Enterprise Computing Stage 6 (Year 11) – teacher support resource

**Networking systems and social computing**

# Teacher support resource

**Teacher note:** this resource has been designed to facilitate the ready conversion into a student booklet by removing the answers within the response windows. Teacher notes can be deleted before distributing to students.

Student name:

Class:

Teacher:

Contents

[Teacher support resource 1](#_Toc149134335)

[Unit overview 4](#_Toc149134336)

[Assessment task overview 5](#_Toc149134337)

[Submission details 6](#_Toc149134338)

[Steps to success 7](#_Toc149134339)

[Glossary 9](#_Toc149134340)

[NESA glossary keywords 13](#_Toc149134341)

[The design and production process 14](#_Toc149134342)

[Introduction to human-centric computing 15](#_Toc149134343)

[Investigate the effects of disruptive technology on everyday computing 16](#_Toc149134344)

[Investigate the application of graph and network theory in the design of social networks 24](#_Toc149134345)

[Internet of Things (IoT) and the Internet of Me (IoMe) 27](#_Toc149134346)

[Outline the business and individual cultural characteristics that contribute to the success of start-ups 38](#_Toc149134347)

[Storage and workflow in enterprise networks 40](#_Toc149134348)

[Investigate how the developments in network connectivity and speed have influenced work practices within an enterprise 40](#_Toc149134349)

[Examine the benefits and limitations of digital workflows operating in an enterprise 43](#_Toc149134350)

[Investigate data storage requirements for an enterprise 45](#_Toc149134351)

[Explore cloud computing services 46](#_Toc149134352)

[Compare different types of cloud-based data storage in terms of access and services 48](#_Toc149134353)

[Network architecture and infrastructure 55](#_Toc149134354)

[Describe key components of an organisation’s information technology infrastructure 55](#_Toc149134355)

[Describe how transmission media is used in networks 57](#_Toc149134356)

[Explain factors that interfere with the transmission of data across a computer and social network 59](#_Toc149134357)

[Investigate ways to improve data flow within a system, considering proximity and modes of connectivity 59](#_Toc149134358)

[Investigate the application of graph theory and network theory in the design of optimised computer networks 61](#_Toc149134359)

[Explore device interoperability within an Internet of Things (IoT) based enterprise network, including supervisory control and data acquisition (SCADA) 68](#_Toc149134360)

[Investigate communication protocols between devices in an Internet of Things (IoT) network 69](#_Toc149134361)

[Explore the benefits of interfacing machine learning (ML) with IoT 70](#_Toc149134362)

[Investigate security measures used to control access to networks 75](#_Toc149134363)

[Examine data security for an intelligent home network 78](#_Toc149134364)

[Creating a network 82](#_Toc149134365)

[Design and model a network of interconnected devices for a specific purpose 83](#_Toc149134366)

[Apply appropriate project management tools to develop a project 84](#_Toc149134367)

[Configure devices within a network 88](#_Toc149134368)

[Implement procedures and security protocols considering cybersecurity 90](#_Toc149134369)

[Explore opportunities for optimising network performance 93](#_Toc149134370)

[Evaluate the role of hardware and software related to the transmission of data 95](#_Toc149134371)

[References 100](#_Toc149134372)

# Unit overview

In this unit students will develop a fundamental understanding of the area of networking systems and social computing. The lessons and sequences in this teacher resource are designed to allow students to develop the knowledge and skills to create a networking product as a solution to a user’s needs while considering social computing.

During Weeks 1 to 4 of the learning sequence, students gain an introduction to human-centric computing. They examine the effects of disruptive technology on everyday computing, investigate graph and network theory in the design of social networks and describe how apps influence the success of social networking. Students investigate how the development of hardware and software has influenced the adoption of the Internet of Things (IoT) and outline the business and individual cultural characteristics that contribute to the success of start-ups.

Students examine the storage and workflow in enterprise networks. They investigate how the developments in network connectivity and speed have influenced work practices within an enterprise. Students examine the benefits and limitations of digital workflows operating in an enterprise and investigate data storage requirements for an enterprise.

During Weeks 5 to 10 of the learning sequence, students will examine network architecture and infrastructure. They describe key components of an organisation’s information technology infrastructure and describe how transmission media is used in networks.

Students explain factors that interfere with the transmission of data across a computer and social network and investigate ways to improve data flow within a system, considering proximity and modes of connectivity.

Students create a network including designing and modelling a network of interconnected devices for a specific purpose. They apply appropriate project management tools to develop a project and configure devices within a network.

# Assessment task overview

**Type of task:** create a network and use video to document the network.

**Outcomes being assessed:**

A student:

* describes how systems are used in a range of enterprises **EC-11-01**
* describes how data is safely and securely collected, stored and manipulated when developing enterprise computing systems **EC-11-03**
* describes how data is used in enterprise computing systems **EC-11-04**
* explains how innovative technologies have influenced enterprise computing systems **EC-11-06**
* explores the social, ethical and legal implications of the application of enterprise computing systems on the individual, society and the environment **EC-11-07**
* documents the management and evaluates the development of an enterprise solution
**EC-11-09**

[Enterprise Computing 11–12 Syllabus](https://curriculum.nsw.edu.au/learning-areas/tas/enterprise-computing-11-12-2022/overview) © NSW Education Standards Authority (NESA) for and on behalf of the Crown in right of the State of New South Wales, 2022.

**Suggested weighting: 35%**

Students may access networking equipment at school, or examine their own home network or that of an investigated enterprise system including a local business or researched organisation. Students who are unable to physically model a network may use software to virtually create their network using a network simulator.

Inspired by the Internet of Things (IoT), students design and model a network of interconnected devices for a specific purpose and create a video to showcase their project.

Students create a video of a network. This video may include footage of components being configured and networked and include diagrams and a network simulator to showcase their interconnected devices.

## Submission details

Students submit a video of their network model. The model may be recorded and filmed or if a virtual network students can use software that creates screen recordings.

Students submit their documentation digitally.

Students should be provided the opportunity to showcase their work in a class presentation that includes a question-and-answer segment.

Opportunities should also be explored for students to peer assess their classmate’s work.

This will enable a forum for the exchange of ideas that may help inform future tasks and projects.

This project may be used to inform the design and development of the student’s Enterprise Project during the Year 12 course.

## Steps to success

The steps to success assessment preparation schedule aligns to the project development cycle used in the Year 12 Enterprise Project. This cycle is used in the development of all projects to provide students with experience in the approach and familiarity with the processes and terminology.

Table 1 – assessment preparation schedule

|  |  |
| --- | --- |
| Steps | What I need to do |
| Identifying and definingInvestigate how you will design and model a network to communicate information for a specific purpose. | * Design and model a network of interconnected devices for a specific purpose.
* Choose an environment or location to represent and model a network.
* Define the specific purpose of the network.
* Examine what IoTs are used in the network.
 |
| Research and planningDocument using project management tools.Plan the video you will create to showcase your network. | * Apply appropriate project management tools to develop a project by creating a storyboard and script to plan the video.
* Use voice narration, titles, relevant graphics, diagrams or videos to describe how systems are used in enterprises and how data is safely and securely collected, stored and manipulated when developing enterprise computing systems.
* Use voice narration, titles, relevant graphics, diagrams or videos to explain how innovative technologies have influenced systems and explore the social, ethical and legal implications of the application of enterprise computing systems on the individual, society and the environment.
 |
| Producing and implementingDevelop your network of interconnected devices with naming conventions and update devices that are configured with safety protocols, and ensure they can connect to the internet. | * Video record how you configure devices within a network

Including* naming the device
* updating the device
* configuring security protocols
* connecting to the internet.
 |
| Producing and implementingDevelop your network of interconnected devices considering security protocols and cybersecurity.Develop your network of interconnected devices optimising network performance. | * Implement procedures and security protocols considering cybersecurity.
* Explore opportunities for optimising network performance

Including* improving bandwidth
* updating drivers and firmware.
 |
| Testing and evaluatingReview and improve your network of interconnected devices. | * Evaluate the role of hardware and software related to the transmission of data

Including* unsecured data
* encrypted data
* infrastructure.
 |

# Glossary

Many of the following words will gather more meaning for you as you work through this booklet.

Each time you see a new word in bold throughout this workbook you can add its definition in the table below in case you need to refer back later.

|  |  |
| --- | --- |
| Word | Definition |
| Bandwidth | Network bandwidth is a measurement indicating the maximum capacity of a wired or wireless communications link to transmit data over a network connection in a given amount of time. |
| Biometric | A term that describes the source of data being human or biological. |
| Buzzword | A word or phrase that is fashionable at a particular time or in a particular context. |
| CAPTCHA | Completely Automated Public Turing test to tell Computers and Humans Apart. |
| Cloud-based data storage | A mode of computer data storage in which digital data is stored on servers in off-site locations. The servers are maintained by a third-party provider who is responsible for hosting, managing and securing data stored on its infrastructure. |
| Communication protocols | A communication protocol is a system of rules that allows 2 or more entities of a communications system to transmit information via any kind of variation of a physical quantity. The protocol defines the rules, syntax, semantics and synchronisation of communication and possible error recovery methods. Protocols may be implemented by hardware, software, or a combination of both. |
| Cybersecurity | The protection of information technology elements, including hardware and software, data or network services. |
| Digital workflows | A digital workflow is the automation of any process that an organisation uses to get things done. It includes the procedures, tools and plan for carrying out a series of tasks. |
| Disruptive technology | Disruptive technology is an innovation that significantly alters the way that consumers, industries or businesses operate. A disruptive technology sweeps away the systems or habits it replaces because it has attributes that are recognisably superior. |
| Drivers | A program that controls the operation of a device such as a printer or scanner. |
| Firmware | The software that is installed on a small chip in almost all hardware devices that makes the hardware function as the manufacturer intended it to. |
| Graph theory | Graph theory is the study of graphs, which are mathematical structures used to model pairwise relations between objects. A graph in this context is made up of vertices (also called nodes or points) which are connected by edges (also called links or lines). A distinction is made between undirected graphs, where edges link 2 vertices symmetrically, and directed graphs, where edges link 2 vertices asymmetrically. |
| Infrastructure as a Service (IaaS) | A form of cloud computing that delivers fundamental computing network and storage resources to consumers on-demand, over the internet, and on a pay-as-you-go basis. IaaS enables end users to scale and shrink resources on an as-needed basis, reducing the need for high, up-front capital expenditures. |
| Internet of Me (IoMe) | The Internet of Me (IoMe) loosely refers to technology which connects our minds and bodies with the online world. It transforms our biological and cognitive life into streams of data which can be monitored, shared and shaped. |
| Internet of Things (IoT) | Internet of Things (IoT) encompasses smart devices and smart objects that send and receive information using the internet and communication infrastructure. |
| machine learning (ML) | The use and development of computer systems that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyse and draw inferences from patterns in data. |
| Network theory | Network theory is a part of [graph theory](https://en.wikipedia.org/wiki/Graph_theory). It defines networks as graphs where the nodes or edges possess attributes. Network theory analyses these networks over the symmetric relations or asymmetric relations between their (discrete) components. |
| Platform as a Service (PaaS) | PaaS, or Platform-as-a-Service, is a cloud computing model that provides customers with a complete cloud platform including hardware, software and infrastructure. PaaS is used for developing, running and managing applications without the cost, complexity and inflexibility that often comes with building and maintaining the platform on-premises. |
| Project management tools | Project management tools are specially designed to assist an individual or team in organising and managing their projects and tasks effectively. They can be broadly defined as software applications that help teams coordinate, plan and execute projects. |
| Security protocols | A sequence of operations that ensure protection of data. They can be thought of as a set of principles which send messages to each other. |
| Social network | A structure that describes the relationships that exist between individuals and/or organisations. Social networking services and tools provide a mechanism for people who share common interests or personal ties to communicate, share and interact using a range of media such as text, images and video. |
| Software as a Service (SaaS) | Software-as-a-Service (SaaS) is a cloud-based software delivery model that allows end users to access software applications over the internet. With a SaaS model, the software is hosted on remote servers, maintained and updated by the service provider, and made available to customers via web browsers, mobile apps and APIs. |
| Supervisory control and data acquisition (SCADA) | SCADA is a computer-based system for gathering and analysing real-time data to monitor and control equipment that deals with critical and time-sensitive materials or events. SCADA systems were first used in the 1960s and are now an integral component in virtually all industrial plant and production facilities. |
| Topology | Topologies are often represented as a graph. Network topologies describe the arrangement of networks and the relative location of traffic flows. |
| Trusted Platform Module (TPM) | Trusted Platform Module is an international standard for a secure cryptoprocessor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys. The term can also refer to a chip conforming to the standard. |
| Virtual private networks (VPNs) | A virtual private network, or VPN, is an encrypted connection over the internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorised people from eavesdropping on the traffic and allows the user to conduct work remotely. |

**Teacher note:** for students with an EALD background, the glossary can be provided complete so that they have additional time to understand the key terms with bilingual dictionaries. The glossary can be provided to students in their preferred communication mode.

# NESA glossary keywords

NESA keywords can be used in the syllabus and in the Higher School Certificate examination. Familiarisation with the keywords in the table below can assist in understanding how to write and respond to questions.

|  |  |
| --- | --- |
| Key term | Definition |
| Apply | Use, utilise, employ in a particular situation |
| Compare | Show how things are similar or different |
| Describe | Provide characteristics and features |
| Examine | Inquire into |
| Explain | Relate cause and effect; make the relationships between things evident; provide why and/or how |
| Investigate | Plan, inquire into and draw conclusions about |
| Outline | Sketch in general terms; indicate the main features of |

[NESA: A Glossary of Key Words](https://educationstandards.nsw.edu.au/wps/portal/nesa/11-12/hsc/hsc-student-guide/glossary-keywords)

**Teacher note:** configure, design, explore and implement are used in this topic and are not listed.

# The design and production process

Throughout your study of Enterprise Computing, you will learn about design processes and how to apply them. You will explore different types of design processes and learn how to apply them in your design project.

The design and production process:

* involves a sequence of organised steps which provide a solution to design needs and opportunities
* may take a few seconds or minutes, such as when you select what clothes to wear, or may take years as in the case with the design of a motor vehicle
* may involve one person or may involve many people
* may be simple or complex, depending on the task
* involves questioning (or evaluating) throughout the iterative process.

Figure 1 – flowchart of design and production process



## Introduction to human-centric computing

The goal of human-centric computing is to create technology that is intuitive, easy to use, and enhances the user's overall experience. This involves understanding human behaviour, cognitive processes and psychological factors that influence user interaction with technology. Human-centric computing also takes into account social and cultural factors that may affect how users interact with technology.

The ultimate aim of human-centric computing is to create technology that is not only usable but also enjoyable and fulfilling for users, while also being beneficial to society as a whole.

Disruptive technology is a term used to describe new innovations or inventions that fundamentally change the way industries, markets and businesses operate. Disruptive technologies typically create new markets or transform existing ones by introducing new products, services or business models that offer superior performance, convenience or affordability compared to existing alternatives.

Disruptive technology often challenges existing dominant players in the industry, forcing them to adapt and change their strategies or risk becoming irrelevant. Examples of disruptive technologies include the personal computer, the internet, mobile phones, digital cameras and cloud computing.

A disruptive technology is **one that displaces an established technology and shakes up the industry or a ground-breaking product that creates a completely new industry**. Harvard Business School professor Clayton M. Christensen coined the term disruptive technology.

Examples of disruptive technology include:

* Netflix and streaming services versus Blockbuster for rentals and places like JB Hi-Fi for media purchasing
* Spotify compared to Apple Music or iTunes, and HMV or Brashs before any of these
* Wikipedia compared to Encarta, and printed encyclopaedias before both of these
* Uber industries compared to taxi and delivery services, including Uber Eats
* Skype, Zoom, Microsoft Teams compared to conference or business travel.

### Investigate the effects of disruptive technology on everyday computing

As a class, students watch the[TEDx Talk on disruptive technology](https://www.youtube.com/watch?v=pk9RVBwiFbM) (12:07).

**Activity 1:** [brainstorm](https://app.education.nsw.gov.au/digital-learning-selector/LearningActivity/Card/542#.ZC4skSv0RLg.link) examples of disruptive technology you have encountered in daily life and write your results in the space below.

|  |
| --- |
| **Sample answers:*** smartphones
* ride-sharing apps
* streaming services
* e-commerce
* cryptocurrencies and blockchain
* voice assistants
* artificial intelligence.
 |

**Activity 2:** define the following concepts in the space below.

What does disruptive technology mean?

|  |
| --- |
| **Sample answer:**Disruptive technology refers to innovations that fundamentally change and often revolutionise industries by introducing new, more affordable, accessible and efficient ways of doing things. It displaces existing products, services or business models and potentially leads to the obsolescence of traditional approaches.These technologies often start with lower performance but rapidly improve, opening up new markets and disrupting established players, ultimately reshaping entire industries and markets. |

What is everyday computing?

|  |
| --- |
| **Sample answer:**Everyday computing refers to the ubiquitous and routine use of computers and digital devices in our daily lives. It encompasses a wide range of activities, from checking emails, browsing the internet, and using smartphones for communication and entertainment, to more specialised tasks like word processing, spreadsheet management, and social media engagement.Everyday computing has become an integral part of modern living, influencing how we work, connect with others, access information, and even manage our homes and personal tasks. |

##### Effects on the individual

Disruptive technology has a significant impact on individuals, both in terms of opportunities and challenges. Here are some of the effects of disruptive technology on individuals:

##### ****New job opportunities****

Disruptive technologies can create new job opportunities and skillsets, particularly in emerging industries such as artificial intelligence (AI), robotics and renewable energy.

##### ****Job**** displacement

On the other hand, disruptive technology can also lead to job displacement, as certain industries or occupations become obsolete. Individuals who are unable to adapt to new technologies may find themselves out of work.

##### ****Changes in work-life balance****

Disruptive technology can change the way individuals work, blurring the boundaries between work and personal life. With the rise of remote work and digital communication tools, individuals may find themselves working longer hours or struggling to maintain a work-life balance.

##### ****Increased**** access ****to information and services****

Disruptive technology can make information and services more accessible and affordable to individuals, particularly in areas such as healthcare, education and finance.

##### ****Privacy and**** security ****concerns****

Disruptive technology can also raise concerns around privacy and security, as individuals' personal data may be collected, stored and used without their knowledge or consent.

**Activity 3:** effects of disruptive technology on the individual

What are the effects of disruptive technology on the individual?

|  |
| --- |
| **Sample answer:**Disruptive technology has multifaceted effects on individuals. On one hand, it enhances convenience, productivity and access to information, offering new opportunities for employment and entertainment. On the other hand, it can lead to job displacement, privacy concerns, social isolation and digital addiction, posing challenges to mental wellbeing and personal relationships. Balancing the benefits and drawbacks of disruptive technology requires individuals to adapt, develop digital literacy, and manage their technology use mindfully to harness its advantages while mitigating its adverse impacts on their lives. |

Describe how job security may be challenged by disruptive technology.

|  |
| --- |
| **Sample answer:**Job security can be challenged by disruptive technology as automation and digitalisation increasingly replace human labour in various industries. As machines and software become more capable and cost-effective, jobs that involve routine, repetitive tasks are at risk of being automated, leading to potential job displacement for individuals in these roles.Additionally, the rapid pace of technological change requires workers to continually update their skills to remain relevant in the job market, making it challenging for some to keep up with evolving demands. While disruptive technology creates new job opportunities, especially in the tech sector, the transition can be difficult for workers in disrupted industries. This emphasises the importance of retraining and reskilling efforts to maintain job security in the face of these changes. |

#### Innovations in infrastructure, hardware and software

Disruptive technology can challenge innovation in infrastructure, hardware and software in several ways. Here are some examples:

##### Infrastructure

Disruptive technology can challenge innovation in infrastructure by requiring new or different infrastructure to support it. For example, the adoption of cloud computing technology requires new data centres and networking infrastructure that can support the increased demand for processing and storage.

##### Hardware

Disruptive technology can also challenge innovation in hardware by requiring new or different hardware to support it. For example, the rise of mobile computing has led to the development of smartphones and tablets that are optimised for mobile use and have different hardware requirements than traditional desktop or laptop computers.

##### Software

Disruptive technology can challenge innovation in software by requiring new or different software applications to support it. For example, the adoption of artificial intelligence (AI) and machine learning technology requires software that can analyse and learn from large amounts of data.

##### Integration

Disruptive technology can also challenge innovation in infrastructure, hardware and software by requiring new approaches to integration. For example, the Internet of Things (IoT) requires integration between devices, sensors, networks and cloud platforms to create a seamless and interconnected ecosystem.

##### Standards

Disruptive technology can also challenge innovation by requiring new or updated standards for infrastructure, hardware and software. For example, the adoption of blockchain technology requires new standards for security, privacy and interoperability.

**Activity 4**: research and provide screen shot examples of each type of disruptive technology that you are familiar with in the table below.

|  |  |
| --- | --- |
| Role | Screen shot examples |
| **Infrastructure** |  |
| **Hardware** |  |
| **Software** |  |

Infrastructure, hardware and software are 3 categories in which disruptive technology has impacted society.

**Activity 5:** complete 3 examples of disruptive technology that you regularly use for each category in the table below.

|  |  |
| --- | --- |
| Category | Identify real-world applications of disruptive technology |
| Infrastructure | * Example 1
* Example 2
* Example 3
 |
| Hardware | * Example 1
* Example 2
* Example 3
 |
| Software | * Example 1
* Example 2
* Example 3
 |

**Activity 6**: as a class, students watch a video on [What are disruptive technologies? (3:45)](https://www.youtube.com/watch?v=S86mAHwiij4)

Examine the [table of disruptive technologies](https://www.dropbox.com/s/6ukp4d6q3z1douj/Tech-Foresight-Table-of-Disruptive-Technologies.pdf?dl=0) discussed in the video.

In the space below, list 10 disruptive technologies and their categories.

|  |
| --- |
|  |

**Teacher note:** please note that in the table of disruptive technologies, there are references to male pregnancy, artificial wombs and humanoid sex robots.

Teachers should be mindful of their students’ backgrounds prior to using this material to ensure suitability for the context and maturity level of the class. Suggested resources may have to be substituted if deemed unsuitable.

Care should also be taken to teach this material in a manner that complies with the [Controversial Issues in Schools](https://education.nsw.gov.au/policy-library/policies/pd-2002-0045) policy. This may include seeking principal approval, or a delegate, prior to delivery.

Students are grouped in small teams and discuss how all of these disruptive technology developments will affect everyday computing.

Student teams choose one of these future technologies and discuss using critical thinking.

Examples could include:

* the history of Netflix and how its rise led to the demise of the home video industry
* Uber and how it revolutionised the taxi industry
* the Apple Music Store and how it revolutionised how we purchased music. Then how Spotify has further revolutionised the field
* the Apple App Store and Google Play, making micro purchases for apps (apps that are either free and ad supported or commonly cost $1–2)
* the development of subscription services, like Microsoft 365, Adobe Creative Cloud, Xbox Game Pass Ultimate, PS Now, from discrete purchase of individual items.

#### Trends and buzzwords

**Activity 7**: the table of trends and buzzwords below can be added to and definitions included.

|  |  |  |  |
| --- | --- | --- | --- |
| Trends and buzzwords |  |  |  |
| Distributed cloud | Cybersecurity Mesh | Business Intelligence (BI) |  |
| Artificial Intelligence (AI) | Digital Immune System (DIS) | Cyber Liability Insurance |  |
| Sustainable technology | Multiexperience |  |  |
| Metaverse | Everything-as-a-Service (XaaS) |  |  |
| Hyper Automation | Multi-Factor Authentication (MFA) |  |  |
| Extended Reality (XR) | Vulnerability Screening |  |  |
| Quantum Computing | Endpoint Detection and Response (EDR) |  |  |

### Investigate the application of graph and network theory in the design of social networks

Graph and network theory have been extensively applied in the design and analysis of social networks. Social networks can be represented as graphs, where nodes represent individuals or entities, and edges represent social connections or relationships between them.

****Watch [What is Social Network Analysis? (3:45)](https://www.youtube.com/watch?v=xT3EpF2EsbQ).

Watch [Social Network Analysis: Graph theory (8:38)](https://www.youtube.com/watch?v=natjwmIGoxQ).

Watch [Basic Concepts in Graph Theory (16:36)](https://www.youtube.com/watch?v=ZHqQDA3be-k).

Graph theory is a branch of mathematics that deals with the study of graphs, which are a set of vertices (also called nodes) connected by edges (also called links or arcs). Graphs are often used to model relationships between objects, and can be applied to many real-world problems. For example, social networks can be modelled as graphs, with people represented as nodes and relationships represented as edges.

**Activity 8:** read and discuss [social network analysis](https://en.wikipedia.org/wiki/Social_network_analysis).

|  |  |
| --- | --- |
| Social network design element | How graph and network theory can be used |
| **Structural analysis** | Graph and network theory can be used to analyse the structure of social networks, such as identifying important nodes (for example influencers) and communities within a network. This information can be used to design more effective social networks that promote engagement and facilitate communication between individuals. |
| **Information diffusion** | Graph and network theory can also be used to model the spread of information within a social network. By understanding how information flows through a network, social network designers can develop strategies to promote the spread of positive information and mitigate the spread of negative information. |
| **Recommendation systems** | Graph and network theory can be used to design recommendation systems that suggest new connections or content to users based on their existing social connections. This can increase user engagement and help users discover new content and opportunities. |
| **Social influence** | Graph and network theory can be used to study the role of social influence in social networks. By understanding how social influence operates within a network, social network designers can develop strategies to increase the positive effects of social influence and mitigate the negative effects (such as groupthink or the spread of false information). |
| **Privacy and security** | Graph and network theory can be used to study the privacy and security implications of social networks. By understanding how data flows through a network and how social connections are formed, social network designers can develop strategies to protect users' privacy and prevent security breaches. |

**Activity 9:** use [Gephi](https://gephi.org/) to visualise a graph.

Create a csv file showing the social media connections you have in your year group. Follow a [tutorial](https://medium.com/swlh/visualizing-databases-using-gephi-591c9530c981) to understand how you can visualise your data.

**Activity 10:** [Firefox lightbeam](https://addons.mozilla.org/en-US/firefox/addon/lightbeam-chikl/) analysis of browser and data tracking habits

Students install and monitor their browsing habits. Figure 2 is a screenshot with less than one hour’s browsing in it. The app is Lightbeam for Firefox.

Figure 2 – Firefox Lightbeam



Image created using [Lightbeam](https://addons.mozilla.org/en-US/firefox/addon/lightbeam-chikl/) and is licensed under [CC BY-SA 3.0 Deed](https://creativecommons.org/licenses/by-sa/3.0/) or any later version.

#### Web applications and mobile apps for social networking

Web applications and dedicated mobile apps have a significant impact on the success of social networking. Both types of applications offer unique advantages and challenges, which can influence the way social networking platforms are designed, marketed and used. By considering the accessibility, user experience, speed, and monetisation potential of web applications and dedicated mobile apps, social networking platforms can design more effective and engaging applications that meet the needs of their users and their business objectives.

##### Accessibility

* Web applications are easily accessible from any device with an internet connection, which can increase the reach of social networking platforms.
* Dedicated mobile apps offer more convenient and personalised access to social networking, as they can be tailored to specific devices and user preferences.

##### User experience

* Web applications can provide a consistent user experience across devices, but may lack the advanced features and interface design that dedicated mobile apps offer.
* Dedicated mobile apps can provide more advanced features and a better user experience, but require more development resources and may be limited by specific device requirements.

##### Speed

* Web applications rely on internet connection speed and may be slower than dedicated mobile apps.
* Dedicated mobile apps can offer faster performance and better response times, but may require more data storage and processing power.

##### Monetisation

* Web applications can be monetised through advertising and subscription models, but may struggle to compete with dedicated mobile apps.
* Dedicated mobile apps can offer more lucrative monetisation opportunities through in-app purchases, but may require more investment in development and marketing.

### Internet of Things (IoT) and the Internet of Me (IoMe)

#### What is the Internet of Things (IoT)?

The Internet of Things (IoT) refers to the network of physical objects or ‘things’ that are embedded with sensors, software and other technologies that enable them to collect and exchange data with other devices and systems over the internet. These objects can range from simple household appliances to complex industrial equipment and can be controlled and monitored remotely through a variety of applications and interfaces. The data collected by IoT devices can be used for a wide range of applications, including optimising performance, improving safety and security, and enhancing the user experience.

The goal of the IoT is to create a more connected and intelligent world, in which physical objects can communicate and interact with each other and with humans in more meaningful and efficient ways.

**Activity 11: **read [What is the IoT?](https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/) and watch the [movie (9:15)](https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/) on the webpage.

As a class, students watch [an explanation of IoT](https://www.youtube.com/watch?v=LlhmzVL5bm8) (3:21).

As a class, discuss what are common IoT devices you are using.

In the space below, define in your own words what is meant by the Internet of Things (IoT).

|  |
| --- |
| **Sample answer:**The Internet of Things (IoT) refers to a network of interconnected physical objects or ‘things’ that are embedded with sensors, software and other technologies, enabling them to collect and exchange data with other devices and systems over the internet.These objects can range from everyday items like appliances, vehicles and wearable devices to industrial machines and infrastructure components.The key idea behind IoT is to enhance the efficiency, functionality and convenience of these objects by enabling them to communicate and share information, leading to improved automation, data analysis, and decision-making processes across various domains, from smart homes and cities to healthcare and manufacturing. |

#### What is the Internet of Me (IoMe)?

The Internet of Me (IoMe) is a concept that refers to the use of data from various sources to create personalised experiences for individuals. It involves collecting and analysing data from various devices and systems, including wearable devices, health and fitness trackers, smart home appliances, and social media platforms, to create a more customised and personalised user experience. The data collected can be used to provide recommendations, insights and personalised services, such as health and wellness coaching, customised entertainment recommendations and personalised shopping experiences.

The IoMe represents a shift towards more personalised and individualised experiences, in which technology can be used to better understand and meet the needs and preferences of individual users. However, there are also concerns around data privacy and security, as the collection and use of personal data raises questions around who has access to this information and how it is being used.

**Activity 12:** IoT innovation challenge

**Objective:** To introduce students to the concept of IoT and engage them in a hands-on project that combines IoT, project management, and design thinking.

**Materials needed:**

* Microcontrollers (for example Micro:bits, Arduino or Raspberry Pi)
* Sensors (for example temperature, light, motion)
* Internet connectivity (Wi-Fi modules)
* Computer with programming software (Arduino IDE, Python, and so on)
* Prototyping materials (breadboards, wires, LEDs, and so on
* Access to IoT platforms (for example Blynk, or IoT platforms like AWS IoT)
* Whiteboard or poster paper
* Markers

**Activity steps:**

**Brainstorm IoT ideas**: divide students into small groups and ask them to brainstorm IoT product ideas that could solve real-world problems or enhance daily life. Encourage them to think creatively and consider how IoT can create immersive experiences or interactive media.

**Project planning**: each group should choose one idea and create a basic project plan. They should outline the key components needed, set a timeline and assign roles within their team. Emphasise to students the importance of an iterative approach to project management.

**IoT prototyping**: provide the necessary materials and guide students in building a simple IoT prototype related to their chosen idea. They should connect sensors to microcontrollers, write basic code to collect data, and send it to an IoT platform. Encourage students to experiment with different sensors and functionalities.

**Testing and iteration**: after building the prototype, students should test it and gather data. Discuss the results as a class and encourage students to identify areas for improvement.

**Design and user experience**: introduce the concept of user experience (UX) design. Have students sketch a user interface (UI) for their IoT device, considering how it will provide an immersive and interactive experience for users.

**Final presentation**: each group presents their IoT project, highlighting the problem it solves, the technology used, the iterative process, and the design thinking behind it. Students can film their system for inclusion in Assessment task 2.

**Reflection and discussion**: conclude the activity with a group discussion on the challenges faced, lessons learned, and the potential impact of IoT on our lives. Relate this back to the computational, design, and systems thinking aspects of the solution.

**Activity 13:** read [The Internet of Me: When the Consumer Becomes the Electronics](https://www.wired.com/brandlab/2018/01/internet-consumer-becomes-electronics/).

In the space below, define in your own words what is meant by the Internet of Me (IoMe).

|  |
| --- |
| **Sample answer:**The ‘Internet of Me’ (IoMe) is a concept that refers to a personalised and highly individualised digital ecosystem where an individual's data, preferences, and digital interactions are at the centre of their online experience.In IoMe, people have greater control over their personal data and how it's utilised, allowing them to tailor their digital environment to their unique needs and desires.This concept encompasses the idea that technology and services adapt to individuals rather than the other way around, creating a more personalised and responsive online world. It involves the seamless integration of various devices, applications and platforms to enhance an individual's quality of life, productivity and overall digital experience while respecting their privacy and preferences. |

#### Development of hardware and software

The development of hardware and software has played a significant role in the adoption of the Internet of Things (IoT) and the Internet of Me (IoMe). Here are some ways in which hardware and software have influenced the adoption of these technologies:

**Connectivity**: the development of low-power wireless communication technologies, such as Bluetooth and Wi-Fi, has made it possible for devices to connect to the internet and communicate with each other. This has enabled the widespread adoption of IoT and IoMe technologies, allowing users to connect and control a wide range of devices and services.

**Sensors and data collection**: the development of small, low-power sensors and data collection devices has enabled the collection of large amounts of data from physical objects and environments. This data can be used to monitor and control everything from home appliances to industrial machinery and can provide valuable insights into user behaviour and preferences.

**Analytics and machine learning**: the development of powerful analytics and machine learning tools has enabled the processing and analysis of the vast amounts of data generated by IoT and IoMe devices. This has enabled the creation of predictive models, real-time monitoring, and automated decision-making, all of which can enhance the user experience and optimise system performance.

**Security and privacy**: the development of secure and private communication protocols and software tools has helped to address concerns around the security and privacy of IoT and IoMe devices. These technologies have enabled the secure transfer and storage of sensitive data, as well as the development of secure authentication and access control systems.

**User interfaces**: the development of intuitive and user-friendly interfaces for IoT and IoMe devices has helped to increase their adoption and usability. These interfaces can be designed for a range of devices, including smartphones, tablets and voice-activated assistants and can be customised to the needs and preferences of individual users.

**Activity 14:** read about and investigate newly developed technology, including [Neuralink](https://www.forbes.com/sites/qai/2022/12/07/elon-musks-neuralink-brain-implant-could-begin-human-trials-in-2023/?sh=60a31aa8147c) and [5G](https://www.zdnet.com/topic/5g-what-it-means-for-iot/) technology.

In the space below, write a summary on the new frontiers in networking systems.

|  |
| --- |
| **Sample answer:**The convergence of 5G and Neuralink technology represents a groundbreaking frontier in networking systems. 5G, the fifth-generation wireless technology, is revolutionising connectivity by offering ultra-fast speeds, low latency, and massive device connectivity, enabling seamless communication between devices and the cloud. When combined with Neuralink, a neurotechnology company aiming to merge the human brain with computers, it opens new frontiers in human-machine interaction.With Neuralink's brain-computer interfaces, individuals could potentially access and control devices, applications and networks with their thoughts. This integration could lead to transformative applications, such as brain-controlled Internet of Things (IoT) devices and real-time data exchange between the brain and the digital world, offering unprecedented opportunities and challenges at the intersection of technology and human cognition. |

#### Impact on the individual

The Internet of Things (IoT) has had a significant impact on individuals in a number of ways. Here are some of the ways in which IoT has influenced our lives:

Increased convenience: IoT devices such as smart speakers, thermostats, and home security systems have made it easier for individuals to control their environments and manage their daily tasks. For example, with a smart speaker, individuals can control their music, set reminders, and even order groceries with just a voice command.

Improved health and safety: IoT devices such as fitness trackers and health monitors have made it easier for individuals to track their health and fitness goals, and to monitor their wellbeing. In addition, IoT-enabled safety devices such as smoke detectors and security cameras have improved home safety and security.

Enhanced productivity: IoT devices such as smartwatches and connected laptops have enabled individuals to work more efficiently and productively, regardless of their location. With access to real-time data and remote communication tools, individuals can work from anywhere and stay connected with their colleagues.

Increased data privacy concerns: with the proliferation of IoT devices, there are increasing concerns around data privacy and security. As more devices collect and store personal data, there is a risk that this data could be hacked or misused.

Changes in employment: the rise of IoT has led to new job opportunities in fields such as data analytics, cybersecurity, and software engineering. However, it has also led to concerns around automation and the potential loss of jobs.

#### Impact on enterprise, including edge computing

The impact of IoT on enterprises has been significant, particularly in the area of edge computing. While there are challenges to be addressed around data management and security, the benefits of IoT for enterprises are clear, and we can expect to see continued growth and innovation in this area in the years to come.

Here are some ways in which IoT has influenced enterprises:

Improved operational efficiency: IoT devices and edge computing technologies have enabled enterprises to gather real-time data from their machines, processes and products, allowing them to optimise operations, reduce downtime, and improve overall efficiency.

Enhanced customer experience: IoT-enabled devices such as smart thermostats and voice assistants have enabled enterprises to create personalised experiences for their customers, delivering services and products that meet their individual needs.

Increased data management challenges: with the proliferation of IoT devices, enterprises are collecting and processing vast amounts of data, leading to significant challenges around data storage, security and management.

New business opportunities: the rise of IoT has created new opportunities for enterprises to develop new products and services, leveraging the data generated by connected devices to gain insights into customer needs and preferences.

Greater reliance on edge computing: as more IoT devices are deployed, enterprises are increasingly relying on edge computing technologies to process and analyse data in real-time, reducing latency and improving overall system performance.

**Activity 15:** read about [10 Edge computing use case examples](https://stlpartners.com/articles/edge-computing/10-edge-computing-use-case-examples/) and [edge computing in enterprise](https://appinventiv.com/blog/edge-computing-in-enterprise/).

In the space below, summarise how edge computing is impacting enterprise systems.

|  |
| --- |
| **Sample answer:**Edge computing is significantly impacting enterprise systems by decentralising data processing and reducing latency. Instead of relying solely on centralised cloud servers, edge computing brings computation and data storage closer to the data source, which is particularly crucial for applications requiring real-time processing.This approach improves the performance of enterprise systems by reducing the time it takes for data to travel to and from the cloud. Furthermore, it enhances security and data privacy as sensitive information can be processed locally without traversing the internet.For enterprises, this means more efficient and responsive systems, enabling innovations in areas like IoT, automation, and analytics while addressing critical concerns surrounding data security and regulatory compliance. |

#### Hardware infrastructure

The impact of IoT on hardware infrastructure has been significant, driving the development of more powerful, energy-efficient and secure hardware capabilities and architectures. As the number of connected devices continues to grow, we can expect to see continued innovation and evolution in IoT hardware infrastructure.

The impact of the Internet of Things (IoT) on hardware infrastructure has been significant, as the proliferation of connected devices has created new demands for hardware capabilities and architecture.

Here are some ways in which IoT has influenced hardware infrastructure:

Increased demand for processing power: with the vast amount of data generated by connected devices, there is a need for more powerful hardware to process and analyse the data in real-time. This has led to the development of more powerful processors and GPUs, as well as the growth of edge computing.

Changes in network architecture: the growing number of connected devices has led to changes in network architecture, with the need for more complex and distributed networks to handle the increased traffic and data flow.

Development of new sensors and devices: the rise of IoT has led to the development of new sensors and devices, such as smart thermostats and wearables, which require new hardware capabilities to operate effectively.

Greater focus on energy efficiency: as the number of connected devices continues to grow, there is a need for hardware that is energy-efficient and can operate on low power. This has led to the development of new hardware architectures, such as ARM-based processors, which are designed to be more energy-efficient.

Greater need for security: with the increased number of connected devices and the data they generate, there is a greater need for hardware security to protect against cyber threats and data breaches.

**Activity 16:** investigate and examine networks for hardware**.**

Examine your home network. In the space below, explain with examples what hardware infrastructure it has.

|  |
| --- |
|  |

Examine the school network. In the space below, explain with examples what hardware infrastructure it has.

|  |
| --- |
|  |

#### Software protocols

Software protocols are standardised rules and guidelines that dictate the format, behaviour and communication methods used between different software systems or components to enable them to interact and exchange data seamlessly.

These protocols ensure that software applications can understand each other's requests, responses and messages, regardless of the programming languages or platforms they are built on.

Protocols define the structure of data packets, the order of messages, error handling mechanisms, and the overall flow of communication. Examples of software protocols include HTTP (Hypertext Transfer Protocol) for web communication, SMTP (Simple Mail Transfer Protocol) for email transmission, and TCP/IP (Transmission Control Protocol/Internet Protocol) for networking and internet communication. These protocols play a vital role in enabling interoperability and reliable communication among diverse software entities.

**Activity 17:** complete the following table, summarising what function the following [protocols (1:59)](https://www.youtube.com/watch?v=znIjk-7ZuqI) have.

|  |  |
| --- | --- |
| Protocol | What function it provides |
| HTTP (Hypertext Transfer Protocol) |  |
| SMTP (Simple Mail Transfer Protocol) |  |
| TCP/IP (Transmission Control Protocol/Internet Protocol) |  |

#### Data backup

Data backup refers to the process of creating copies or duplicates of digital data, files or information and storing them in a secure location separate from the original source.

The primary purpose of data backup is to safeguard against data loss, whether due to hardware failures, accidental deletion, cyberattacks or other unforeseen events. By maintaining backup copies of critical data, organisations and individuals can restore their information to its previous state in case of data corruption or loss.

Data backup strategies can involve various methods and technologies, such as external hard drives, network-attached storage (NAS), cloud storage and backup software. Regular and consistent data backups are essential to ensure business continuity, protect valuable information and mitigate potential disruptions caused by data-related incidents.

**Activity 18:** complete the following table, defining the following backup strategies.

|  |  |
| --- | --- |
| Backup strategy | Definition |
| External hard drives |  |
| Network-attached storage (NAS) |  |
| Cloud storage |  |
| Backup software |  |

#### Regulation, compliance and cybersecurity

In networking systems, these 3 concepts are interconnected: adherence to regulations ensures legal and ethical operation, compliance guarantees adherence to industry standards, and cybersecurity safeguards against threats that could compromise data and compliance efforts. Organisations must adopt a holistic approach that integrates these elements to create a secure and compliant networking environment.

##### Regulation

Regulation refers to rules, laws and guidelines established by governmental bodies or industry authorities to govern and control various aspects of networking systems. These regulations are designed to ensure fair practices, protect user privacy, promote competition, and maintain the integrity of digital communications.

An example is the *Privacy Act 1988* and Australian Privacy Principles (APPs). The *Privacy Act 1988* establishes regulations for the collection, use and handling of personal information by organisations. The Australian Privacy Principles (APPs) outline specific requirements for managing personal data, including consent, data breach notification, and individuals' rights to access and correct their information. This law ensures the protection of individuals' privacy rights within networking and data management practices.

##### Compliance

Compliance refers to the adherence to regulatory requirements, industry standards and best practices within networking systems. Organisations must ensure that their networking practices and data handling align with the applicable regulations to avoid legal consequences and reputational damage. Compliance often involves implementing specific security measures, data protection protocols and reporting mechanisms to demonstrate adherence to the established rules.

##### Cybersecurity

Cybersecurity focuses on safeguarding networking systems and digital assets from malicious activities, unauthorised access and potential threats. It encompasses the strategies, practices and technologies used to protect data, networks and devices from cyberattacks, data breaches and other security vulnerabilities. Robust cybersecurity measures involve firewall protection, intrusion detection systems, encryption, access controls, regular software updates, employee training and incident response plans.

**Activity 19:** Notifiable Data Breaches scheme

In Australia, under the *Privacy Act 1988*, the Notifiable Data Breaches (NDB) scheme requires organisations to notify individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach occurs that is likely to result in serious harm. This scheme promotes transparency and accountability in the event of data breaches.

Research recent data breaches that have been in the news and list them in the space below.

|  |
| --- |
| **Sample answers:*** Canva May 2019 – impacts 137 million users
* Latitude March 2023 – impacts 14 million users
* Optus September 2022 – impacts 9.8 million users
* Medibank December 2022 – impacts 9.7 million users
* Australian National University November 2018 – impacts 200,000 students
* Service NSW April 2020 – impacts 104,000 users
 |

### Outline the business and individual cultural characteristics that contribute to the success of start-ups

**Activity 20:** in your own words describe what is meant by a start-up in the space below.

|  |
| --- |
|  |

**Activity 21:** read about the [Sydney Startup Hub](https://www.investment.nsw.gov.au/living-working-and-business/sydney-startup-hub/) and outline the characteristics which contribute to success under Business in the table below.

Read [Thirteen key characteristics of a great startup culture](https://www.bizjournals.com/seattle/blog/techflash/2009/05/Thirteen_characteristics_of_a_great_startup_culture_45678557.html) and outline the characteristics which contribute to success under Individual in the table below.

|  |  |
| --- | --- |
| Business | Individual |
|  |  |

The table below outlines characteristics that contribute to the success of a start-up.

|  |  |
| --- | --- |
| Characteristic | Start-up company |
| Entrepreneurial mindset | Successful start-ups typically have founders and team members with an entrepreneurial mindset, which is characterised by a willingness to take risks, experiment and pivot as needed. This mindset is critical in a start-up environment, where uncertainty and ambiguity are often the norm. |
| Innovation | Start-ups must be able to offer something new and innovative in order to stand out in a crowded market. This often requires a focus on research and development, as well as a willingness to challenge existing assumptions and ways of doing things. |
| Customer focus | Successful start-ups tend to be highly customer-focused, with a deep understanding of their customers' needs and pain points. This can involve conducting market research, gathering feedback, and iterating based on customer input. |
| Agile culture | Start-ups must be able to move quickly and adapt to changing circumstances in order to succeed. This often requires an agile culture, with a focus on collaboration, communication and flexibility. |
| Lean approach | Start-ups often operate with limited resources and funding, which requires a lean approach to operations and decision-making. This can involve prioritising the most critical tasks, minimising waste, and being creative in finding solutions to problems. |
| Resilience | Start-ups are often faced with setbacks and challenges, and it's important for founders and team members to be resilient in the face of adversity. This can involve staying focused on long-term goals, learning from failures, and persevering through difficult times. |
| Strong network | Building a strong network of mentors, advisors, investors and partners can be critical to the success of a start-up. This network can provide valuable support, advice and connections to help the start-up grow and succeed. |

## Storage and workflow in enterprise networks

### Investigate how the developments in network connectivity and speed have influenced work practices within an enterprise

#### Remote working opportunities

Network connectivity and speed have had a significant impact on work practices within enterprises, particularly in terms of remote working opportunities. With high-speed connectivity, employees can collaborate more effectively, work from anywhere, improve productivity, reduce costs, and enhance recruitment efforts. As network technology continues to evolve, it is likely that these trends will continue to shape the future of work within enterprises.

|  |  |
| --- | --- |
| Key issue | Way in which network connectivity and speed have influenced work practices |
| Increased collaboration | High-speed network connectivity has enabled employees to collaborate more easily and efficiently, regardless of their physical location. With video conferencing, instant messaging and other collaboration tools, employees can work together in real-time, share ideas and communicate more effectively. |
| Greater flexibility | High-speed network connectivity has also made it possible for employees to work from anywhere, at any time. This has enabled more flexible work arrangements, such as telecommuting, remote work and flexible schedules. This has the potential to improve work-life balance, reduce commute times and costs, and increase productivity. |
| Improved productivity | With faster network speeds, employees can access and share data more quickly and easily, which can improve productivity. This can include faster download and upload speeds, quicker access to cloud-based applications and data, and more reliable connectivity. |
| Reduced costs | Remote working opportunities enabled by high-speed network connectivity can also help to reduce costs for enterprises. With fewer employees in the office, enterprises can save on rent, utilities and other expenses associated with maintaining a physical office space. |
| Enhanced recruitment | The ability to offer remote working opportunities can also make enterprises more attractive to potential employees, particularly those who prioritise work-life balance and flexibility. This can help enterprises to recruit and retain top talent. |

#### File sharing

The developments in network connectivity and speed have revolutionised file sharing and collaboration within enterprises, leading to increased productivity and efficiency. As network speeds continue to improve, it's likely that we will see even more advances in file sharing and collaboration tools in the years to come.

**Activity 22:** complete the table below, including definitions for common file sharing software and concepts.

|  |  |
| --- | --- |
| Concept | Description in relation to file sharing |
| Dropbox, Google Drive, OneDrive |   |
| Security |   |
| Teamwork |   |
| Fast Network Speeds |  |

With faster network speeds and more reliable connectivity, file sharing has become much more efficient and streamlined. In the past, sharing large files between employees within an organisation often required physically transferring the files via external drives or other storage devices. This process was time-consuming and often prone to errors and delays.

Today, with faster network speeds and more reliable connectivity, file sharing can be done instantly and securely over the enterprise network. Cloud-based file sharing services such as Dropbox, Google Drive, and Microsoft OneDrive have become increasingly popular among businesses, as they allow employees to access and share files from anywhere with an internet connection.

In addition to improving efficiency and convenience, these developments have also had a significant impact on collaboration within an enterprise. With cloud-based file sharing, employees can easily share and collaborate on documents and other files in real-time, regardless of their physical location. This has led to increased productivity and teamwork, as employees can work together on projects regardless of their physical location or work schedule.

However, it's important to note that file sharing also comes with some security risks. Enterprises must implement robust security protocols to ensure that sensitive data is not accessed by unauthorised parties, and that files are properly encrypted and secured during transmission and storage.

#### Task delegation and monitoring

With faster network speeds and more reliable connectivity, it has become easier for managers to delegate tasks to employees and monitor their progress in real-time. For example, cloud-based project management tools such as Asana and Trello allow managers to assign tasks to employees, set deadlines, and track progress in real-time. This has streamlined the task delegation process and has allowed managers to more efficiently oversee their team's work.

In addition, faster network speeds have also made it possible for remote employees to work more effectively, regardless of their physical location. With the rise of telecommuting and remote work, employees can now work from anywhere with an internet connection, which has made it easier for enterprises to expand their workforce beyond their local area. This has also made it easier for managers to delegate tasks to remote employees and monitor their progress in real-time.

Furthermore, the availability of real-time communication tools such as Slack and Microsoft Teams has made it easier for employees and managers to communicate with each other in real-time, regardless of their physical location. This has further facilitated task delegation and monitoring, as managers can quickly provide feedback and make adjustments to tasks as needed.

**Activity 23:** complete the table below, including definitions and descriptions for how software is used for task delegation and monitoring impacts on work practices.

|  |  |
| --- | --- |
| Software | Definition and description of impact on work practices |
| Asana |   |
| Trello |   |
| Slack |   |
| Microsoft Teams |   |
| Microsoft Remote Desktop |  |

### Examine the benefits and limitations of digital workflows operating in an enterprise

Network connectivity and speed have had a significant impact on file sharing practices within enterprises. With high-speed connectivity, employees can transfer files quickly and efficiently, collaborate more effectively, access files from anywhere, enhance security and reduce costs. As network technology continues to evolve, it is likely that these trends will continue to shape the future of file sharing practices within enterprises.

**Activity 24:** read about [how digital workflows streamline business](https://signaturely.com/digital-workflows/). Look at the 5 case studies provided on the website to complete the table below.

|  |  |
| --- | --- |
| Case study | Describe the workflows used in this enterprise |
| Wareing buildings – warehouse solutions |  |
| Delta Clinic – online medical services |  |
| Eurofound – government agency |  |
| Outwood Grange Academy – educational organisation |  |
| Influence & Co – content marketing agency |  |

The following table summarises the benefits of digital workflows.

|  |  |
| --- | --- |
| Benefit | Digital workflow explanation |
| Faster file transfers | With high-speed network connectivity, employees can transfer files quickly and efficiently. This can include large files such as videos, images and other multimedia content, which may have been difficult or impossible to share in the past. Faster file transfers can help to improve productivity and collaboration among employees. |
| Improved collaboration | High-speed network connectivity has enabled more efficient collaboration among employees, including in the area of file sharing.With cloud-based file sharing platforms, employees can access and share files from anywhere, at any time. This can help to facilitate collaboration across different departments and locations. |
| Greater flexibility | With network connectivity, employees can access files from anywhere, at any time, using a variety of devices. This can include desktops, laptops, tablets and smartphones. This can help to improve productivity and collaboration, as employees can access and share files on-the-go. |
| Enhanced security | With network connectivity, enterprises can implement more secure file sharing practices. This can include encryption, password protection and access controls to ensure that sensitive files are only accessible to authorised personnel. This can help to protect confidential data and prevent data breaches. |
| Reduced costs | With cloud-based file sharing platforms, enterprises can reduce costs associated with physical storage and hardware. This can include savings on servers, data centres and other infrastructure. This can also help to reduce the environmental impact of enterprise file sharing practices. |

### Investigate data storage requirements for an enterprise

|  |  |
| --- | --- |
| Factor | Description |
| Capacity | The amount of storage capacity required to store an enterprise's data, which can vary based on the volume and types of data |
| Accessibility | The ability to access data quickly and easily, both within the enterprise and remotely, using a variety of devices |
| Location | The physical location of data storage, which can include on-premises solutions such as servers, as well as cloud-based storage |
| Security | The measures in place to ensure data is secure, which can include access controls, encryption and other security features |

**Activity 25:** Scenario: You are an IT manager in charge of the network at a small business with 20 employees in a rural office location. In the space below, describe what data storage solutions you would purchase from [Bleuwire](https://bleuwire.com/enterprise-data-storage-101/) when considering capacity, accessibility, location and security?

|  |
| --- |
|  |

#### Capacity

The capacity of an enterprise's data storage system is one of the most important considerations. This includes the amount of storage required to accommodate current data, as well as projected future growth.

#### Accessibility

Data accessibility is another important factor to consider. This includes the ability to access data quickly and efficiently, as well as ensuring that authorised users have access to the data they need.

#### Location

The physical location of data storage is another important consideration. This includes whether the data will be stored on-premises or in the cloud, as well as the geographic location of the data centre.

#### Security

Data security is a critical consideration for any enterprise, particularly when storing sensitive or confidential information. This includes both physical security (for example secure data centre facilities) and cybersecurity measures (for example encryption, access controls).

### Explore cloud computing services

There are several types of cloud computing services including IaaS, SaaS and PaaS.

|  |  |
| --- | --- |
| Service Model | Description |
| Infrastructure as a Service (IaaS) | In an IaaS model, a cloud provider offers virtualised computing resources over the internet. This can include servers, storage, networking and other infrastructure components.The customer can then deploy and manage their own operating systems, applications and data on the cloud infrastructure, while the cloud provider is responsible for maintaining the underlying hardware and infrastructure. |
| Software as a Service (SaaS) | In a SaaS model, a cloud provider offers a complete software application over the internet, which the customer can access and use through a web browser or other client application.The cloud provider is responsible for managing the underlying infrastructure and platform, while the customer is only responsible for using the software application. |
| Platform as a Service (PaaS) | In a PaaS model, a cloud provider offers a platform for developing, deploying and managing software applications over the internet. This can include programming languages, development tools, databases and other components.The customer can then build and deploy their own applications on the platform, while the cloud provider is responsible for managing the underlying infrastructure and platform. |

#### Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) provides access to computing infrastructure, such as virtual machines, storage, and networking resources.

#### Software as a Service (SaaS)

Software as a Service (SaaS) provides access to software applications that are hosted and managed by a third-party provider, such as email, CRM and collaboration tools.

#### Platform as a Service (PaaS)

Platform as a Service (PaaS) provides a platform for building, testing, and deploying applications, including development tools, databases and middleware.

### Compare different types of cloud-based data storage in terms of access and services

|  |  |  |
| --- | --- | --- |
| Storage Type | Access | Services/Features |
| Public cloud | Internet-based | * Scalability
* Affordability
* Self-service
* Flexibility
 |
| Private cloud | Internet or intranet | * Customisation
* Control
* Security
* Compliance
 |
| Hybrid cloud | Combination of public and private cloud storage | * Scalability
* Control
* Flexibility
* Security
 |
| Non-cloud on premises | On-site, within the organisation's own infrastructure | * Control
* Security
* Customisation
* High initial costs
 |

**Teacher note:** the following paragraphs are for background information and may be used as needed to complement student understanding.

#### Public cloud

Public cloud refers to a type of cloud computing in which the computing resources and services are offered over the internet by third-party providers to multiple users and organisations. These providers own and operate the infrastructure and hardware necessary to provide cloud services, including servers, storage and networking equipment.

Public cloud services are typically offered on a subscription basis, with users paying for the resources and services they use on an as-needed basis. Public cloud providers offer a variety of services, including infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

One of the key advantages of public cloud services is their scalability. Public cloud providers can quickly and easily add computing resources to meet the needs of their customers, allowing users to scale up or down their usage as needed. Public cloud services also offer cost savings, as users do not need to invest in their own infrastructure or pay for maintenance and upgrades.

Public cloud services are used by a wide range of organisations and individuals, from small businesses to large enterprises. Common use cases for public cloud services include data storage and backup, website hosting, application development and deployment, and collaboration and communication tools.

While public cloud services offer many benefits, they also come with potential security and privacy risks, as users must entrust their data and applications to third-party providers. It is important for users to carefully evaluate the security and privacy policies of public cloud providers before entrusting their data and applications to them.

#### Private cloud

Private cloud refers to a type of cloud computing that provides computing resources and services within a single organisation or entity. Private cloud infrastructure is owned and operated by the organisation that uses it, either on-premises or hosted by a third-party provider.

Unlike public cloud services, private cloud services are not shared with other organisations or users. This offers greater control and customisation over the infrastructure and services, as well as increased security and privacy.

Private cloud services can be implemented using a variety of technologies, including virtualisation and software-defined networking. Private cloud infrastructure can be hosted on-premises in a data centre or in a third-party data centre, and can be managed by the organisation's internal IT department or by a third-party provider.

One of the key advantages of private cloud services is their flexibility and scalability. Private cloud infrastructure can be customised to meet the specific needs of the organisation, and can be scaled up or down as needed to meet changing demands. Private cloud services can also offer greater control over security and compliance, as the organisation has full control over the infrastructure and can implement their own security and privacy policies.

Private cloud services are commonly used by large enterprises, government agencies, and organisations with specific security and compliance requirements. Common use cases for private cloud services include data storage and backup, application development and deployment, and high-performance computing.

While private cloud services offer greater control and security, they can also be more expensive and complex to manage than public cloud services. Organisations considering private cloud services should carefully evaluate the costs, benefits and risks before making a decision.

#### Hybrid cloud

Hybrid cloud refers to a cloud computing environment that combines both public and private cloud services to allow for greater flexibility, scalability and control. In a hybrid cloud environment, an organisation can use both public and private cloud services to meet their specific needs.

The hybrid cloud environment is made up of 2 or more interconnected cloud infrastructures, which can be managed and orchestrated through a single interface. The public cloud component of a hybrid cloud environment typically consists of third-party cloud services, while the private cloud component can be hosted on-premises or in a third-party data centre.

Organisations often use hybrid cloud environments to take advantage of the benefits of both public and private cloud services. Public cloud services offer scalability, cost-effectiveness and flexibility, while private cloud services offer greater control, customisation and security. By using a hybrid cloud environment, organisations can leverage the benefits of both public and private cloud services to optimise their infrastructure and meet their specific needs.

Hybrid cloud environments are commonly used by organisations with fluctuating or unpredictable workloads, as well as those with specific security and compliance requirements. Common use cases for hybrid cloud environments include data storage and backup, application development and deployment, and disaster recovery.

While hybrid cloud environments offer many benefits, they can also be more complex to manage than single-cloud environments. Organisations must carefully plan and orchestrate their hybrid cloud environments to ensure optimal performance, security and compliance.

#### Non-cloud on premises

Non-cloud on premises refers to a traditional computing environment in which an organisation owns and operates its own physical hardware, software and networking infrastructure on its premises. In a non-cloud on premises environment, all computing resources are managed and maintained by the organisation's internal IT department.

In a non-cloud on premises environment, all data and applications are stored and processed locally on the organisation's servers and hardware. This offers greater control over the infrastructure, as the organisation has full control over the hardware and software, and can customise and configure it to meet their specific needs.

Non-cloud on premises environments are typically used by organisations with specific security, compliance or performance requirements. They are commonly used for critical applications or sensitive data that cannot be stored or processed in a public cloud environment.

One of the main advantages of non-cloud on premises environments is their control and security. Organisations have complete control over their infrastructure, and can implement their own security and privacy policies. Non-cloud on premises environments can also offer greater performance and reliability, as all resources are dedicated solely to the organisation's use.

However, non-cloud on premises environments can also be more expensive and complex to manage than cloud environments. Organisations must invest in their own hardware and software, and must hire and train staff to manage and maintain the infrastructure. Additionally, non-cloud on premises environments may not offer the same scalability or flexibility as cloud environments.

**Activity 26:** as a class, students watch a video on [cloud computing (6:23)](https://www.youtube.com/watch?v=M988_fsOSWo) that covers the key points:

* Cloud computing versus on premises
* Infrastructure as a Service (IaaS)
* Software as a Service (SaaS)
* Platform as a Service (PaaS)
* Public, private and hybrid cloud.

Answer the following questions, in the space below using information from the video.

What are the key roadblocks faced by the owner of the small software development firm when trying to scale their business?

|  |
| --- |
| **Sample answer:**The key roadblocks faced by the owner of the small software development firm when trying to scale their business include a small team size, the unpredictability of demand and limited resources. |

How does cloud computing differ from on-premises computing in terms of scalability?

|  |
| --- |
| **Sample answer:**Cloud computing differs from on-premises computing in terms of scalability because with on-premises setups, you pay more and have fewer options for scaling.It's difficult to scale down once you've scaled up, leading to heavy losses in infrastructure and maintenance costs.In contrast, cloud computing allows you to pay only for what you use and provides easier and faster options for scaling up or down. |

What are the advantages of cloud computing when it comes to server storage compared to on-premises systems?

|  |
| --- |
| **Sample answer:**Cloud computing solutions require less server storage space compared to on-premises systems.On-premises systems need a lot of space for servers, along with the associated power and maintenance hassles.Cloud service providers manage and maintain the servers, saving both money and space. |

In terms of data security, why do cloud computing systems have an edge over on-premises systems?

|  |
| --- |
| **Sample answer:**Cloud computing systems offer better data security compared to on-premises systems.On-premises systems rely on a combination of physical and traditional IT security measures, which can be complex.In contrast, cloud computing systems provide better security and relieve users from constantly monitoring and managing security protocols. |

What are the implications of data loss in on-premises setups compared to cloud computing systems?

|  |
| --- |
| **Sample answer:**In the event of data loss, on-premises setups have a very small chance for data recovery.Cloud computing systems, on the other hand, have robust disaster recovery measures in place to ensure faster and easier data recovery. |

How does maintenance for on-premises systems differ from maintenance for cloud computing systems?

|  |
| --- |
| **Sample answer:**On-premises systems require additional teams for hardware and software maintenance, leading to increased costs.Cloud computing systems, on the other hand, are maintained by the cloud service providers, reducing costs and resource allocation. |

Provide a concise definition of cloud computing based on the video.

|  |
| --- |
| **Sample answer:**Cloud computing refers to the delivery of on-demand computing services over the internet on a pay-as-you-go basis.Instead of managing files and services on a local storage device, everything is done over the internet in a cost-efficient manner. |

What are the 3 deployment models in cloud computing, and how do they compare to different modes of transportation?

|  |
| --- |
| **Sample answer:**The 3 deployment models in cloud computing are public, private, and hybrid cloud.Public cloud is like taking a bus, where the cloud infrastructure is available to the public over the internet and owned by cloud service providers.Private cloud is like using your own car, where the cloud infrastructure is exclusively operated by a single organisation.Hybrid cloud is like hailing a cab, representing a combination of functionalities from both public and private clouds. |

Explain the 3 major service models in cloud computing: IaaS, PaaS and SaaS.

|  |
| --- |
| **Sample answer:**The 3 major service models in cloud computing are IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service).IaaS provides basic computing infrastructure, PaaS offers cloud platforms and runtime environments for developing applications, and SaaS involves cloud services for hosting and managing software applications. |

## Network architecture and infrastructure

### Describe key components of an organisation’s information technology infrastructure

#### Networking, including servers, storage and end-point devices

In a network, servers and storage devices typically act as central points of control, providing resources and services to end-point devices. End-point devices can communicate with each other and with the servers and storage devices to access data, applications and other resources.

Servers are a type of computer that provides resources and services to other devices on a network. They can store and manage data, host applications and manage network traffic.

Storage refers to the technology and devices used to store and retrieve data on a network. This can include hard drives, solid-state drives, and network-attached storage (NAS) devices.

End-point devices, also known as client devices, are the devices that connect to a network and use its resources and services. These can include computers, smartphones, tablets and other devices that can access the internet or a local network.

#### On-premises computing

On-premises computing refers to a traditional computing model in which an organisation owns and operates its own physical hardware, software and networking infrastructure on its premises. In an on-premises computing environment, all computing resources are managed and maintained by the organisation's internal IT department.

In an on-premises computing environment, all data and applications are stored and processed locally on the organisation's servers and hardware. This offers greater control over the infrastructure, as the organisation has full control over the hardware and software, and can customise and configure it to meet their specific needs.

On-premises computing is typically used by organisations with specific security, compliance or performance requirements. They are commonly used for critical applications or sensitive data that cannot be stored or processed in a public cloud environment.

One of the main advantages of on-premises computing is their control and security. Organisations have complete control over their infrastructure, and can implement their own security and privacy policies. On-premises computing can also offer greater performance and reliability, as all resources are dedicated solely to the organisation's use.

However, on-premises computing can also be more expensive and complex to manage than cloud environments. Organisations must invest in their own hardware and software, and must hire and train staff to manage and maintain the infrastructure. Additionally, on-premises computing may not offer the same scalability or flexibility as cloud environments.

#### Cloud computing

Cloud computing refers to the delivery of computing resources and services over the internet, rather than from a local computer or an on-premises data centre. Cloud computing provides users with access to a wide range of computing resources, including servers, storage, databases, software and other services, all of which are managed and maintained by a third-party provider.

Cloud computing offers several advantages over traditional on-premises computing models, including:

##### Scalability

Cloud resources can be scaled up or down quickly and easily to meet changing needs, without requiring additional hardware or software investments.

##### Cost-effectiveness

Cloud computing can be more cost-effective than on-premises computing, as users only pay for the resources and services they use, rather than investing in and maintaining their own hardware and software.

##### Flexibility

Cloud computing allows users to access their data and applications from anywhere with an internet connection, enabling remote work and collaboration.

##### Reliability

Cloud providers typically offer high levels of reliability and uptime, ensuring that services and data are available when users need them.

**Activity 27:** read about [7 components of IT infrastructure and how they work together](https://houseofit.ph/blog/7-components-of-it-infrastructure-and-how-they-work-together).

In the table below, describe how your home network makes use of the following components. If you do not use a component describe how it could be used at home or in business.

|  |  |
| --- | --- |
| Component | Use in home or business network |
| Networking, including servers, storage and end point devices |  |
| On-premises computing |  |
| Cloud computing |  |

### Describe how transmission media is used in networks

The type of transmission media used in a network depends on a variety of factors, such as the distance over which data needs to be transmitted, the speed at which data needs to be transmitted, and the amount of interference that is present in the network environment. Choosing the right transmission media is important for ensuring that data is transmitted accurately and efficiently within a network.

|  |  |
| --- | --- |
| Transmission media | Use in networks |
| Copper wires | Copper wires are commonly used in Local Area Networks (LANs) for transmitting data between devices. Copper wires can be twisted pair cables, which use 2 insulated copper wires twisted together to reduce interference, or coaxial cables, which have a single copper conductor surrounded by insulation and a braided shield to reduce interference. |
| Fibre optic cables | Fibre optic cables are used in Wide Area Networks (WANs) for transmitting data over long distances at high speeds. Fibre optic cables use light to transmit data through glass or plastic fibres, which can transmit data over longer distances without signal loss or interference. |
| Wireless transmissions | Wireless transmissions are used in networks for transmitting data over the airwaves, without the need for physical cables or wires. Wireless transmissions can use radio waves, microwave frequencies or infrared signals to transmit data between devices. |

Figure 3 – diagram of transmission media organised by guided and unguided media



**Activity 28**: in the table below, examine your home network and describe how your network makes use of the following components. If you do not use a component describe how it could be used at home or in business.

|  |  |
| --- | --- |
| Component | Use in home or business network |
| Copper wires |  |
| Fibre optic cable |   |
| Wireless transmission |   |

### Explain factors that interfere with the transmission of data across a computer and social network

|  |  |  |
| --- | --- | --- |
| Factors | Description | Examples |
| Distance | The distance between the devices transmitting and receiving data can affect the quality of the signal. | Signal strength decreases as the distance increases. |
| Topography | The topography or layout of the physical environment can impact the quality of the signal. | Tall buildings or mountains can block or weaken signals. |
| Physical barriers | Physical objects or structures can block or interfere with the transmission of data. | Walls, buildings and other structures can weaken signals. |
| Environmental barriers | Environmental conditions such as weather or electromagnetic interference can affect signal quality. | Thunderstorms, solar flares and radio frequency interference can weaken signals. |

### Investigate ways to improve data flow within a system, considering proximity and modes of connectivity

The physical location of devices and the mode of connectivity can greatly affect data flow within a system. Using wired connections, such as Ethernet or fibre optic cables, can provide faster and more reliable data transfer than wireless connections. Additionally, positioning devices closer to each other can also improve data transfer speeds.

#### Size, location and power of antennae when using satellite and microwave

When using satellite and microwave communications, the size, location and power of antennae can greatly affect signal strength and transmission quality. Larger antennae typically provide better signal strength, while the location and orientation of the antennae can also impact signal quality. It is also important to ensure that the power of the antennae is appropriate for the desired transmission range.

#### Traffic filtering

Traffic filtering involves managing and regulating the flow of data within a network to ensure that only relevant traffic is transmitted. This can reduce network congestion and improve overall performance by prioritising critical data over non-critical data.

#### Flow scheduling and traffic monitoring on telecommunications, including wireless broadband for mobile devices (3G→), Bluetooth and wi-fi

Flow scheduling involves managing the order and timing of data transmission within a network. By prioritising critical data and regulating the flow of non-critical data, flow scheduling can improve network efficiency and reduce congestion.

Traffic monitoring involves tracking and analysing network traffic to identify potential issues and optimise network performance. This can involve monitoring bandwidth usage, identifying bottlenecks, and analysing network traffic patterns to optimise network performance.

To improve data flow for wireless broadband, it is important to ensure that there is adequate network coverage and signal strength in the area. This can be achieved by installing additional cell towers or other wireless access points. Additionally, implementing traffic filtering, flow scheduling and traffic monitoring can help optimise data transfer speeds and improve overall network performance.

When using Bluetooth and Wi-Fi, it is important to ensure that devices are within range and that the network is secure. Implementing traffic filtering and flow scheduling can also improve data transfer speeds and reduce network congestion. In addition, regular network monitoring can help identify potential security risks and optimise network performance.

**Activity 29:** examine your home network and describe how you could improve data flow.

|  |  |
| --- | --- |
| Idea | Description |
|  |  |
|  |  |
|  |  |

### Investigate the application of graph theory and network theory in the design of optimised computer networks

By applying these concepts, network designers can optimise the performance and efficiency of computer networks, ensuring that data is transmitted quickly, reliably and securely.

|  |  |  |
| --- | --- | --- |
| Graph theory concept | Description | Application in network design |
| Adjacency | Adjacency refers to the relationship between 2 nodes in a network. | In network design, adjacency is used to identify which nodes are connected to each other and how they are connected. By analysing adjacency, network designers can determine the most efficient way to route data between different nodes in the network. |
| Centrality | Centrality measures the importance of a node in a network. | In network design, centrality can be used to determine which nodes are the most important and which ones should be prioritised in terms of connectivity and bandwidth allocation. For example, nodes with high centrality might include routers or switches that connect multiple devices in a network, or servers that host critical applications or data. |
| Connectedness | Connectedness refers to the degree to which nodes in a network are connected to each other. | In network design, connectedness can be used to identify areas of the network that are vulnerable to outages or other disruptions. By analysing the connectedness of different nodes, network designers can create redundancy and backup systems that can help ensure that data can be transmitted even if certain parts of the network are damaged or unavailable. |
| Weighted graphs | Weighted graphs assign a weight or value to each edge in a network, which can be used to represent different characteristics of the network. | In network design, weighted graphs can be used to model different aspects of network performance, such as bandwidth, latency or reliability. By analysing the weights of different edges, network designers can optimise the routing of data through the network to ensure that it meets specific performance goals. For example, a network might use a weighted graph to prioritise data transmission over high-bandwidth connections or to avoid congested or unreliable nodes. |

#### Adjacency

Adjacency refers to the direct connections or relationships between nodes (devices) in a network. Adjacency is a key factor in designing reliable, high-performance computer networks.

##### Network topology representation

* Computer networks are often represented as graphs, with nodes representing devices and edges representing connections. Adjacency signifies the presence of a direct link between 2 devices.

##### Efficient routing

* Adjacency data is essential for designing efficient routing algorithms. Routers use adjacency information to determine the shortest paths for forwarding data packets. This results in minimised latency and optimised data flow.

##### Redundancy and fault tolerance

* Establishing redundant links (adjacency) enhances network reliability. Even if some links fail, the network can continue to function. This results in improved fault tolerance and seamless data rerouting.

#### Centrality

Centrality measures the importance or influence of nodes within a network. Centrality is a key tool for designing high-performance, optimised computer networks. It assists in identifying critical nodes, influencers and efficient communication paths.

##### Node centrality

* Node centrality assesses the importance of individual devices in a network. Nodes with higher centrality are influential and have a greater impact on network dynamics.

##### Edge centrality

* Edge centrality evaluates the significance of connections between nodes. High edge centrality indicates critical communication paths or potential bottlenecks.

##### Applications in network design

* Centrality plays a crucial role in optimising computer networks. Centrality metrics (for example degree, betweenness, closeness) help identify critical nodes. Critical nodes are vital for data flow, and their failure can impact network performance.

#### Connectedness

Connectedness refers to the degree of connectivity or how well devices are linked in a network. Connectedness is essential for creating optimised computer networks. It ensures reliable communication, fault tolerance and efficient data flow.

##### Ensuring network reachability

* Connectedness ensures that every device in the network is reachable from any other device. It guarantees seamless communication and data exchange.

##### Redundancy and fault tolerance

* High connectedness improves network robustness against failures. If a link or node fails, alternative paths ensure continuity of communication.

##### Optimal path availability

* Connectedness leads to multiple available paths between devices. It optimises data routing, reducing congestion and enhancing network efficiency.

#### Weighted graphs

Weighted graphs are a powerful extension of basic graphs in graph theory. They incorporate weights or values on edges to represent varying relationships. Weighted graphs are essential tools for optimising computer networks as they enable precise resource allocation, traffic management and cost-efficient routing.

##### Representation of relationships

* In weighted graphs, edges are assigned values (weights) that indicate the strength, distance or cost between nodes.

##### Resource allocation

* Weighted edges represent resource capacities, such as bandwidth or link speed. This enables efficient resource allocation based on the demands of network traffic.

##### Traffic management

* Assigning weights to edges assists in managing network traffic flow. This ensures balanced data distribution and minimises congestion.

|  |  |  |
| --- | --- | --- |
| Concept | Application in Optimised Computer Networks | Explanation |
| Adjacency matrix | Representing network topology | An adjacency matrix represents connections between nodes, aiding in visualising network links. |
| Node centrality | Identifying critical nodes and influencers | Centrality measures (for example degree, betweenness) help identify influential nodes and potential points of failure |
| Edge centrality | Optimising routing and communication paths | Edge centrality guides efficient data flow by identifying key links or bottlenecks in the network. |
| Connectedness | Ensuring network reachability and redundancy | Analysing connectedness ensures reliable communication and resilience against node failures. |
| Weighted graphs | Optimising resource allocation and traffic management | Weighted graphs represent varying link capacities or costs, aiding in efficient network design. |

**Activity 30:** in the space below, draw an adjacency matrix to show your classroom and school environment.

|  |
| --- |
|  |

**Activity 31:** in the space below, create a diagram to show the nodes and their weight in your home environment.

|  |
| --- |
|  |

### Explore device interoperability within an Internet of Things (IoT) based enterprise network, including supervisory control and data acquisition (SCADA)

Device interoperability is an important aspect of creating a successful Internet of Things (IoT) based enterprise network. In this context, interoperability refers to the ability of different IoT devices to communicate with each other and exchange data seamlessly, regardless of their manufacturer, operating system or communication protocols.

Supervisory control and data acquisition (SCADA) is a system used to control and monitor industrial processes. It allows operators to collect data from sensors and other devices, analyse the data, and make decisions based on the information gathered. SCADA systems are often used in conjunction with IoT devices to create a unified system that can control and monitor a wide range of industrial processes.

To achieve interoperability within an IoT based enterprise network, several standards and protocols have been developed, such as:

Message Queuing Telemetry Transport (MQTT): this is a lightweight messaging protocol that enables devices to publish and subscribe to messages over the internet. MQTT is often used in IoT networks to connect low-powered devices with limited processing capabilities.

Constrained Application Protocol (CoAP): CoAP is a protocol designed for use with constrained devices and networks. It allows devices to communicate with each other using web services and is often used in IoT networks to provide low-power, low-bandwidth communication between devices.

Extensible Messaging and Presence Protocol (XMPP): XMPP is a protocol for instant messaging and presence. It can be used to create real-time messaging systems that support IoT devices and can be used to connect devices and systems in IoT networks.

OPC Unified Architecture (OPC UA): OPC UA is a machine-to-machine communication protocol for industrial automation. It is designed to provide a secure and reliable way to exchange data between devices and systems in an IoT network.

The use of standard protocols and formats can help ensure that IoT devices are interoperable with each other and with other systems in an enterprise network, such as SCADA systems. In addition, the use of open-source software and hardware can help reduce costs and increase flexibility, making it easier to adapt to changes in the network and to integrate new devices and services as needed.

Overall, interoperability is essential for creating a successful IoT based enterprise network that can help improve efficiency, reduce costs, and provide new insights into industrial processes.

### Investigate communication protocols between devices in an Internet of Things (IoT) network

In an Internet of Things (IoT) network, communication protocols are used to enable devices to exchange data and commands. These protocols define the rules and standards for how data is transmitted and received between devices. There are several communication protocols that are commonly used in IoT networks, each with its own strengths and weaknesses. Here are some of the most commonly used IoT communication protocols:

* MQTT (Message Queuing Telemetry Transport): MQTT is a lightweight, publish-subscribe protocol that is designed for use in low-bandwidth, high-latency environments. It is often used in IoT applications where devices need to send small amounts of data over unreliable networks.
* CoAP (Constrained Application Protocol): CoAP is a lightweight, web-based protocol that is designed for use in resource-constrained IoT devices. It is often used in IoT applications where devices need to communicate with web services.
* HTTP (Hypertext Transfer Protocol): HTTP is a widely used protocol for communication between web servers and clients. It is often used in IoT applications where devices need to communicate with web services.
* AMQP (Advanced Message Queuing Protocol): AMQP is a protocol for message-oriented middleware that is designed for use in distributed systems. It is often used in IoT applications where devices need to exchange large amounts of data over reliable networks.
* Zigbee: Zigbee is a low-power wireless communication protocol that is designed for use in IoT applications where devices need to communicate over short distances.
* Z-Wave: Z-Wave is a wireless communication protocol that is designed for use in IoT applications where devices need to communicate over longer distances.
* Bluetooth: Bluetooth is a wireless communication protocol that is widely used in IoT applications where devices need to communicate over short distances.
* Wi-Fi: Wi-Fi is a widely used wireless communication protocol that is often used in IoT applications where devices need to communicate over longer distances.

Each communication protocol has its own advantages and disadvantages, and the choice of protocol will depend on the specific requirements of the IoT application. Factors that may influence the choice of protocol include the amount of data that needs to be transmitted, the reliability of the network and the power requirements of the devices.

**Activity 32:** using your home network, describe how the following components could be relevant in the table below.

|  |  |
| --- | --- |
| Component | Relationship to home or business network |
| Device interoperability within an IOT network |  |
| Communication protocols between devices in an IOT network |  |
| Benefits of interfacing machine learning with an IOT network (See below for more information before attempting this question.) |  |

### Explore the benefits of interfacing machine learning (ML) with IoT

Interfacing machine learning (ML) with IoT has several benefits, including:

|  |  |
| --- | --- |
| Benefit | Explanation |
| Predictive maintenance | By analysing sensor data from IoT devices, machine learning algorithms can identify patterns that indicate when maintenance is needed. This can help to reduce downtime and extend the lifespan of equipment. |
| Anomaly detection | Machine learning algorithms can be used to analyse data from IoT devices to identify anomalies that may indicate a problem. This can help to prevent issues before they become serious and avoid costly downtime. |
| Real-time decision making | By interfacing machine learning with IoT devices, real-time decisions can be made based on the data being generated. This can help to optimise processes and improve efficiency. |
| Improved automation | Machine learning algorithms can be used to automate decision-making processes based on IoT data. This can help to reduce human error and increase efficiency. |
| Personalisation | By analysing data from IoT devices, machine learning algorithms can be used to personalise experiences for individual users. This can help to improve customer satisfaction and increase loyalty. |
| Improved safety | By analysing data from IoT devices, machine learning algorithms can be used to identify potential safety hazards. This can help to prevent accidents and improve overall safety in various industries. |

Overall, interfacing machine learning with IoT devices has the potential to improve efficiency, reduce costs and enhance the overall performance of IoT systems.

#### Data-driven optimisation to enable predictive maintenance and logistics in manufacturing

Data-driven optimisation is a powerful tool for manufacturers looking to improve the efficiency and performance of their operations. By leveraging the power of data analysis and machine learning, manufacturers can gain insights into their systems and processes, identify areas for improvement, and make data-driven decisions to optimise their operations.

Predictive maintenance involves using data analysis to predict when maintenance is needed before a breakdown occurs. By analysing data from sensors, machine learning algorithms can identify patterns that indicate when equipment is likely to fail. This information can then be used to schedule maintenance before a failure occurs, reducing downtime and improving equipment reliability.

Logistics optimisation involves using data analysis to optimise the flow of materials, products and information through the supply chain. By analysing data from sensors, machine learning algorithms can identify patterns that indicate when materials or products are likely to be needed. This information can then be used to optimise the scheduling of production, transportation, and inventory management, reducing costs and improving efficiency.

The combination of predictive maintenance and logistics optimisation can provide significant benefits for manufacturers. By using data-driven optimisation, manufacturers can reduce downtime, improve equipment reliability, reduce costs and improve overall performance. This can help to improve customer satisfaction, increase competitiveness and drive business growth.

#### Data acquired from medical imaging to improve accuracy of diagnosis

The use of data acquired from medical imaging, combined with machine learning, has the potential to revolutionise the field of medical diagnosis and treatment. By providing automated diagnostic support and improving accuracy, machine learning can help to improve patient outcomes and reduce healthcare costs.

Medical imaging technologies such as X-rays, CT scans, MRIs and ultrasounds provide detailed images of the inside of the body that can help doctors to diagnose and treat a wide range of medical conditions. However, the interpretation of these images can be challenging and requires a high level of expertise.

By using data acquired from medical imaging, machine learning algorithms can be trained to analyse the images and provide automated diagnostic support. For example, a machine learning algorithm can be trained to identify patterns in CT scans that are indicative of lung cancer or to detect early signs of Alzheimer's disease in brain scans.

Machine learning algorithms can also be used to analyse large datasets of medical images to identify patterns and trends that may be missed by human experts. This can help to improve the accuracy of diagnosis and reduce the risk of misdiagnosis.

In addition to improving accuracy, the use of machine learning in medical imaging can also help to reduce costs and improve efficiency. By automating the analysis of medical images, machine learning can help to reduce the time and resources required for diagnosis, allowing doctors to focus on providing personalised care to their patients.

#### Improving traffic control through ML and sensors

The combination of machine learning and sensor technologies has the potential to revolutionise traffic control and improve the quality of life for people living in cities around the world.

Improving traffic control is an important goal for cities around the world. By reducing traffic congestion and improving traffic flow, cities can reduce air pollution, improve safety and save time and money for commuters.

Machine learning and sensor technologies can play an important role in improving traffic control. By collecting data from sensors such as cameras, radar and traffic sensors, machine learning algorithms can be trained to analyse traffic patterns, predict congestion and optimise traffic flow.

For example, machine learning algorithms can be used to predict traffic flow and congestion based on data from traffic sensors. This information can be used to adjust traffic signals in real-time, optimising the flow of traffic and reducing congestion. Machine learning can also be used to predict accidents and other traffic incidents, allowing traffic controllers to respond quickly and efficiently.

In addition, machine learning algorithms can be used to analyse data from cameras and other sensors to detect traffic violations such as speeding or running red lights. This information can be used to identify problem areas and to enforce traffic laws more effectively.

The use of machine learning and sensors in traffic control can provide significant benefits for cities. By reducing traffic congestion and improving traffic flow, cities can reduce air pollution, improve safety, and save time and money for commuters. The use of machine learning and sensors can also help to reduce the workload for traffic controllers and improve their ability to respond quickly to incidents.

#### Automating soil moisture data collection to manage farm irrigation

Managing irrigation is an important part of modern agriculture, as it helps to ensure that crops receive the right amount of water to grow and thrive. However, traditional methods of soil moisture monitoring can be time-consuming and labour-intensive, requiring farmers to physically measure soil moisture levels at regular intervals.

Automating soil moisture data collection can help to streamline this process and improve irrigation management. By installing sensors that continuously monitor soil moisture levels, farmers can obtain real-time data that can be used to optimise irrigation schedules and prevent over-watering or under-watering of crops.

Machine learning algorithms can also be used to analyse soil moisture data and provide insights into how much water is needed by different crops under different conditions. For example, machine learning can be used to analyse soil moisture data from multiple sensors and predict when irrigation is needed, based on factors such as crop type, weather conditions and soil type.

In addition to improving irrigation management, automating soil moisture data collection can also help to reduce water waste and improve the efficiency of water use on farms. By providing farmers with real-time data on soil moisture levels, they can optimise irrigation schedules and reduce the amount of water used, saving money and conserving water resources.

Overall, the automation of soil moisture data collection, combined with machine learning algorithms, has the potential to revolutionise irrigation management in agriculture. By providing real-time data and insights, farmers can optimise irrigation schedules, reduce water waste and improve crop yields, ultimately leading to more sustainable and efficient farming practices.

**Activity 33:** read about [agriculture use cases and machine learning applications](https://vitalflux.com/agriculture-use-cases-machine-learning-applications/). In the space below, summarise how machine learning can be used for agriculture.

|  |
| --- |
|  |

**Activity 34:** read about [how computer vision can be used to improve crop yields](https://www.analyticsvidhya.com/blog/2023/01/ai-in-agriculture-using-computer-vision-to-improve-crop-yields/). In the space below, explain how crop yields are improved with computer vision.

|  |
| --- |
|  |

### Investigate security measures used to control access to networks

|  |  |
| --- | --- |
| Security measure | Description |
| Password systems | Require users to enter a password to gain access to the network or specific resources within the network. Passwords should be complex and changed frequently to prevent unauthorised access. |
| Biometric measures | Use physical characteristics, such as fingerprints or facial recognition, to authenticate users and grant access to the network or specific resources. Biometric measures can be more secure than passwords since they are unique to each individual. |
| CAPTCHA | A test that verifies whether the user is human or a robot. CAPTCHAs are often used to prevent automated attacks, such as brute force attacks, by requiring the user to perform a task that a robot cannot easily complete. |
| Trusted Platform Module | A hardware-based security feature that provides a secure environment for storing cryptographic keys and other sensitive data. TPMs can help prevent unauthorised access and protect against tampering and other attacks. |
| Automatic software updates | Regularly updating software can help protect against security vulnerabilities and exploits that could be used to gain unauthorised access to the network. Automatic updates can help ensure that all software is up-to-date and patched against known vulnerabilities. |

In addition to these measures, other security measures used to control access to networks can include firewalls, intrusion detection systems, and access control lists. It's important for organisations to implement multiple layers of security measures to protect against a variety of threats and to regularly review and update security protocols to ensure they remain effective.

These measures collectively contribute to a layered approach to network security, reducing the risk of unauthorised access and data breaches. Organisations often implement a combination of these methods based on their security requirements and the sensitivity of the data being protected. It is important to continually assess and adapt security measures to address evolving threats and vulnerabilities.

#### Password systems

* Strong password policies: organisations implement policies that require users to create strong passwords with a combination of uppercase and lowercase letters, numbers and special characters.
* Multi-Factor Authentication (MFA): this involves using at least 2 different types of authentication methods, such as a password and a one-time code sent to a mobile device, to verify a user's identity.
* Password managers: encourage users to use password managers that generate, store and autofill complex passwords, reducing the risk of weak or reused passwords.

#### Biometric measures

* Fingerprint recognition: biometric sensors scan users’ fingerprints to verify their identity. This method offers high accuracy and convenience.
* Facial recognition: facial features are analysed to authenticate users. This method is gaining popularity due to its user-friendly nature.
* Iris scanning: iris patterns are unique to individuals and can be used for secure authentication.

#### CAPTCHA

* CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart.
* CAPTCHA is used to differentiate between human users and automated bots. It presents challenges that are easy for humans to solve but difficult for bots, reducing the risk of automated attacks.

#### Trusted Platform Module (TPM)

* TPM is a hardware-based security solution that provides secure storage and cryptographic capabilities. It can be used to securely store encryption keys and certificates, enhancing overall system security.

#### Automatic software updates

* Regularly updating operating systems, applications and firmware is essential to patch known vulnerabilities and improve security. Automatic updates ensure that systems are protected against the latest threats.

**Activity 35:** as a class, students watch this video on [Why CAPTCHAs are getting harder (8:03)](https://www.youtube.com/watch?v=lUTvB1O8eEg). In the space below, describe how CAPTCHA works.

|  |
| --- |
| **Sample answer:**CAPTCHA operates by presenting users with a challenge that distinguishes between humans and automated bots on the internet. When a user attempts a specific action, like signing up for an account or submitting a form, a CAPTCHA challenge is generated. This challenge can take various forms, such as distorted text, image recognition or solving puzzles, that are easy for humans to complete but difficult for automated scripts. Users must interact with the challenge, providing a response that proves their human identity. Once the response is submitted, the website or service verifies it, allowing legitimate users to proceed while blocking or limiting access for automated bots. CAPTCHAs serve as an essential security measure, protecting websites and online services from spam, fraud and other malicious activities perpetrated by automated programs. |

### Examine data security for an intelligent home network

|  |  |
| --- | --- |
| Data security measure | Description |
| Access levels, including universal plug and play (UPnP) | Ensure that all devices on the network are properly configured with access levels that limit access to only authorised users. Universal Plug and Play (UPnP) should be disabled to prevent unauthorised devices from being added to the network. |
| Passwords and firewalls | Use strong passwords for all devices and services on the network, and regularly update them. Install a firewall to block unauthorised access and to control traffic between the home network and the internet. |
| Port management on routers and switches | Configure routers and switches to block all incoming traffic except for traffic that is specifically authorised. Only open ports that are needed for specific applications or services. |
| Wi-Fi device positioning | Place Wi-Fi devices in a location that is secure and inaccessible to unauthorised users and ensure that they are updated with the latest security patches and firmware updates. |
| Virtual private networks (VPNs) and hidden networks | Set up a virtual private network (VPN) to encrypt traffic between the home network and the internet and create a hidden network name to prevent unauthorised users from discovering the network. |
| Backup and disaster recovery | Regularly back up all data on the home network to a secure location and ensure that disaster recovery procedures are in place in case of a security breach or other catastrophic event. |

In addition to these measures, it is important to regularly review and update security protocols to ensure they remain effective against new and evolving threats. It is also important to educate all users on safe internet practices, such as avoiding clicking on suspicious links or downloading files from unknown sources, to minimise the risk of security breaches.

#### Access levels, including universal plug and play (UPnP)

**Access levels**

* Set up appropriate access levels for devices and users, ensuring sensitive devices and data are adequately protected from unauthorised access.

**UPnP**

* Review and disable UPnP if not required, as it can potentially expose vulnerabilities in your network security.

**Guest network**

* Set up a separate guest network for visitors to prevent them from accessing your main network and sensitive data.

**IoT security**

* Research and choose IoT devices with strong security features and update capabilities.

#### Passwords and firewalls

**User training**

* Educate all household members about basic security practices, such as avoiding suspicious links and keeping devices updated.

**Secure configuration**

* Teach users to change default passwords and configure devices securely upon installation.

**Strong passwords**

* Ensure all devices and accounts have strong, unique passwords to prevent unauthorised access.

**Firewalls**

* Enable firewalls on both the network router and individual devices to filter incoming and outgoing traffic, enhancing security.

#### Port management on routers and switches

**Port forwarding**

* Configure port forwarding only when necessary, and only open the ports required for specific services.

**Port security**

* Disable unused or unnecessary ports on switches to prevent unauthorised access.

**Firmware updates**

* Regularly update firmware for routers and devices to patch vulnerabilities and ensure optimal performance.

#### Wi-Fi device positioning

**Wi-Fi coverage**

* Position routers strategically to provide even coverage throughout the living space, minimising dead zones and improving overall network performance.

**Signal range**

* Adjust the router's transmission power to prevent the Wi-Fi signal from extending too far beyond your property, reducing the risk of unauthorised access.

#### Virtual private networks (VPNs) and hidden networks

**VPN setup**

* Consider setting up a VPN to encrypt your network traffic, enhancing privacy and security, especially when accessing your home network remotely.

**Hidden SSID**

* Enable the option to hide the Wi-Fi network's SSID (network name) to make it less visible to potential attackers.

**Network segmentation**

* Consider segmenting your network into separate VLANs for different types of devices to minimise potential attack vectors.

#### Backup and disaster recovery

**Regular backups**

* Implement a regular backup strategy for critical data, ensuring you can recover your information in case of device failure or cyberattacks.

**Off-site storage**

* Store backups off-site or in the cloud to protect against physical damage or loss.

**Regular audits**

* Periodically review and audit your network's security settings and configurations.

### Creating a network

To create a network, you will need to follow these general steps:

1. Determine the type of network you want to create.

There are 2 main types of networks – LAN (Local Area Network) and WAN (Wide Area Network). A LAN is a network that covers a small geographic area, such as a home, office or building, while a WAN covers a larger geographic area, such as a city or country.

1. Choose the network topology.

The network topology refers to the physical layout of the network, including the devices and connections used to connect them. The most common network topologies include bus, star and mesh.

1. Choose the networking hardware.

You will need to select the hardware devices that will be used to create your network, such as routers, switches, hubs, modems and network cables.

1. Configure the devices.

Once you have selected your networking hardware, you will need to configure each device to work together as a network. This will involve assigning IP addresses, configuring network settings, and setting up security measures such as firewalls and passwords.

1. Test and troubleshoot the network.

After the network is set up, you will need to test it to ensure that it is functioning properly. This may involve running diagnostic tests, checking network performance, and troubleshooting any problems that arise.

### Design and model a network of interconnected devices for a specific purpose

Consider an example of designing and modelling a network of interconnected devices for a smart home system. The purpose of this network is to provide the homeowner with remote control and automation of various home appliances, security systems and energy management systems.

1. Determine the network topology.

For a smart home system, a star topology would be the most suitable option. This is because all the devices in the network will be connected to a central hub, which will act as a control centre for the entire system.

1. Choose the networking hardware.

The networking hardware for a smart home system would include a wireless router, a smart hub, and various smart devices such as smart lights, smart thermostats, smart security cameras and smart locks.

1. Configure the devices.

Once the hardware is selected, each device will need to be configured to connect to the wireless network and to the smart hub. The smart hub will act as a central control centre for all the smart devices in the home, and the homeowner will be able to control and monitor all the devices through a mobile app on their smartphone.

1. Test and troubleshoot the network.

After the network is set up, it will need to be tested to ensure that all the devices are functioning properly. The homeowner can test each device individually, and also test the system as a whole to make sure that all the devices are working together seamlessly.

1. Add additional features.

Once the basic system is set up, additional features can be added to enhance the functionality of the system. For example, the homeowner may choose to add voice control functionality using a virtual assistant like Amazon Alexa or Google Assistant.

This network of interconnected devices for a smart home system would provide the homeowner with a convenient and efficient way to control and monitor various aspects of their home. The system would be scalable and flexible, allowing the homeowner to add or remove devices as needed, and the network could be easily expanded to include additional features and functionality.

### Apply appropriate project management tools to develop a project

**Activity 36:** scenario – Digital home specialist

Imagine you are in a new career called a Digital home specialist.

In the space below, design the ultimate home network for a client who wants access to the newest, fastest and most innovative technology.

Be sure to include the following in your report:

* diagrams and images
* hardware
* software
* communications technology
* security protocols
* network transmission media
* configure devices within a network
* naming the device
* updating the device
* configuring security protocols
* connecting to the internet
* explore opportunities for optimising network
* improving bandwidth
* updating drivers and firmware
* implement procedures and security protocols.

**Teacher note:** this activity can see the report become the basis of the dialogue or script for Assessment task 2.

|  |
| --- |
|  |

**Activity 37:** scenario – building a Raspberry Pi-based network as a Digital home specialist.

**Objective:** To create a local network using Raspberry Pi to support the Ultimate Home network.

**Materials Needed:**

* Raspberry Pi (multiple if available)
* MicroSD cards with Raspbian OS installed
* Ethernet cables
* Router with multiple Ethernet ports
* Computer with SSH client (for example PuTTY)
* Internet connection (optional)

**Instructions:**

1. Raspberry Pi setup:
2. Divide participants into small groups (if applicable) and provide each group with a Raspberry Pi and necessary accessories.
3. Instruct participants to insert the MicroSD card with Raspbian OS into their Raspberry Pi and connect it to a monitor and keyboard.
4. Guide them through the initial setup process, including connecting to Wi-Fi (if available) or using Ethernet.
5. Network configuration:
6. Explain the basics of network terminology, such as IP addresses, subnet masks, and gateways.
7. Instruct participants to connect their Raspberry Pi devices to the router using Ethernet cables.
8. Show them how to access the Raspberry Pi remotely using SSH from a computer.
9. Assist them in configuring static IP addresses for their Raspberry Pi devices within the same subnet.
10. Test the network:
11. Have participants verify that their Raspberry Pi devices can communicate with each other over the network.
12. Suggest simple tasks like sharing files or running basic commands remotely.
13. Collaborative immersive project:
14. Encourage participants to brainstorm and plan a collaborative immersive project (AR, MR, or VR) that could benefit from the local network they've created.
15. Discuss how networked Raspberry Pi devices can enhance the project's capabilities.
16. Project presentation:
17. Each group presents their project idea and explains how the local network will support it.
18. Reflection and discussion:
19. Lead a discussion on the benefits and challenges of setting up a Raspberry Pi-based network for immersive experiences.
20. Relate the activity to developing content for Assessment task 2.

**Teacher note:** Cisco has a selection of online courses that can benefit students called [Skills for All](https://skillsforall.com/). Some courses use their emulation software Cisco Packet Tracer which does require installation but can help students to create networks and test them in an online environment. These resources would complement the practical nature of physically working with network devices.

The following courses may be used in the teaching of networks and IoT and can be used to extend students’ understanding:

[Getting started with Cisco Packet Tracer](https://skillsforall.com/course/getting-started-cisco-packet-tracer?courseLang=en-US) – 2 hours

[Exploring Networking with Cisco Packet Tracer](https://skillsforall.com/course/exploring-networking-cisco-packet-tracer?courseLang=en-US) – 3 hours

[Exploring Internet of Things with Cisco Packet Tracer](https://skillsforall.com/course/exploring-iot-cisco-packet-tracer?courseLang=en-US) – 3 hours

### Configure devices within a network

Configuring devices within a network involves several essential steps to ensure proper functionality, security and connectivity.

Here's a guide on how to configure devices when creating your Assessment task 2.

#### Naming the device

Choose a descriptive name

* Assign a meaningful name to the device that reflects its purpose or location. This makes it easier to identify and manage devices within the network.

Avoid duplicates

* Ensure that each device has a unique name to prevent confusion and conflicts on the network.

#### Updating the device

Check for updates

* Regularly check for firmware updates, operating system patches and application updates provided by the device manufacturer.

Apply updates

* Install updates to address security vulnerabilities, improve performance and access new features. Ensure the updates are obtained from official sources to prevent potential risks from malicious software.

#### Configuring security protocols

Change default credentials

* Modify default usernames and passwords for the device to prevent unauthorised access. Use strong, unique passwords.

Enable firewall

* If applicable, activate the device's built-in firewall to block unauthorised network traffic and protect against external threats.

Encryption

* Configure encryption protocols such as WPA3 for Wi-Fi networks to secure data transmission.

Disable unnecessary services

* Turn off any unnecessary services or features that could potentially introduce vulnerabilities.

#### Connecting to the internet

Wired connection

* Connect Ethernet cable.
* Plug one end of an Ethernet cable into the device and the other end into a network port or router.
* Obtain IP address
* In most cases, devices will automatically acquire an IP address through DHCP (Dynamic Host Configuration Protocol) when connected via Ethernet.

Wireless connection

* Select Wi-Fi network.
* Access the device's Wi-Fi settings and choose the appropriate network.
* Enter Wi-Fi credentials.
* Provide the network's SSID (name) and security passphrase to establish a secure connection.
* Verify connection.
* Confirm successful connectivity by accessing a website or performing a network test.

### Implement procedures and security protocols considering cybersecurity

|  |  |
| --- | --- |
| Procedure | Security protocol |
| Risk assessment and planning | Conduct a risk assessment: identify potential threats, vulnerabilities and their potential impacts on your network.Develop a cybersecurity plan: create a comprehensive strategy that outlines your organisation's approach to cybersecurity, including prevention, detection, response and recovery. |
| Access control and authentication | Strong authentication: implement multi-factor authentication (MFA) for all users accessing the network and devices.Least Privilege Principle: assign the minimum required privileges to users and limit access to sensitive resources. |
| Regular updates and patch management | Enable automatic updates: ensure that operating systems, software applications and device firmware receive regular updates and patches automatically.Vulnerability management: monitor security advisories and promptly address known vulnerabilities. |
| Firewall and network segmentation | Install firewalls: deploy firewalls to filter incoming and outgoing network traffic and block unauthorised access.Network segmentation: divide your network into segments to isolate sensitive systems from less secure areas, reducing the potential impact of a breach. |
| Data encryption | Data in Transit: implement encryption protocols like SSL/TLS for data transmitted over networks.Data at Rest: encrypt sensitive data stored on devices and servers, and in cloud storage. |
| Regular monitoring and intrusion detection | Intrusion Detection Systems (IDS): deploy IDS to monitor network traffic and detect suspicious activities or unauthorised access attempts.Security Information and Event Management (SIEM): use SIEM solutions to aggregate and analyse security events for timely response. |
| Employee training and awareness | Security training: educate employees about cybersecurity best practices, social engineering risks, and how to recognise phishing attempts.Incident reporting: establish clear procedures for reporting security incidents to the appropriate teams. |
| Backup and recovery | Regular backups: schedule regular backups of critical data and systems to facilitate recovery in case of data loss or ransomware attacks.Offline backups: store backups in an offline location to prevent them from being compromised by online threats. |
| Incident response plan | Develop an incident response plan: outline the steps to take in the event of a cybersecurity incident, including who to contact, how to contain the threat and how to recover. |
| Vendor and third-party risk management | Assess third-party vendors: evaluate the cybersecurity practices of vendors and partners that have access to your network or sensitive data.Contractual agreements: ensure contracts include cybersecurity requirements and responsibilities. |
| Regular audits and testing | Security audits: conduct regular security audits to assess the effectiveness of your cybersecurity measures.Penetration testing: perform ethical hacking tests to identify vulnerabilities and weaknesses. |
| Legal and regulatory compliance | Stay informed: be aware of relevant cybersecurity laws, regulations and compliance standards that apply to your industry. |

**Activity 38:** read current news headlines on recent [data breaches](https://www.webberinsurance.com.au/data-breaches-list#twentythree)and complete the following questions.

What caused the data breach? Explain the main reason behind the data breach in the space below.

|  |
| --- |
|  |

What were the consequences of the breach? Describe the negative outcomes resulting from the breach in the space below.

|  |
| --- |
|  |

How did the organisation respond to the breach? Share the actions taken by the organisation to address the breach in the space below.

|  |
| --- |
|  |

What can be learnt from this incident? Summarise the key lessons that can help prevent similar breaches in the space below.

|  |
| --- |
|  |

What measures have been implemented to prevent future breaches? Highlight the steps taken to enhance security and avoid future breaches in the space below.

|  |
| --- |
|  |

### Explore opportunities for optimising network performance

By strategically optimising network performance, organisations can provide a more efficient user experience and accommodate the growing demands of modern digital operations.

#### Improving bandwidth

* Bandwidth management: implement Quality of Service (QoS) settings to prioritise critical applications and allocate bandwidth appropriately. This ensures that essential tasks receive sufficient bandwidth while preventing bandwidth-intensive applications from overwhelming the network.
* Traffic shaping: use traffic shaping techniques to control the flow of data, preventing certain applications from consuming excessive bandwidth and causing congestion
* Content caching: utilise content caching solutions to store frequently accessed content locally, reducing the need to fetch it from external sources and saving bandwidth
* Load balancing: employ load balancers to distribute network traffic across multiple servers or links, preventing any single component from becoming a bottleneck and maximising overall bandwidth utilisation.

#### Updating drivers and firmware

* Network Interface Cards (NICs): regularly update drivers for NICs to ensure compatibility with the latest networking protocols and improvements. Updated drivers can enhance stability and performance.
* Router and switch firmware: keep router and switch firmware up to date to benefit from bug fixes, security enhancements, and performance optimisations provided by manufacturers.
* Wireless Access Points (APs): update AP firmware to improve security, stability and compatibility with the latest devices. New firmware releases often include performance enhancements as well.
* Firewalls and security appliances: update the firmware of security appliances to ensure that they are effectively inspecting and managing traffic without slowing down the network.

#### Network monitoring and analysis

* Packet analysis: utilise packet analysis tools to identify bandwidth-hungry applications, protocol inefficiencies, and network bottlenecks. This information can guide optimisation efforts.
* Network monitoring tools: deploy network monitoring solutions to track network performance metrics, detect anomalies, and proactively address potential issues before they impact performance.

#### Hardware upgrades

* Switches and routers: consider upgrading network switches and routers to higher-capacity models that can handle increased bandwidth demands. This is particularly important in growing organisations.
* Network cabling: ensure that the network cabling infrastructure supports the desired bandwidth. Upgrading to higher-grade cabling (for example Cat 6a or Cat 7) can provide better performance.

#### Cloud and Content Delivery Networks (CDNs)

* Cloud services: leverage cloud-based services to offload certain network activities and improve overall performance, especially for remote or distributed teams.
* CDNs: use content delivery networks to cache and deliver frequently accessed content from servers geographically closer to users, reducing latency and optimising bandwidth usage.

### Evaluate the role of hardware and software related to the transmission of data

The role of hardware and software in the transmission of data is crucial in ensuring that data is transmitted reliably and securely.

|  |  |  |
| --- | --- | --- |
| Aspect | Hardware | Software |
| Transmission of unsecured data | Network interface card (NIC), cables, routers, switches, hubs | Network protocols, operating system |
| Transmission of encrypted data | Encryption hardware (for example security tokens, smart cards, encryption accelerators), NIC, cables, routers, switches, hubs | Encryption software (for example SSL, TLS, IPsec), decryption software, authentication software |
| Infrastructure | Servers, storage devices, backup devices, power supplies, cooling systems | Network management software, security software, backup and recovery software |

#### Unsecured data

Unsecured data transmission refers to the transmission of data that is not protected by any security measures, making it vulnerable to interception and unauthorised access.

In the case of unsecured data, hardware such as network interface cards (NICs), cables, routers, switches and hubs are used to establish and maintain network connections.

Network protocols and operating systems are used to facilitate unsecured data transmission.

#### Encrypted data

Encrypted data transmission refers to the transmission of data that has been encrypted to prevent unauthorised access.

For encrypted data, encryption hardware such as security tokens, smart cards and encryption accelerators are used to encrypt and decrypt data.

Encryption software such as SSL, TLS and IPsec is used to encrypt and decrypt data in encrypted data transmission. In addition, authentication software is used to verify the identity of users and devices in encrypted data transmission.

#### Infrastructure

Infrastructure, which refers to the physical components of a network, is also an important consideration. This includes servers, storage devices, backup devices, power supplies and cooling systems among others. Network management software, security software, and backup and recovery software are also important components of infrastructure, as they are used to manage and protect network resources.

**Activity 39**: as a class recall examples of [hardware components involved in data transmission](https://in.indeed.com/career-advice/career-development/what-is-network-hardware#:~:text=Questions%20(With%20Answers)-,Router,data%20flow%20within%20a%20network) and discuss how software contributes to the transmission of data.

**Activity 40:** individually research and answer the following questions.

What hardware components are essential for data transmission in immersive technologies?

|  |
| --- |
| **Sample answer:**Immersive technologies, such as virtual reality (VR) and augmented reality (AR), rely on several essential hardware components for data transmission and a seamless user experience. These components include high-performance processors and graphics cards to render immersive environments with realistic detail. Fast and stable internet connections, preferably with low latency, are crucial for streaming content and enabling real-time interactions. Specialised sensors, like accelerometers and gyroscopes, capture user movements and gestures, while cameras and depth sensors provide the input necessary for AR applications. In addition, high-resolution displays and optics deliver the immersive visuals, and spatial audio systems create 3D soundscapes. Collectively, these hardware components ensure the smooth transmission of data, enabling users to fully immerse themselves in virtual or augmented worlds. |

How do sensors, cameras and input devices contribute to data transmission?

|  |
| --- |
| **Sample answer:**Sensors, cameras and input devices are integral to data transmission in various technological applications, including immersive experiences like virtual reality (VR) and augmented reality (AR). Sensors such as accelerometers and gyroscopes capture physical movements and gestures, providing real-time data that informs the system about the user's actions and orientation. Cameras capture the surrounding environment or specific objects, enabling spatial mapping, object recognition and gesture tracking, which are vital for both VR and AR applications. Input devices, ranging from handheld controllers to voice recognition systems, allow users to interact with the virtual or augmented world, transmitting their commands and intentions to the system. These components collectively ensure the seamless flow of data between the user and the technology, enriching the immersive experience and enabling responsive interactions in these immersive environments. |

What challenges may arise when dealing with hardware-related data transmission issues?

|  |
| --- |
| **Sample answer:**When dealing with hardware-related data transmission issues, several challenges can arise. Firstly, hardware failures or malfunctions in sensors, cameras or input devices can disrupt the flow of data, leading to system instability or loss of critical information. Secondly, compatibility issues between different hardware components or between hardware and software can hinder seamless data transmission, requiring extensive debugging and troubleshooting efforts. Additionally, maintaining the synchronisation and accuracy of data from various sensors and cameras can be challenging, particularly in complex systems. Finally, ensuring data security and privacy is crucial, as hardware-related vulnerabilities may expose sensitive information to potential threats. Addressing these challenges demands careful hardware design, robust testing, and ongoing maintenance to guarantee reliable and secure data transmission in various technological applications. |

How do software applications and algorithms manage data transmission?

|  |
| --- |
| **Sample answer:**Software applications and algorithms play a fundamental role in managing data transmission by orchestrating the flow of information efficiently and reliably. They are responsible for data packetisation, error checking and encryption to ensure data integrity and security during transmission. Protocols and algorithms, such as the Transmission Control Protocol (TCP) and Internet Protocol (IP), govern how data is routed across networks, handling issues like congestion control and packet retransmission to guarantee the successful delivery of data. Additionally, application-layer software manages higher-level data transmission tasks, such as establishing connections, handling user requests, and formatting data for presentation. Overall, software and algorithms act as the bridge between the hardware components and the data being transmitted, optimising the process for speed, accuracy and security in various communication systems and technologies. |

What role does coding and programming play in optimising data transmission?

|  |
| --- |
| **Sample answer:**Coding and programming play a pivotal role in optimising data transmission by enabling the development of efficient and reliable communication protocols, algorithms and software. Programmers write code that governs how data is packetised, compressed and encrypted for secure transmission, as well as how it is decoded and reconstructed at the receiving end. They design algorithms that manage issues like error correction, data compression and quality of service to ensure data is transmitted accurately and efficiently. Coding also allows for the implementation of adaptive techniques that can respond to network conditions in real-time, such as adjusting transmission rates or rerouting data in case of congestion. In essence, coding and programming empower the fine-tuning of data transmission processes, making them faster, more resilient and adaptable to various communication scenarios, ultimately optimising the way data is transmitted across networks and systems. |

How do software updates and improvements impact the overall user experience?

|  |
| --- |
| **Sample answer:**Software updates and improvements have a significant impact on the overall user experience by enhancing functionality, security and usability. Updates often introduce new features, fix bugs and optimise performance, ensuring that the software runs smoothly and efficiently. Security patches included in updates protect users from emerging threats and vulnerabilities, safeguarding their data and privacy. User interfaces are refined and streamlined to make applications more intuitive and user-friendly. Overall, software updates and improvements provide users with a more reliable, secure and feature-rich experience, ensuring that their software remains up-to-date and capable of meeting evolving needs and expectations. |

# References

This resource contains NSW Curriculum and syllabus content. The NSW Curriculum is developed by the NSW Education Standards Authority. This content is prepared by NESA for and on behalf of the Crown in right of the State of New South Wales. The material is protected by Crown copyright.

Please refer to the NESA Copyright Disclaimer for more information <https://educationstandards.nsw.edu.au/wps/portal/nesa/mini-footer/copyright>.

NESA holds the only official and up-to-date versions of the NSW Curriculum and syllabus documents. Please visit the NSW Education Standards Authority (NESA) website [https://educationstandards.nsw.edu.au/](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Feducationstandards.nsw.edu.au%2F&data=05%7C01%7CCaitlin.Pace1%40det.nsw.edu.au%7C9c2c1a9f59c94d2df30708dafa7edb23%7C05a0e69a418a47c19c259387261bf991%7C0%7C0%7C638097720042599463%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=NzFc%2Bg75dh42X2SUZ1JxGsPBapsGv7KoRkSbJ1MjiTE%3D&reserved=0) and the NSW Curriculum website [https://curriculum.nsw.edu.au/home](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fcurriculum.nsw.edu.au%2Fhome&data=05%7C01%7CCaitlin.Pace1%40det.nsw.edu.au%7C9c2c1a9f59c94d2df30708dafa7edb23%7C05a0e69a418a47c19c259387261bf991%7C0%7C0%7C638097720042599463%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=SYVPECiogUlm2Ck2OkCJ8LGVJ3ZUXn%2Bm5%2F%2FbO4ocGOM%3D&reserved=0).

[Enterprise Computing 11–12 Syllabus](https://curriculum.nsw.edu.au/learning-areas/tas/enterprise-computing-11-12-2022/overview) © NSW Education Standards Authority (NESA) for and on behalf of the Crown in right of the State of New South Wales, 2022.

Anderson M (2018) ['The Internet of Me: When the Consumer Becomes the Electronics'](https://www.wired.com/brandlab/2018/01/internet-consumer-becomes-electronics/), *Wired*, accessed 15 September 2023.

Bay T (31 August 2020) ['What are disruptive technologies?' [video],](https://www.youtube.com/watch?v=S86mAHwiij4) *Tomas Bay*, YouTube, accessed 15 September 2023.

Cannon W (30 March 2023) [*How digital workflows streamline your business*](https://signaturely.com/digital-workflows/), Signaturely website, accessed 15 September 2023.

Cepero R (5 November 2019) [*Everything you need to know about enterprise storage*](https://bleuwire.com/enterprise-data-storage-101/), Bleuwire website, accessed 15 September 2023.

Cisco Networking Academy (2023) [Exploring Internet of Things with Cisco Packet Tracer](https://skillsforall.com/course/exploring-iot-cisco-packet-tracer?courseLang=en-US), Cisco, accessed 15 September 2023.

Cisco Networking Academy (2023) [Exploring Networking with Cisco Packet Tracer](https://skillsforall.com/course/exploring-networking-cisco-packet-tracer?courseLang=en-US), Cisco, accessed 15 September 2023.

Cisco Networking Academy (2023) [Getting started with Cisco Packet Tracer](https://skillsforall.com/course/getting-started-cisco-packet-tracer?courseLang=en-US), Cisco, accessed 15 September 2023.

Cisco Networking Academy (2023) [Skills for All](https://skillsforall.com/) [website], accessed 15 September 2023.

edureka! (1 August 2018) ['IoT explained'](https://www.youtube.com/watch?v=LlhmzVL5bm8) [video], *edureka!*, YouTube, accessed 15 September 2023.

Firefox Browser Add-ons (n.d.) [*Firefox lightbeam*](https://addons.mozilla.org/en-US/firefox/addon/lightbeam-chikl/)[website], accessed 15 September 2023.

Forbes (7 December 2022) ['Elon Musk's Neuralink Brain Implant Could Begin Human Trials in 2023'](https://www.forbes.com/sites/qai/2022/12/07/elon-musks-neuralink-brain-implant-could-begin-human-trials-in-2023/?sh=60a31aa8147c), *Money*, Forbes website, accessed 15 September 2023.

Gephi (2008–2022) [Gephi](https://gephi.org/) [website], accessed 15 September 2023.

Gottesman G (21 May 2009) ['Thirteen key characteristics of a great startup culture'](https://www.bizjournals.com/seattle/blog/techflash/2009/05/Thirteen_characteristics_of_a_great_startup_culture_45678557.html), *Puget Sound Business Journal*, accessed 15 September 2023.

House of IT (2021) [*7 components of IT infrastructure and how they work together*](https://houseofit.ph/blog/7-components-of-it-infrastructure-and-how-they-work-together), House of IT website, accessed 15 September 2023.

Imperial College London (2018) [*Table of Disruptive Technologies*](https://www.dropbox.com/s/6ukp4d6q3z1douj/Tech-Foresight-Table-of-Disruptive-Technologies.pdf?dl=0) [PDF 63KB], Tech Foresight website, accessed 15 September 2023.

Indeed (2023) [*What is Network Hardware? (With Types and Best Practices)*](https://in.indeed.com/career-advice/career-development/what-is-network-hardware), Indeed website, accessed 15 September 2023.

Investment NSW (2023) [*Sydney Startup Hub*](https://www.investment.nsw.gov.au/living-working-and-business/sydney-startup-hub/), NSW Government website, accessed 15 September 2023.

Kumar A (30 September 2021) [*Agriculture Use Cases & Machine Learning Applications*](https://vitalflux.com/agriculture-use-cases-machine-learning-applications/), Analytics Yogi website, accessed 15 September 2023.

Leaders’ Decision Making Lab (21 January 2021) ['Social Network Analysis: Graph theory' [video]](https://www.youtube.com/watch?v=natjwmIGoxQ), *Leaders’ Decision Making Lab*, YouTube, accessed 15 September 2023.

Mod U: Powerful concepts in Social Science (22 August 2015) ['What is Social Network Analysis?' [video]](https://www.youtube.com/watch?v=xT3EpF2EsbQ), *Mod U*, YouTube, accessed 15 September 2023.

NSW Education Standards Authority (NESA) (n.d.) *A Glossary of Key Words*, NESA website, accessed 23 October 2023.

Ohio State MSLC (13 June 2014) ['Basic Concepts in Graph Theory' [video]](https://www.youtube.com/watch?v=ZHqQDA3be-k), *Ohio State MSLC*, YouTube, accessed 15 September 2023.

Ranger S (3 February 2020) ['What is the IoT? Everything you need to know about the Internet of Things right now'](https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/), *ZDNet*, accessed 15 September 2023.

Shrivastav A (3 December 2020) ['Visualizing Graph Databases Using Gephi'](https://medium.com/swlh/visualizing-databases-using-gephi-591c9530c981), *Medium*, accessed 15 September 2023.

Siersted N (2017) [10 Edge computing use case examples](https://stlpartners.com/articles/edge-computing/10-edge-computing-use-case-examples/), STL Partners website, accessed 15 September 2023.

Simplilearn (29 July 2020) ['Cloud computing In 6 Minutes' [video]](https://www.youtube.com/watch?v=M988_fsOSWo), *Simplilearn*, YouTube, accessed 15 September 2023.

Singh S (16 January 2023) [*AI In Agriculture: Using Computer Vision To Improve Crop Yields*](https://www.analyticsvidhya.com/blog/2023/01/ai-in-agriculture-using-computer-vision-to-improve-crop-yields/), Analytics Vidhya website, accessed 15 September 2023.

Srivastava S (2 December 2022) ['What is Edge Computing and Why It Matters to Enterprises?'](https://appinventiv.com/blog/edge-computing-in-enterprise/), *appinventiv*, accessed 15 September 2023.

TEDx Talks (17 June 2016) ['Technology Disruption | Vidia Mooneegan'](https://www.youtube.com/watch?v=pk9RVBwiFbM) [video], *TEDx Talks*, YouTube, accessed 15 September 2023.

Vox (15 May 2021) ['Why captchas are getting harder' [video]](https://www.youtube.com/watch?v=lUTvB1O8eEg), *Vox*, YouTube, accessed 15 September 2023.

Webber Insurance Services Pty Ltd (2022) [*Data Breach Notifications in Australia*](https://www.webberinsurance.com.au/data-breaches-list#twentythree), Webber Insurance Services website, accessed 15 September 2023.

Wikipedia (2023) [Social network analysis](https://en.wikipedia.org/wiki/Social_network_analysis), Wikipedia, accessed 15 September 2023.

ZDNet (2023) [‘5G:What it means for IoT’](https://www.zdnet.com/video/5g-what-it-means-for-iot/) [video], ZDNet website, accessed 15 September 2023.

**© State of New South Wales (Department of Education), 2023**

The copyright material published in this resource is subject to the *Copyright Act 1968* (Cth) and is owned by the NSW Department of Education or, where indicated, by a party other than the NSW Department of Education (third-party material).

Copyright material available in this resource and owned by the NSW Department of Education is licensed under a [Creative Commons Attribution 4.0 International (CC BY 4.0) license](https://creativecommons.org/licenses/by/4.0/).

 

This license allows you to share and adapt the material for any purpose, even commercially.

Attribution should be given to © State of New South Wales (Department of Education), 2023.

Material in this resource not available under a Creative Commons license:

* the NSW Department of Education logo, other logos and trademark-protected material
* material owned by a third party that has been reproduced with permission. You will need to obtain permission from the third party to reuse its material.

**Links to third-party material and websites**

Please note that the provided (reading/viewing material/list/links/texts) are a suggestion only and implies no endorsement, by the New South Wales Department of Education, of any author, publisher, or book title. School principals and teachers are best placed to assess the suitability of resources that would complement the curriculum and reflect the needs and interests of their students.

If you use the links provided in this document to access a third-party's website, you acknowledge that the terms of use, including licence terms set out on the third-party's website apply to the use which may be made of the materials on that third-party website or where permitted by the *Copyright Act 1968* (Cth). The department accepts no responsibility for content on third-party websites.