Y10 COMPUTER SCIENCE SUMMER SUPPORT BOOKLET 1

Paper 1 topics

Software, Communications and Networking

Contents

1. Software

Software, meaning programs on your computer, on an optical disk or online and available for download, is divided into **system software** and **application software**.

Operating systems

System software has a wide range of responsibilities, some of which are visible to the user and some of which occur in the background. Tasks you need to be aware of are listed below, and these are overseen by a piece of software called the **operating system**.

- Providing a user interface
- Memory management
- Peripheral management
- Multitasking
- Security
- Utility program management

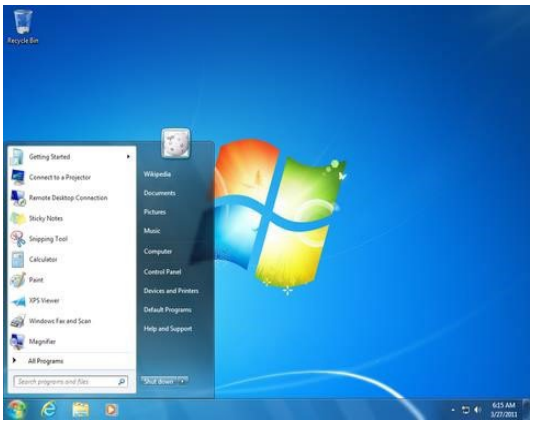
Providing a User Interface

An interface is simply a way of allowing the human to communicate with the machine and vice versa. An interface is normally intended to be user-friendly, but, as there are many different groups of users with different needs and skill levels, different types of interface are available. Most of these can be categorised as either a **graphical user interface (GUI)** or **command-line interface (CLI)**.

Graphical User Interface (GUI)

These interfaces communicate with the user by way of images. The most common type of GUI is a **WIMP (Windows, Icons, Menus, Pointer)** interface, in which the user clicks on **icons** that represent actions they want to carry out, e.g. dragging an icon to a bin either deletes or recycles it.

Advantages	Disadvantages
• Instinctive to use – most users could ascertain the purpose of the recycle bin without reading any instructions. • A beginner does not need to learn a set of commands, as in command-line interfaces.	• A lot of processing power is used on displaying icons rather than text. • High RAM and backup store capacities are required. • A good graphical display is essential. • Typically, GUIs run slower than CLIs.



Used with permission from Microsoft

Command-Line Interface (CLI)

Command-line interfaces typically require only typed input from the user, who must learn a set of commands before they are able to use the operating system. One such interface is MS-DOS 6.0, which is operated by typing in commands such as those below:

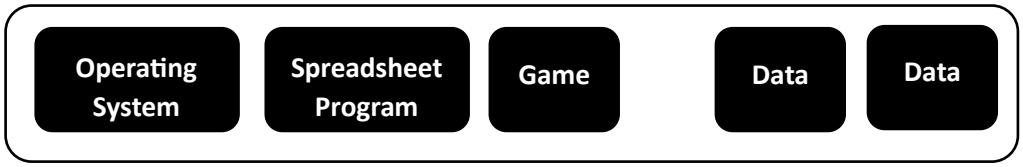
`DELETE C:/FILE.TXT`	Deletes a file from one location
`COPY C:/FILE2.TXT A:/FILE2.TXT`	Copies a file from one location to another

As computers have become more powerful and more and more novices have become regular users, GUIs are far more in demand than CLIs.

Advantages	Disadvantages
• Can be installed on less advanced machines, as there is less need for an interface requiring advanced graphics or an abundance of memory and backup storage. • Run very quickly, particularly when used by an expert user.	• Users are required to learn an instruction set before they can use the interface.

Process Management

A computer's main memory can only contain so much. Programs that are open and data that is being used take up space in the main memory. Among the roles of the operating system are loading programs or data into memory and removing them when they are no longer needed.



Multitasking

Running more than one program at the same time is called **multitasking**. Most computers multitask, even if you think you are only running one program. An operating system might be open, scanning for a virus while keeping the clock at the correct time, while you are creating a presentation and listening to some music. Countless other **processes** (programs that are in main memory) will also be running in the background.

A processor can really only perform one task at any one time (assuming it is a single-core processor). The reason it appears to be able to run several at once is that it switches, very quickly, between processes, working on each for a split second in turn. The role of the operating system here is dividing up the processor time between all of the processors. Sometimes, a process deemed **high priority** will take a larger share of processor time than others, and another task for the operating system is managing these priorities.

Peripheral Management

A **peripheral** is a hardware device, not part of the CPU or main memory, that is plugged into the computer. Common peripherals include the keyboard, mouse, monitor, printer and speakers, with less obvious ones including barcode scanners, sensors and servomechanisms.

The role of the operating system is to manage these devices and their **drivers** (a driver is a small piece of software that tells a computer how to operate a particular peripheral). The operating system may sometimes need to coordinate peripherals that run at different speeds (for example, a digital camera can transmit pictures to print much faster than a printer could print them). The operating system will also ask the user for a driver if the correct one cannot be found.

User management

User management enables a network administrator to allocate accounts and set different access rights for different users. Administration software can also identify all the users currently on the network, manually log out users and monitor when and for how long each user is logged in over a period of time.

Utility software

Security

An operating system will contain features to keep the data and the programs secure. These may include:

- An **anti-malware software** capability to guard against malicious software
- A **firewall** to protect against both software and remote hackers
- Password facilities; different users may have their own usernames and passwords and only be allowed access to things they need to access, e.g. on a school system, a student cannot typically delete software when they log in, but a technician can

Utility Program Management

Backup utilities

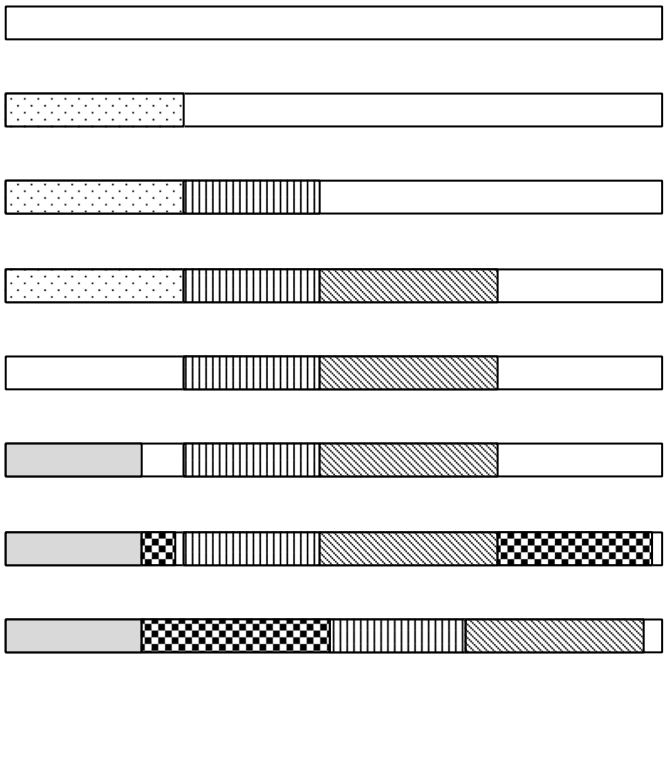
Backup software is designed to create a copy of files, folders or even an entire computer system. This allows easy restoration of data if the main storage drive is damaged or breaks.

A **full backup** will take an exact copy of all files on a computer. This takes a long time to complete as there could be hundreds of gigabytes or terabytes of data to backup.

Incremental backups first take a full backup. Then at regular intervals an incremental backup is then made of just the files and folders that have changes since the previous backup. This speeds up the backup process and it also allows snapshots of a drive to be taken without needing as much storage space as full backups.

Defragmentation software

When a disk has been written to and re-written to several times, files may not be stored as efficiently as they might be, and files can be split and spread across the disk, increasing disk access time. Defragmentation moves file segments, physically, from one disk location to another, in an attempt to minimise these gaps and to ensure that files are stored, as much as possible, in a single location. This reduces disk access time, making disk access speed faster.



An empty part of a disk

A file is created

A second file is added

A third file is added

The first file is deleted

A smaller file replaces it

A large file must be split
this file is now fragmented

The disk has been **defragmented**. The split file is joined into one and gaps have been minimised

Data compression software

Compression software such as WinZip will reduce the size of a file. There are two types of compression: **Lossy** and **Lossless**. Lossy compression can be used on photos where some detail is lost but will be undetectable when viewed on screen. Lossless compression is used on text files where it has to be possible to restore the file exactly.

Compressed files can be transmitted over the internet much more quickly than uncompressed files. Often there is a document file size limit when transmitting eg via email. This is to ensure that heavy files do not slow down the internet.

System Maintenance

System information and diagnosis utilities provide information to the user and any other software about the computer, such as hard disk capacity, processor speed and the name of the operating system. They can also attempt to solve problems when something is not working correctly. If, for example, the user is unable to access a web page, a diagnosis utility might be available to help the user to identify the source of the problem.

System cleanup tools are essential, along with regular defragmentation to keep a computer operating efficiently. Files that are no longer needed can be deleted (including a great many unnecessary background programs and browser add-ons that are downloaded and built up over time). Cleanup tools can also change system settings that are incorrect, or advise the user to do so.

Automatic updating ensures that a computer always has the most up-to-date version of a program available. Newer versions of programs might run quicker, have more features, have better security or have bugs (errors) removed. This utility is found more and more often in mobile phones as well as on computers.

Choosing Application Software

Application software (programs that are loaded from within an operating system by the user) can be obtained from a number of sources, each with advantages and disadvantages:

- **Custom-written** software is produced specifically for you (or, more likely, your company). While this is the best way to ensure you get a program that is exactly what you want, you will have to wait for it to be written first, and it will be very expensive.

- **Off-the-shelf** software is the kind that you buy from a shop or pay to download. It is instantly available and cheaper than custom-written software; lots of people buy it, so the cost is spread across many customers. However, there is a possibility it may not do everything you want it to do.

- **Open source** software gives you access to the code and allows you to make changes to customise it to meet your exact needs. It is also free, although you would need a high level of programming skill to be able to customise it.

Sample Examination Questions

1. Describe each of the following aspects of an operating system.

   a. Process management [2]

.....

.....

.....

   b. Peripheral management [2]

.....

.....

.....

2. Dave wants to use a touch-screen interface to keep track of cars that are being repaired and maintained at a garage. He is thinking of using either off-the-shelf or custom-written software. Discuss the implications of each of these options. The quality of written communication will be assessed in your answer to this question. [6]

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

3. State what is meant by *multi-tasking operating system*. [2]

.....

.....

4. Owen is considering purchasing a *custom-written* program to deal with orders at his takeaway restaurant.

   a. State what is meant by *custom-written*. [1]

.....

.....

   b. Give **one** advantage and **one** disadvantage of using custom-written software. [2]

.....

.....

.....

2. Communications and Networking

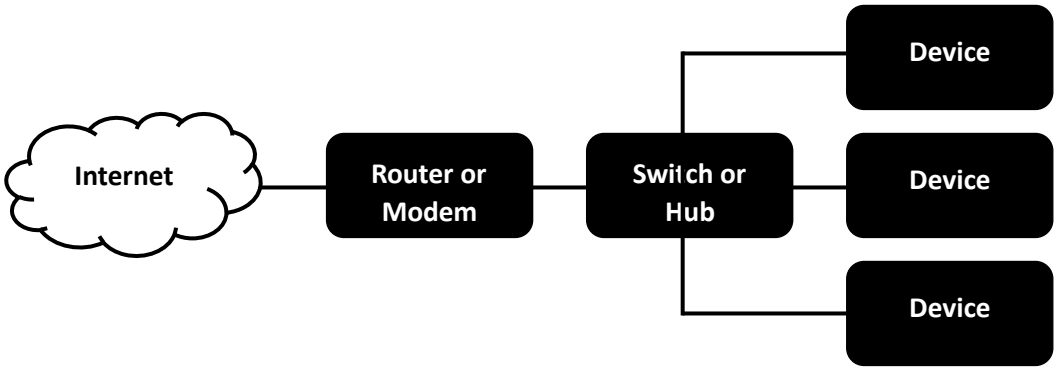
A **network** is a collection of computers and other hardware that has been connected together in order to allow communication and sharing of resources. A resource might be a file, a program, access to a printer or security (if logon names and passwords are stored on a network, a user can usually log on using any computer on that network).

Networks also allow software to be installed and controlled across the network from a single computer, rather than individually on every machine, thus saving time.

A computer can be part of a **local area network (LAN)**, which might occupy an office or building, or a **wide area network (WAN)**, the largest of which is the Internet. Being part of a network as opposed to using a **stand-alone** computer (not in a network) has many advantages:

- **Communication** – email, instant messaging and the transferring of files is possible across a network.
- **Sharing of resources** – files on one computer can be accessed by others, multiple computers on a network can share a single printer and, within a LAN, a connection to the Internet can be shared.
- **Network management** – you may be able to log onto any computer within a LAN and have access to your own files, which is particularly useful in schools and colleges.

Creating a network is more complex than simply plugging computers into each other (although two computers plugged together with the correct cable is, technically, a network). Specialist hardware is needed:



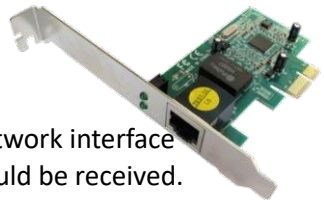
This is not the only way that a network can be set up; there are many different configurations and many different devices. This diagram also does not take into account wireless devices, which are explained below.

Router – This allows communication between a local area network (LAN) and the Internet. This is the device by which you can access the Internet.

Hub – A hub is a device to which lots of computers can be connected, usually with Ethernet cables. It allows computers connected to it to communicate with one another. In the above diagram, it also allows the Internet connection coming via the router to be shared.

Switch – A switch performs the same job as a hub, but it learns the locations of the computers and other devices plugged into it. This makes the network much more efficient, as far fewer unnecessary signals travel down the wrong cables.

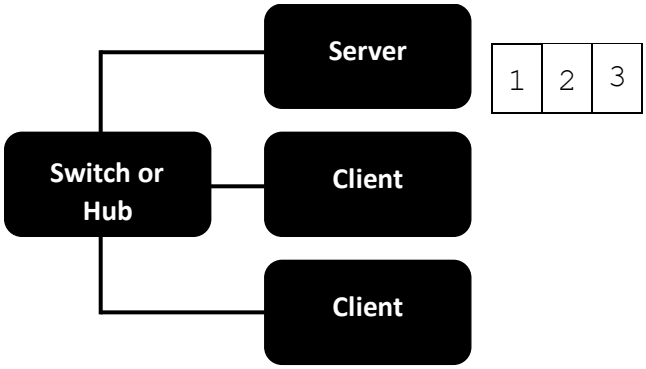
Wireless Access Point – This can be any device that allows connection to the network without any cables. In a house, this is usually the router, but in a large building in which wireless access is possible, devices that connect a wireless transmitter/receiver might plug directly into a hub or a switch. This is how laptops, phones and other portable devices could connect to a network.



Network Interface Card (NIC) – Each computer to be added to a network must have a network interface card. This is where an Ethernet cable would be attached, or where the wireless signal would be received.

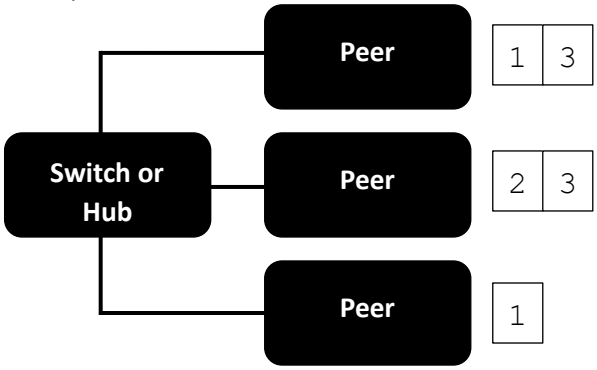
Client-Server or Peer-to-Peer Model

When creating a network, two common models are the **client-server** model and the **peer-to-peer** model. Each one essentially describes how files are stored and shared within a network. This is the client-server model:



A server (which is a computer) holds all the files. In this case, for simplicity, there are only three. If either of the clients (which are also computers; they just play a different role in this model) wants access to any of the files, they would need to request those files from the server.

This is the alternative – the peer-to-peer model:

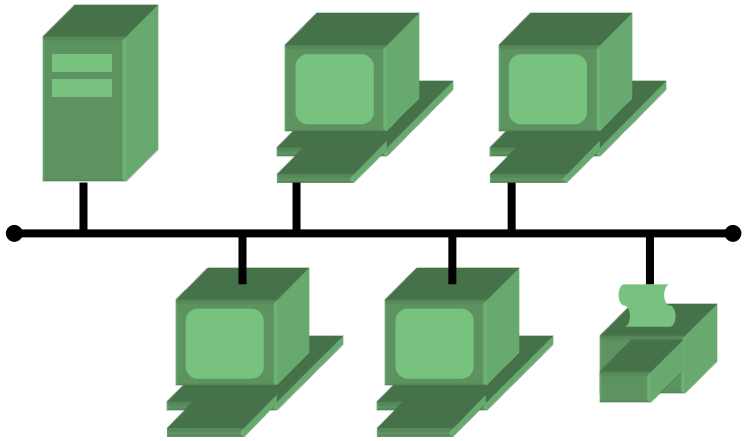


In this model, all computers have equal standing. All of them can store files, and any peer can transmit a file to any other peer. This model is generally less secure than a client-server model, where security can be concentrated on the machine that holds all the files. There is also an issue of duplication, as you can see, but this can be a good thing. If one peer were to go offline, there is a good possibility that any files that are needed also exist on another peer.

Topologies

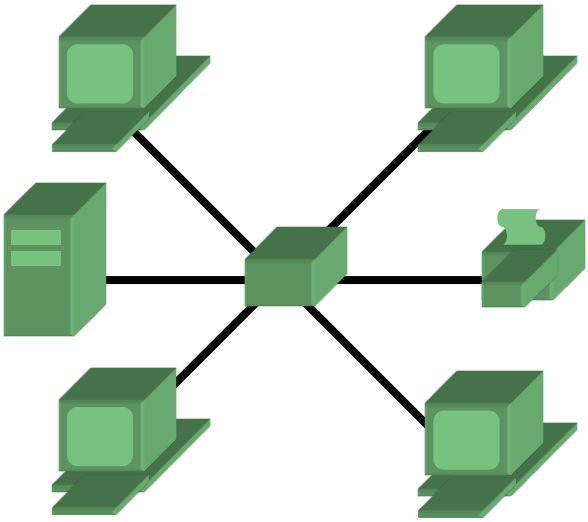
There are several ways in which computers can be connected together, the most common of which are the **bus**, **star** and **ring topologies** (the word 'topology' means the layout of the network), each of which has advantages and disadvantages. Please note that in the following diagrams, the lines do not necessarily represent wires – they could just as easily be wireless connections.

Bus Topology



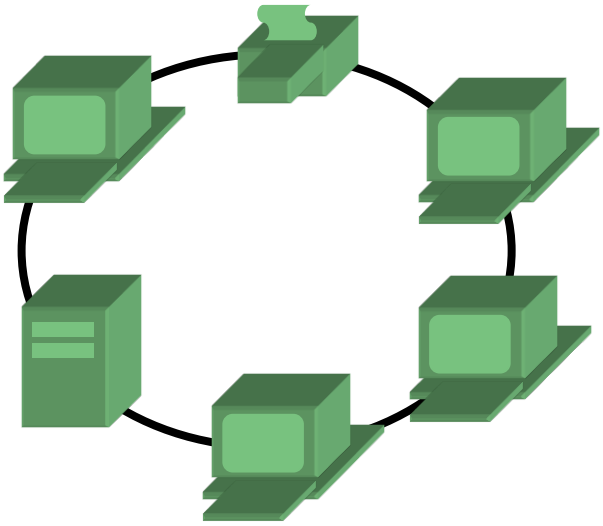
All devices are attached to a common connection medium, known as the **backbone**. Any communication must travel through this shared medium. A server might be attached to the backbone, or a printer, or a router if the network needs to provide access to the Internet. At either end of the backbone is a **terminator**, which marks the end of the network.

Star Topology



All devices are connected to a single central device, such as a **switch** or a **hub**. Communication must go via this central device. Servers, printers and routers would also be connected to this device.

Ring Topology



Each device is connected to two other devices, so that the devices and connection media make up the shape of a ring (in practice, it is rarely round – it may pass from desk to desk in an office). To communicate with a particular device, a signal often has to pass through several other devices on route. For an Internet connection, one of these devices must either be a router or connected to a router. Some networks can be a combination of several topologies.

Network Topology	Advantages	Disadvantages
Bus	• Very cheap, as it requires a minimal amount of cabling • Easy to add or remove computers	• Failure in the main cable will cause failure of the network • The network can be significantly slowed by high network traffic
Star	• If one cable fails, only the device attached to it is isolated from the network • Faults are easy to find • It is easy to add extra devices • The system is secure, as data is only sent to devices that need that data	• Lots of cable, which means more expensive to install than other topologies
Ring	• No collisions, as there is typically only one batch of data allowed on the network at any one time • Very high rates of transmission are possible	• Failure of a single cable can bring down the entire network • Failure of a single device can bring down the entire network • Security is not ensured, as data passes through other devices en route to its final destination

Some Networking Terms You Need to Know

IP (Internet Protocol) address – This is a unique number assigned to a device (computer, telephone, mobile phone, switch, router) on a network. No two devices on a network can share the same IP address, as it is used to ensure the right data reaches the right device. IP addresses are divided into four sections, and this is an example:

`192.168.0.5`

Each section contains a number between 0 and 255 (0 and FF in hexadecimal, 00000000 to 11111111 in binary). This system provides over four billion separate addresses, not enough for the long term, so it is being replaced with a system that can provide more addresses.

A device does necessarily have the same IP address all the time. Each time it joins a network, it may be given the same IP address as last time, or perhaps a different one. Each website you visit will have its own IP address. You type in the name of a website into a browser (such as www.bbc.co.uk) and a **Domain Name System (DNS)** would use this name to identify the IP address of the computer, somewhere in the world, that contains the website you are trying to access.

MAC (Media Access Control) address – This number, also unique, is hard-wired into a device and cannot be changed. It is a 12-digit hexadecimal number, with each pair of digits separated by a colon or a hyphen. This is an example MAC code:

`53:a0:6f:10:44:bd`

Protocols – These are used in communication between computers and their peripherals (such as printers, scanners, etc.) and between computers across a network. A protocol is simply a set of rules that computers must follow in order for the communication to be successful.

Protocols cover every activity that can be engaged in using the Internet and the worldwide web. Although there are many hundreds of such protocols, some are more commonly used than others:

- **TCP/IP** – **Transport Control Protocol/Internet Protocol**. This protocol consists of two separate protocols. TCP is a standard that defines how messages are broken up into packets and reassembled at the destination. IP identifies the location of a device on the internet and routes the packets from source to destination.
- **HTTP** – **Hypertext Transfer Protocol (and HTTPS)**. This protocol is used for accessing and receiving web pages in the form of HTML (Hyper Text Markup Language) files on the internet. HTTPS ensures added layers of encryption for more secure transmission of data.
- **POP** – **Post Office Protocol**. This is a protocol for receiving and holding emails on a server until it is picked up in the receivers' email inbox. POP creates local copies of emails and deletes the originals from the server. The emails are tied to that specific device and cand be viewed offline.
- **SMTP** – **Simple Mail Transfer Protocol**. While POP might be used to retrieve emails, SMTP is used to send emails from one server to another. This is necessary if the sender and receiver use different email service providers.
- **FTP** – **File Transfer Protocol**. This is a standard network protocol used when transferring computer files between a client and server on a computer network. FTP is faster than HTTP for transferring files. Users log in with a username and password to transfer files.

Packet switching

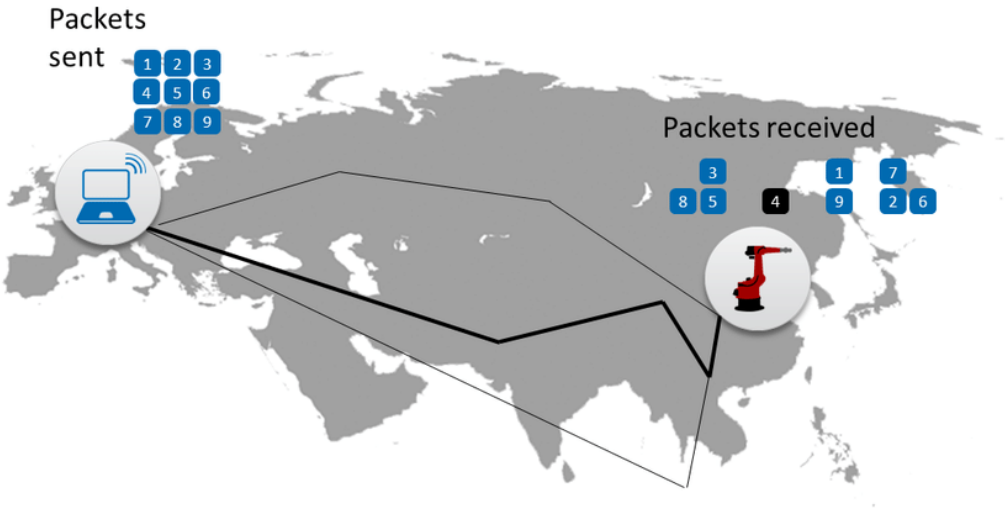
Suppose you want to send a file of 3MB across the internet. The file is broken up into data 'packets' of around 512 bytes. Each packet is given a header and sent across the network via routers.

The header includes:

- the source address (IP address it has come from)
- the destination address of the packet (IP address it is going to)
- sequence number of the packet
- number of packets in the whole communication
- error checking data.

Transmitting data in this way has several advantages:

- The packets do not need to take the same route around the network as each other.
- The packets do not even need to arrive in the same order that they left, as they are reassembled by the recipient computer.
- If one packet is not delivered correctly, only that packet needs to be re-sent – not the entire piece of data.

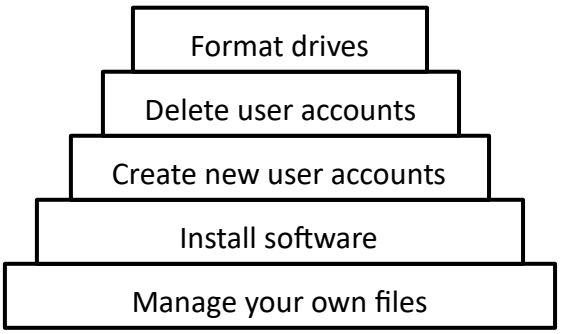


Network Security Measures

Passwords are the most obvious means of security. If you don't know the password, you cannot have access to the computer. In order to keep a computer truly secure, **strong passwords** are needed:

- `james` – This is a weak password (especially if the user's name is James or has a child named James). Other people could guess this quite easily, so whatever this password protects is not really secure.
- `fencepost186` – This is a better password. Combining words with other words or words with numbers makes passwords harder to guess.
- `fN%^601t` – This is a strong password. With a combination of upper case, lower case, numbers and symbols, as well as the fact that this password contains no words, it would be nearly impossible to guess. Even if someone were looking over your shoulder as you typed, it would be very difficult for them to remember.

User access levels – Passwords are often tied to **usernames**, so the computer knows who you are when you log in. Different users have different user access levels. Depending on who you are, you will have certain **privileges** within the network, i.e. you will be allowed to do certain things. Consider this:



These are some of the tasks that could be performed on a network, and not everyone can do all of the tasks, for example:

- If this were a school or college network, a *student* could only manage their own files.
- A *trainee network technician* might be able to do the bottom two. They would not be able to create user accounts, because their access level does not allow them to do this.
- A *network manager* would be able to do any of these things. They would also be able to change the access level of any other user.

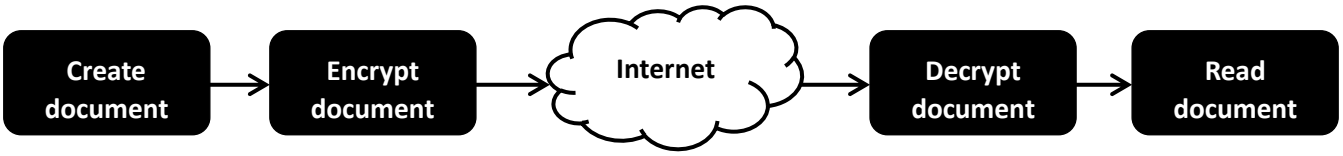
Encryption processes turn readable data into what seems to a human being to be complete nonsense. Let's take the following sentence and encrypt it:

```
I like mopping
```

We will now take each character as it was typed, on a standard keyboard, and move it two keys to the right:

```
P 'p;t .[]]p,j
```

Unless the person who reads this knows how it was derived, it will make no sense to them whatsoever. This data could be sent across the Internet safely. In reality, data that needs to be encrypted would be much more sensitive, and the encryption method would be far more sophisticated, but that's how it works.



The word **decrypt** means the opposite of **encrypt**. The apparent nonsense would be turned back into sensible data that can be read. As long as the recipient knows how to decrypt the transmission, and assuming no one else does, this is a secure method of transmitting data.

In order for it to work, both the sender and the receiver need to have access to the **encryption key**, which would be a small program that either encrypts or decrypts the data. This key itself would need to be kept secure.

Network Policies

Acceptable use – This policy sets down what users (who may be employees or students) are permitted to do and not permitted to do within a network. The policy document may include the following:

- Whether or not users are allowed to play games, use instant messaging services or access certain websites
- What personal information should and should not be entered onto the network
- What sanctions (punishments) might be applied to users who violate the acceptable use policy

Without employees having signed an acceptable use policy, they may unknowingly break laws and cause their organisation legal problems.

Backup – A backup policy states what data will be backed up from the network, how often it will be backed up, where it will be physically stored (ideally in a fireproof safe or at a different location) and how it would be used to restore any lost data. Without a backup policy, data is more likely to be permanently lost.

Failover – Sometimes, a computer, other device or communication media (such as an Ethernet cable) will stop working correctly, and a failover policy contains information on how to keep the network functioning if this happens. Files need to still be available and devices still need to communicate with one another, even in the event of such network failures.

Disaster Recovery – This policy describes how an organisation's IT infrastructure will keep an organisation running in the event of a disaster along the lines of fire, flood or earthquake. Such a policy may contain parts of the backup and failover policies, and is important because an organisation without an IT capability is likely to lose income as well as people's trust in their ability to operate.

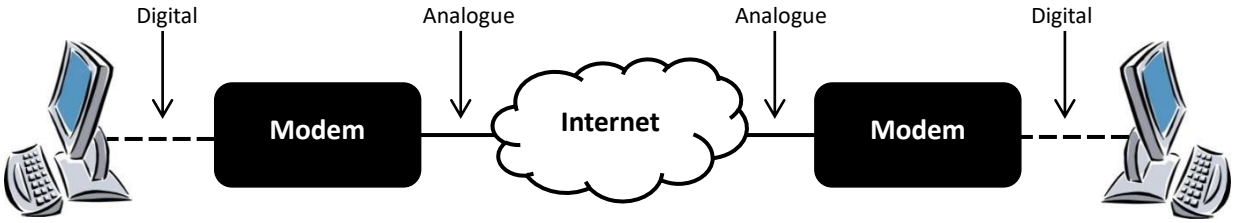
Archive – An archive is long-term storage for data that is not needed on a day-to-day basis any more. An archive policy will stipulate what data is to be archived, where it will be stored and how old data needs to be before it is archived. Sometimes, for legal reasons, organisations need to keep data for longer than it is useful to them.

The Internet

The Internet is simply a worldwide network, containing many millions of computers and related hardware such as routers, switches and mobile devices. When you go to a web page, your computer becomes part of the Internet.

In order to connect to the Internet, you need a **router**, which forms a connection between either a LAN or a standalone computer and the rest of the Internet.

If you are connecting to a communication line that does not work with **digital** signals (binary 1s and 0s are digital), such as a standard telephone line, you would need a **modem** (modulator demodulator). This device converts signals from digital (which computers use) to analogue (which telephone lines use).



Compression

To send large files across the Internet, **compression** can be used, in which files are made smaller so that they can be transmitted over a shorter time. Compression can be lossless or lossy.

Compression Type	Description	Example
Lossy	An individual file is made smaller, although not all data is stored.	• JPG (not all pixels are stored exactly as they were originally, but with photographs, this is not usually obvious to the human eye) • MP3 (not all frequencies are stored in an MP3)

Lossless	An individual file is made smaller and all data is stored, meaning when uncompressed again the file will be exactly the same as the original.	• PNG • GIF (although this is a lossless format, it can only work with 256 colours)
Zipped	Several files are compressed into a single, smaller file that can be easily stored or transmitted. This type of compression is **lossless**.	• ZIP • RAR

Choice of compression type might depend on a number of factors:

- If data needs to be precise, such as in money transactions, lossless compression would be used.
- If data does not need to be precise, typically in photographs or music, lossy compression might be considered to save disk space or transmission time.
- If lots of files need to be compressed, but remain in the same location or are transmitted together, zipping is most common.

Sample Examination Questions

1. A school office contains three stand-alone computers, one of which has an Internet connection. There is also a printer. State two advantages of connecting these devices to form a network. [2]

   .....

   .....

   .....

   .....

2. Some of the more popular file formats on the Internet include **MP3**, **MPEG**, **PDF**, **GIF** and **JPG**. Into each of the boxes below, enter the file format that would be most appropriate for the description. The first one has been done for you. [4]

Description	Format
An animated logo at the top of a web page	GIF
An instruction manual on how to operate a piece of software	
An instructional video on using a piece of software	
A screenshot of a piece of software	
An audio description of how to operate a piece of software	

3. A college connects its computers into a *LAN*.

   a. Explain what is meant by *LAN*. [1]

.....

.....

   b. Some *LANs* are implemented using a *bus topology*. Name and describe **two other** *topologies* that might be considered when designing a *LAN*. [4]

.....

.....

.....

.....

.....

4. Draw and label a diagram that shows how computers on a *bus topology* might be connected to one another and to the Internet. [6]