Santiago uses audit trails to help protect the network.
(i) State what is meant by an audit trail. (1)
(ii) Give one way the data from audit trails can be used to help keep the network secure. (1)

2021Nov

6).

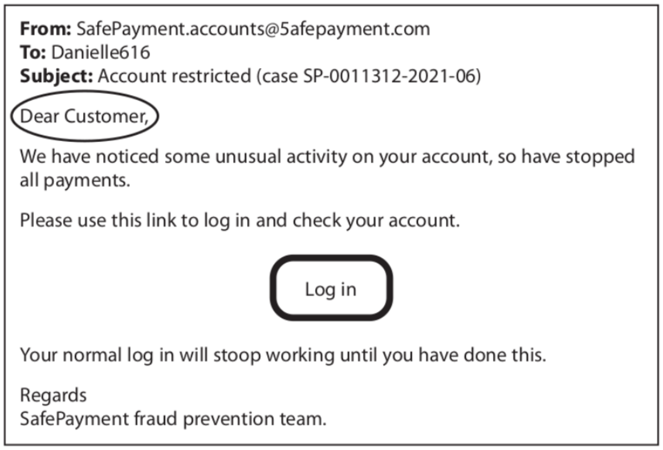
Danielle manages network security for a small business.

(a) Identify one action Danielle could take to protect the network from unauthorised access. (1)

- A Give each user a separate account
- B Enforce a strong password policy
- C Make a backup plan
- D Encrypt sensitive files

(b) Danielle has received this email.

She is a customer of SafePayment.com but thinks this is a phishing attempt.



From: SafePayment.accounts@5afepayment.com
To: Danielle616
Subject: Account restricted (case SP-0011312-2021-06)

Dear Customer,

We have noticed some unusual activity on your account, so have stopped all payments.

Please use this link to log in and check your account.

Log in

Your normal log in will stoop working until you have done this.

Regards
SafePayment fraud prevention team.

(i) Danielle has circled the words Dear Customer.

Give one reason why the use of these words might make Danielle suspect that the email is a phishing attempt.

(ii) Draw circles around two other aspects of the email that might make Danielle suspect it is a phishing attempt. (2)

(c) Some employees use company laptops in public places.

Danielle is concerned that shoulder surfing could pose a risk to security.

(i) Describe what is meant by shoulder surfing. (2)

(ii) Explain one way to prevent shoulder surfing. (2)

(d) Danielle wants to protect the network from cyberattacks.

(i) Identify the purpose of penetration testing.

- A To decompile executable code (1)
- B To identify security vulnerabilities
- C To test the strength of an encryption algorithm
- D To enforce a network user policy

(ii) Danielle is sent a software patch for the network operating system but is too busy to install it straight away.

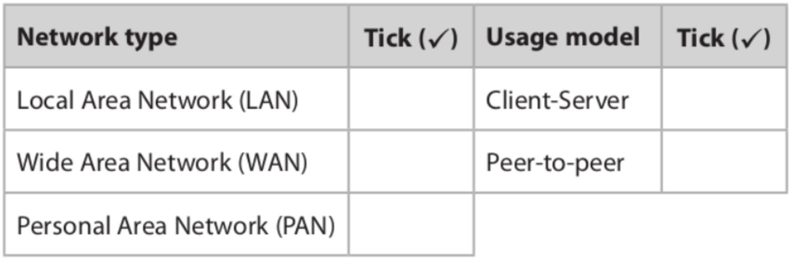
Explain why this delay could pose a threat to the security of the network. (2)

7).

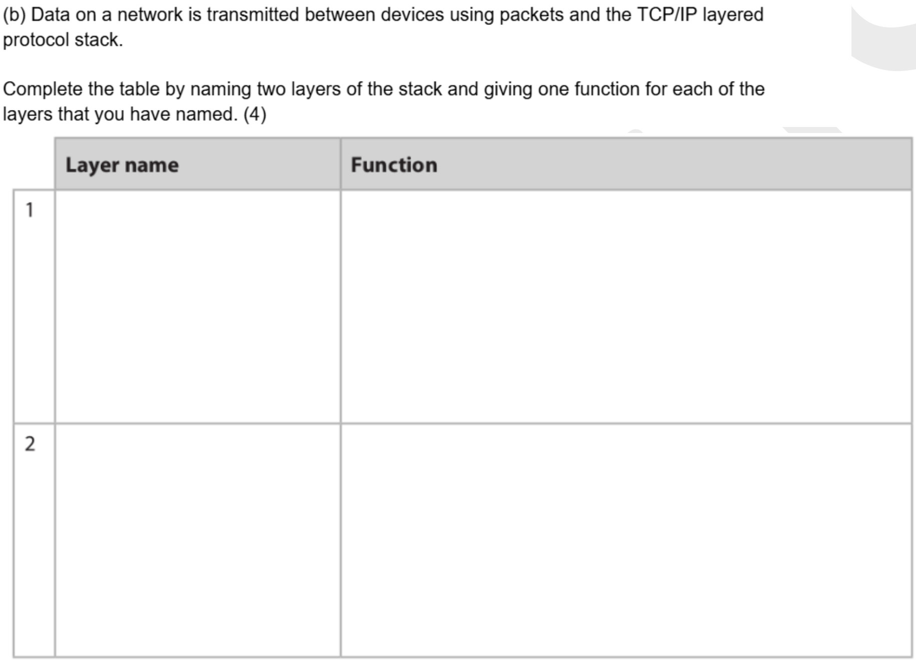
Carlo uses his smartphone to make hands-free calls from the car.

(a) The smartphone connects to the car wirelessly forming a network.

Complete the table by adding a tick (√) to indicate the network type and a tick (√) to indicate the usage model the network uses.



Network type	Tick (✓)	Usage model	Tick (✓)
Local Area Network (LAN)		Client-Server	
Wide Area Network (WAN)		Peer-to-peer	
Personal Area Network (PAN)			



(b) Data on a network is transmitted between devices using packets and the TCP/IP layered protocol stack.

Complete the table by naming two layers of the stack and giving one function for each of the layers that you have named. (4)

	Layer name	Function
1		
2		

(c) The smartphone can communicate using Wi-Fi.

Identify which one of these is a radio frequency used by smartphones to connect to Wi-Fi. (1)

- A 2.4 GHz
- B 3 KHz
- C 4.1 GHz
- D 5 KHz

(d) Carlo’s smartphone can use 3G, 4G and 5G mobile communication standards.

(i) Give one advantage of using a higher frequency band for mobile communications. (1)

(ii) Explain one benefit to Carlo of using 5G rather than 3G. (2)