GCE AS/A LEVEL

WJEC GCE AS/A Level in

DIGITAL TECHNOLOGY

APPROVED BY QUALIFICATIONS WALES

GUIDANCE FOR TEACHING Unit 3

Teaching from 2022

For AS award from 2023
For A level award from 2024

This Qualifications Wales regulated qualification is not available to centres in England.

CONTENTS

AIMS OF THE GUIDANCE FOR TEACHING

The principal aim of the Guidance for Teaching is to support teachers in the delivery of the new **WJEC GCE Digital Technology** specification and to offer guidance on the requirements of the qualification and the assessment process. The Guidance for Teaching is **not intended as a comprehensive reference**, but as support for professional teachers to develop stimulating and exciting courses tailored to the needs and skills of their own students in their particular institutions.

AIMS OF THE UNIT GUIDES

The principal aim of the Unit Guides is to support teaching and learning and act as a companion to the Specification. Each Unit Guide will offer detailed explanation of key points in the Specification and aim to explain complex areas of subject content. An overview of the whole course can be found in the Delivery Guide.

Fig 1.

1 INTRODUCTION

The WJEC GCE in Digital Technology qualification, approved by Qualifications Wales for first teaching from September 2022 is available to:

all schools and colleges in Wales
- schools and colleges in independent regions such as Northern Ireland, Isle of Man and the
- Channel Islands

It will be awarded for the first time in Summer 2024, using grades A*–G.

The purpose of the Guidance for Teaching is to aim to support teaching and learning and act as a companion to the Specification.

The Guidance for Teaching will offer detailed explanation of key points in the Specification and aim to explain complex areas of subject content.

1.1 Additional ways that WJEC can offer support:

- specimen assessment materials and mark schemes
- exemplar materials for performing and composing
- face-to-face CPD events
- examiners 'reports on each question paper
- free access to past question papers and mark schemes via the secure website
- direct access to the subject officer
- free online resources including practice questions and detailed set work notes
- Exam Results Analysis
- Online Examination Review.

Fig 2.

2 OVERVIEW OF THE SPECIFICATION ASSESSMENT OBJECTIVES

2.3.1 Contemporary practices involved in collecting, storing, analysing and using data

In this section learners will gain knowledge and understanding of contemporary practices involved in:

- collecting data
- storing data
- analysing data
- using data.

Collecting data

Learners should understand:

- *the purposes of collecting data*

The main purpose of data collection is to gather information in a measured and systematic manner to ensure accuracy and facilitate data analysis. Since the data collected is meant to provide content for data analysis, the information gathered must be of the highest quality for it to be of value.

Learners should understand that data can be collected for a variety of purposes including but not limited to, commercial e.g. sales or marketing, decision making, research, strategic planning; scientific; governmental e.g. statistical data.

Learners should understand:

- *appropriate means of collecting data including:*
  - *autonomous devices*
  - *passive and active data collection*
  - *manual data collection*
  - *usage data.*

- **Autonomous devices**
  This includes but is not limited to autonomous vehicles, home assistants e.g. Siri, robots especially those with specific functionality e.g. warehouse, defence, prosthetic limbs etc.
- **Passive and active data collection**
  Learners should understand the difference between passive and active data collection and be able to describe situations where either occurs. Learners should also understand the advantages and disadvantages associated with each method.
- **Manual data collection**
  Learners should understand the different method of manual data collection and their appropriateness to any given situation. Learners should also understand the advantages and disadvantages associated with manual collection.
- **Usage Data**
  Learners should understand what usage data means, how it would be collected and in what circumstances. Learners should also understand the advantages and disadvantages associated with this method.

Learners should understand:

- *the legal and ethical implications of collecting data via various means, both with and without prior consent.*

Learners should understand how data protection law relates to the collection of data and its use. Learners should be able to understand and discuss the ethical implications of collecting data in a variety of contexts.

Storing data

Learners should understand:

- *the relationship between binary data and storage units*

For the avoidance of doubt, and in common with the GCSE qualification, 1KB = 1024 bytes other measurements will refer to powers of 2 unless otherwise stated.

Bit as `1` or `0`
Nybble as 4 bit block (and usefulness in conversion from hex-binary) e.g. $1101_2 \rightarrow$ C

Byte as 8 bits e.g. 10110110_2

Understand that prefix multipliers work from bytes as 2^3 increments.

	Symbol	Value
Byte	B	8 bits
Kilobyte	KB	1024 bytes
Megabyte	MB	1024 Kb
Gigabyte	GB	1024 MB
Terabyte	TB	1024 GB
Petabyte	PB	1024 TB
Exabyte	EB	1024 PB
Zettabyte	ZB	1024 EB
Yottabyte	YB	1024 ZB

Learners should understand:

- *how to calculate appropriate storage requirements for varying types of files*

- **Representation of characters**
  Understand that characters are represented by binary numbers
  e.g. in ASCII
  01100001 represents **a**
  01000001 represents **A**
  (There is no need to remember the number that represents a character).

Understand that standardised character sets allow for data interchange between different programs.

Understand that ASCII and Unicode are two such standards.

Unicode can represent more characters than ASCII, but is more memory-hungry.

- **Representation of graphics**
  Understand that both raster and vector graphics can be stored on a computer.

Understand that raster graphics are dot matrix data structures representing a grid of pixels and cannot scale up without loss of apparent quality. They tend to be large in terms of the memory required to store them.

A bitmap image is a type of raster image and is composed of many tiny parts, called pixels, which are often many different colours. It is possible to edit each individual pixel.

Vector graphics use geometrically primitive objects (geometric primitives) such as points, lines, curves, and shapes or polygons which are based on mathematical expressions to represent images. Vector graphics can be scaled up without loss of apparent quality. They are smaller than

Bits per pixel	Max number of colours
1 bpp	2
2 bpp	4
3 bpp	8
4 bpp	16
5 bpp	32
6 bpp	64
7 bpp	128
8 bpp	256
10 bpp	1024
16 bpp	65536
24 bpp	16777216 (16.7 million)
32 bpp	4294967296 (4.3 billion)

bitmap graphics in terms of the memory required to store them.

The storage requirement will depend on the number of bits per pixel (bpp), the number of rows and the number of columns.
The size of an image = rows * cols * bpp

In a colour image of 640 x 480 at 24 bpp the size of the image will be:

640 x 480 x 24 = 7372800 bits, or 921600 bytes or 900 kilobytes

- **Representation of sound**
  That sound is stored as a digital representation. The digital representation is achieved by sampling (signal processing).

  The sample quality can be affected by the sample rate and sample frequency. The higher the sample rate and frequency, the larger the resultant sample.

  The size of the storage requirement will depend on the sample rate, the sample resolution and the length of the sound.

  File size = sample rate x sample resolution x length of sound

  or

  File size = bit rate x length of sound

  e.g.
  Sample rate = 8KHz
  Sample resolution = 16 bit
  Length of sound = 30 seconds

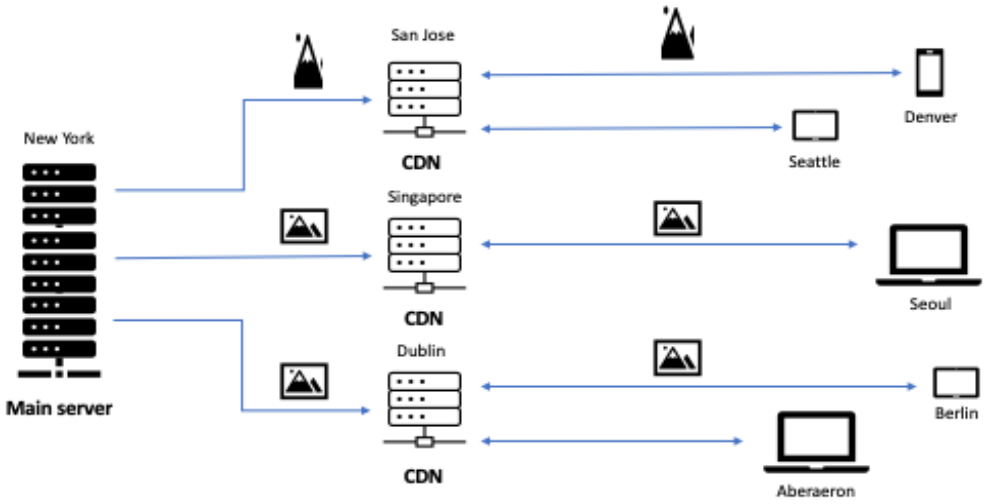
  => 8000 x 16 x 30 = 3840000 bits => 480000 bytes
  => 468.75KB

Learners should understand:

- *that monitoring data usage and size is key to modern distribution networks, especially Content Delivery Networks (CDNs)*

Content Delivery Network

Uses a series of content caching servers (CDN servers) grouped together as Points of Presence (PoPs) in various strategic geographic locations. Using GeoIP users are referred to their closes PoP based on their IP address which will map them to a geographic location. Regularly used



content is cached on a CDN server to facilitate its download or streaming to an end user. Understanding what data and how big it is is key to it being cached correctly.

Learners should understand:

- *the following general storage methods and their application:*
- *digitally sampled sound*
- *bitmapped graphics*
- *compressed audio*
- *compressed video.*

- **Digitally Sampled Sound**
  Digital audio is a representation of sound recorded in or converted into, digital form. Digital audio replaced analogue audio in many areas of audio engineering, record production and telecommunications in the 1990s and 2000s. Conversion to a digital format allows convenient manipulation, storage, transmission, and retrieval of an audio signal.
  In a digital audio system, an analogue electrical signal representing the sound is converted with an analogue-to-digital converter. This digital signal can then be recorded, edited, modified, and copied using computers, audio playback machines, and other digital tools. Unlike analogue audio, in which making copies of recording results in generation loss and degradation of signal quality, digital audio allows an infinite number of copies to be made without any degradation of signal quality.

- **Bitmapped Graphics**
  A bitmap (also called "raster") graphic is created from rows of different coloured pixels that together form an image. Examples of bitmap graphic formats include GIF, PNG, TIFF, XBM, BMP, and PCX. They are created using paint programs like Adobe Photoshop.

- **Compressed Audio**
  Audio data compression has the potential to reduce the transmission bandwidth and storage requirements of audio data. In both lossy and lossless compression, information redundancy is reduced. The acceptable trade-off between loss of audio quality and transmission or storage size depends upon the application. A digital sound recorder can typically store around 200 hours of clearly intelligible speech in 640 MB.

- **Compressed Video**
  Video compression is the process of reducing the total number of bits needed to represent a given image or video sequence. Video compression algorithms such as H.264/AVC or H.265/HEVC reduce the raw content data by as much as 1,000 times. This allows real-time video streams or the resultant files to be easily transmitted across networks.

Learners should be aware of the uses of more advanced storage techniques, including:

- *Redundant Array of Inexpensive Disks (RAID)*
- *Network Attached Storage (NAS)*
- *high availability storage*
- *Storage Area Networks usage (SAN)*
- *cloud storage*
- *hosted storage.*

- **RAID**
  This is a technique used to both improve the responsiveness and the resilience of both SSD (Solid State Drive) and HDD (Hard Disk Drive) storage systems. RAID arrays are typically found in the following modes:

  RAID 0 Striped: This provides improved performance and additional storage. However, it does not provide any fault tolerance, so any errors on the disks could destroy the RAID. Works on one disk.

  RAID 1 Mirrored: Each disk provides the same information, which provides some fault tolerance. As data is repeated, read speed is increased (because it can be read from any disk), but write speed is decreased (because all disks must be updated). Needs at least 2 disks or an even number of disks to function.

  RAID 3-6 Striped Parity: This requires at least 3 disks in an array. As well as fault tolerance it provides parity checks and error correction. The parity information is stored on a single disk, so the other disks can continue working should one of them fail. The lost data can be calculated using the parity data stored on the parity disk. This configuration means losing storage space to increase redundancy.

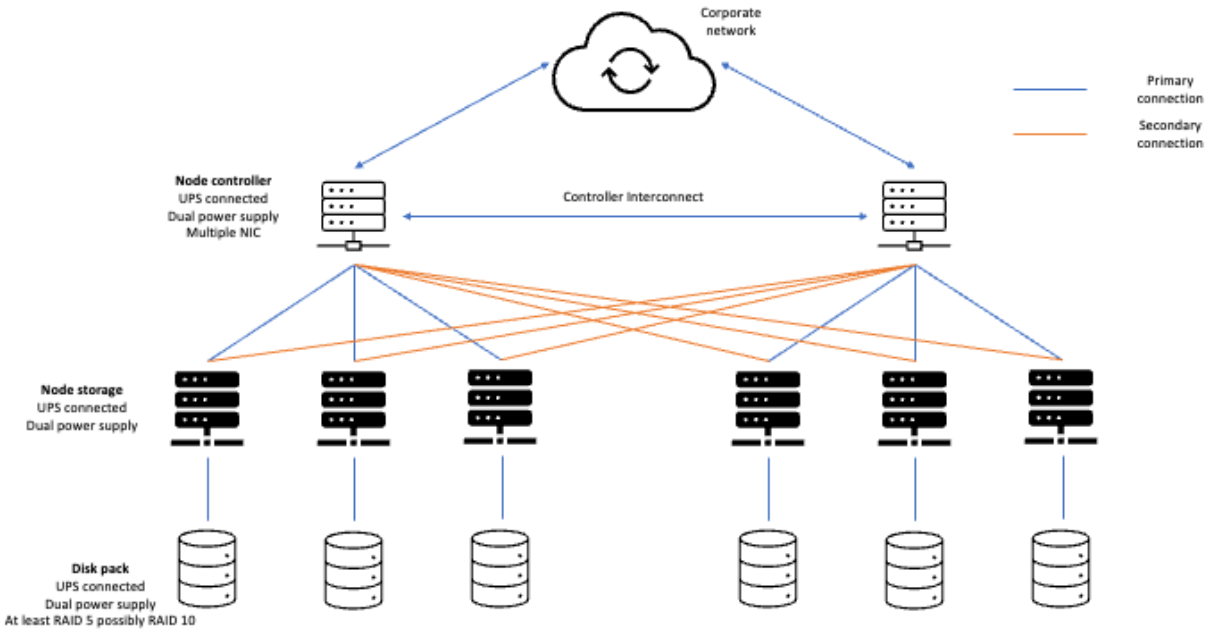
  Various other forms of RAID exist which improve resilience and performance.

- **NAS**

  Network-attached storage (NAS) is a file-level (as opposed to block-level storage) connected to a computer network. NAS devices began gaining popularity as a convenient method of sharing files among multiple computers, as well as removing the responsibility of file serving from other servers on the network.

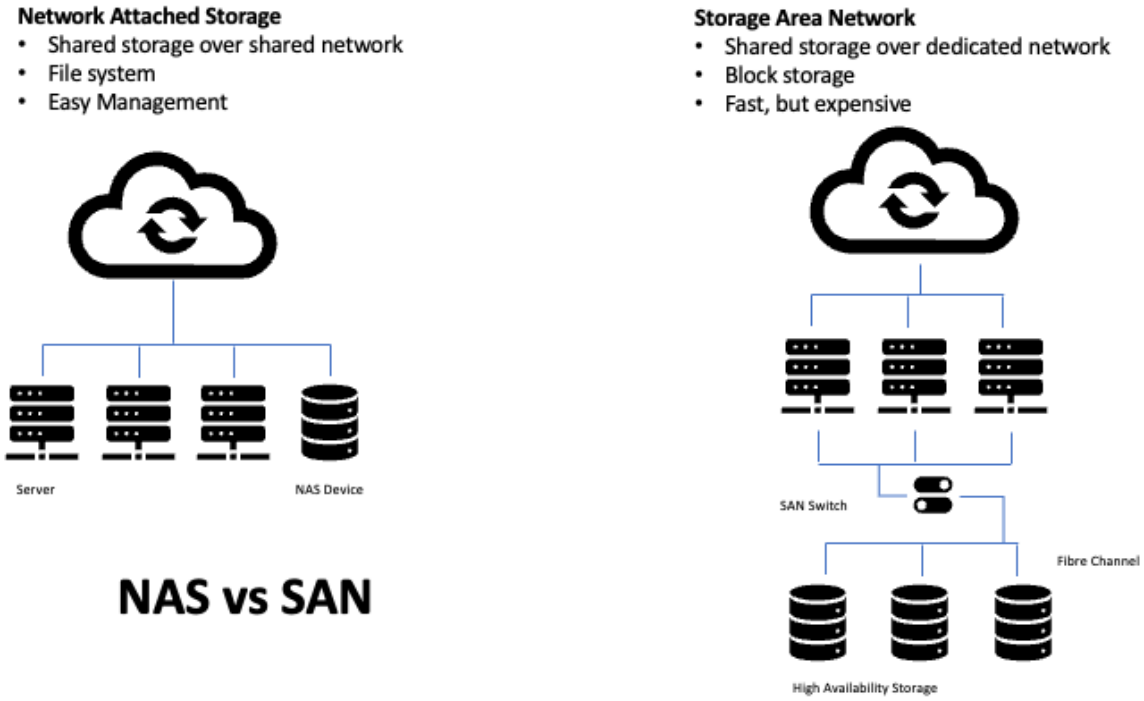
- **High availability storage**

  High availability usually means what is called Five 9's availability (uptime of 99.999% which equates to approximately 5 and a half minutes of downtime in a 24x7x365 year). Learners should understand that kind of reliability requires a lot of duplication and resilience.



- **SAN**

  A storage area network (SAN) is a dedicated, independent high-speed network that interconnects and delivers shared storage. A SAN is typically assembled with cabling, host bus adapters, and SAN switches attached to storage arrays and servers. While a SAN is a local network composed of multiple devices, NAS is a single storage device that connects to a local area network.



- **Cloud storage**

  Cloud storage is a cloud computing model that stores data on the Internet. It's delivered on demand with just-in-time capacity and costs, and eliminates buying and managing data storage infrastructure. This gives agility, global scale and durability, with "anytime, anywhere" data access.

- **Hosted storage**

  "Hosted services" is the general term for technology services with infrastructure located outside the recipient's physical location. A traditional hosted services provider owns and operates the infrastructure at a private location. Hosted services can include email to SaaS, storage, monitoring, and more. This infrastructure is used to deliver services to offsite clients.

Learners should understand:

- *virtualisation*
- *hosted instance*
- *hosted solution*
- *clustering*
- *blockchain storage.*

- **Virtualisation**

  - Virtualisation is the process of turning hardware into a software equivalent without sacrificing functionality. It's largely used as a way of saving space, cutting costs, and improving functionality and security. But it can also be used to create extra capabilities on top of existing hardware. For example, it can take storage or some of its capabilities and divide them across a number of virtual machines.

  - **Virtual Machines**
  - One of the elements of virtualisation. When deployed, a virtual machine can open an operating system on a single device, and that's including its own software. The VM's working is independent of the host, meaning that it won't be affected if something goes wrong with the hardware used to access it.

  - **Virtual memory**
  - To ensure VMs work as smoothly as possible, it's vital there's a high level of virtual memory available on the host computer.
  - This helps applications improve overall performance and store and receive data. It's enabled by small additions to a machine's hardware, called segments or pages, that store the extra data a physical machine cannot.

  - **Virtual Desktop Infrastructure**
  - Virtual desktops are hosted by a third party and companies don't have to deploy the technology to their on-site infrastructure, lowering costs and simplifying deployments.

  - **Virtual Applications**
  - Applications that are hosted remotely without users and companies having to store and maintain them locally. For example databases.

  - **Virtual storage**
  - Much like cloud storage virtual storage is hosted off-site and appears to users as if it were a local networked drive. It can be managed, added to, backed up and made resilient in the case of disaster recovery.

  - **Hosted instance**
  - Instances are the virtual machines that run operating systems' images such as Linux or Windows. Instances can be spun up or down depending on demand giving the ability to dynamically add or reduce capacity as need increases or decreases.

  - **Hosted Solution**
  - When you rent a virtual server from a company that takes over the responsibility for maintaining and keeping your server running, this is referred to as a hosted solution (sometimes also referred to as Cloud hosting).

- **Clustering**

- **Cloud Computing** - the use of a layer of abstraction to use remote resources to perform activities. E.g. using a cloud computing offering to convert a PDF file without having that software on your local machine.

Cluster Computing - the use of multiple less powerful machines in a unique way to create a more powerful machine. E.g. The animation studio, Pixar, has used a 2,000 machine, 24,000 core networked cluster of machines to render its movies - the power of all the machines together is far greater than any single machine could ever hope to be.

Cluster Cloud Computing - the use of a layer of abstraction to use remote cluster computer systems to carry out large data operations.For example, you contract a cluster cloud computer system to run data analytics on every picture of text currently publicly available to train your Optical Character Recognition system.

- **Blockchain storage**

Blockchain storage is a way of saving data in a decentralised network, which utilises the unused hard disk space of users across the world to store files. The decentralised infrastructure is an alternative to centralised cloud storage and can solve many problems found in a centralised system.
The goal of a blockchain is to allow digital information to be recorded and distributed while remaining unchanged. A blockchain serves as the foundation for immutable ledgers, or records of transactions that cannot be changed, erased, or destroyed. As a result, it is often referred to as distributed ledger technology (DLT).
Blockchain data storage improves users' privacy and security through encryption. However, it cannot, at present, provide the same fast speeds, low latency, and scalability as traditional storage solutions, such as hard disks or hard drives.

Learners should understand how cloud computing provides services, including:

- *data storage*
- *email*
- *virtualised software*
- *remotely hosted applications.*

- **Data storage**

Cloud storage uses data centres with massive computer servers that physically store the data and make it available online to users via the web. Cloud storage is a storage space available to store data on remote servers which can be accessed from the cloud (or the internet). The data is managed, maintained and backed up remotely.
Cloud storage works by using a data server that is connected to the Internet. When a user sends files over the Internet to the data server, the cloud storage saves a copy of them. When the user wants to retrieve this information, they access the server through a web-based interface.

- **Email**

Cloud email provides comprehensive email features and allows you to access them through the internet. A 3rd party host runs the email server on your behalf in a distributed environment ensuring access 24/7 and maximising uptime. Examples include Gmail, Hotmail.

- **Virtualised software**

  In software virtualisations, an application will be installed which will do all the normally associated with running an operating system on a physical computer. There are 3 kinds:

  - Operating System Virtualisation:
    In operating system virtualisation, a thin client connects to a server which emulates the OS. One server can emulate many different OS.

  - Application Virtualisation
    Application virtualisation is a technology, that encapsulates the computer program within the operating system allowing an application to run as if it were native.

  - Service Virtualisation
    In service virtualisation, a development team can use virtual servers rather than physical ones. With the help of service virtualisation, a complex application can go through testing much earlier in the development process. It can said that service visualisation is a technique to simulate the behaviour of some components in a mixture of component-based applications

Learners should understand cloud computing in terms of its business benefits.
In terms of:

- *Cost*
- *Scalability and extensibility*
- *Business continuity*
- *Collaboration*
- *Automatic updates*
- *Flexibility.*

- **Cost**
  Moving to cloud computing may reduce the cost of managing and maintaining IT systems. The cost of system upgrades, new hardware and software may be included in a contract. There may no longer need to pay wages for expert staff and energy consumption costs may be reduced.

- **Scalability and extensibility**
  Using the cloud means you can scale up or scale down an operation and its storage needs quickly to suit the situation. Rather than purchasing and installing expensive upgrades, a cloud computer service provider can handle this.

- **Business continuity**
  Having data stored in the cloud ensures it is backed up and protected in a secure and safe location. Being able to access data again quickly allows a company to conduct business as usual. It also minimises any downtime and loss of productivity during a natural or man-made disaster.

- **Collaboration**
  Cloud computing gives the ability to share and collaborate with employees, contractors and third parties in a variety of ways. For example, you could choose a cloud computing model that makes it easy for you to share your records with your advisers or accountants. It could also give you a quick and secure way to share accounting records with them.

- **Automatic updates**

  Cloud computing is a way for businesses to stay up-to-date with the latest technology. Access to automatic updates for IT requirements may be included in the service fee. This could include upgrades to servers and computer processing power, as well as software and hardware.

- **Flexibility**

  Cloud computing allows access to data in a variety of ways - at home, on holiday, or via the commute. If access to data is needed off-site, you can connect to your virtual office, quickly and easily through the internet.

Analysing data

Learners should understand:

- *how descriptive data analytics can provide useful information*
- *how this can be achieved by carrying out descriptive analysis and data visualisation*
- *the role of specialised Management Information Systems (MIS) in supporting decision making*
- *the role of specialised Project Management Software (PMS).*

- **How descriptive data analytics can provide useful information**

  Descriptive analytics involves parsing (or breaking down) data and summarising its main features and characteristics. It presents what has happened in the past without exploring why or how. Because it is merely explanatory, descriptive analytics uses basic descriptive statistics such as measures of distribution (frequency or count) and central tendency. It uses different tools to present its findings, such as pivot tables, line graphs, pie charts, and box and whisker plots.

  Data analysts can use descriptive statistics to summarise more or less any type of data. While descriptive statistics may describe trends or patterns, it won't dig deeper. For this, we need tools like diagnostic and predictive analytics.

  The following kinds of data, and more, can all be summarised using descriptive analytics:

  - Financial statements
  - Surveys
  - Social media engagement
  - Website traffic
  - Scientific findings
  - Weather reports
  - Traffic data

- **How this can be achieved by carrying out descriptive analysis and data visualisation**

  Data visualisation involves presenting the data visually or graphically to detect patterns, trends, and correlations that are not usually apparent from the raw data. Most Business Intelligence applications software heavily emphasise data visualisation and have strong data visualisation capabilities. One of the reasons for the popularity of visualisation tools is that they are easier to use and comprehend.

  Data visualisation is a powerful tool for analysing large data sets as it makes it easier to see trends, patterns and outliers in data sets. Data visualisation gives us a clear idea of what the information means by giving it visual context through maps or graphs. This makes the data more natural for the human mind to comprehend and therefore easier to analyse.

- **The role of specialised Management Information Systems (MIS) in supporting decision making**

  Suitable management information systems can structure the basic data available from company operations and records into reports that give guidance for decisions. You have to make sure the management information system you choose can work with the information formats available in your company and has the features you need.

  - Information from Company Operations
    Management information systems contain sales figures, expenses, investments and workforce data. E.g. If you need to know how much profit your company has made each year for the past five years, a management information system can give you that information

  - Capability to Run Scenarios
    What-if scenarios show how different variables change when a decision is made. You can enter reduced staff levels or increased promotion budgets and see what happens to revenue, expenses and profit for different levels of cuts or increases. Some management information systems have this feature built-in, while others provide the information required for running scenarios on other applications such as spreadsheets.

  - Projections to Assist in Decision Making
    Any decisions made in a business will affect the projected company results and may require modifications to business strategy. Management information systems either have trend analysis built-in or can provide information that enables such an analysis. Typical business strategies include projections for all fundamental operating results.

  - Implementation and Evaluation
    Management information systems give you the data you need to determine whether your decisions have had the desired effect. If specific results are not on track, you can use management information systems to evaluate the situation and decide to take additional measures.

- **The role of specialised Project Management Software (PMS)**

  A Project Management System (PMS) is a software tool that helps organise, manage, and track projects.

  - Planning
    Project management software allows you to map out the entire life of a project. It can be a general but robust software or a specialised solution that targets an industry. This software helps you to do the following:
    - define the critical path for the project and visualise the tasks that are interdependent.
    - outline the project schedule and set milestone deadlines
    - break down the completion of tasks and who is responsible for each task
    - allocate staff and resources to complete the tasks.

  - Manage tasks
    A PMS helps you manage tasks and track them. It can be robust for complex projects or simple for small projects. This function can be applied at the unit level (carpenter to nail together the roof) or macro level (contractor to build the house). A PMS is a powerful tool that lets you map out your team's skills and assign them specific tasks, deadlines and budgets.

- Collaborate
  Collaboration with team members, suppliers, senior management, and stakeholders is critical to any project. Many PMS focus on this function to ride on the back of outsourcing and workforce mobility trends. These solutions are also used outside of project management in e.g. education and marketing

- Schedule priorities
  A project schedule can deviate from the original plan because of unforeseen events or adjustments. Most PMS have a basic calendaring feature, while some focus on strengthening this function. These apps allow you to plot the shortest time to accomplish deliverables by prioritising schedules.

- Manage issues
  Issues can be bugs, malfunctions, loopholes, glitches, or gaps that come up after a task or project is completed. A PMS can track bugs and identify the source of the problem so it can be resolved. The software can also archive long documents or discussions as a reference to how the issue was resolved.

Learners should be aware of the use of:
- *data warehouses*
- *data mining*
- *large data sets.*

- **Data warehouses**

  A data warehouse (DW or DWH) is a system used for reporting and data analysis. DWs are central repositories of integrated data from one or more disparate sources. Extract, transform, load (ETL) and extract, load, transform (ELT) are the two main approaches.

  - ETL DW
    An extract, transform, load (ETL)-based data warehouse uses three layers to house its key functions. The staging layer or staging database stores raw data extracted from each of the disparate source data systems. The integration layer integrates the data sets by transforming the data from the staging layer. The access layer helps users retrieve data.

  - ELT DW
    A separate ETL tool isn't used in ELT for data transformation. Instead, there is a staging area inside the data warehouse itself. In this approach, data gets extracted, and then loaded into the same data warehouse.

- **Data mining**

  Data mining is considered an interdisciplinary field that joins the techniques of computer science and statistics. The main purpose of data mining is to extract valuable information from available data. It is primarily concerned with discovering patterns and anomalies within datasets, but it is not related to the extraction of the data itself.

- **Large data sets**

  Large data sets (Big data) refer to data sets that are too large or complex to be dealt with by traditional data-processing application software. Data with many fields (rows) offer greater statistical power, while data with higher complexity (more attributes or columns) may lead to a higher false discovery rate. Large data set analysis challenges include capturing data, data storage, data analysis, search, transfer, visualisation, querying, updating and information privacy.

Using data

Learners should understand:

- *what is meant by Artificial Intelligence (AI)*
- *the significance of the Turing test*
- *the main features of neural network modelling*
- *the structure of an expert system and its components*

- **What is meant by Artificial Intelligence (AI)**

  Artificial Intelligence is the simulation of human intelligence processes by machines, especially computer systems and encompasses the development of these systems that are then able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.
  Artificial intelligence can be divided into two different categories: weak and strong. Weak artificial intelligence embodies a system designed to carry out one particular job. These kinds of systems can be found in applications like self-driving cars or in hospital operating rooms. Strong artificial intelligence systems are systems that carry on tasks considered to be human-like. These tend to be more complex and complicated systems.

- **The significance of the Turing test**

  The test is based on the "imitation game", a party game in which a man pretends to be a woman and a judge tries to guess who is who by asking the concealed players questions.

  The Turing Test lets us look for the ability of computers to share in human culture by demonstrating their grasp of language in a social context. It can reveal the thing that is arguably most distinctive about humans - our different cultures. These give rise to enormous variations in belief and behaviour that aren't seen among animals or most machines.

- **The main features of neural network modelling**

  A neural network is a series of algorithms that tries to recognise underlying relationships in a set of data through a process that mimics the way the human brain operates. Neural networks can adapt to changing input; so the network generates the best possible result without needing to change the output criteria.

  A neural network is a mathematical function that collects and classifies information according to a specific architecture. The network bears a strong resemblance to statistical methods such as curve fitting and regression analysis. A "neuron" in a neural network contains layers of interconnected nodes. Each node is a known as perceptron and is similar to a multiple linear regression.

- Feed-forward neural Networks
  A neural network that conveys information in one direction through input nodes which continues to be processed in this single direction until it reaches the output mode. Feed-forward neural networks may have hidden layers for functionality, and this type of network is most often used for facial recognition technology.

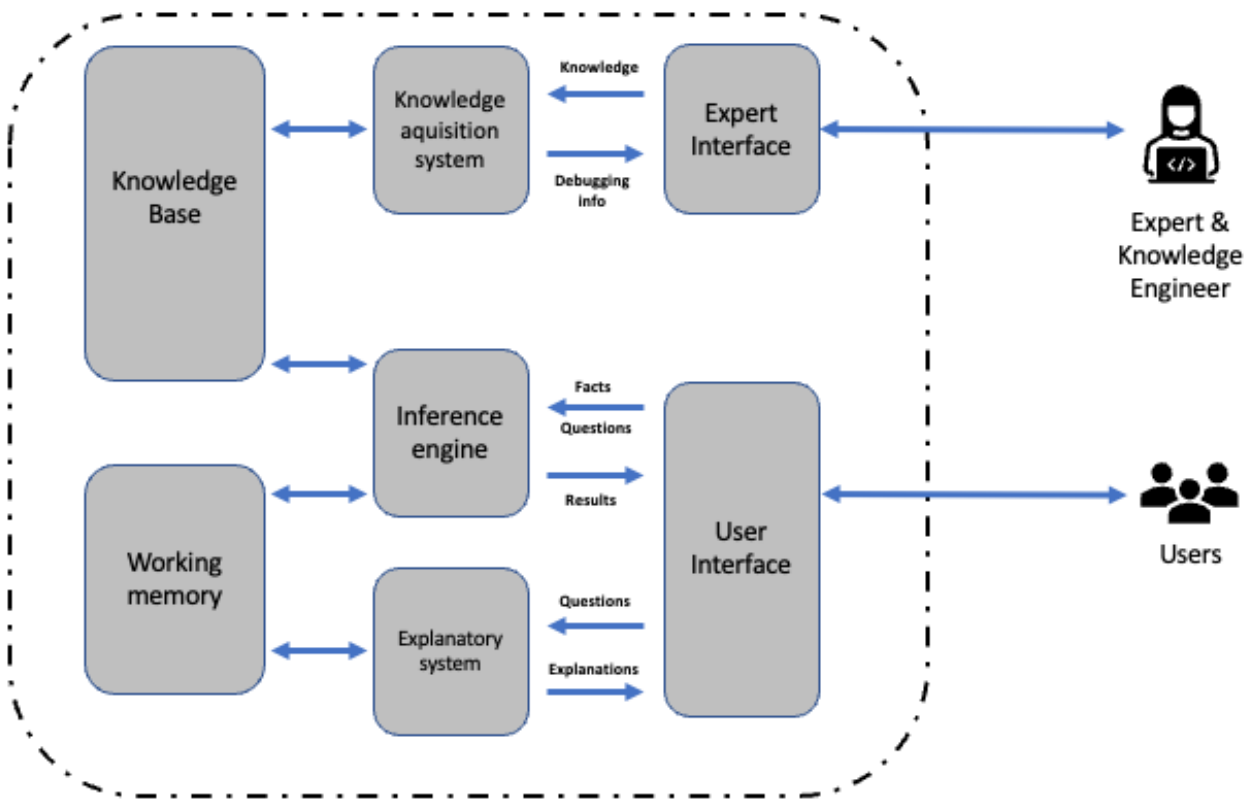
- Recurrent Neural Networks
  Recurrent Neural Networks are networks of nodes, where each node stores historical processes and these processes are reused in future processing. A more complex type of neural network, recurrent neural networks, take the output of a processing node and transmit the information back into the network. This type of network is often used in text-to-speech applications.

- Convolutional Neural Networks
  Convolutional neural networks are especially beneficial for image recognition applications. These networks have an input layer, an output layer, and a hidden multitude of convolutional layers in between. The layers create feature maps that record areas of an image that are broken down further until they generate valuable outputs. Used for image processing.

- Deconvolutional Neural Networks
  Deconvolutional neural networks are a type of neural network that works in reverse of convolutional ones. The application of the network is to detect items that might have been recognised as important under a convolutional neural network. These items would likely have been discarded during the convolutional neural network execution process. Also used for image processing.

- Modular Neural Networks
  Modular neural networks contain several computer networks that work independently from one another. This allows complex, elaborate computing processes to be done more efficiently. The goal is to have each module responsible for a particular part of an overall bigger problem.

- **The structure of an expert system and its components**



Learners should be aware of the following terms in relation to expert systems:

- *shell*
- *heuristics*
- *fuzzy logic*
- *knowledge engineer.*

- **Shell**

  Expert system shells are toolkits that can be used to develop expert systems. They consist of some built expert system components with an empty knowledge base. It is essentially a special-purpose tool that is built-in in line with the requirements and standards of a particular domain.

- **Heuristics**

  A heuristic system is designed to work with uncertainty and to simulate producing decisions based on experience. Heuristics captures information about accurate judgement and the ability to estimate and evaluate. Such rules are not derived from logic alone but are derived from a person's experience.

- **Fuzzy logic**

  Fuzzy logic can be implemented in systems such as micro-controllers, workstation-based or large network-based systems for achieving a definite output. The concept provides possibilities which are not given by computers, but are similar to the range of possibilities generated by humans. E.g. the concept of being tall would not have a definite outcome but would depend on the context and observer - a child's view of being tall would be different to an adult's.

- **Knowledge Engineer**

  A knowledge engineer is a professional engaged in the science of building advanced logic into computer systems in order to try to simulate human decision-making and high-level cognitive tasks. A knowledge engineer supplies some or all of the "knowledge" that is eventually built into the technology.[1]

Learners should understand:

- *the use of expert systems or neural networks in different contexts (e.g. health, employment, manufacturing)*
- *the technology required for natural language and voice recognition systems*
- *the ethical considerations of expert systems and AI.*

- **The use of expert systems or neural networks in different contexts (e.g. health, employment, manufacturing)**

Learners should be able to apply their knowledge of these contexts in exam questions relating them to the general knowledge specified earlier.

[1] https://en.wikipedia.org/wiki/Knowledge_engineer

- **The technology required for natural language and voice recognition systems**

  Natural language and voice recognition systems are essentially the same system one being the reverse of the other. Both rely heavily on large data sets and the AI principles of Machine Learning.

Consider the Amazon Alexa[2]:

There is some minimum capability built into whatever device you may use i.e. speakers, microphone, Internet connectivity, a small computer that wakes the device up and turns the lights on but it's mostly software driven as all such systems are.

1. Amazon first records your speech. Because interpreting sounds takes up a lot of computational power, the recording of your speech is sent to Amazon's servers to be analysed more efficiently.
2. Amazon breaks down what you said into individual sounds. It then consults a database containing various words' pronunciations to find which words most closely correspond to the combination of individual sounds.
3. It then identifies keywords to make sense of the tasks and carry out corresponding functions. For example, if Alexa notices words like *"weather"* or *"temperature"*, it would open the weather app.
4. Amazon's servers send the information back to your device and Alexa may speak. If Alexa needs to say anything back to us, it would go through the same process described above, but in reverse order.

- **The ethical considerations of expert systems and AI**

  Candidates should be aware of the ethical considerations surrounding expert systems and AI which include privacy, surveillance, bias and discrimination. There are also concerns about the accuracy of such systems (because of data bias) and data breaches.
  Learners should understand how to:
  - *use different forms of data analysis to identify trends and patterns*
  - *present data and analyses, and adapt the presentation to differing audience needs*
  - *analyse given situations and use the data presented to produce data flow diagrams illustrating the flows of information:*
  - *within an organisation*
  - *between an organisation, its customers, suppliers and other external agencies.*

- **Use different forms of data analysis to identify trends and patterns**

  Candidates should be familiar with the use and application of the different types of data analysis:
  - descriptive analysis
    diagnostic analysis
    predictive analysis
    prescriptive analysis.

[2] https://www.quora.com/How-does-Alexa-work?

- **Present data and analyses, and adapt the presentation to differing audience needs**

  Candidates should be able to adapt their presentations according to the audience receiving them.

- **Analyse given situations and use the data presented to produce data flow diagrams illustrating the flows of information:**
  - **within an organisation**
  - **between an organisation, its customers, suppliers and other external agencies**

Data Flow Diagrams (DFDs) are used to show the flow of data in a business information system. They can be used either logically or physically. Logical DFDs show the flow of data through a system to perform functionality. Physical DFDs describe the implementation of the logical data flow.

- **Data Flow Diagram (DFD)**

  There are 4 basic symbols used in a DFD:

Process box - with text inside describing the process (verb followed by a noun e.g. calculate tax)

Data flow - arrow indicates the direction of the flow. Labelled with either the data element or set e.g. Customer ID or Customer record

Data Store/Repository - text inside indicating the name of the repository e.g. Customer Database

External Entity - label with a description. A person, department or external organisation or system that provides or receives data to or from the organisation.

Rules

- A process must have at least one data flow entering a process and one exiting.
- An external entity cannot provide data to another entity without a process taking place.
- Data cannot move directly from an entity to a data repository without being processed.
- Data cannot move from one repository to another without being processed
- A data repository must be connected to a process with a data flow.
- A data repository must have at least one input flow and at least one output flow (even if it's a message)
- External entities do not process data.
- An external entity must be connected to a process with a data flow.
- Data flows must not cross.
- Objects cannot be duplicated e.g. only one customer external entity is allowed

Learners should understand how AI technologies use large data sets and the potential social implications which may arise.

AI Technologies are often used to refer to IT systems that perform functions that have been performed by human capabilities. Big Data Analytics (BDA) commonly refers to large data sets that can be generated, processed and increasingly used by digital tools and information systems for making predictive, descriptive and prescriptive analyses. Machine learning is one subcategory of AI, where computers have the ability to learn from data through appropriate algorithms.

Learners should understand that, amongst other things, the use of AI and large data sets can:

- disenfranchise minorities
- discriminate against people not represented in the data sets e.g. women in car safety data
- lead to huge improvements in the accuracy of medical diagnoses
- improve business methods and efficiency
- remove ethics and emotion as a consideration for decisions
- lead to large-scale unemployment
- remove privacy.

2.3.2 Cyber security

In this section learners will gain knowledge and understanding of cyber security including:

- *introduction to cyber security*
- *threats and vulnerabilities*
- *resilience controls*
- *social engineering.*

Introduction to cyber security

Candidates should understand that cyber security:

- *is how individuals and organisations reduce the risk of cyber-attack*
- *protects devices and services*
- *prevents unauthorised access to personal information.*

Cyber security is how individuals and organisations reduce the risk of cyber attacks. It's also about preventing unauthorised access to the vast amounts of personal information we store on our devices, and online. From banking and shopping, to email and social media, it's more important than ever to take steps that can prevent cyber criminals from getting hold of our accounts.

Candidates should understand what cyber security is and what it does.

Threats and vulnerabilities

Learners should understand:

- *accidental damage – identifying how data can be at risk from accidental destruction*
- *malicious and deliberate damage*
- *the legal and professional responsibilities in identifying and mitigating threats and vulnerabilities.*

- **Accidental damage – identifying how data can be at risk from accidental destruction**

This broadly falls into the following categories:

- Human Error
  The day-to-day running of a business involves a lot of data manipulation through typing, editing, updating, and deletions, processes that are prone to error by users. Human error is the root cause of most data loss in business as humans are, by nature, not perfect.

- Accidental data file deletion
  This usually results from a user error where a file or folder is accidentally deleted without an available backup. If there is no backup, unintentionally erased files may be permanently lost. Therefore, it is crucial to set up appropriate workflow processes, including routine work saving and methods for systematic data backup.

- Software corruption
  Another significant factor in data loss is software failure or crash. Any programme that is used to request data has the potential to crash, causing data loss or corruption. When updating several files, file editing software can potentially malfunction, causing some files to fail to save or update and end up being erased. The same thing can happen when backing up data.

  Common backup issues include the system's inability to make file copies and its incapacity to halt file deletions automatically. Incorrect malware detection by antivirus software might potentially result in data deletion. Additionally, file format conversion errors that result in data loss and corruption can happen.

- Hardware Malfunction
  Data loss that is irretrievable is a common result of hardware that contains or maintains data failing. Hardware degradation may be caused by internal or external factors. Hard drives and other data storage units are vulnerable to physical or mechanical failures. Misuse or improper treatment may also be the cause of the defects.

  Overheating, water and fire damage, power outages, human error, and faulty connection are all ways that hard drives can get harmed. Additionally, read/write head failure, bad sector corruption, and firmware corruption can all cause hardware to malfunction. The devices may also stop working or lose their effectiveness over time as a result of the gradual ageing of all or some of their parts.

- Natural disasters
  These include floods, earthquakes and fire.

- Power failure
  If data were not routinely stored, a disruption in the power supply or an electrical outage while a user was writing a document may lead to a loss of data. Only the stored portion of the data would be successfully recovered by auto-recovery processes.

  A sudden loss of power can harm the hardware and operating system and cause data loss. Computers may experience rebooting issues, making it impossible to retrieve data. Data loss and hardware damage from sudden voltage fluctuations (usually increased voltage) can occur.

- **Malicious and deliberate damage**

  Malicious or deliberate damage in computer science refers to any action or set of actions that are intended to cause harm or disruption to computer systems, networks, or data. This can take many forms, including:

  - malware, such as viruses, worms, and trojan horses, which can infect and damage computer systems, steal sensitive information, and disrupt network operations
  - phishing and social engineering attacks, use deception and manipulation to trick people into revealing sensitive information or installing malware on their devices
  - distributed denial of service (DDoS) attacks, flood a network or website with traffic in order to overload and disable it
  - SQL injection and other forms of code injection, allow attackers to execute malicious code on a server by injecting it into a web application
  - insider threats, involve employees or other insiders intentionally causing harm or stealing sensitive information
  - ransomware, is a type of malware that encrypts a victim's files and demands a ransom payment to restore access.

The intent and impact of this malicious or deliberate damage can be very different. The attackers may be motivated by financial gain, political beliefs, or simply a desire to cause disruption. The damage can range from minor inconvenience to complete system failure and loss of data.

Preventing and mitigating the damage caused by malicious or deliberate attacks requires a multi-layered approach that includes security awareness training, regular security updates, penetration testing and incident response planning.

Learners should understand:

- *the following security measures:*
- *encryption*
- *firewalls*
- *antivirus software*
- *hierarchical access levels.*

- **Encryption**

  Encryption is a security measure that uses mathematical algorithms to convert plaintext (readable data) into ciphertext (unreadable data) in order to protect it from unauthorised access. The process of converting plaintext to ciphertext is called encryption, and the reverse process of converting ciphertext back to plaintext is called decryption.

  There are two main types of encryption: symmetric and asymmetric encryption.

  - symmetric encryption uses the same secret key for both encryption and decryption. This means that whoever encrypts the data must also share the secret key with whoever needs to decrypt the data
  - asymmetric encryption uses a pair of keys: a public key, which is used for encrypting data, and a private key, which is used for decrypting data. Data encrypted with the public key can only be decrypted with the corresponding private key. This allows for secure communication even when the two parties have never met before and do not have a pre-existing shared secret key.

  Encryption can be used to protect data at rest, such as data stored on a hard drive, and data in transit, such as data sent over a network. For example, encryption can be used to secure email and instant messaging communications, and to protect sensitive data stored in the cloud.

- **Firewalls**

  A firewall is a security measure that controls incoming and outgoing network traffic based on a set of rules and policies. It acts as a barrier between a trusted internal network and an untrusted external network, such as the internet.

  Firewalls can be hardware-based or software-based, and they typically use a combination of technologies such as packet filtering, stateful inspection, and application-level gateways to control network traffic.

  Packet filtering is the process of examining the header of each network packet to determine its source and destination and whether it should be allowed to pass through the firewall. This is typically based on IP address and port number.

  Stateful inspection is a more advanced technique that not only examines the header of a packet, but also tracks the entire conversation or "state" of the connection. This allows the firewall to make more informed decisions about whether to allow or block traffic.

  Application-level gateways, also known as proxy servers, inspect the data in the application layer of the OSI model. This allows the firewall to understand the specific application-level protocol being used, such as HTTP or FTP, and to make decisions based on that information. Firewalls can be placed at different points in a network, such as at the border of a network, between different segments of a network, or on individual devices.

- **Antivirus software**

  Anti-virus (AV) software is a security measure that is designed to detect, prevent, and remove malware, such as viruses, worms, trojan horses, and other malicious software.

  AV software typically uses a combination of techniques to detect malware, including:

  - signature-based detection, which compares the code of a file or program to a database of known malware signatures in order to identify a match
  - heuristic-based detection, which looks for patterns or behaviour that are typical of malware in order to identify new or unknown threats
  - behavioural-based detection monitors the behaviour of a program or process in order to identify malicious activity.

  Once malware is detected, the AV software will typically take one of several actions, such as:

  - quarantine the malware, which isolates it from the rest of the system so that it cannot cause any further damage.
  - delete the malware, which removes it from the system entirely
  - repair the malware, which attempts to reverse any damage caused by the malware.

  AV software is typically installed on individual devices, such as computers or mobile devices, and can run in the background as a service, constantly monitoring the system for any suspicious activity.

- **Hierarchical access levels**

  Hierarchical access levels is a security measure that divides access to a system or network into different levels or tiers, each with its own set of privileges and restrictions. This approach helps to limit the scope of damage that can be caused by an unauthorised user or a malicious insider.

  The most common example of hierarchical access levels is the use of user accounts and permissions. For example, a system administrator would have more privileges and access to more resources than a regular user.

  A typical hierarchy might include:

  - the highest level of access is typically reserved for system administrators or superusers, who have the ability to make changes to the system configuration and manage other users' access
  - the next level of access is typically for managers or power users, who have access to more resources and functionality than regular users, but less than the system administrator
  - regular users have the least amount of access and privileges, and can only perform a limited set of tasks or access a limited set of resources.

  Hierarchical access levels can also be applied to networks, with different levels of access to different parts of the network. For example, a DMZ (demilitarised zone) network segment would have less access and privileges than the internal network.

  This approach allows for more fine-grained control over access to resources and helps to limit the impact of security breaches.

Learners should understand:

- *the risks associated with online marketing communications*

- **The risks associated with online marketing communications**

  - spam and unwanted email: Unsolicited email marketing can be considered spam and can be annoying or even harmful to recipients. This can lead to a loss of customer trust and damage to an organisation's reputation

  - phishing and scam attempts: Online marketing communications can be used to impersonate legitimate organisations in an attempt to steal personal information, such as login credentials or financial information. This can lead to identity theft and financial loss

  - privacy concerns: Online marketing communications often rely on collecting and using personal data, such as email addresses or browsing history. Organisations must ensure that they comply with data protection and privacy regulations and be transparent about how personal data is collected, used, and stored

  - ad fraud: Online advertising is vulnerable to fraud, such as bots artificially inflating the number of clicks on an ad, this can lead to a wasted marketing budget and loss of credibility

  - brand safety: Online ads can appear on sites that may be inappropriate or offensive, which can damage an organisation's reputation

  - misinformation: Online marketing communications can spread misinformation or false information, which can lead to confusion, mistrust, or even harm.

Learners should understand:

- *the special security and integrity problems which can arise during online updating of files*

- **The special security and integrity problems which can arise during online updating of files**

  - unauthorised access: if an attacker gains access to the update server, they can potentially alter or replace the files that are being updated, leading to a compromise of the integrity of the updated files.

  - man-in-the-middle attacks: an attacker can intercept and alter the update files as they are being transmitted, leading to a compromise of the integrity of the updated files

  - malicious software: an attacker can include malicious software, such as malware or viruses, in the update files, leading to a compromise of the security of the updated files

  - incomplete updates: an attacker can cause an update to fail, leaving the system in an insecure state

  - denial of service: an attacker can overload the update server, making it unavailable to legitimate users, which can cause the system to be out of date

  - rollback attacks: an attacker can use old versions of files to perform an attack.

To mitigate these risks, organisations should use secure methods for transmitting and verifying the integrity of update files, such as using secure protocols like HTTPS or SFTP, digital signatures, and hash functions to ensure that the update files have not been tampered with. Additionally, organisations should have a robust incident response plan in place and conduct regular security assessments to ensure that the system is secure and up-to-date.

Learners should understand:

- *the need for and the purpose of cryptography*
- *techniques of cryptography*
- *symmetric and asymmetric encryption.*

- **The need for and the purpose of cryptography**

Cryptography is the practice of securing communication and data through the use of mathematical algorithms. The need for cryptography arises from the fact that information transmitted over networks or stored electronically is vulnerable to interception, alteration, and unauthorised access.

The main purpose of cryptography is to protect the confidentiality, integrity, and authenticity of data.

- confidentiality: Cryptography is used to protect the confidentiality of data by encrypting it so that it can only be read by authorised parties who possess the proper decryption key
- integrity: Cryptography is used to protect the integrity of data by creating a digital signature or a message authentication code, which can be used to detect any unauthorised changes to the data
- authenticity: Cryptography is used to ensure the authenticity of data by verifying the identity of the sender through the use of digital certificates or public key infrastructure.

Additionally, cryptography is also used for:

- non-repudiation: ensures that a sender of data cannot deny having sent the data
- key exchange: ensure secure communication between parties by securely exchanging keys
- random number generation: for various security applications.

- **The techniques of cryptography**

There are several techniques of cryptography that are commonly used to secure communication and data, including:

- Symmetric Key Cryptography: This technique uses the same secret key for both encryption and decryption. It is fast and efficient but requires that both the sender and the receiver have a copy of the secret key and must ensure the key is kept secure. Examples of symmetric key algorithms include AES, DES, and Blowfish
- Asymmetric Key Cryptography (Public Key Cryptography): This technique uses a pair of keys, one for encryption and one for decryption, and the keys are not identical. The encryption key is made public, while the decryption key is kept private. The most widely used public key algorithm is RSA

- Hash functions: This technique is used to create a unique digital fingerprint of a file or message, which can be used to verify its integrity. Hashing algorithms such as SHA-256, SHA-512 are widely used

- Digital Signatures: This technique is used to ensure the authenticity of the sender of a message. The sender creates a digital signature of the message using their private key and the recipient verifies the signature using the sender's public key

- Steganography: This technique is used to hide a message or other data within another file, such as an image or audio file, in order to conceal its existence

- Random number generation: This technique is used to generate random numbers for various security applications such as encryption key, digital signatures and more

- Quantum Cryptography: This technique uses the principles of quantum mechanics to secure communication, it is considered to be more secure than traditional cryptographic methods.

The choice of technique will depend on the specific security requirements and the type of data being protected. In practice, multiple techniques are often used in combination to provide a more robust level of security.

- **Symmetric and asymmetric encryption**

  Symmetric encryption and asymmetric encryption are two different techniques used to secure communication and data.

  - Symmetric encryption:

    - symmetric encryption uses the same secret key for both encryption and decryption
    - it is fast and efficient, but the key must be exchanged securely between the sender and the receiver before any communication can take place
    - examples of symmetric key algorithms include AES, DES, and Blowfish.

  - Asymmetric encryption (also known as Public Key Cryptography):

    - asymmetric encryption uses a pair of keys, one for encryption and one for decryption. The keys are not identical and are often referred to as a public key and a private key
    - the encryption key is made public, allowing anyone to encrypt a message and send it to the owner of the corresponding decryption key
    - the decryption key is kept private, allowing only the owner to decrypt the message
    - the most widely used public key algorithm is RSA.

    In practice, both symmetric and asymmetric encryption are often used in combination to provide a more robust level of security. For example, a symmetric key algorithm is used to encrypt the data and an asymmetric key algorithm is used to securely exchange the symmetric key between the sender and the receiver.

    Asymmetric encryption is more secure than symmetric encryption because it eliminates the need to share the secret key. But it's computationally more expensive and it's typically slower than symmetric encryption.

  Learners should understand:
  - *the purpose and use of contemporary biometric technologies*

- **The purpose and use of contemporary biometric technologies**

  Biometrics is the use of unique physiological or behavioural characteristics to identify individuals. Contemporary biometric techniques are used to verify the identity of a person in a secure and convenient manner. The main purpose of biometrics is to provide a reliable means of identification and authentication that is difficult to forge or imitate.

  Some common contemporary biometric techniques include:

  - Fingerprint recognition: This technique uses the unique patterns of an individual's fingerprints to verify their identity. Fingerprint recognition is widely used in mobile devices, laptops, and other electronic devices for secure access
  - Facial recognition: This technique uses the unique characteristics of an individual's face to verify their identity. Facial recognition is increasingly being used in security systems, such as surveillance cameras and smartphone unlocking
  - Iris recognition: This technique uses the unique patterns of an individual's iris to verify their identity. Iris recognition is considered to be one of the most accurate and secure biometric techniques and is used in a variety of applications, including border control and ATM banking
  - Voice recognition: This technique uses the unique characteristics of an individual's voice to verify their identity. Voice recognition is used in phone-based authentication, such as call centres and voice assistants
  - Signature recognition: This technique uses the unique characteristics of an individual's signature to verify their identity. Signature recognition is used in financial and legal transactions, such as signing contracts
  - Behavioural biometrics: This technique uses the unique characteristics of an individual's behaviour, such as typing rhythm or mouse movements, to verify their identity. Behavioural biometrics is increasingly being used as an additional layer of security in online banking and other sensitive applications.

  The use of biometric techniques is increasing in various areas such as government, healthcare, finance, and transportation, as well as in consumer devices, such as smartphones and laptops. Biometric authentication can provide a high level of security and convenience as it does not require users to remember passwords or carry identification cards.

  Learners should understand:
  - *a range of mechanisms for:*
  - *attacking vulnerabilities*
  - *defence from threats and vulnerabilities.*

- **A range of mechanisms for attacking vulnerabilities**

  These include but are not limited to:

  - Brute force attacks: Try all possible combinations of passwords, keys, etc
  - SQL injection: Insert malicious SQL code into a database query to manipulate or extract data
  - Cross-Site Scripting (XSS): Inject malicious scripts into web pages viewed by other users
  - Cross-Site Request Forgery (CSRF): Make malicious requests on behalf of a user without their knowledge or consent
  - Buffer overflow: Overwrite memory locations with malicious data to exploit vulnerabilities in software
  - Remote Code Execution (RCE): Execute arbitrary code on a remote system by exploiting vulnerabilities
  - Directory Traversal: Attempt to access restricted files or directories on a system
  - Man-in-the-middle (MitM) attacks: Interception and manipulation of network communications between two parties
  - Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks: Overwhelming a system with traffic to make it unavailable to users
  - Social engineering: Manipulating individuals into divulging confidential information.

- **A range of mechanisms for defence from threats and vulnerabilities**

  These include but are not limited to:

  - Firewalls: Network security systems that control incoming and outgoing traffic based on defined security rules
  - Encryption: Transformation of data into a secret code to protect its confidentiality and integrity
  - Access control: Restricting access to resources based on predefined security rules and policies
  - Antivirus software: Detect and prevent malware from infecting systems and networks.
  - Patches and updates: Regular application of software updates and patches to fix known vulnerabilities
  - Backups: Regularly creating backups of important data to protect against data loss or corruption
  - User education and awareness training: Educating users on safe computing practices and how to identify potential threats
  - Network segmentation: Dividing a network into smaller, isolated segments to reduce the potential impact of security breaches
  - Intrusion detection and prevention systems: Detect and prevent unauthorised access to systems and networks
  - Virtual Private Network (VPN) technology: Establishing secure, encrypted connections over public networks.

  Learners should understand:
  - *cryptocurrencies and why they can sometimes be associated with cyber security.*

  Blockchain is a decentralised, digital ledger that records transactions across a network of computers. It uses cryptography to secure and validate transactions, ensuring that the ledger is tamper-proof. The most well-known application of blockchain technology is cryptocurrency, but it has potential uses in many other areas.

Blockchain technology is used in cybersecurity in the following ways:

- Decentralised Identity Management: Blockchain can be used to store and manage digital identities securely, reducing the risk of identity theft
- Secure Record Keeping: The immutable and transparent nature of blockchain can be used to store sensitive data such as financial records, medical records, and other personal information
- Supply Chain Security: Blockchain can be used to track the movement of goods and ensure the authenticity of products, reducing the risk of counterfeits entering the supply chain
- Cyber Threat Intelligence Sharing: Blockchain can be used to create a decentralised network for sharing and analysing cyber threat intelligence data, improving the overall security of the network
- Data Privacy: Blockchain can be used to secure data privacy by implementing privacy-focused technologies such as zero-knowledge proofs
- Cyber Insurance: Blockchain can be used to streamline the process of purchasing and managing cyber insurance, making it more efficient and secure

Learners should be aware of:

- *the benefits and drawbacks of biometric technologies*
- *the complexities of capturing, storing and processing biometric data and the legal and ethical considerations of doing so.*

- **The benefits and drawbacks of using biometric technology**

Benefits of using biometric technology:

- Increased Security: Biometric technology, such as fingerprint scanning or facial recognition, provides a more secure form of identification than traditional passwords or PINs
- Convenience: Biometric technology can simplify and streamline the authentication process, making it faster and more user-friendly
- Reduced Fraud: Biometric technology makes it more difficult for fraudsters to impersonate someone, reducing the risk of fraud and identity theft
- Increased Accuracy: Biometric technology is more accurate than traditional forms of identification, reducing the risk of errors and improving security.

Drawbacks of using biometric technology:

- Privacy Concerns: The use of biometric data raises privacy concerns, as this data is personal and sensitive and can be misused by unauthorised parties
- Technical Limitations: Biometric technology is not foolproof and can be subject to errors, such as false rejections or false acceptance
- Cost: Implementing and maintaining biometric technology can be expensive, especially for smaller organisations
- Bias and Discrimination: There is a risk that biometric technology can perpetuate or exacerbate existing biases, leading to discrimination based on race, gender, or other factors
- Dependence on technology: Relying solely on biometric technology for authentication can lead to a loss of access in the event of technical failure or system breakdown.

- **The complexities of capturing, storing and processing biometric data and the legal and ethical considerations of doing so**

  - Data Collection: Capturing biometric data accurately and consistently can be challenging, especially for certain biometric traits such as iris recognition or vein patterns
  - Data Privacy: Storing biometric data raises privacy concerns, as it is personal and sensitive information that could be misused if it falls into the wrong hands
  - Data Security: Ensuring the security of biometric data is crucial, as it is vulnerable to theft, hacking, or other forms of cyberattack
  - Data Storage: Storing large amounts of biometric data requires significant amounts of storage space and computational resources, leading to higher costs for organisations.
  - Data Integration: Integrating biometric data with existing systems and processes can be complex, requiring specialised expertise and significant investment
  - Data Accuracy: Processing biometric data accurately can be challenging, especially in cases where the data is low-quality or inconsistent, and organisations must take steps to ensure that the data they collect is accurate and up-to-date
  - Data Management: Managing biometric data involves complying with privacy regulations, such as the General Data Protection Regulation (GDPR), and ensuring the data is up-to-date and accurate
  - Data Protection Laws: The collection and use of biometric data is regulated by the General Data Protection Regulation (GDPR) in the UK, which sets out strict requirements for data protection and privacy
  - Consent: The collection of biometric data requires informed consent from individuals, and organisations must ensure that individuals understand how their data will be used and who will have access to it
  - Data Retention: Organisations must ensure that they comply with data retention laws, which limit the length of time that biometric data can be stored
  - Data Sharing: Sharing biometric data between organisations raises privacy and security concerns, and organisations must ensure that they have appropriate measures in place to protect the data
  - Bias and Discrimination: There is a risk that biometric data and the algorithms used to process it could perpetuate or exacerbate existing biases, leading to discrimination based on race, gender, or other factors
  - Human Rights: The use of biometric data can raise ethical concerns and questions about human rights, such as the right to privacy and the right to protection from discrimination.

  Learners should be aware of:
  - *the types and operation of malicious software*
  - *black hat hacking, white hat hacking and penetration testing*

- **The types and operation of malicious software**

  Malicious software, also known as malware, can be classified into several types, including:

  - Virus: a self-replicating program that attaches itself to other files and spreads from one device to another
  - Trojan: a hidden program that appears as legitimate software but performs malicious actions
  - Worm: a self-replicating program that spreads through networks and causes damage to computer systems

- Ransomware: a type of malware that encrypts a user's files and demands payment for the decryption key
- Adware: a type of software that displays unwanted advertisements
- Spyware: a program that collects and sends personal information from a user's device without their knowledge
- Rootkit: a type of malware that is designed to hide its presence and give attackers full control over the infected device.

Operations of malware include:

- Data theft: stealing personal information or confidential data
- System disruption: disrupting the normal functioning of a device or network
- Spamming: sending unsolicited emails or messages
- Cryptojacking: using a victim's device to mine cryptocurrency without their knowledge
- Extortion: demanding payment in exchange for not carrying out malicious actions.

Black hat hacking, white hat hacking and penetration testing

- **Black hat hacking**

  Black hat hacking refers to the practice of using technology to gain unauthorised access to computer systems, networks, or data with malicious intent. This type of hacking is illegal and unethical, and the individuals who engage in it are known as black hat hackers. They use their skills to engage in malicious activities such as stealing sensitive information, spreading malware, or disrupting websites and computer systems. The purpose of black hat hacking is typically financial gain or causing harm to others, rather than improving security or advancing knowledge.

- **White hat hacking**

  White hat hacking, also known as ethical hacking, is the practice of using technology and hacking techniques for the purpose of improving security. White hat hackers are security professionals who use their skills to identify vulnerabilities and weaknesses in computer systems and networks, and then report them to the relevant organisations so that they can be fixed. This approach helps organisations to prevent cyber attacks from black hat hackers and improve the overall security of their systems. White hat hacking is legal and widely accepted as an important tool for improving the security of computer systems and networks. White hat hackers are valued for their knowledge and skills, and many organisations hire them to perform security assessments and penetration testing to identify and fix security issues.

- **Penetration testing**

  Penetration testing, also known as pen testing, is a security testing technique used to evaluate the security of a computer system, network, or web application by simulating an attack. The goal of pen testing is to identify security vulnerabilities and weaknesses in the target system and provide recommendations for improving its security.

  Penetration testing is performed by a team of security experts, known as penetration testers or ethical hackers, who use their skills to attempt to gain unauthorised access to the target system. They use a combination of automated tools and manual techniques to test the system's defences and identify vulnerabilities. This process mimics the methods and techniques that real-world attackers use, allowing organisations to assess the effectiveness of their security measures and identify areas for improvement.

Penetration testing is an important aspect of an overall security strategy and is widely used by organisations to ensure the security of their systems and data. The results of a pen test can provide valuable insights into an organisation's security posture and help prioritise security improvements.

Learners should be aware of:

- *the importance of large data sets to the operation and competitiveness of organisations in the health, finance and retail sectors*
- *the threats to the privacy of the individual from the use of data mining*

- **The importance of large data sets to the operation and competitiveness of organisations in the health, finance and retail sectors.**

  Large data sets play a crucial role in the operation and competitiveness of organizations in the health, finance, and retail sectors.

  - Health sector: Large data sets, such as electronic health records (EHRs), patient data, and clinical trial data, are used by healthcare organisations to improve patient care, support medical research, and streamline operations. For example, EHRs provide healthcare providers with a comprehensive view of a patient's medical history, enabling them to make informed decisions and provide better care.

  - Finance sector: Financial institutions use large data sets, such as transaction data, credit history, and market data, to make informed investment decisions, identify fraud, and improve their risk management strategies. For example, credit card companies use transaction data to detect fraudulent activity and prevent financial losses.

  - Retail sector: Retail organisations use large data sets, such as customer data, sales data, and supply chain data, to improve their marketing and sales efforts, optimise their supply chain operations, and provide personalised customer experiences. For example, retail companies use customer data to personalise their marketing campaigns and offer tailored recommendations to customers.

- **The threats to the privacy of the individual from the use of data mining**

  Data mining involves the collection and analysis of large amounts of personal data, which can pose significant threats to an individual's privacy. Some of these threats include:

  - Data breaches: Data breaches can occur when sensitive personal information is illegally obtained by unauthorised parties. This can lead to identity theft, financial fraud, and other forms of abuse

  - Unauthorised data sharing: Companies may share personal data with third parties without the individual's consent, exposing their information to further risks

  - Discrimination: Data mining algorithms can be used to make decisions that unfairly discriminate against certain groups of people, such as individuals with specific medical conditions or those in certain geographic locations

  - Profiling: Data mining can be used to create detailed profiles of individuals, which can be used for targeted advertising, but can also be misused for purposes such as discriminatory decision-making

- Lack of control: Individuals may have limited control over how their personal information is collected, used, and shared through data mining practices

- Inaccurate data: Data mining algorithms can produce inaccurate results, leading to false conclusions about an individual that can negatively impact their life.

To mitigate these privacy threats, it is important for organisations to implement strong data protection policies and technologies, as well as for individuals to be aware of their rights and to take steps to protect their personal information. This includes being cautious about the information they share online and carefully reviewing privacy policies before agreeing to them.

Learners should be aware of:

- *the use of mac addresses and mac address spoofing*
- *the basic tools for diagnosing and tracing data over packet switched networks, including:*
- *Tracert*
- *Whois*
- *IP address masking and impersonating.*

- **The use of mac addresses and mac address spoofing**

The Media Access Control (MAC) address is a unique identifier assigned to a Network Interface Controller (NIC) for use as a network address in communications within a network segment. This use of unique MAC addresses can create security risks, especially when it comes to MAC spoofing.

- MAC Spoofing: MAC spoofing is the practice of changing the MAC address of a device to impersonate another device on a network. This can be used to bypass security measures such as access controls based on MAC addresses or to evade network monitoring and detection

- Network Security: MAC addresses are used by many network security systems to identify and control access to a network. MAC spoofing can be used to bypass these security measures and gain unauthorised access to the network

- Privacy Concerns: In some cases, the MAC address of a device can be used to track its location and activity on a network. MAC spoofing can be used to conceal the identity and activity of a device, potentially violating the privacy of the user

- Network Performance: MAC spoofing can also negatively impact network performance, as it can cause network devices to become confused and send data to the wrong device, leading to lost or duplicated data packets.

To mitigate these security risks, it is important to implement strong network security measures, such as using encryption, firewalls, and access controls, and to regularly monitor network traffic for signs of MAC spoofing. Additionally, organisations can use technologies such as MAC authentication, which requires a device to present a valid MAC address before accessing the network.

- **The basic tools for diagnosing and tracing data over packet switched networks, including:**

  - **Tracert**
    Tracert (also known as traceroute) is a network diagnostic tool used to track the path taken by data packets from a source computer to a destination computer. It is used to determine the network route, the number of hops between the source and destination, and the time taken for data packets to travel from source to destination. Tracert works by sending a series of packets with incrementing Time-to-Live (TTL) values to the destination and measuring the time taken for each packet to reach its destination or be returned as undeliverable.

    Tracert is useful for troubleshooting network connectivity issues, such as slow or unreliable network performance, and identifying bottlenecks or network failures along the path. It can also be used to verify the configuration of network devices, such as routers, and to verify that the correct network path is being used.

  - **Whois**

    Whois is a protocol and database system that stores information about registered domain names and the associated organisations and individuals. The information stored in the Whois database includes the name and contact information of the domain owner, the domain's technical and administrative contact information, and the domain's creation and expiration dates.

    Whois is used to retrieve information about the owner of a particular domain name, and to verify the accuracy of the information listed in the database. This can be useful for a variety of purposes, such as resolving disputes over domain names, verifying the authenticity of a domain registration, and determining the ownership of a domain for security purposes.

  - **IP address masking and impersonating.**

    IP address masking refers to the process of hiding or changing the real IP address of a device or network to appear as if it originates from a different location or device. This can be done for privacy and security, or to bypass geographical restrictions.

    Impersonating an IP address refers to the act of pretending to be another device or network by using a false IP address. This can be done for malicious purposes, such as attempting to access restricted resources, launching cyber attacks, or for other criminal activities.

    It's important to note that IP address masking and impersonating can be illegal in many jurisdictions and can have serious consequences.

Resilience controls

Learners should understand:

- *cyber resilience*
- *the potential consequences to a company of a cyber-attack*

- **Cyber resilience**

  Cyber resilience refers to the ability of an organisation to withstand and quickly recover from cyber attacks, system failures, or other security incidents. It involves having the necessary processes, technologies, and people in place to prepare for and respond to cyber threats, minimise the impact of a security breach, and ensure the continued availability of critical systems and data.

- **The potential consequences to a company of a cyber-attack**

  A cyber-attack can have a number of potential consequences for a company, including:

  - Financial loss: The cost of the attack itself, as well as loss of revenue, legal fees, and compensation to customers
  - Reputational damage: Loss of trust and credibility with customers, partners, and stakeholders, which can lead to a decline in business and brand value
  - Legal liability: Companies may face legal action or fines if they fail to comply with regulations, such as those related to data protection and privacy
  - Intellectual property theft: Hackers may steal trade secrets, confidential information, or other valuable intellectual property
  - System downtime: Cyber-attacks can result in significant disruptions to operations, resulting in system downtime and loss of productivity
  - Long-term damage: The consequences of a cyber-attack can be long-lasting and may impact a company for years to come.

Learners should understand:

- *the difference between temporary or permanent loss of data and information, how this can occur and how it can be mitigated against*
- *the impact of damaged or corrupted software*
- *the effects of websites being unavailable in terms of:*
  - *loss of reputation*
  - *loss of competitive advantage*
  - *legal and social implications*
  - *financial loss.*

- **The difference between temporary or permanent loss of data and information, how this can occur and how it can be mitigated against**

  Temporary loss of data refers to a temporary loss of access to information due to technical issues such as power outages, system crashes, or other issues that can be resolved. This type of loss can usually be restored from backups or through other recovery processes.

Permanent loss of data refers to the complete and permanent destruction of information and cannot be restored. This type of loss can occur due to physical damage to storage devices, the deliberate destruction of data, or due to the permanent failure of storage devices.

Mitigating permanent loss of data can involve implementing proper backup and disaster recovery procedures, regularly updating software and systems to prevent cyber-attacks, and physically securing storage devices. This can include creating regular backups, storing backups in a secure location, and testing the ability to restore data from backups. Additionally, implementing access controls and monitoring systems can help prevent unauthorised access and the destruction of data.

- **The impact of damaged or corrupted software**
  - System crashes: The software may stop functioning properly, leading to system crashes and errors
  - Loss of data: The software may become unable to save or retrieve data, resulting in data loss
  - Security vulnerabilities: Damaged software may contain security vulnerabilities that can be exploited by malicious actors to gain unauthorised access to sensitive information
  - Inefficient performance: Software that is damaged or corrupted may run more slowly or inefficiently, reducing productivity and causing frustration
  - Compatibility issues: Damaged software may cause compatibility issues with other software or hardware, making it difficult or impossible to use
  - Overall, damage or corruption of software can cause significant disruption and lead to significant losses, both in terms of time and resources.

- **The effects of websites being unavailable in terms of:**
  - **Loss of reputation**
    - User Experience: A website that frequently goes down can result in a poor user experience, leading to frustration and loss of trust in the website and its brand
    - Lost Business Opportunities: The unavailability of a website can result in lost business opportunities and sales as users are unable to access the website to make purchases or access information
    - Damaged Brand Image: The unavailability of a website can be perceived as a sign of untrustworthiness, unprofessionalism, or inefficiency, damaging the brand's image and reputation
    - Decreased Search Engine Rankings: Search engines may penalize websites that are frequently down, leading to a decrease in search engine rankings, and reducing visibility and traffic to the website.
  - **Loss of competitive advantage**
    - Lost Market Share: The unavailability of a website can result in lost market share as users are unable to access the website and are directed to competitors instead
    - Missed Opportunities: A website that frequently goes down can miss out on potential sales and business opportunities, giving competitors an advantage

- Decreased Visibility: The unavailability of a website can lead to decreased visibility and traffic, reducing the website's impact and reach in the market
- Damaged Reputation: As mentioned in my previous answer, the unavailability of a website can be perceived as a sign of untrustworthiness or inefficiency, damaging the brand's reputation and competitive advantage.

- **Legal and social implications**

  - Legal Liabilities: If a website's unavailability results in financial loss or harm to customers, the website owner may be held liable under UK consumer protection laws
  - Contractual Obligations: If a website's unavailability breaches a contract with a client or customer, the website owner may be held responsible for damages
  - Reputational Damage: The unavailability of a website can result in negative press coverage, damaging the website's and the brand's reputation
  - Loss of Trust: If a website is frequently unavailable, users may lose trust in the website and its brand, potentially leading to a loss of customers and revenue
  - Customer Complaints: The unavailability of a website can result in a high volume of customer complaints, leading to increased pressure on the website owner to resolve the issue.

- **Financial loss**

  - Lost Revenue: The unavailability of a website can result in lost sales and revenue as users are unable to access the website to make purchases or access information
  - Increased Costs: Website unavailability can result in increased costs, such as the cost of fixing technical issues, compensating customers, and repairing damage to the brand's reputation
  - Decreased Ad Revenue: If a website is down for an extended period, it can result in a decrease in ad revenue as users are unable to view or click on ads
  - Decreased Search Engine Rankings: The unavailability of a website can result in a decrease in search engine rankings, reducing visibility and traffic to the website, and leading to a decline in revenue
  - Lost Customers: If a website is frequently down, users may turn to competitors, leading to a loss of customers and revenue for the website owner.

Learners should understand:

- *the following resilience controls a company may use to prevent a cyber-attack:*
- *using a boundary firewall and internet gateway*
- *having secure system configuration including admin accounts, audit trails, account management and backup*
- *implementing access control, including restricted access to valuable data*
- *implementing malware protection*
- *having patch management to ensure the latest updates of software are applied*
- *implementing staff training.*

- **the following resilience controls a company may use to prevent a cyber-attack:**
  - **using a boundary firewall and internet gateway**

    A boundary firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and an untrusted external network, such as the Internet. By enforcing these rules, the firewall helps to prevent unauthorised access to the internal network and protects against cyber-attacks such as malware infections, data theft, and hacking attempts. The firewall examines incoming traffic to ensure it meets the specified security criteria and either allows or blocks the traffic accordingly, providing an extra layer of security for the network.

    An internet gateway is a network device that allows for the exchange of traffic between an internal network and the Internet. It acts as a bridge between these two networks and is typically used to provide access to the Internet for internal devices.

    The use of an internet gateway to prevent cyber-attacks involves implementing security measures such as firewalls, intrusion detection and prevention systems, and virtual private networks (VPNs). These measures can help to block unauthorised access, detect and prevent malicious traffic, and encrypt sensitive data as it travels over the Internet.

    Additionally, regular software updates, network segmentation, and access control can further enhance the security of an internet gateway and reduce the risk of cyber-attacks. By implementing these measures, an internet gateway can play a crucial role in protecting internal networks from external threats and helping to prevent cyber-attacks.

  - **having secure system configuration including admin accounts, audit trails, account management and backup**

    Having secure system configurations including admin accounts, audit trails, account management, and backups helps prevent cyber attacks by providing multiple layers of protection.

    Admin accounts with proper access controls prevent unauthorised access to sensitive systems and data. Audit trails help detect and investigate any suspicious activity on the system. Account management ensures that users have only the necessary permissions for their roles, reducing the risk of exploitation. Regular backups provide a way to recover from any data loss or damage in case of a cyber attack.

    Together, these measures reduce the attack surface, increase visibility, and provide ways to respond to a security incident, making it more difficult for attackers to successfully carry out an attack and minimise the damage if an attack does occur.

    - **implementing access control, including restricted access to valuable data**

      Access control helps prevent cyber-attacks by limiting the number of individuals who have access to sensitive data and systems. This reduces the attack surface and the number of potential attackers. With restricted access, only authorised users can access valuable data, reducing the risk of unauthorised access, theft, or manipulation. Additionally, access control can be accompanied by measures such as logging and monitoring to detect suspicious behaviour and prevent attacks. By implementing access control, organisations can strengthen their security posture and reduce the risk of a successful cyber-attack.

- **implementing malware protection**

  Implementing malware control helps prevent cyber-attacks because it detects and blocks malicious software from infecting a computer or network. Malware, such as viruses, worms, Trojans, and spyware, can cause harm to systems, steal sensitive information, and give attackers unauthorised access to the network. By using anti-malware software, firewalls, and other security measures, organisations can reduce the risk of malware-based cyber-attacks and improve their overall security posture.

- **having patch management to ensure the latest updates of software are applied**

  Patch management is the process of identifying, acquiring, testing and installing patches (updates) to software programs and operating systems. By regularly updating software and operating systems, patch management helps prevent cyber-attacks in several ways:

- Closing Security Vulnerabilities: Patches often address known security vulnerabilities that could be exploited by attackers. By applying these patches, organisations reduce the risk of these vulnerabilities being used against them

- Protecting against New Threats: As new threats emerge, software vendors release patches that address these new threats. By having an up-to-date patch management system in place, organisations can protect themselves against new cyber threats as soon as they are detected

- Maintaining Compliance: Some industry regulations and standards require organisations to keep their systems updated and secure. By implementing patch management, organisations can ensure that they remain in compliance with these regulations.

- **implementing staff training**

  Staff training is a critical component of an organisation's overall cyber security strategy because it helps prevent cyber-attacks by educating employees about potential threats and how to avoid them. Here are several reasons why staff training is important:

  - Awareness of Threats: Staff training can raise awareness among employees about the various types of cyber threats, how they are executed, and how to identify them. This can help employees recognise potential threats and avoid falling for phishing scams, for example
  -
  - Safe Computing Practices: Training can also teach employees safe computing practices, such as how to create strong passwords, how to avoid downloading suspicious attachments or clicking on unknown links, and how to keep their personal and company data secure

  - Compliance with Policies: By providing staff training, organisations can ensure that employees understand and comply with their company's cyber security policies and procedures. This can help prevent accidental or deliberate violations that could lead to a security breach

  - Early Detection: Employees who are well-informed about cyber security can play a crucial role in the early detection of potential cyber-attacks. With the right training, employees can know what to look for and take the necessary steps to report any suspicious activity to the appropriate person or department.

Learners should understand:

- *the resilience controls a company could use to recover from and mitigate a cyber-attack, including:*
  - *making arrangements for the use of alternative premises, communication methods and facilities*
  - *exploring various what-if scenarios*
  - *ensuring regular backups of data.*

- **Making arrangements for the use of alternative premises, communication methods and facilities**

  Making arrangements for the use of alternative premises, communication methods, and facilities is an important component of Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP). These plans are designed to ensure that critical business operations can continue even in the event of a disruptive incident such as a cyber-attack.

  Having alternative premises, communication methods, and facilities in place provides organisations with the ability to continue operations in the event that their primary locations, communication systems, and facilities are impacted by a cyber-attack. For example, if a company's primary office building is damaged or inaccessible due to a cyber-attack, having arrangements in place for employees to work from an alternative location can help to minimise downtime and ensure that critical business operations can continue.

  Similarly, having alternative communication methods and facilities can ensure that employees can continue to communicate and collaborate with each other even if the primary communication systems are impacted by a cyber-attack. This could include having backup phone systems, email servers, and other critical communication infrastructure in place.

- **Exploring various what-if scenarios**

  Exploring various "what-if" scenarios is an important part of preparing for and mitigating the impact of a cyber-attack. This involves simulating hypothetical scenarios to understand how the organisation would respond in the event of a cyber-attack and identify potential weaknesses or vulnerabilities in existing systems, processes, and protocols.

  Through "what-if" scenario planning, organisations can identify potential attack vectors, evaluate the impact of a successful cyber-attack, and prioritise their response and recovery efforts. This helps organisations to better prepare for and respond to real-world cyber-attacks, minimising downtime and minimising the impact on critical business operations.

  For example, an organization might explore what would happen if its primary data centre were to be impacted by a cyber-attack, including the impact on employees, customers, and stakeholders. Based on this analysis, the organization might implement additional controls to prevent the attack or improve its disaster recovery and business continuity plans to minimise the impact in the event of an attack.

- **Ensuring regular backups of data**

  Regular backups of data play an important role in disaster recovery and business continuity planning, especially in the event of a cyber-attack. Backups ensure that critical data can be restored in the event of a data loss, minimising the impact on the organisation and its operations.

If an organisation experiences data loss due to a cyber-attack, such as through ransomware or data theft, having regularly updated backups can minimise the impact on critical business operations. The organisation can quickly restore the lost data from the backup, reducing downtime and minimising the impact on employees, customers, and stakeholders.

It is important for organisations to store backups in secure and easily accessible locations, such as off-site data centres or cloud-based storage solutions. This helps to ensure that the backups are protected from the effects of a cyber-attack and can be quickly restored if needed.

In addition to reducing the impact of data loss, regular backups can also help organisations to comply with data retention and privacy regulations. By regularly backing up data, organisations can ensure that they are able to meet their obligations to retain data for a certain period of time and provide access to it when necessary.

Learners should understand:

- *the legal and professional responsibilities associated with the placement of resilience controls.*

- Compliance with relevant laws and regulations, such as the General Data Protection Regulation (GDPR) and the Network and Information Systems Regulations (NISR) which outline specific requirements for ensuring the security and resilience of critical infrastructure and systems

- Adherence to professional standards, such as ISO 27001, which outlines best practices for information security management, and the Cyber Essentials scheme, which provides a baseline for cyber security

- Responsibility for the protection of personal data, including the implementation of appropriate security measures to prevent unauthorised access, use, disclosure, and destruction of personal information

- Duty of care to ensure the continuity of critical business functions, through the implementation of business continuity planning and disaster recovery strategies

- Ensuring the security and confidentiality of sensitive information, such as financial data and intellectual property.

Social engineering

Learners should be aware of social engineering, including the following techniques:

- *phishing*
- *baiting*
- *email hacking*
- *contact spamming pretexting*
- *quid pro quo scam*
- *vishing*
- *exploiting passive and active digital footprints.*

- **Phishing**

  Phishing is a type of cyber attack that aims to trick individuals into revealing sensitive information such as passwords, credit card numbers, and bank account details. This is typically done through fraudulent emails, text messages, or websites that appear to be from a trustworthy source, such as a bank or well-known company. The attacker will often ask the victim to provide personal information, and login credentials, or to click on a malicious link that leads to a fake website designed to steal information.

  Phishing attacks are becoming increasingly sophisticated and can be difficult to detect. It is important to be vigilant when receiving unexpected emails or messages and to never provide personal information in response to unsolicited requests.

- **Baiting**

  Baiting is a type of social engineering attack where an attacker leaves a physical item, such as a USB drive or CD, in a public place with the intention of tricking someone into taking it and using it on their computer. The device may appear to contain valuable or interesting information, but in reality, it contains malicious software that can infect the victim's computer and steal sensitive information or cause other harm.

  Baiting attacks rely on the natural human tendency to be curious and to take advantage of seemingly good opportunities. To prevent baiting attacks, it is important to be wary of unexpected or unfamiliar physical items and to follow good security practices, such as not inserting unknown or untrusted devices into your computer or network.

- **Email hacking**

  Email hacking refers to the unauthorised access or manipulation of someone else's email account or email messages. This can be done through various methods, including phishing, brute force attacks, or exploiting vulnerabilities in email systems.

  In a phishing attack, the attacker may send a fake email that appears to be from a trusted source and asks the victim to enter their email credentials or to click on a malicious link that leads to a fake login page. In a brute force attack, the attacker uses automated tools to try multiple username and password combinations until they gain access to the email account. Exploiting vulnerabilities in email systems involves finding and exploiting weaknesses in the software or infrastructure that support the email service.

  Email hacking can have serious consequences, including the theft of sensitive information, the spread of malware, and damage to the reputation of the victim. It is important to use strong and unique passwords, to be cautious when opening emails or links from unknown or suspicious sources, and to regularly check for and update security measures for email accounts and systems.

- **Contact spamming pretexting**

  Pretexting is a type of attack where the attacker creates a false scenario or cover story to manipulate someone into divulging sensitive information or performing a certain action. In the context of contact spamming, pretexting is a technique where the attacker creates a fake identity or pretends to be someone else in order to trick the victim into opening an email or responding to a message.

  Contact spamming pretexting often involves sending mass emails or messages that appear to be from a trustworthy source, such as a bank, government agency, or well-known company. The message may contain a request for personal information, such as login credentials or financial information, or a link to a malicious website. The attacker's goal is to trick the victim into believing the request is legitimate and to obtain sensitive information that can be used for identity theft or other malicious purposes.

  To prevent contact spamming pretexting, it is important to be cautious when receiving emails or messages from unknown or suspicious sources, to never provide personal information in response to unsolicited requests, and to verify the identity of the sender before responding to any requests.

- **Quid pro quo scam**

  Quid pro quo is a type of social engineering scam where the attacker offers something of value in exchange for access to a victim's computer or sensitive information. In a quid pro quo scam, the attacker may contact the victim and claim to be a representative of a reputable organisation, such as a technology company or government agency. The attacker may then offer to provide technical support or a software upgrade or to resolve an issue with the victim's computer.

  In exchange, the attacker will ask the victim to grant them remote access to the computer or to provide sensitive information, such as login credentials or financial information. Once the attacker has access, they can install malware, steal sensitive information, or cause other harm to the victim's computer or network.

  Quid pro quo scams can be difficult to detect and can have serious consequences. It is important to be cautious when receiving unsolicited requests for remote access to your computer or sensitive information and to verify the identity of the sender before responding to any requests.

- **Vishing**

  Vishing, also known as voice phishing, is a type of social engineering attack that uses voice calls, voicemails, or interactive voice response (IVR) systems to trick individuals into revealing sensitive information or installing malware on their devices. The attacker will typically pose as a representative of a trustworthy organisation, such as a bank or government agency, and ask the victim to provide personal information or to follow a set of instructions.

  In a vishing attack, the attacker may use caller ID spoofing or other techniques to make it appear that the call is coming from a legitimate source. They may also use automated systems to make large numbers of calls in a short amount of time, increasing the chances of reaching a victim.

- **Exploiting passive and active digital footprints**

  Exploiting passive and active digital footprints involves using information that individuals or organisations have inadvertently made available online to gain unauthorised access to their systems or steal sensitive information.

  Passive digital footprints are data or information that individuals or organisations have left behind as a result of their online activities, such as website browsing history, social media posts, or IP addresses. Attackers can use this information to gather intelligence on their targets and to construct more convincing phishing scams or social engineering attacks.

  Active digital footprints, on the other hand, are created when individuals or organisations actively share information online, such as through social media, email, or instant messaging. Attackers can use this information to build trust with their targets, steal sensitive information, or carry out attacks that are more likely to succeed.

  Exploiting passive and active digital footprints is often part of a larger cyber attack campaign, where the attacker uses multiple tactics to gain access to a target's systems and steal sensitive information. To prevent digital footprint exploitation, it is important to be aware of the information you are sharing online and to follow good security practices, such as using strong and unique passwords, avoiding the use of public Wi-Fi, and not clicking on links from unknown or suspicious sources.

- **Learners should be aware of the legal framework that exists to protect against social engineering.**

  The UK has a number of laws and regulations in place to protect against social engineering and other forms of cybercrime. Some of the key legal frameworks that exist to protect against social engineering in the UK include:

  - The Computer Misuse Act 1990: This act makes it a criminal offence to make unauthorised access to computer systems, including hacking, viruses, and other forms of cyberattacks

  - The Fraud Act 2006: This act makes it a criminal offence to carry out deception with the intention of making a gain or causing a loss. Social engineering scams, such as phishing and vishing, are often covered under the Fraud Act

  - The General Data Protection Regulation (GDPR): This regulation, which is enforced by the Information Commissioner's Office (ICO), requires organisations to protect the personal data of individuals and to report data breaches to the ICO within 72 hours

  - The Privacy and Electronic Communications (EC Directive) Regulations 2003: This regulation regulates the use of electronic communication services, including email, voice calls, and text messages. It requires organisations to obtain consent from individuals before sending marketing communications and to provide individuals with the option to opt out of such communications.

Learners should understand and give appropriate use case examples of where social engineering has been used to gain access within specific sectors including:

- *commerce*
- *personal finance and home banking*
- process control.

Candidates should be able to highlight the risks in these areas as well as be able to exemplify the use of social engineering in the areas indicated.

2.3.3 Digital technology networks

In this section learners will gain knowledge and understanding of digital technology networks, including cloud environments, and their roles in:

- *communications networks*
- *data transmission*
- *cloud services*
- *mobile technologies.*

Communications networks

Learners should be aware of:

- *the Internet as a global communications network which uses interconnected computers*
- *the infrastructure of the Internet*
- *the environmental concerns related to providing infrastructure, power and production.*

- **The Internet as a global communications network which uses interconnected computers**

  The Internet is a massive network of computers, servers, and other devices that are connected to each other and can communicate with one another using standardised communication protocols. This allows individuals, businesses, and organisations all over the world to share information, communicate, and collaborate in real-time, regardless of their location. The Internet has transformed the way we live, work, and interact with each other, enabling new forms of communication and commerce, and has become an essential tool for people and businesses alike.

- **The infrastructure of the Internet**

  The infrastructure of the Internet consists of various physical components, including:

  - Servers: powerful computers that store and manage data, websites, and applications.
  - Data centres: secure facilities that house and manage large numbers of servers
  - Network routers: devices that direct data traffic between computers and across networks
  - Fibre optic cables: high-speed data transmission lines that connect data centres, routers, and other parts of the network
  - Wireless towers: structures that allow data to be transmitted wirelessly using technologies such as Wi-Fi and cellular networks.

  These components work together to form the backbone of the Internet, allowing data to travel quickly and reliably between devices around the world. Additionally, various software and protocols, such as the Transmission Control Protocol/Internet Protocol (TCP/IP), enable the various components of the infrastructure to communicate and exchange information with one another.

- **The environmental concerns related to providing infrastructure, power and production.**

  The provision of Internet infrastructure, power, and production can have significant environmental impacts, including:
    - Energy consumption: Data centres and other Internet infrastructure consume large amounts of electricity, which contributes to greenhouse gas emissions and climate change
  - E-waste: The production of electronics and other components used in Internet infrastructure generates significant amounts of electronic waste, which can harm the environment and human health if not properly managed
  - Resource depletion: The production of electronics and other components often requires the extraction and processing of finite natural resources, such as rare earth minerals, which can have negative impacts on the environment and local communities
  - Water usage: Energy production, electronics manufacturing, and other components of Internet infrastructure can consume large amounts of water, which can lead to water scarcity in some regions
  - Land use: The construction of data centres and other Internet infrastructure can lead to the destruction of natural habitats and loss of biodiversity.

    Therefore, it is important to implement sustainable practices and technologies in the provision of Internet infrastructure, power, and production to minimise these environmental impacts and ensure sustainability.

Learners should understand:

- *the importance of standards and the role that W3C and IETF (RFCs) plays in them*

  Internet standards are critical for ensuring the interoperability, functionality, and security of the Internet. They define the protocols, technologies, and practices that are used to transmit information and provide common ground for communication between different devices and systems.

  The World Wide Web Consortium (W3C) and the Internet Engineering Task Force (IETF) are two key organisations that play a role in the development and maintenance of Internet standards.

  The W3C is focused on the development of standards for the World Wide Web, including HTML, CSS, and JavaScript. It aims to ensure the Web is accessible to everyone, regardless of their abilities, and is an open platform for innovation.

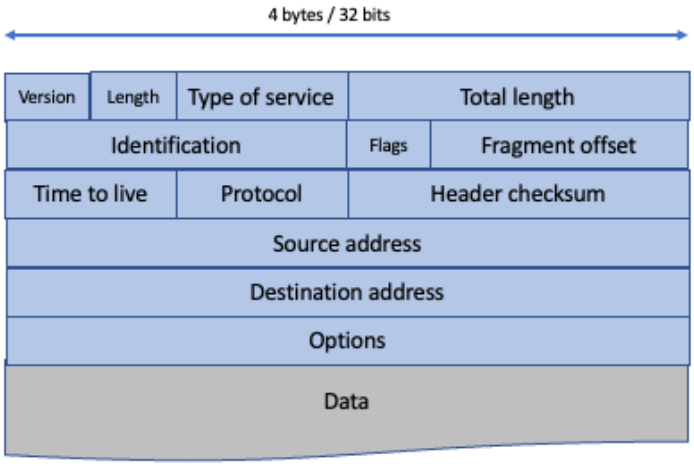
  The IETF develops and maintains technical standards for the Internet as a whole, including the Internet Protocol (IP), the Transmission Control Protocol (TCP), and the Domain Name System (DNS). It also deals with security, mobility, and other issues related to the Internet's technical infrastructure.

  By working together, these organisations ensure that the Internet is a stable and secure platform for communication, commerce, and innovation. They also ensure that the Internet evolves to meet the changing needs of users and the development of new technologies.

Learners should understand:

- *aspects of the TCP/IP protocol, including:*
- *packet contents*
- *packet switching*
- *routing and its possible risks.*

- **Packet contents**

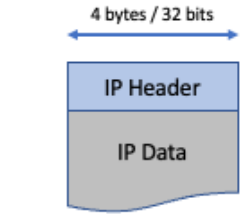


IP Packet

IP Packet

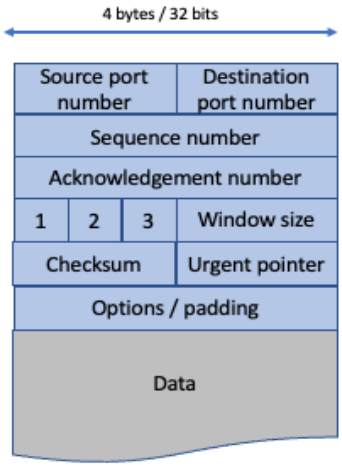
Item	Description
Version	Which version of IP
Length	Header length (measured in 32 bit words)
Type of service	Not generally used
Total length	Length of the datagram (packet) including header and data
Identification	Unique integer that identifies this datagram
Flags	Controls fragmentation and if so whether this is the last fragment
Fragment offset	Whereabouts this fragment is in the total datagram
Time to live	How long this datagram can remain in the internet (default is 255 seconds) prevents non-delivered packets hanging around forever
Protocol	Which protocol e.g. TCP, UDP etc
Header checksum	Validation of the header
Source address	IP address where the packet has come from
Destination address	IP address where the packet is going to
Options	Network testing and debugging

TCP Segment



IP Packet

The TCP segment forms the IP Data part of the IP Packet.



1. Offset
2. Reserved
3. Checkbits
   a. URG
   b. ACK
   c. PSH
   d. RST
   e. SYN
   f. FIN

TCP segment

Item	Description
Source port number	Port number of source application program
Destination port number	Port number of destination application program
Sequence number	Sequence number of the first byte of data
Acknowledgement number	Identifies the position of the highest byte received
Offset	The offset of the data portion
Reserved	Not used
Checkbits	Checkbits to identify the purpose of the segment: • URG: Urgent • ACK: Acknowledgement • PSH: PUSH • RTS: Reset connection • SYN: Synchronises the sequence numbers • FIN: Reached the end of the stream
Window size	How much data the destination can receive
Checksum	Validation of the header
Urgent Pointer	Indicates data that is to be delivered ASAP. Points to where the urgent data ends
Options / padding	Various options

- **Packet switching**
  - TCP/IP (Transmission Control Protocol/Internet Protocol) packet switching is the method by which data is transmitted over a network using the Internet Protocol (IP). It works by dividing large amounts of data into smaller, manageable units called packets and then transmitting each packet individually over the network.
  - Here is the process in more detail:
  - Data Segmentation: The data to be transmitted is divided into smaller units, typically ranging from several hundred bytes to a few kilobytes in size. Each unit is called a packet
  - Packet Header: Each packet is then given a header, which contains information about the source and destination of the packet, as well as other information, such as the packet's sequence number and the type of data being transmitted
  - Transmission: The packets are then transmitted individually over the network, using the IP protocol. During transmission, the packets may take different paths to reach their destination, depending on network conditions
  - Reassembly: When the packets reach their destination, they are reassembled into their original form to reconstruct the original data. This is done using the sequence number information included in the packet headers
  - Error Checking: To ensure accurate transmission of data, error checking is performed at both the packet and data link layer. For example, the TCP protocol, which operates at the transport layer, performs error checking to ensure that packets are transmitted accurately and that no packets are lost or corrupted during transmission
  - Flow Control: TCP/IP also implements flow control mechanisms to regulate the flow of data between the sender and receiver. For example, the TCP protocol uses a sliding window mechanism to regulate the flow of data and prevent network congestion.
- **Routing and its possible risks**

  In TCP/IP networks, routing refers to the process of determining the path that an IP packet should take to reach its destination. This is accomplished by routers, which are network devices that receive incoming IP packets and forward them to the next hop on their journey to the destination.

  Here's how routing works in more detail:

  - Destination IP address: Each IP packet contains the destination IP address of the machine that the data is intended for
  - Routing tables: Routers maintain routing tables, which are lists of known network destinations and the best next hop for each destination. The routing table is used to determine the next hop for each incoming packet
  - Determining the next hop: When a router receives an incoming IP packet, it looks up the destination IP address in its routing table to determine the next hop for the packet. If the destination is directly connected to the router, the packet is forwarded directly to the destination. If the destination is not directly connected, the router looks for the best route to the destination in its routing table

- Routing protocols: Routers exchange information about the network topology and available routes with each other using routing protocols, such as OSPF, BGP, or RIP. This information is used to build and update the routing tables

- Forwarding the packet: Once the next hop for a packet is determined, the router forwards the packet to the next hop. This process continues until the packet reaches its destination.

IP routing, while essential for the functioning of the Internet and other TCP/IP networks, is not without its risks. Some of the risks associated with IP routing include:

- Security: Routing protocols and routing tables can be vulnerable to attack and exploitation by malicious actors. For example, an attacker could inject false information into a routing table, causing packets to be redirected to an unintended destination. This type of attack is known as a routing attack or route hijacking

- Network congestion: Routing algorithms may not always make optimal decisions, leading to network congestion and reduced performance. For example, a routing algorithm may choose a suboptimal path that passes through a congested link, leading to increased delay and decreased reliability

- Configuration errors: Routing configurations can be complex and difficult to manage, especially in large, dynamic networks. Configuration errors, such as misconfigured filters or incorrect static routes, can cause routing problems and negatively impact network performance

- Scalability: As networks grow larger and more complex, routing can become a scalability challenge. Routing algorithms and protocols must be able to handle large amounts of routing information and route updates in a timely and efficient manner

- Interoperability: Routing protocols from different vendors may not be fully compatible with one another, leading to interoperability issues and difficulties in connecting different parts of a network.

Learners should understand:

- *the functionality provided by the DNS system and its basic vulnerabilities including DNS poisoning*

DNS (Domain Name System) is a critical component of the Internet that provides several key functions:

- Name Resolution: DNS is used to translate human-readable domain names, such as "www.example.com", into IP addresses that machines can understand. This allows users to access websites and other Internet resources using easily remembered names, rather than IP addresses

- Load Balancing: DNS can be used to distribute the load of incoming requests across multiple servers by returning the IP address of a server that is not heavily loaded

- Redirection: DNS can be used to redirect incoming requests from one domain name to another, or from one IP address to another, allowing network administrators to redirect traffic as needed

- Authentication: Some DNS servers can be configured to use cryptographic signatures to authenticate the source of DNS information, helping to prevent cache poisoning attacks and other forms of DNS-based fraud

- Service Discovery: DNS can be used to advertise the availability of services on a network, such as mail servers, web servers, and database servers, allowing clients to discover and connect to these services automatically.

Some of the most significant vulnerabilities of DNS include:

- Cache Poisoning: Cache poisoning is a type of attack where an attacker injects false information into the cache of a DNS resolver, causing it to return incorrect IP addresses for domain names. This can be used to redirect traffic to malicious websites, steal sensitive information, or spread malware

- Spoofed Responses: An attacker can send spoofed DNS responses to a DNS resolver, either by forging the source address of the response or by exploiting a weakness in the DNS protocol. This can be used to redirect traffic to a malicious site, steal sensitive information, or interfere with the operation of the network

- Zone Transfer Attacks: An attacker can request a copy of the entire zone file from a DNS server, which contains information about all of the domain names managed by that server. This information can be used to mount further attacks against the network, such as cache poisoning attacks or DDoS attacks

- DDoS Attacks: DNS servers can be targeted by DDoS (Distributed Denial of Service) attacks, which flood the servers with a large number of requests, causing them to become overwhelmed and unavailable. This can disrupt the operation of the network and make it difficult for users to access Internet resources

- Name Server Hijacking: An attacker can compromise a DNS server and change the information stored on the server, allowing them to redirect traffic to malicious sites, steal sensitive information, or spread malware.

Learners should understand:

- *the main components of computer networks including hardware, software and infrastructure*

The main hardware components of computer networks are:

- Routers: direct and control network traffic
- Switches: provide network connectivity by forwarding data between devices
- Firewalls: protect the network from external security threats
- Hubs: allow multiple devices to connect to a single network segment
- Bridges: connect separate network segments
- Access Points: provide wireless network access for Wi-Fi enabled devices
- Modems: provide internet connectivity by converting digital signals to analogue signals for transmission over telephone lines
- Network Interface Cards (NICs): provide a physical connection between the device and the network cable.

The main software components of computer networks are:

- Operating Systems: provide the underlying platform for networked devices such as servers, workstations, and mobile devices
- Network Management Software: monitor and manage network devices and services.
- Network Security Software: protect the network from security threats such as viruses, malware, and unauthorised access
- Communication Protocols: define the rules and standards for communication between networked devices
- Network Performance Monitoring and Analysis Tools: measure and analyse network performance to identify bottlenecks and improve efficiency
- Virtual Private Network (VPN) software: enables secure remote access to the network.
- Remote Access Software: allows remote users to connect to the network
- Backup and Recovery Software: provides backup and recovery services to protect against data loss in the event of a disaster.

The main infrastructure components of computer networks are:

- Cables and Wiring: provide the physical connection between network devices.
- Network Servers: provide centralised resources such as storage, processing, and applications for network users
- Storage Area Networks (SANs): provide centralised storage for large amounts of data.
- Wireless Access Points (WAPs): provide wireless connectivity for Wi-Fi enabled devices
- Data Centres: provide centralised and secure locations for storing and processing large amounts of data
- Network Racks and Cabinets: provide secure and organised storage for network devices
- Power Backup Systems: provide backup power in case of a power outage to ensure network uptime
- Cooling Systems: regulate the temperature in data centres to prevent overheating of equipment.

Learners should understand:

- *the main considerations involved in the selection of an Internet Service Provider (ISP)*
- *how to analyse user requirements and produce specifications for suitable network and internet components, including hardware, software and infrastructure*

- **The main considerations involved in the selection of an Internet Service Provider (ISP)**

  - Speed: Ensure that the ISP offers the desired internet speed for your needs, such as bandwidth for heavy internet usage or gaming
  - Availability: Check if the ISP services your location and if there are any coverage gaps or black spots
  - Reliability: Consider the ISP's reputation for network uptime, stability and consistency.
  - Cost: Compare pricing plans, fees and other costs, such as installation fees, equipment rental fees, and monthly fees
  - Data Caps: Determine if the ISP has any data caps or usage restrictions and if they are appropriate for your needs
  - Customer Support: Consider the quality of customer support, including response time, available hours, and options for support
  - Contract Terms: Read the fine print on contract terms, including the length of the contract, termination fees, and any early termination penalties
  - Service Level Agreements (SLAs): Look for an ISP with a solid SLA that guarantees network uptime, response times and other key service metrics.

- **How to analyse user requirements and produce specifications for suitable network and internet components, including hardware, software and infrastructure**

  - Gather User Requirements: Start by conducting a thorough analysis of the user requirements, including the specific needs, goals, and constraints of the organization. This could involve conducting surveys, focus groups, or interviews with key stakeholders

  - Evaluate Network Requirements: Based on the gathered user requirements, determine the network's requirements, including the desired network topology, the number of users, the type of applications to be used, and the required bandwidth

  - Determine Network Components: Based on the network requirements, select the appropriate network components, including hardware, software, and infrastructure components. This may involve evaluating multiple options and making trade-off decisions based on factors such as cost, reliability, scalability, and performance

  - Produce a Network Architecture: Based on the selected components, create a high-level network architecture that outlines the components and how they will be integrated and configured

  - Create Detailed Specifications: Based on the network architecture, create detailed specifications for each component, including hardware specifications, software requirements, and infrastructure specifications. This may involve working with vendors and suppliers to ensure that the specifications meet their requirements

  - Validate and Test: Before finalising the specifications, validate the proposed network architecture and components through testing and simulation. This may involve pilot testing, lab testing, or end-to-end testing to ensure that the network meets the user requirements and performs as expected

  - Finalise the Network: Based on the results of the testing and validation, finalise the network architecture and specifications and implement the selected components.

Learners should understand:

- *the main properties and characteristics of local area, (LAN) and wide area (WAN) networks*
- *the characteristics of: VLAN, WLAN and VPN networks, their use and the equipment required to utilise them*
- *contemporary issues involving usage of VPN technologies, their advantages and disadvantages (e.g. increased security, decreased visibility, dependence on third-party hardware)*
- *the benefits of computer networks in terms of:*
- *efficient use of software and hardware resources*
- *data access and sharing*
- *collaborative working*
- *effective communication*
- *central management/monitoring of users, security and data*
- *that in a distributed network, the sharing of resources is arranged by the operating system, without any action being required by the user*
- *the different types of server, including:*
- *file server*
- *printer server*
- *internet (proxy) server and mail server*
  in terms of the facilities and resources they provide to authorised client stations.

- **The main properties and characteristics of local area, (LAN) and wide area (WAN) networks**

  A Local Area Network (LAN) has the following main characteristics:

  - Geographic scope: LANs typically cover a small geographic area, such as a single building or campus
  - Network size: LANs are typically limited to a few dozen to a few thousand devices.
  - Data transfer speed: LANs offer high data transfer speeds, typically in the range of 10 Mbps to 100 Gbps
  - Cost: LANs are generally less expensive to implement than other types of networks, such as WANs or Metropolitan Area Networks (MANs)
  - Security: LANs can be secured through the use of firewalls, access controls, and encryption
  - Network topology: LANs can be configured in various topologies, including star, bus, ring, and mesh
  - Protocols: LANs use various communication protocols, such as Ethernet, TCP/IP, and Wi-Fi.

A Wide Area Network (WAN) has the following main characteristics:

  - Geographic scope: WANs typically cover a large geographic area, such as a city, a country, or even the entire world
  - Network size: WANs can connect an unlimited number of devices
  - Data transfer speed: WANs typically offer lower data transfer speeds compared to LANs, in the range of a few kilobits per second to several gigabits per second
  - Cost: WANs are generally more expensive to implement and maintain than LANs, due to the need for specialised equipment and the use of long-distance communication technologies
  - Security: WANs are vulnerable to various security threats, such as hacking, eavesdropping, and man-in-the-middle attacks, and require the use of multiple security measures to ensure the confidentiality, integrity, and availability of data.
  - Network topology: WANs can be configured in various topologies, including point-to-point, star, mesh, and hybrid
  - Protocols: WANs use various communication protocols, such as Frame Relay, ATM, MPLS, and VPN.

- **The characteristics of: VLAN, WLAN and VPN networks, their use and the equipment required to utilise them**

  - VLANs

    Virtual LAN (VLAN) is a concept in computer networking that allows administrators to logically segment a physical network into smaller broadcast domains. VLANs are used to logically segment a physical network into smaller broadcast domains. The main purpose of using VLANs is to increase network security, improve scalability, and enhance network management.

Here are some of the key characteristics of a VLAN network:

- Logical Segmentation: VLANs allow a physical network to be divided into smaller, logically separate broadcast domains. This provides network administrators with greater control over the flow of data and helps to improve network security and performance
- Increased Security: By dividing a physical network into smaller logical segments, VLANs make it more difficult for unauthorised users to access sensitive data. This is because VLANs can be configured to allow only specific types of network traffic between particular groups of devices
- Improved Scalability: VLANs help to improve network scalability by allowing administrators to add more devices to the network without having to physically reconfigure the underlying infrastructure
- Reduced Broadcast Traffic: In a VLAN network, broadcast traffic is limited to the specific VLAN segment, reducing the overall amount of broadcast traffic on the network and improving overall performance
- Enhanced Network Management: VLANs allow administrators to easily manage network resources and devices, and to quickly reconfigure network settings as required
- Reduced Network Complexity: By reducing the size of broadcast domains and allowing administrators to logically segment the network, VLANs can help to reduce the overall complexity of a network and improve network reliability.

The equipment needed to set up a VLAN network:

- Switch: A network switch is a central device that connects all the other devices in a network. In a VLAN network, the switch must support VLAN tagging and be able to create multiple virtual interfaces, each representing a separate VLAN
- Router: A router is used to route traffic between different VLANs. The router must be capable of handling VLAN-tagged traffic and have the ability to perform inter-VLAN routing
- Network Interface Cards (NICs): Each device in a VLAN network must have a network interface card that supports VLAN tagging
- Cables: Cables are used to connect devices to the switch. Depending on the switch, either Ethernet or fibre-optic cables may be required
- Network Management Software: Network management software is used to manage and configure the VLAN network. This can be done using a command-line interface or a graphical user interface, depending on the software being used.

- WLANs

A Wireless Local Area Network (WLAN) is a type of network that uses wireless communication technology to connect devices. WLANs are used to connect devices wirelessly within a limited area, such as a home, small office, or campus environment. WLANs provide users with the ability to connect to the network and access network resources from any location within the coverage area.

Here are some of the key characteristics of a WLAN network:

- Wireless Connectivity: The main characteristic of a WLAN network is that it uses wireless communication to connect devices, eliminating the need for physical cables
- Mobility: WLANs allow devices to connect and disconnect from the network dynamically, enabling users to move around freely within the coverage area without losing their connection
- Flexibility: WLANs can be set up quickly and easily, making them ideal for temporary or ad-hoc network deployments. They can also be easily reconfigured as needed

- Limited Range: WLANs have a limited range, typically a few hundred feet, and are best suited for smaller areas such as homes, small offices, or campus environments
- Interference: WLANs are susceptible to interference from other wireless devices and can experience reduced performance in areas with high levels of wireless activity
- Security: WLANs can be vulnerable to security threats such as eavesdropping and unauthorised access. To mitigate these risks, WLAN networks should be secured using encryption and authentication methods such as WPA or WPA2
- Network Management: WLANs require proper network management and monitoring to ensure reliable and secure operation. This can be done using network management software or hardware
- Standardisation: WLANs are standardised through the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard, which defines the specifications for wireless communication in a WLAN network.

Here is the equipment needed to set up a WLAN network:

- Wireless Access Point (AP): A wireless access point (AP) is the central device that provides wireless connectivity to devices. The AP acts as a bridge between the wireless devices and the wired network
- Wireless Network Adapter: Each device that needs to connect to the WLAN must have a wireless network adapter installed. This adapter allows the device to communicate with the wireless access point
- Router: A router is used to route traffic between the WLAN and the wired network. The router must support wireless connectivity and be able to connect to the wireless access point
- Cables: Cables are used to connect the router to the wired network. Ethernet or fibre-optic cables may be required, depending on the specific network setup
- Network Management Software: Network management software is used to manage and configure the WLAN network. This can be done using a command-line interface or a graphical user interface, depending on the software being used.

- VPNs

A Virtual Private Network (VPN) is a type of network that allows users to securely access resources over a public network, such as the Internet. VPNs are commonly used by remote workers, businesses, and organisations to securely access their internal networks, resources, and applications from outside the office. Here are some of the key characteristics of a VPN network:

- Encryption: VPNs use encryption to protect the data being transmitted over the public network, ensuring that it cannot be intercepted by unauthorised users
- Remote Access: VPNs allow users to securely access network resources from remote locations, such as from home or while travelling
- Secure Communication: VPNs provide secure communication between devices, even over a public network, by encrypting the data being transmitted
- Tunnelling: VPNs use tunnelling protocols, such as PPTP, L2TP/IPSec, or OpenVPN, to create a virtual tunnel between the client device and the network. The data being transmitted is encapsulated within the tunnel, providing an extra layer of protection
- Network Segmentation: VPNs can be used to segment a network into multiple virtual networks, providing an additional layer of security and allowing different departments or users to access different resources
- Authentication: VPNs use authentication methods, such as passwords, certificates, or biometric authentication, to ensure that only authorised users can access the network

- Compatibility: VPNs are compatible with a wide range of devices, including laptops, smartphones, tablets, and servers, making it possible to securely access network resources from anywhere
- Network Management: VPNs require proper network management and monitoring to ensure reliable and secure operation. This can be done using network management software or hardware.

Here is the equipment needed to set up a VPN network:

- VPN Server: A VPN server is the central device that provides VPN connectivity to clients. The VPN server acts as the gateway between the client device and the internal network
- Client Devices: Each device that needs to connect to the VPN network must have a VPN client installed. The VPN client allows the device to communicate with the VPN server
- Router: A router is used to route traffic between the VPN network and the public network. The router must support VPN connectivity and be able to connect to the VPN server
- Cables: Cables are used to connect the router to the internal network. Ethernet or fibre-optic cables may be required, depending on the specific network setup
- Network Management Software: Network management software is used to manage and configure the VPN network. This can be done using a command-line interface or a graphical user interface, depending on the software being used.

- **Contemporary issues involving usage of VPN technologies, their advantages and disadvantages (e.g. increased security, decreased visibility, dependence on third-party hardware)**

Contemporary issues involving the usage of VPN technologies include:

- Security Concerns: Despite providing a secure connection over public networks, VPNs have their own set of security risks and concerns. For example, a VPN server can be hacked or compromised, leading to sensitive information being exposed. Additionally, VPNs are only as secure as the encryption methods used, and weak encryption can be easily broken by malicious actors
- Dependence on Third-Party Hardware: VPNs rely on the reliability and security of third-party hardware, such as routers, to provide VPN connectivity. This can increase the risk of outages and security breaches, as well as the cost of managing and maintaining the VPN network
- Decreased Visibility: VPNs can hide the origin of network traffic, making it difficult to detect and prevent malicious activity. This can make it more difficult to monitor network security and enforce security policies
- Complexity: VPNs can be complex to set up and maintain, requiring specialised knowledge and skills. Additionally, compatibility issues can arise between different VPN clients and servers, making it difficult to ensure reliable and secure operation.

Despite these issues, VPNs have several advantages, including:

- Increased Security: VPNs provide a secure connection over public networks, ensuring that sensitive information is protected from theft or interception. This can help to prevent data breaches and protect sensitive information
- Remote Access: VPNs allow users to securely access network resources from remote locations, making it possible for employees to work from home or while travelling
- Cost Savings: VPNs can be a cost-effective solution for businesses and organisations, as they can eliminate the need for expensive leased lines or dedicated network connections

- Increased Productivity: VPNs can increase employee productivity by providing access to network resources from anywhere, at any time
- Network Segmentation: VPNs can be used to segment a network into multiple virtual networks, allowing different departments or users to access different resources.

- **The benefits of computer networks in terms of:**

  Efficient use of software and hardware resources

  - Centralised Resource Sharing: Computer networks allow multiple users to access and use shared resources, such as printers, scanners, and storage devices, reducing the need for each user to have their own devices. This can lead to cost savings and improved resource utilisation
  - Centralised Software Management: Computer networks can be used to centrally manage and distribute software, ensuring that all users have access to the latest software versions. This can simplify software updates and reduce the risk of software compatibility issues
  - Load Balancing: Computer networks can be used to distribute the processing load across multiple computers, improving overall system performance and reliability. This can be especially useful in large organisations where many users may be accessing the same applications and resources
  - Improved Collaboration: Computer networks allow multiple users to collaborate on projects and share information, improving communication and coordination among team members
  - Remote Access: Computer networks allow users to access network resources from remote locations, improving productivity and flexibility. This can be especially useful for telecommuters or employees who travel frequently
  - Data Backup and Recovery: Computer networks can be used to back up and recover data, reducing the risk of data loss due to hardware failure or other issues.

  - **data access and sharing**

    - Centralised Data Storage: Computer networks allow for centralised data storage, where all data can be stored in a single location and accessed by multiple users. This makes it easier to manage and protect sensitive information and ensures that all users have access to the latest data
    - Improved Data Access: Computer networks allow users to access and share data from any location, improving collaboration and coordination among team members. This can be especially useful for remote workers or employees who travel frequently
    - Data Backup and Recovery: Computer networks can be used to back up and recover data, reducing the risk of data loss due to hardware failure or other issues
    - Enhanced Data Security: Computer networks can be secured using encryption and other security measures, protecting sensitive data from theft or unauthorised access
    - Improved Data Management: Computer networks can be used to manage and organise data, making it easier to find and retrieve information. This can improve overall efficiency and productivity
    - Data Sharing: Computer networks allow multiple users to access and share data, improving collaboration and communication among team members. This can lead to more effective decision-making and problem-solving.

- **collaborative working**

  - Improved Communication: Computer networks allow multiple users to communicate and collaborate in real time, regardless of their location. This can lead to more efficient and effective problem-solving and decision-making
  - Shared Workspaces: Computer networks allow multiple users to access and work on shared files and documents, improving collaboration and coordination among team members
  - Remote Access: Computer networks allow users to access network resources from remote locations, making it possible for team members to work together even if they are not in the same location. This can be especially useful for telecommuters or employees who travel frequently
  - Centralised Resource Sharing: Computer networks allow multiple users to access and use shared resources, such as printers, scanners, and storage devices, reducing the need for each user to have their own devices. This can lead to cost savings and improved resource utilisation
  - Centralised Software Management: Computer networks can be used to centrally manage and distribute software, ensuring that all users have access to the latest software versions. This can simplify software updates and reduce the risk of software compatibility issues
  - Improved Decision-Making: Computer networks can be used to collect and analyse data, making it possible for team members to make informed decisions based on accurate and up-to-date information.

- **effective communication**

  - Real-Time Communication: Computer networks allow for real-time communication, allowing team members to exchange information and collaborate in real time, regardless of their location
  - Improved Accessibility: Computer networks allow users to communicate and access information from any location, making it easier for team members to stay connected and informed, even when they are not in the same location
  - Enhanced Collaboration: Computer networks can be used to support collaboration and coordination among team members, improving the effectiveness of group projects and tasks
  - Centralised Communication: Computer networks can be used to centralise communication, making it easier to manage and archive important messages and conversations
  - Multimedia Communication: Computer networks support multimedia communication, allowing team members to exchange audio, video, and other forms of multimedia, improving the effectiveness of communication
  - Email and Instant Messaging: Computer networks support email and instant messaging, allowing team members to quickly exchange messages and collaborate in real time

- **central management/monitoring of users, security and data**

  - Centralised Management: Computer networks allow for centralised management of network resources, including users, security, and data. This makes it easier to monitor, manage, and secure network resources and ensure that they are used in an effective and efficient manner

- Improved Security: Computer networks can be used to enhance security by implementing security measures such as firewalls, antivirus software, and encryption. This helps to protect sensitive data and prevent unauthorised access to network resources
- Centralised Data Backup: Computer networks allow for centralised data backup, making it easier to protect important data and ensure that it is recoverable in the event of a disaster or data loss
- User Management: Computer networks allow for centralised management of user accounts, making it easier to control access to network resources and ensure that they are used in an appropriate manner
- Monitoring and Tracking: Computer networks can be used to monitor and track network usage, helping to identify potential security threats and ensuring that network resources are used efficiently
- Remote Management: Computer networks can be managed remotely, making it possible to monitor and manage network resources from any location, even if you are not in the same location as the network.

- **In a distributed network, the sharing of resources is arranged by the operating system, without any action being required by the user**

  In a distributed network, the operating system is responsible for managing and sharing network resources such as hardware, software, and data. This means that the operating system automatically manages and distributes resources to users, without requiring any manual intervention from the user.

  For example, if a user on a distributed network wants to access a file stored on a remote server, the operating system will automatically manage the communication and data transfer between the user's computer and the server. The user does not need to manually initiate the transfer or manage the communication process.

  This type of resource sharing enables users to access network resources seamlessly and efficiently, without the need for manual intervention. This can improve productivity and simplify the process of using network resources.

  Additionally, a distributed network allows for load balancing and fault tolerance, as the operating system can dynamically allocate resources and redirect traffic to other nodes in the network in the event of a failure or overload. This can improve the reliability and availability of network resources.

- **the different types of servers, in terms of the facilities and resources they provide to authorised client stations, including:**

  - **file server**

    - Storage: The file server provides storage space for shared files, allowing multiple users to access and store data in a centralised location
    - File sharing: The file server facilitates the sharing of files among users, enabling them to collaborate on projects and access shared data
    - Backup and recovery: The file server provides backup and recovery capabilities, allowing administrators to create regular backups of data and restore files in the event of data loss
    - Access control: The file server provides access control mechanisms to ensure that only authorised users have access to sensitive files and data

- Version control: The file server provides version control capabilities, allowing users to keep track of changes made to files and revert to previous versions if needed
- Network protocols: The file server supports various network protocols, such as SMB, NFS, FTP, and others, enabling users to access and transfer files over a network
- Scalability: The file server can be scaled to meet growing storage and processing needs, making it a flexible solution for organisations of all sizes
- Performance: The file server provides fast and efficient access to files and data, ensuring that users can work efficiently and without delays.

- **printer server**

- Printer sharing: The printer server enables multiple users on a network to access and use the same printer, eliminating the need for each user to have a separate printer
- Print job management: The printer server manages print jobs, ensuring that they are sent to the correct printer and that they are printed in the order they were received
- Queuing: The printer server provides queuing capabilities, allowing users to submit print jobs even if the printer is currently in use, and ensures that they are printed in the order they were received
- Load balancing: The printer server can distribute print jobs across multiple printers, ensuring that no single printer is overwhelmed with too many jobs and improving overall print performance
- Print job tracking: The printer server provides tracking capabilities, allowing users to monitor the status of their print jobs and receive notifications when jobs are completed
- Network protocols: The printer server supports various network protocols, such as LPD, IPP, SMB, and others, enabling users to submit print jobs from various devices and platforms
- Driver management: The printer server manages the drivers for the connected printers, ensuring that the correct drivers are installed and used for each printer
- Security: The printer server provides security features, such as user authentication and access control, to ensure that only authorised users have access to the printers and their functions.

- **Internet (proxy) server and mail server**

  An Internet proxy server is a server that acts as an intermediary between a client and a server, forwarding requests and responses between them. It provides several key facilities and resources to its users, including:

- Internet access control: The proxy server acts as a gatekeeper, allowing or denying access to the Internet based on specific policies and rules
- Caching: The proxy server caches frequently accessed websites and content, reducing the amount of data that needs to be transmitted over the Internet and improving the response time for users
- Anonymity: The proxy server can provide anonymity to its users by hiding their IP address and other identifying information, allowing them to browse the Internet securely and privately
- Content filtering: The proxy server can filter Internet content based on specific policies, blocking access to websites or content that is deemed inappropriate or harmful
- Network security: The proxy server provides network security by acting as a firewall, protecting against external threats and attacks, such as malware and hacking attempts
- Load balancing: The proxy server can distribute Internet traffic across multiple servers, improving the performance and reliability of the network

- Bandwidth optimisation: The proxy server can optimise bandwidth usage by compressing data and reducing the amount of data that needs to be transmitted over the Internet
- Remote access: The proxy server can provide remote access to the Internet, allowing users to access the Internet from remote locations.

A mail server is a computer system that provides email services to users. It provides several key facilities and resources to its users, including:

- Email storage: The mail server provides storage space for email messages, allowing users to receive, store, and send messages
- Email delivery: The mail server facilitates the delivery of email messages between users, whether they are on the same network or on different networks
- Spam and virus protection: The mail server provides mechanisms for filtering out unwanted or malicious emails, such as spam and virus-infected messages, to ensure that users receive only legitimate emails
- Mailing lists: The mail server can manage mailing lists, allowing users to send messages to large groups of recipients and manage their subscriptions
- Access control: The mail server provides access control mechanisms to ensure that only authorised users have access to email services and data
- Message retrieval: The mail server enables users to retrieve their email messages from any location, using standard email protocols such as POP3, IMAP, and others
- Authentication: The mail server provides authentication mechanisms to verify the identity of users and prevent unauthorised access to email services
- Backup and recovery: The mail server provides backup and recovery capabilities, allowing administrators to create regular backups of email data and restore it in the event of data loss.

Data transmission

Learners should understand:

- *the function and performance of common hardware devices, including:*
- *hubs*
- *switched hubs*
- *routers*
- *repeaters*
- *wireless access points*
- *media converters*
- *the role of, and facilities provided by, network operating and accounting software, including:*
- *resource and applications management*
- *data security*
- *data storage*
- *back up*
- *monitoring*
- *activity management*
- *the role and facilities of firewall software or appliances*
- *the characteristics of contemporary communication infrastructures, including:*
- *twisted pair wire (UTP and STP)*
- *fibre optic cable*
- *wireless (radio, infrared, microwave and satellite)*
- *how to calculate transmission speeds and times to transfer files and the effect on end user experience.*

- **The function and performance of common hardware devices, including:**
  - **Hubs**
    A hub is a networking device that allows multiple devices to be connected to a single network. It operates at the physical layer of the OSI model and functions as a central point for transmitting data between connected devices.

    - Data transmission: When a device connected to the hub wants to send data, it transmits the data to the hub, which then broadcasts the data to all other devices connected to the hub. This allows multiple devices to communicate with each other on the same network
    - Broadcasting: Hubs broadcast data to all connected devices, regardless of the intended recipient. This means that all connected devices receive the data and must process it to determine if it is intended for them
    - Collision detection: Hubs do not have the ability to detect collisions, which can occur when multiple devices try to transmit data at the same time. If a collision occurs, the data will be corrupted, and the devices will need to resend the data.
    - Speed: Hubs operate at a fixed speed, which is typically 10 Mbps or 100 Mbps, depending on the model. This means that the speed of the network is limited by the speed of the hub
    - Security: Hubs do not provide any security features, so all connected devices are exposed to potential security threats.

  - **Switched hubs**

    Switched hubs, also known as switches, are advanced versions of traditional hubs that provide improved performance and functionality. They operate at the data link layer of the OSI model and provide dedicated connections between devices, allowing for faster data transmission and reduced network congestion.

    - Data transmission: Switches use a process called address learning to create a table of device addresses, allowing them to determine which device to send data to. When a device wants to transmit data, the switch uses this table to send the data directly to the intended recipient, rather than broadcasting it to all devices as with a traditional hub. This results in faster data transmission and reduced network congestion
    - Collision detection: Switches use a process called collision detection to prevent data collisions from occurring. If two devices try to transmit data at the same time, the switch will detect the collision and temporarily block the transmission of one of the devices until it is safe to resume
    - Speed: Switches typically operate at faster speeds than traditional hubs, with speeds ranging from 100 Mbps to 10 Gbps or higher. This allows for faster data transmission and improved overall network performance
    - Security: Some switches include basic security features, such as port security, which allows administrators to limit the number of devices that can be connected to a specific port
    - VLANs: Switches can also support Virtual LANs (VLANs), allowing administrators to create multiple isolated network segments on the same switch. This provides improved network security and can help reduce network congestion.

  - **Routers**

    Routers are networking devices that perform the task of forwarding data packets between computer networks. They use routing tables and protocols to determine the best path for forwarding the data packets and to prevent loops in the network.

- Packet Receiving: Routers receive data packets from connected devices and store them in memory
- Determining the Best Path: The router then examines the destination address of the incoming data packet and consults its routing table to determine the best path for forwarding the packet
- Packet Forwarding: Once the best path is determined, the router sends the packet to the next hop along that path
- Updating Routing Information: Routers exchange information with other routers in the network using routing protocols. This allows routers to update their routing tables and ensure that they have the most up-to-date information about the network topology
- Packet Filtering: Routers can also be configured to block or filter certain types of data packets based on criteria such as source or destination address.

- **Repeaters**

  Repeaters are networking devices that are used to extend the range of a network. They work by receiving a weak or degraded signal, amplifying it, and then retransmitting it to extend the overall range of the network.

  - Signal Receiving: The repeater receives a weak or degraded signal from a device on the network
  - Signal Amplification: The repeater amplifies the signal to improve its strength and clarity
  - Signal Retransmission: The repeater then retransmits the amplified signal to extend the range of the network
  - Supporting Multiple Devices: Repeaters can support multiple devices on the network by forwarding signals between them
  - Transparency: Repeaters are typically transparent to the devices on the network, meaning that the devices are unaware of their presence and do not need to be configured to work with the repeater.

- **Wireless access points**

  Wireless Access Points (WAPs) are networking devices that allow devices to connect to a wireless network and access network resources, such as the internet. They provide wireless connectivity to devices by using radio waves to transmit and receive data.

  - Broadcasting a Wireless Signal: The WAP broadcasts a wireless signal that devices can detect and connect to
  - Authentication and Authorisation: The WAP can be configured to require authentication and authorisation from devices before they are allowed to connect to the network. This can be done using security protocols such as WEP, WPA, or WPA2
  - Network Access: Once a device is authenticated and authorised, it can access the network resources and communicate with other devices on the network
  - Signal Strength and Range: The range and strength of the wireless signal depend on the WAP's specifications and the surrounding environment. WAPs can be placed in strategic locations to extend the range of the wireless network
  - Network Management: The WAP can be configured and managed through a web-based interface or other network management tools. This allows network administrators to monitor network activity, control access, and make changes to the network configuration.

- **Media converters**

  Media converters are networking devices that are used to convert signals from one type of physical medium to another. They are used to connect devices that use different types of physical media, such as copper and fibre optic cables, to allow them to communicate with each other.

  - Signal Conversion: Media converters receive signals from one type of physical medium, such as a copper Ethernet cable, and convert the signals into a form that can be transmitted over a different type of physical media, such as a fibre optic cable
  - Signal Regeneration: Some media converters also regenerate the signals to improve their quality and reliability
  - Data Rate Conversion: Media converters can also be used to convert between different data rates, such as converting from Fast Ethernet (100 Mbps) to Gigabit Ethernet (1 Gbps)
  - Network Extension: Media converters can be used to extend the distance of a network by allowing signals to be transmitted over longer distances using fibre optic cable
  - Support for Multiple Protocols: Many media converters support multiple protocols, such as Ethernet, Fibre Channel, and ATM, allowing them to work with a variety of network configurations.

- **The role of, and facilities provided by, network operating and accounting software, including:**

  - **Resource and applications management**
    Resource and application management software is designed to help organizations optimise the use of their computing resources and manage the deployment, execution, and performance of applications.

    - Resource allocation: The software can dynamically allocate computing resources such as CPU, memory, and storage to different applications based on their current and predicted resource requirements
    - Application deployment: The software can automate the deployment and configuration of applications, reducing the time and effort required to get them up and running
    - Performance management: The software can monitor the performance of applications and identify and resolve performance bottlenecks, helping to ensure that they run smoothly and efficiently
    - Resource utilisation: The software can provide detailed information on the utilisation of computing resources, helping organisations to understand where their resources are being used and identify any inefficiencies
    - Scalability: The software can support the scaling of applications to meet changing demands, automatically adding or removing resources as needed
    - Disaster recovery: The software can support disaster recovery by automatically transferring applications to alternative computing resources in the event of a failure
    - Cost optimisation: By optimising the use of computing resources, resource and application management software can help organisations to reduce their costs and improve their return on investment.

- **Data security**

  Data security software plays a critical role in protecting sensitive and confidential information from unauthorised access, theft, and loss.

  - Encryption: The software can encrypt data to protect it from unauthorised access and ensure that it can only be read by authorised users
  - Authentication: The software can require users to provide credentials such as a password or fingerprint to access the data, ensuring that only authorised users can access it
  - Access control: The software can define who can access specific data and what actions they can perform, such as reading, writing, or deleting
  - Firewall: The software can act as a firewall to block unauthorised access to a network, protecting data from external threats
  - Data backup and recovery: The software can automatically back up data to protect against data loss and provide the ability to recover data in the event of a disaster
  - Antivirus protection: The software can detect and remove viruses and other malicious software, protecting data from cyber-attacks
  - Intrusion detection: The software can detect and alert administrators to potential security breaches, allowing them to take action to prevent unauthorised access
  - Compliance: The software can help organisations to meet regulatory requirements such as HIPAA, PCI-DSS, and GDPR by providing data security measures that comply with these regulations.

- **Data storage**

  Data storage software plays a critical role in managing and storing large amounts of data in an organised and secure manner.

  - File management: The software can manage and organise large amounts of data, allowing users to easily store, access, and retrieve files
  - Data backup and recovery: The software can automatically back up data to protect against data loss and provide the ability to recover data in the event of a disaster
  - Data compression: The software can compress data to reduce the amount of storage space required, helping to save costs and improve storage efficiency.
  - Data encryption: The software can encrypt data to protect it from unauthorised access and ensure that it can only be read by authorised users
  - Data replication: The software can replicate data across multiple storage devices to ensure data availability and protect against data loss in the event of a failure
  - Data deduplication: The software can identify and remove redundant data, reducing the amount of storage space required and improving storage efficiency
  - Storage virtualisation: The software can abstract physical storage resources and present them as a single logical storage pool, improving storage management and flexibility
  - Compliance: The software can help organisations to meet regulatory requirements such as HIPAA, PCI-DSS, and GDPR by providing secure data storage that complies with these regulations.

- **Back up**

  Backup software plays a critical role in protecting data from loss due to hardware failure, software corruption, or other disasters.

  - Data backup: The software can automatically back up important data to protect against data loss and ensure that it can be recovered in the event of a disaster
  - Data recovery: The software can provide the ability to recover data from backups, restoring it to its previous state in the event of data loss
  - Incremental backups: The software can perform incremental backups, backing up only changes to the data since the last backup, reducing the time and storage space required for backups
  - Compression: The software can compress data to reduce the amount of storage space required for backups, helping to save costs and improve backup efficiency
  - Encryption: The software can encrypt backups to protect sensitive data from unauthorised access and ensure that it can only be read by authorised users
  - Remote backups: The software can perform backups to remote locations, protecting against data loss in the event of a local disaster
  - Scheduling: The software can be scheduled to perform backups at specific times, reducing the manual effort required to initiate backups
  - Monitoring and reporting: The software can monitor backups and provide detailed reports on the status of backups, helping organisations to ensure that their data is being backed up effectively.

- **Monitoring**

  Monitoring software plays a critical role in ensuring the health and performance of systems, networks, and applications.

  - System and resource monitoring: The software can monitor system and resource utilisation, including CPU, memory, disk, and network usage, providing insight into system performance and availability
  - Application monitoring: The software can monitor the performance of specific applications, providing insight into their availability and response times, and helping to identify and resolve performance issues
  - Event logging: The software can log events, such as errors or performance issues, allowing organisations to analyse historical data to identify trends and resolve problems
  - Alerts and notifications: The software can alert administrators to issues, such as system failures or performance degradation, allowing them to take prompt action to resolve problems
  - Customisable dashboards: The software can provide customisable dashboards, allowing administrators to view relevant performance metrics and quickly identify issues
  - Network monitoring: The software can monitor the performance of networks, including the availability of network resources and the response times of network services
  - Cloud monitoring: The software can monitor the performance of cloud resources, providing insight into the health and performance of cloud-based systems, applications, and services
  - Integrations: The software can integrate with other IT tools and systems, such as ticketing systems and log management tools, to provide a unified view of system and application performance.

- **Activity management**

  Network Activity Management software plays a crucial role in monitoring, managing, and analysing network activity in an organization. The primary function of this software is to provide visibility into the network and to give network administrators the ability to detect, diagnose, and resolve issues related to network performance, security, and reliability.

  - Network Monitoring: The software provides real-time visibility into the network performance, availability, and usage. It allows administrators to detect and resolve issues before they impact the users
  - Traffic Analysis: The software provides a detailed analysis of network traffic patterns and trends, enabling administrators to identify bottlenecks, optimise network performance, and detect security threats
  - Security Management: The software provides security features such as intrusion detection, firewall management, and threat intelligence to help secure the network and protect against malicious attacks
  - Performance Management: The software provides performance management features that help administrators to identify and resolve performance issues and optimise network performance
  - Inventory Management: The software provides an inventory of all network devices, including hardware and software, to help administrators manage their network assets
  - Reporting and Analytics: The software provides customisable reports and dashboards that provide valuable insights into network activity, including performance metrics, traffic analysis, and security information.

- **The role and facilities of firewall software or appliances**

  A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. Its primary role is to protect a network from unauthorised access and other security threats by creating a barrier between the trusted internal network and the untrusted external network (such as the Internet).

  - Traffic filtering: Firewalls examine incoming and outgoing network traffic and block or allow it based on defined rules
  - Packet inspection: Firewalls inspect the header and payload of individual packets to ensure they meet the specified security rules
  - Network address translation (NAT): Firewalls can be used to translate the addresses of internal devices to a single external address, allowing the devices to be hidden behind the firewall
  - VPN support: Many firewalls support virtual private network (VPN) connections, allowing remote users to securely access the internal network
  - Intrusion detection and prevention: Firewalls can detect and prevent security threats such as malware, viruses, and unauthorised access attempts
  - Centralised management: Firewalls often have a centralised management interface that allows administrators to monitor and configure the firewall from a single location.

- **The characteristics of contemporary communication infrastructures, including:**
  - **Twisted pair wire (UTP and STP)**

    Twisted pair wire is a type of cable that consists of two insulated copper wires that are twisted together to form a single cable. There are two types of twisted pair cable: unshielded twisted pair (UTP) and shielded twisted pair (STP).

Unshielded Twisted Pair (UTP) Cable:

- UTP cables have no metal shield around the twisted wires, making them lighter and more flexible than STP cables
- UTP cables are widely used in modern communication networks because they are relatively cheap and easy to install
- UTP cables can transmit data at speeds of up to 10 Gbps over short distances.

Shielded Twisted Pair (STP) Cable:

- STP cables have a metal shield around the twisted wires to protect against electromagnetic interference (EMI)
- STP cables are typically used in environments where high levels of EMI are present, such as industrial settings or near high-voltage electrical equipment
- STP cables are typically more expensive and less flexible than UTP cables, but they offer better protection against interference.

- **Fibre optic cable**

  A fibre optic cable is a type of cable that is used to transmit data using light. It consists of a core made of glass or plastic fibres, surrounded by cladding and a protective coating. The core of the cable is designed to transmit light, which is used to transmit data in the form of pulses.

  Fibre optic cables are used in a variety of applications, including telecommunications, internet connectivity, and data centres. They are preferred over traditional copper cables because they have several advantages, including higher bandwidth, longer distances, and immunity to electromagnetic interference.

  Fibre optic cables are typically made up of a bundle of individual fibres, each of which is capable of transmitting data. They are used in both single-mode and multi-mode applications, depending on the needs of the system. In general, fibre optic cables are considered to be more reliable, secure, and efficient than traditional copper cables, making them a popular choice for transmitting data over long distances.

  - Light Transmission: Fibre optic cables use light to transmit data, which is much faster and more reliable than traditional electrical signals
  - Bandwidth: Fibre optic cables have a much higher bandwidth than traditional copper cables, allowing for the transmission of large amounts of data at high speeds
  - Immunity to Interference: Fibre optic cables are immune to electrical interference, making them suitable for use in environments where electromagnetic interference is a concern
  - Durability: Fibre optic cables are made of glass or plastic fibres, which are more durable than copper wires and less susceptible to breakage
  - Lightweight: Fibre optic cables are much lighter than traditional copper cables, making them easier to install and less likely to cause damage during installation
  - Low Loss: Fibre optic cables have low loss, which means that the light signal transmitted through the cable does not lose strength over long distances
  - Security: Fibre optic cables are difficult to tap or intercept, making them a more secure option for transmitting sensitive information.

- **Wireless (radio, infrared, microwave and satellite)**

  Wireless communication can be achieved through various methods, including radio waves, infrared, microwave, and satellite.

  Radio Waves:
  - they have longer wavelengths compared to other forms of wireless communication
  - they can easily penetrate walls and other obstacles, making them suitable for indoor and outdoor communication
  - they are used in various applications, including broadcast radio, television, mobile phones, and Wi-Fi.

  Infrared:
  - they have shorter wavelengths compared to radio waves, and are not visible to the human eye
  - they are used for short-range communication, such as remote control for televisions and other electronics
  - they cannot penetrate walls or other obstacles.

  Microwave:
  - they have shorter wavelengths compared to radio waves and longer wavelengths compared to infrared
  - they are used for both short-range and long-range communication, including microwave ovens, cell phone towers, and satellite communication
  - they can penetrate walls and other obstacles to a limited extent.

  Satellite:
  - they use satellites orbiting the Earth to communicate with each other and with devices on the ground
  - they are used for global communication and navigation, including GPS and satellite television
  - they are highly reliable and can provide broad coverage, but can be disrupted by the Earth's atmosphere.

- **How to calculate transmission speeds and times to transfer files and the effect on end user experience.**

  The transmission speed can be calculated by dividing the size of the file by the time it takes to transfer the file. The time to transfer a file can be calculated by dividing the size of the file by the transmission speed.

  To calculate the effect on end-user experience, it is important to consider the user's expectations and the purpose of the file transfer. For example, a slow transfer speed may be acceptable for a non-urgent file but may be frustrating for a time-sensitive transfer.

  Factors that can affect transmission speeds and times include network bandwidth, congestion, and latency, as well as the size and type of file being transferred. To improve end-user experience, it may be necessary to optimise these factors or to provide alternative methods of file transfer, such as compression or streaming.

Cloud services

Learners should understand:

- *the differences between file synchronisation, file backup and file archive systems*
- *how cloud services work*
- *the difference between cloud computing and cloud storage*
- *the advantages and disadvantages of using cloud services (e.g. ease of building a new system, data are saved remotely from local hardware, reliance on internet connectivity, potential on going costs)*
- *the environmental concerns around cloud server resource usage*
- *different types of cloud services:*
- *Software as a Service (SaaS)*
- *Infrastructure as a Service (IaaS)*
- *Platform as a Service (PaaS)*
- *how the following cloud services are delivered:*
- *public cloud services*
- *private cloud services*
- *hybrid cloud environment*
- *the future of cloud services, including:*
- *content collaboration*
- *access control*
- *app delivery management*
- *virtual desktop solutions.*

- **The differences between file synchronisation, file backup and file archive systems**

  File synchronisation systems are designed to keep the contents of two or more folders or devices identical in real time, whereas file backup systems create a copy of important files and data at a specific point in time for recovery purposes in case of data loss.

  On the other hand, file archive systems are used to store files that are no longer needed in the regular workflow but may need to be accessed in the future. The files are typically compressed and stored in a way that minimises space usage while still allowing for easy retrieval.

- **How cloud services work**

  Cloud services are provided by remote servers that are accessed over the internet, typically owned and managed by a third-party service provider. These servers store data and applications, allowing users to access them from anywhere with an internet connection.

  Cloud services work by providing access to a shared pool of computing resources such as servers, storage, applications, and services. These resources are delivered to users on demand and can be easily scaled up or down as required.

  When a user accesses a cloud service, their request is routed to the appropriate server, and the data or application is returned over the internet. The user typically pays for the service on a subscription or pay-per-use basis, and the provider is responsible for managing the underlying infrastructure and ensuring the availability and security of the service.

Common examples of cloud services include web-based email services like Gmail, file storage and sharing services like Dropbox, and software as a service (SaaS) applications like Microsoft Office 365.

- **The difference between cloud computing and cloud storage**

  Cloud computing refers to the delivery of computing services over the internet, such as servers, storage, databases, software, analytics, and more. It allows users to access and use these computing resources on demand, without the need for their own physical infrastructure or hardware.

  Cloud storage, on the other hand, refers to the storage of data on remote servers that are accessed over the internet. It allows users to store and access files and data from anywhere, as long as they have an internet connection.

  In other words, cloud computing involves the delivery of a range of computing services over the internet, while cloud storage specifically refers to the storage of data on remote servers. Cloud computing may involve cloud storage, but it also includes other services such as processing power, software, and more.

- **The advantages and disadvantages of using cloud services (e.g. ease of building a new system, data are saved remotely from local hardware, reliance on internet connectivity, potential on going costs)**

  Advantages of using cloud services include:

  - Scalability: Cloud services are easily scalable, meaning that users can quickly and easily add or remove computing resources as needed
  - Flexibility: Cloud services provide users with the flexibility to access computing resources from anywhere with an internet connection, using any device
  - Cost-effective: Cloud services often have a pay-as-you-go pricing model, which means that users only pay for the resources they use, rather than investing in costly hardware and infrastructure
  - Remote access to data: Cloud services provide users with remote access to their data, which can be particularly useful for mobile or remote workers
  - Easy to set up and use: Cloud services are typically easy to set up and use, as most of the underlying infrastructure and maintenance are handled by the service provider.

  Disadvantages of using cloud services include:

  - Reliance on internet connectivity: Cloud services require a reliable internet connection to function properly, which can be a problem in areas with poor or no connectivity
  - Security concerns: Storing data on remote servers can raise security concerns, especially if sensitive or confidential data is involved
  - Ongoing costs: Cloud services typically involve ongoing costs, which can add up over time and make them less cost-effective in the long run
  - Limited control over infrastructure: Users may have limited control over the underlying infrastructure of cloud services, which can be a problem for organisations with specific security or compliance requirements.

- **The environmental concerns around cloud server resource usage**

  The use of cloud server resources has a significant impact on the environment. Some of the key environmental concerns associated with cloud server resource usage are:

  - Energy consumption: Cloud servers require a large amount of energy to power and cool the equipment. The energy used by data centres that support cloud computing is a significant contributor to greenhouse gas emissions and global warming
  - Carbon emissions: The energy consumed by cloud servers is often generated from fossil fuels, which release carbon emissions that contribute to climate change
  - E-waste: The rapid growth in cloud computing has led to a corresponding increase in the production of electronic waste. When cloud servers reach the end of their useful life, they can contribute to the e-waste problem, which can be harmful to the environment if not disposed of properly
  - Water usage: Data centres require significant amounts of water for cooling and other purposes. In areas with water scarcity, this can contribute to environmental concerns.
  - Land use: Data centres require a large amount of land, which can contribute to deforestation and other environmental concerns.

- **Different types of cloud services:**
  - **Software as a Service (SaaS)**

    SaaS stands for "Software as a Service." It is a cloud computing model in which a third-party service provider hosts software applications and makes them available to users over the internet. Instead of installing and running the software on their own computers or servers, users access the software through a web browser or mobile app.

    SaaS applications are typically provided on a subscription or pay-per-use basis, with the service provider responsible for managing the underlying infrastructure, including servers, storage, and networking. SaaS applications are often highly scalable and flexible, allowing users to add or remove features or users as needed.

    Examples of SaaS applications include online productivity tools like Google Workspace or Microsoft Office 365, customer relationship management (CRM) software like Salesforce, and project management software like Asana. SaaS has become a popular way for businesses and individuals to access powerful software applications without having to invest in their own hardware and infrastructure.

  - **Infrastructure as a Service (IaaS)**

    IaaS stands for "Infrastructure as a Service." It is a cloud computing model in which a third-party service provider offers virtualised computing resources over the internet. IaaS provides users with access to servers, storage, networking, and other computing infrastructure, which they can use to build, deploy, and manage their own software applications and services.

    With IaaS, users have complete control over their computing environment, including the operating system, middleware, and applications. They can create, manage, and delete virtual servers as needed, without having to invest in physical hardware or infrastructure.

    IaaS providers typically offer a range of virtualised resources, such as virtual machines, storage, and networking, which users can configure and manage using a web-based dashboard or API. This allows users to scale their infrastructure up or down as needed, depending on their workload or usage patterns.

Examples of IaaS providers include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform. IaaS has become a popular way for businesses and organisations to quickly and easily deploy and manage their own computing infrastructure without having to invest in physical hardware or maintain their own data centre.

- **Platform as a Service (PaaS)**

  PaaS stands for "Platform as a Service." It is a cloud computing model in which a third-party service provider offers a platform that enables developers to build, deploy, and manage their own software applications over the internet.

  With PaaS, developers have access to a complete development and deployment environment, including tools, frameworks, and services. The PaaS provider typically manages the underlying infrastructure, including servers, storage, and networking, allowing developers to focus on building and deploying their applications.

  PaaS provides a range of features and tools that help developers build and deploy applications more quickly and efficiently, such as pre-built components, application templates, and automated deployment processes. PaaS platforms can also provide additional services such as databases, messaging systems, and application monitoring and management.

  Examples of PaaS providers include Heroku, Microsoft Azure App Service, and Google App Engine. PaaS has become a popular way for developers and organisations to build and deploy their own software applications more quickly and efficiently, without having to worry about the underlying infrastructure.

- **How the following cloud services are delivered:**
  - **Public cloud services**

    Public cloud services are delivered over the internet by third-party service providers that own and manage the underlying infrastructure. These service providers offer a range of cloud-based services, such as computing power, storage, networking, and software applications, which customers can access and use on demand.

    To access public cloud services, customers typically sign up for an account with the cloud service provider and pay for the resources they consume. They can then access and manage their cloud resources through a web-based dashboard or API, which provides a range of tools and features for creating and managing their applications and services.

    Public cloud services are delivered using a multi-tenant architecture, which means that multiple customers share the same physical infrastructure. The cloud provider uses virtualisation and other technologies to ensure that each customer's data and applications are isolated and secure.

    Public cloud services offer a range of benefits, including high scalability, flexibility, and cost-efficiency, as customers only pay for the resources they consume. They also provide access to the latest technologies and tools, without the need for customers to invest in their own hardware or infrastructure.

    Examples of public cloud service providers include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform.

- **Private cloud services**

  Private cloud services are typically delivered using a combination of virtualisation and cloud management technologies, deployed on dedicated hardware and network infrastructure within an organisation's data centre or hosted in a service provider's data centre.

  In a private cloud environment, the organisation has complete control over the underlying infrastructure and resources, which are dedicated to its use alone. This allows the organisation to configure the infrastructure and services to meet its specific needs and requirements and to ensure high levels of security and data privacy.

  Private cloud services can be deployed on-premises using an organisation's own infrastructure, or hosted by a third-party service provider. Private cloud service providers typically offer a range of deployment models, such as dedicated private clouds or virtual private clouds, which provide a higher level of control and security than public cloud services.

  To access private cloud services, users typically connect to the cloud infrastructure using a secure network connection, such as a VPN, and access cloud resources through a web-based portal or API. Private cloud services can offer many of the same benefits as public cloud services, such as scalability, flexibility, and cost-efficiency while providing a higher level of control and security.

  Examples of private cloud service providers include VMware, Dell Technologies, and IBM.

- **Hybrid cloud environment**

  A hybrid cloud environment is typically delivered by combining private and public cloud services, which are connected and integrated using a range of technologies and tools.

  In a hybrid cloud environment, organisations can run some of their workloads and applications on-premises, in a private cloud environment, while using public cloud services to run other workloads and applications. The private and public clouds are connected using a hybrid cloud management platform, which provides a range of tools for managing and monitoring the hybrid environment.

  Hybrid cloud environments can be architected in a variety of ways, depending on the organisation's needs and requirements. For example, an organisation might use a public cloud for its customer-facing applications and a private cloud for its internal business applications. Alternatively, an organisation might use a private cloud for its most sensitive workloads and applications and a public cloud for less sensitive workloads.

  To access a hybrid cloud environment, users typically connect to the cloud infrastructure using a secure network connection, such as a VPN, and access cloud resources through a web-based portal or API.

  Hybrid cloud environments can offer many benefits, such as increased flexibility, scalability, and cost-efficiency, while providing a higher level of control and security than public cloud services alone. However, they can also be more complex to manage than either private or public cloud services alone, and require careful planning and architecture to ensure that they meet the organisation's needs and requirements.

  Examples of hybrid cloud platforms and services include AWS Outposts, Microsoft Azure Stack, and Google Anthos.

- **The future of cloud services, including:**
  - **Content collaboration**

    Cloud-based content collaboration services, such as Microsoft SharePoint, Google Drive, and Dropbox, allow users to store, share, and collaborate on documents, files, and other content from anywhere, using any device with an internet connection. These services offer a range of features and tools, such as version control, commenting, and real-time co-authoring, which make it easy for teams to work together on projects and collaborate on content in real time.

    In the future, content collaboration services are likely to become even more integrated and connected, allowing users to collaborate seamlessly across different platforms and services. For example, content collaboration services may be integrated with project management tools, communication platforms, and other cloud-based services, making it even easier for teams to work together on complex projects.

    Content collaboration services are also likely to become more intelligent and automated, using machine learning and other AI technologies to help users find and organise content more efficiently. For example, AI tools may be used to automatically tag and categorise documents and files, or to suggest relevant content based on user preferences and behaviours.

  - **Access control**

    The future of access control as a cloud service is expected to be driven by the growing demand for secure, flexible, and scalable access control solutions that can be easily integrated with cloud-based applications and services.

    Cloud-based access control solutions allow organisations to manage access to their data and applications from anywhere, using any device with an internet connection. These solutions offer a range of features and tools, such as multi-factor authentication, role-based access control, and identity management, which help organisations secure their data and applications against unauthorised access.

    In the future, cloud-based access control solutions are expected to become even more advanced and sophisticated, using machine learning and other AI technologies to provide more intelligent and context-aware access control. For example, AI tools may be used to analyse user behaviour and other contextual information to determine whether access to a particular resource or application should be granted or denied.

    Cloud-based access control solutions are also likely to become more integrated and interoperable with other cloud-based services and applications, such as SaaS applications, cloud storage services, and collaboration tools. This will make it easier for organisations to manage access to their data and applications across different platforms and services.

  - **App delivery management**

    The future of application delivery management as a cloud service is expected to be shaped by the increasing demand for fast, secure, and reliable application delivery across a range of devices and platforms.

Cloud-based application delivery management solutions allow organisations to manage and optimise the delivery of their applications from the cloud, using a range of tools and technologies such as load balancing, content caching, and application acceleration. These solutions help organisations ensure that their applications are delivered quickly and reliably to end-users, regardless of their location or device.

In the future, application delivery management solutions are likely to become even more advanced and sophisticated, using machine learning and other AI technologies to optimise application delivery based on user behaviour and other contextual information. For example, AI tools may be used to automatically route traffic to the closest and fastest data centre or to identify and address performance issues before they impact end-users.

Cloud-based application delivery management solutions are also expected to become more integrated with other cloud-based services and platforms, such as SaaS applications, cloud storage services, and content delivery networks. This will make it easier for organisations to manage and optimise the delivery of their applications across different platforms and services.

- **Virtual desktop solutions.**

  More organisations are adopting cloud-based solutions to provide secure, flexible, and cost-effective access to desktop applications and resources from anywhere, using any device.

  Cloud-based virtual desktop solutions, such as Amazon WorkSpaces, Microsoft Azure Virtual Desktop, and VMware Horizon Cloud, allow organisations to provision and manage virtual desktops and applications from the cloud, using a range of tools and technologies such as desktop virtualisation, application streaming, and remote display protocols. These solutions offer a range of benefits, such as increased security, improved manageability, and lower costs, compared to traditional on-premises desktop solutions.

  In the future, cloud-based virtual desktop solutions are likely to become even more advanced and sophisticated, using machine learning and other AI technologies to optimise the end-user experience and improve performance. For example, AI tools may be used to automatically adjust display resolution and quality based on network conditions or to identify and address performance issues before they impact end-users.

  Cloud-based virtual desktop solutions are also expected to become more integrated with other cloud-based services and platforms, such as SaaS applications, cloud storage services, and collaboration tools. This will make it easier for organisations to provide secure and flexible access to desktop applications and resources across different platforms and services.

Mobile technologies

Learners should understand:

- *the social impacts of the proliferation of mobile technologies*
- *the environmental impacts of providing infrastructure*
- *how technology supports mobile phone communication, including:*
- *mobile phone masts*
- *cells*
- *handoffs*
- *base station controller*
- *IMIE and IMSI*

- *the working of SIP, SS7 and IPv6 protocols*
- *stateful and non-stateful calls*
- *mobile switching centre and Public Switched Telephone Network (PSTN) telephone systems.*

- **The social impacts of the proliferation of mobile technologies**

  - Increased connectivity and communication: Mobile technologies have enabled people to communicate and connect with each other more easily and quickly, regardless of their location
  - Changes in social behaviour: The use of mobile technologies has changed social behaviour, including how people interact with each other, how they consume information, and how they engage in social and political activism
  - Access to information and services: Mobile technologies have increased access to information and services, particularly in areas with limited infrastructure
  - Economic impacts: Mobile technologies have created new industries and job opportunities, particularly in the areas of app development and mobile device manufacturing
  - Health impacts: Mobile technologies have been linked to both positive and negative health outcomes, including increased sedentary behaviour, addiction, and improved access to healthcare services
  - Privacy and security concerns: The proliferation of mobile technologies has raised concerns about privacy and security, particularly with regard to the collection and use of personal data by companies and governments.

- **The environmental impacts of providing infrastructure**

  - Energy consumption: The operation of mobile infrastructure, including cell towers and data centres, requires a significant amount of energy, which can contribute to carbon emissions and climate change
  - Electronic waste: The production and disposal of mobile devices and related infrastructure can lead to electronic waste, which can be hazardous to the environment if not disposed of properly
  - Land use: The construction and maintenance of mobile infrastructure can require the use of land, which can lead to deforestation, habitat destruction, and fragmentation of ecosystems
  - Water use: The operation of mobile infrastructure can require a significant amount of water, particularly for cooling data centres, which can lead to water scarcity in areas with limited resources
  - Resource extraction: The production of mobile devices and infrastructure requires the extraction of natural resources, such as rare earth metals, which can have negative environmental impacts, including pollution and habitat destruction.

  To mitigate these environmental impacts, the mobile industry can adopt sustainable practices, such as using renewable energy sources, reducing electronic waste through recycling programs, and implementing responsible resource extraction practices.

- **How technology supports mobile phone communication, including:**
  - **Mobile phone masts**

    Mobile phone masts, also known as cell towers, work by transmitting and receiving radio waves between a mobile device and the mobile network.

When a person makes a call or sends a text message, their device sends a signal to the nearest cell tower, which then relays the signal to the mobile network. The network then routes the signal to the recipient's device through another cell tower, and the communication is established.

The cell tower consists of several components, including an antenna that transmits and receives the radio waves, a transmitter that amplifies the signal, and a receiver that detects incoming signals. The tower is connected to the mobile network through a wired or wireless connection.

In areas with high mobile device usage, multiple cell towers may be installed to provide coverage and ensure that the network can handle the volume of traffic.
Mobile network operators use a combination of cell towers, wireless connections, and other infrastructure to provide seamless coverage and connectivity to their customers.

- **Cells**

Mobile cells, also known as "cellular networks," work by dividing a geographic area into smaller geographic areas, called cells. Each cell is served by a low-power transceiver (base station) that is located within the cell and communicates with mobile devices within the cell.

When a mobile device moves from one cell to another, it establishes a connection with the base station in the new cell and hands off the connection from the previous base station. This allows for continuous coverage and connectivity as the mobile device moves across different cells.

The base stations are connected to a mobile switching centre, which routes the voice and data traffic between the mobile device and the core network of the mobile service provider. The core network provides services such as call routing, authentication, and billing.

Mobile cells use radio frequency waves to communicate with mobile devices. The frequency band used by a cell determines the amount of data that can be transmitted, and higher frequency bands typically allow for faster data transmission speeds. Mobile cells operate using a licensed spectrum, which is regulated by national governments to ensure that the use of the spectrum does not interfere with other wireless services or cause harm to human health.

Overall, the use of mobile cells allows for efficient use of limited radio spectrum and enables widespread mobile communication services that can be used by millions of people simultaneously.

- **Handoffs**

Mobile handoffs, also known as "handovers," are the process of transferring a mobile device's communication from one cell to another as the device moves from one geographic area (cell) to another. The handoff process ensures that communication is maintained and uninterrupted as the device moves across different cells.

There are two types of handoffs: hard handoff and soft handoff.

- Hard handoff: In a hard handoff, the mobile device disconnects from the first cell before connecting to the second cell. The signal strength of the first cell must drop to a level where the device can no longer communicate before the device can connect to the second cell. Hard handoffs are typically faster than soft handoffs but can result in brief disruptions in communication.

- Soft handoff: In a soft handoff, the mobile device establishes communication with the second cell before disconnecting from the first cell. The mobile device communicates with both the first and second cell simultaneously, and the call or data session is transferred seamlessly from one cell to another. Soft handoffs are typically slower than hard handoffs but result in no disruption to communication.

  The handoff process is managed by the mobile network infrastructure, which continuously monitors the signal strength and quality of the communication between the mobile device and the base station. When the mobile device moves towards the edge of one cell, the network infrastructure begins to search for a neighbouring cell with a stronger signal. Once a suitable neighbouring cell is found, the network infrastructure coordinates with the base stations in both cells to execute the handoff process.

- **Base station controller**

  A Mobile Base Station Controller (BSC) is a key component of a cellular network that controls and manages multiple Base Transceiver Stations (BTSs) within a specific geographic area, called a “cell."

  The BSC acts as an intermediary between the mobile devices and the mobile network's core infrastructure, handling call setup, call routing, and other signalling functions.

  Here are the steps involved in how a mobile BSC works:

  - Call Setup: When a mobile device is activated, the BSC allocates a unique identifier to the device, called a Temporary Mobile Subscriber Identity (TMSI). When the device initiates a call, the BSC verifies the TMSI and then assigns a Traffic Channel (TCH) to the call
  - Call Routing: The BSC manages the routing of calls within its coverage area, and it selects the appropriate BTS for the call based on several factors, including the signal strength of the mobile device, the available channel capacity, and the location of the mobile device
  - Handoff Management: The BSC coordinates handoff procedures when a mobile device moves from one BTS to another. It manages the handoff process by initiating and terminating calls, transferring call setup data, and monitoring the quality of the communication
  - Call Control: The BSC provides real-time call control, such as call barring, call forwarding, and call waiting services
  - Performance Management: The BSC monitors the performance of the BTSs and reports data to the mobile network's core infrastructure. It also manages and optimises the use of the available frequency spectrum to ensure that the network's capacity is utilised efficiently.

- **IMIE and IMSI**

  An IMEI (International Mobile Equipment Identity) is a unique 15-digit number that is assigned to each mobile device, such as a smartphone or tablet. The IMEI is used to identify the mobile device on the network and can be used to block a device from accessing the network in case of theft or loss.

  The IMEI is typically printed on the back of the device or can be found by dialling *#06# on the device. The first eight digits of the IMEI represent the Type Allocation Code (TAC), which identifies the manufacturer and model of the device, while the last seven digits are unique to each device and identify the device's serial number.

  Mobile service providers use the IMEI to track the status of mobile devices on their network, such as whether a device is currently active, blocked, or stolen. Law enforcement agencies also use the IMEI to track stolen mobile devices and investigate crimes related to mobile devices.

  An IMSI (International Mobile Subscriber Identity) is a unique identifier assigned to each mobile device user on a GSM (Global System for Mobile Communications) network. The IMSI is a 15-digit number that identifies the user's SIM (Subscriber Identity Module) card, which is inserted into the mobile device.

  The IMSI is stored on the SIM card and is used to identify the user on the network. When a user makes a call or sends a text message, the IMSI is used to authenticate the user and to determine the user's billing information.

  The IMSI is comprised of three parts:

  - Mobile Country Code (MCC): A three-digit code that identifies the country where the user is registered
  - Mobile Network Code (MNC): A two or three-digit code that identifies the mobile network operator
  - Mobile Subscriber Identification Number (MSIN): A 10-digit number that identifies the user on the network.

    The IMSI is also used in conjunction with other network identifiers, such as the International Mobile Station Equipment Identity (IMEI), to facilitate the delivery of mobile services and to maintain the security and integrity of the network.

- **The working of SIP, SS7 and IPv6 protocols**

  SIP (Session Initiation Protocol) is a signalling protocol used for initiating, maintaining, and terminating real-time sessions that involve video, voice, messaging, and other communications applications. SIP can be used in a mobile environment to enable voice and video communication services over cellular networks.

  When a user initiates a voice or video call using a mobile device, the device sends a SIP request to a SIP server in the mobile network, typically a Proxy Server. The Proxy Server then locates the recipient's mobile device or SIP endpoint, and sends a SIP request to the recipient's device, establishing a session.

  During the call, the mobile device sends SIP messages to the Proxy Server to manage the call, such as for call setup, call control, and call termination. The Proxy Server manages the flow of SIP messages and ensures that they are correctly routed to the intended device.

In a mobile environment, SIP can be used to facilitate a range of services, such as voice and video calling, instant messaging, presence detection, and multimedia conferencing. SIP can also be integrated with other protocols and technologies, such as 3GPP, LTE, and VoLTE (Voice over LTE), to enable the delivery of high-quality, reliable voice and video services over mobile networks.

SS7 (Signalling System 7) is a protocol suite used for signalling and controlling communication services in telecommunication networks, including mobile networks. SS7 provides a common language for mobile devices and network elements to exchange control messages and manage calls and other services.

In a mobile environment, SS7 is used for a variety of functions, such as call setup, routing, location management, and billing. When a user initiates a call or sends a message, the mobile device sends a signalling message to the nearest base station, which then forwards the message to the mobile switching centre (MSC).

The MSC uses SS7 messages to locate the recipient's mobile device, determine its availability, and establish a connection. Once the connection is established, SS7 messages are used to manage the call, such as for call transfer, call forwarding, and call termination.

In addition, SS7 messages are used for location management, such as for determining the location of a mobile device, enabling roaming services, and supporting emergency services. SS7 is also used for billing purposes, such as for identifying the calling party, the called party, and the duration of the call.

SS7 is a critical component of mobile networks, enabling the reliable and secure delivery of voice, data, and messaging services. However, SS7 vulnerabilities have been identified, leading to potential security and privacy issues in mobile networks. As a result, newer protocols and technologies, such as Diameter and LTE, are being adopted to enhance the security and reliability of mobile communication services.

The role of IPv6 (Internet Protocol version 6) in a mobile environment is to provide a larger and more flexible address space to accommodate the growing number of mobile devices and applications that require network connectivity. IPv6 is the latest version of the Internet Protocol, which provides a unique address to each device connected to the internet, allowing them to communicate with each other.

In a mobile environment, IPv6 is used to address the limitations of the previous version, IPv4, which has a limited address space of 32 bits and is unable to accommodate the increasing number of mobile devices and services. IPv6 has a 128-bit address space, which provides trillions of unique addresses, allowing for the growth of mobile networks and services.

IPv6 also supports new features and technologies that are important in a mobile environment, such as improved security and quality of service (QoS) mechanisms. Additionally, IPv6 provides features that support seamless mobility, allowing mobile devices to maintain network connectivity as they move across different networks and locations.

- **Stateful and non-stateful calls**

  In a mobile context, stateful and non-stateful communication refer to different approaches to managing the session information that is required for communication between a mobile device and a network.

  Stateful communication in a mobile context requires the establishment of a persistent session between the mobile device and the network. This means that the session information, including the status and context of the communication, is stored on both the mobile device and the network and updated as the communication progresses. The session remains open until one of the endpoints terminates the connection. Examples of stateful communication in a mobile context include GPRS (General Packet Radio Service) and LTE (Long-Term Evolution) networks, which maintain a persistent session between the mobile device and the network.

  Non-stateful communication in a mobile context does not require the establishment of a persistent session between the mobile device and the network. Instead, the communication is managed through individual packets of data, each of which contains all the necessary information to route the packet to the destination endpoint. The packets are sent independently of each other and are not related to previous or subsequent packets in the communication. An example of non-stateful communication in a mobile context is SMS (Short Message Service), which does not require a persistent session between the mobile device and the network.

  The key difference between stateful and non-stateful communication in a mobile context is that stateful communication requires the establishment of a session that stores and updates the status and context of the communication, while non-stateful communication operates independently of previous and subsequent packets of data. Stateful communication is often used for more complex communication that requires a persistent session, such as voice and video calling, while non-stateful communication is used for simpler, lower-level communication, such as messaging and data transfer.

- **Mobile switching centre and Public Switched Telephone Network (PSTN) telephone systems.**

  The Mobile Switching Centre (MSC) is a core component of a mobile network, responsible for routing voice calls, SMS, and data between mobile devices and other parts of the network. It provides the necessary connectivity to enable communication between mobile devices and the Public Switched Telephone Network (PSTN) or other mobile networks. The MSC also manages the mobility of subscribers, allowing them to move between different cells or locations while maintaining their network connections.

  The Public Switched Telephone Network (PSTN) interfaces with a mobile network through the Mobile Switching Centre (MSC). When a call is made from a landline or another mobile phone to a mobile device, the call is routed through the PSTN to the MSC. The MSC then uses the mobile device's unique identifier (IMSI) to locate it in the network and route the call to the appropriate cell or base station.
  When a mobile device initiates a call, the MSC receives the call setup request and checks if the mobile device is authorised to make the call. If so, the MSC establishes a connection between the mobile device and the PSTN to complete the call. SMS messages and data transmissions also follow a similar process, with the MSC serving as a gateway between the mobile network and the PSTN.

Learners should be aware of:

- *the history and contemporary developments in transmitting data over mobile technologies, and understand the evolution from:*
- *GPRS*
- *Edge*
- *3G*
- *4G or LTE*
- 5G or Wideband and Ultrawide band.

- **The history and contemporary developments in transmitting data over mobile technologies, and understand the evolution from:**

Mobile technology has a long and complex history, with numerous developments and advancements over the years. Here is a brief overview of some of the key milestones and contemporary developments:

- In 1973, the first mobile phone was invented by Motorola, although it was large and expensive, and not widely available to the public
- In the 1980s, the first analogue cellular networks were launched, allowing mobile devices to communicate wirelessly over large distances
- In the 1990s, the first digital cellular networks were introduced, offering better call quality and data transfer speeds. The Global System for Mobile Communications (GSM) became the dominant standard in Europe, while Code Division Multiple Access (CDMA) was adopted in the United States and some other regions
- In the early 2000s, the first 3G networks were launched, offering faster data transfer speeds and enabling new mobile applications like video calls and mobile internet browsing
- The late 2000s saw the widespread adoption of smartphones, led by the launch of the iPhone in 2007. Smartphones brought a new level of functionality and convenience to mobile devices, with touch screens, app stores, and high-speed internet access
- In the 2010s, 4G LTE networks became the standard for mobile connectivity, providing even faster data transfer speeds and enabling new applications like mobile video streaming and augmented reality
- In recent years, there has been a growing focus on 5G technology, which promises even faster data transfer speeds, lower latency, and more reliable connectivity. Other contemporary developments include the Internet of Things (IoT), which is connecting a wide range of devices and systems to mobile networks, and the development of foldable phones and other innovative form factors.

  - **GPRS**

    - Packet Switching: GPRS uses packet switching technology, which enables data to be transmitted in small, discrete packets, rather than in a continuous stream
    - High-Speed Data: GPRS can deliver data at speeds of up to 114 kbps, making it suitable for applications that require moderate amounts of data, such as email and web browsing
    - Always-On Connection: GPRS provides an "always-on" connection to the internet, meaning that users can stay connected and receive data even when not actively using the device
    - Wide Coverage: GPRS networks are widely available in many countries and can provide coverage over a large geographic area
    - Compatibility: GPRS is compatible with many different types of devices, including smartphones, laptops, and tablets.

- **Edge**
    - Increased Data Speed: EDGE provides faster data transfer rates compared to the original GSM network, with speeds of up to 384 kbps
    - Backward Compatibility: EDGE is backwards compatible with GSM networks, allowing older devices to access data services on an EDGE network
    - Efficient Use of Spectrum: EDGE uses more efficient modulation schemes, allowing more data to be transmitted within the same amount of spectrum as GSM
    - Improved Voice Quality: EDGE provides improved voice quality compared to GSM, with reduced background noise and clearer sound
    - Widespread Coverage: EDGE has widespread coverage and is available in many countries, making it a popular choice for global roaming.
- **3G**
    - High Data Speed: 3G provides faster data transfer rates compared to 2G technologies, with speeds ranging from 144 kbps to 2 Mbps
    - Improved Network Capacity: 3G networks have improved network capacity, allowing for more simultaneous connections and increased data traffic
    - Multimedia Support: 3G networks support multimedia applications such as video streaming, video calls, and mobile TV
    - Global Roaming: 3G networks are available in many countries and provide global roaming capabilities, allowing users to access services while travelling abroad
    - Security: 3G networks provide enhanced security features, such as encryption and authentication, to protect user data and prevent unauthorised access.
- **4G or LTE**
    - High Data Speed: 4G and LTE provide significantly faster data transfer rates compared to previous generations, with LTE providing peak download speeds of up to 1 Gbps
    - Low Latency: 4G and LTE networks have low latency, meaning that there is minimal delay between sending and receiving data
    - High-Quality Voice and Video: 4G and LTE networks support high-quality voice and video calling, as well as streaming of high-definition video and audio
    - Spectral Efficiency: 4G and LTE use more efficient modulation and multiple access schemes, allowing for more efficient use of the available spectrum
    - Seamless Connectivity: 4G and LTE provide seamless connectivity between different networks, including Wi-Fi, cellular, and broadband networks
    - Backward Compatibility: LTE is backwards compatible with 3G and 2G networks, allowing older devices to access data services on an LTE network
    - Security: 4G and LTE networks provide advanced security features, such as encryption and authentication, to protect user data and prevent unauthorised access.

- **5G or Wideband and Ultrawide band**

  - 5G:
    - High Data Speed: 5G provides significantly faster data transfer rates compared to previous generations, with peak download speeds of up to 20 Gbps
    - Low Latency: 5G networks have very low latency, meaning that there is minimal delay between sending and receiving data
    - Massive Machine-Type Communications (mMTC): 5G networks support the connection of a large number of IoT devices with low power consumption and extended battery life
    - Network Slicing: 5G networks can be divided into multiple virtual networks, allowing for customised service offerings and more efficient use of network resources
    - Enhanced Mobile Broadband (eMBB): 5G networks offer high-speed data transfer rates that enable new applications and use cases such as virtual reality and augmented reality

  - Wideband:
    - Wider Frequency Range: Wideband wireless systems operate at a wider frequency range than conventional narrowband systems, allowing for more data to be transmitted in a given amount of time
    - Increased Data Rates: Wideband systems can deliver faster data transfer rates than narrowband systems, making them suitable for high-bandwidth applications such as video streaming and high-speed data transfer.

  - Ultrawideband (UWB):
    - High Data Rates: UWB can provide very high data transfer rates, with theoretical maximums of up to 1 Gbps
    - Low Power Consumption: UWB requires very little power to operate, making it well-suited for IoT devices and other low-power applications
    - Short-Range Communication: UWB is typically used for short-range wireless communication, such as wireless USB and wireless sensor networks
    - Precise Location Tracking: UWB can be used for precise location tracking, making it useful for applications such as asset tracking and indoor navigation.

- *the relative data transmission speeds and what applications and experiences these allow for end users*

  - 2G (Second Generation): 2G mobile technology provides data transfer rates up to 64 kbps. This is suitable for basic applications such as sending text messages and making voice calls
  - 3G (Third Generation): 3G mobile technology provides data transfer rates ranging from 144 kbps to 2 Mbps. This allows for more advanced applications such as web browsing, video streaming, and video calls
  - 4G (Fourth Generation): 4G mobile technology provides data transfer rates up to 1 Gbps. This allows for more demanding applications such as high-quality video streaming, online gaming, and large file downloads
  - 5G (Fifth Generation): 5G mobile technology provides data transfer rates up to 20 Gbps. This allows for even more advanced applications such as augmented reality, virtual reality, and autonomous vehicles.

Some example apps and experiences for each generation of mobile technology are:

- 2G: Voice calls, text messaging, basic web browsing
- 3G: Video calls, video streaming, mobile gaming, social media
- 4G: High-quality video streaming, online gaming, large file downloads, and cloud-based applications
- 5G: Augmented reality, virtual reality, telemedicine, remote education, smart city applications.

It's worth noting that actual data transfer rates may vary depending on network conditions, device capabilities, and other factors.

- *future developments of mobile technologies, including:*
  - *borderless technologies (no bezel)*
  - *'transparent' phones*
  - *chip phones/'bionic interface' communication devices.*

- Borderless Technologies (No Bezel): Mobile devices with no bezel or a very thin bezel around the screen may become more common in the future. This will allow for larger screens in smaller form factors and an enhanced immersive user experience
  - 'Transparent' Phones: There is research being done on making transparent screens for mobile devices. This would allow for a unique and futuristic design, as well as new user experiences
  - Chip Phones/'Bionic Interface' Communication Devices: There is a possibility that in the future, mobile devices may become smaller and more integrated with the human body This could take the form of "chip phones" that are implanted under the skin, or "bionic interface" communication devices that allow for seamless communication without needing to hold a device.

  Other potential future developments in mobile technologies include:

  - Foldable Phones: Foldable phones with flexible screens are already on the market, but there is still room for improvement in terms of durability and design
  - Augmented Reality (AR) and Virtual Reality (VR): AR and VR technologies are already being used in mobile apps and games, but they have the potential to become more mainstream in the future as technology advances
  - Artificial Intelligence (AI) and Machine Learning (ML): AI and ML are already being used in various mobile applications, but they have the potential to become more sophisticated and integrated into mobile devices
  - It's important to note that these are all potential developments and may or may not become mainstream in the future. The direction of mobile technology development will depend on various factors such as consumer demand, technological advancements, and market trends.

WJEC RESOURCES

Resources available on the WJEC website:	WJEC GCE Digital Technology website GCE Digital Technology Specification Sample Assessment Materials (online version) Sample Assessment Materials (paper version) Guidance for Teaching resources
WJEC Online Exam Review:	WJEC OER website

IMPORTANT DATES

First Teaching of GCE Digital Technology	September 2022
First Entries for AS Digital Technology	February 2023
First Examination for Unit 1 GCE Digital Technology	May/June 2023
First Submission of NEA for Unit 2 GCE Digital Technology	May 2023
First Entries for A Level Digital Technology	February 2024
First Examination for Unit 3 GCE Digital Technology	May/June 2024
First Submission of NEA for Unit 4 GCE Digital Technology	May 2024
First Resit for Unit 1 Digital Technology	May/June 2024
First Certification for AS Digital Technology	August 2023
First Resit for Unit 3 Digital Technology	May/June 2024
First Certification for A level Digital Technology	August 2024

KEY CONTACTS

Contact our specialist Subject Officer and administrative support team for digital technology with any queries:

Andy Parker Subject Officer

Kwai Wong Subject Support Officer

E mail: digitech@wjec.co.uk

Tel: 029 2065 5401