1.3 – Computer networks, connections and protocols

Sub topic	Guidance
1.3.1 Networks and topologies	

☐ Types of network:
   ○ LAN (Local Area Network)
   ○ WAN (Wide Area Network)
	Required
	✓ The characteristics of LANs and WANs including common examples of each
	✓ Understanding of different factors that can affect the performance of a network, e.g.:

☐ Factors that affect the performance of networks	▪ Number of devices connected
☐ The different roles of computers in a client-server and a peer-to-peer network	▪ Bandwidth

☐ The hardware needed to connect stand-alone computers into a Local Area Network:
   ○ Wireless access points
   ○ Routers
   ○ Switches
   ○ NIC (Network Interface Controller/Card)
   ○ Transmission media
	✓ The tasks performed by each piece of hardware
	✓ The concept of the Internet as a network of computer networks
	✓ A DNS's role in the conversion of a URL to an IP address
	✓ Concept of servers providing services (e.g. Web server → Web pages, File server → file storage/retrieval)
	✓ Concept of clients requesting/using services from a server

☐ The Internet as a worldwide collection of computer networks:
   ○ DNS (Domain Name Server)
   ○ Hosting
   ○ The Cloud
   ○ Web servers and clients
	✓ The Cloud: remote service provision (e.g. storage, software, processing)
	✓ Advantages and disadvantages of the Cloud
	✓ Advantages and disadvantages of the Star and Mesh topologies
	✓ Apply understanding of networks to a given scenario

☐ Star and Mesh network topologies	

J277 - 1.3 Computer networks, connections and protocols

What is a Network?

A computer network is where two, or more, computing devices are connected together so that they can share resources.
Computers that are not connected to a network are called stand-alone computers.

Advantages of Networks

- Sharing devices such as printers saves **money**.
- Site (software) licences are likely to be **cheaper** than buying several standalone licences.
- Files can easily be **shared** between users.
- Network users can **communicate** by email and instant messenger.
- **Security** is **good** - users cannot see other users' files unlike on stand-alone machines.
- Data is easy to **backup** as all the data is stored on the file server.

Disadvantages of Networks

- Purchasing the network cabling and file servers can be **expensive**.
- Managing a large network is complicated, **requires training** and a network manager usually needs to be employed.
- If the file server breaks down the files on the file server become **inaccessible**.
- **Viruses** can spread to other computers throughout a computer network.
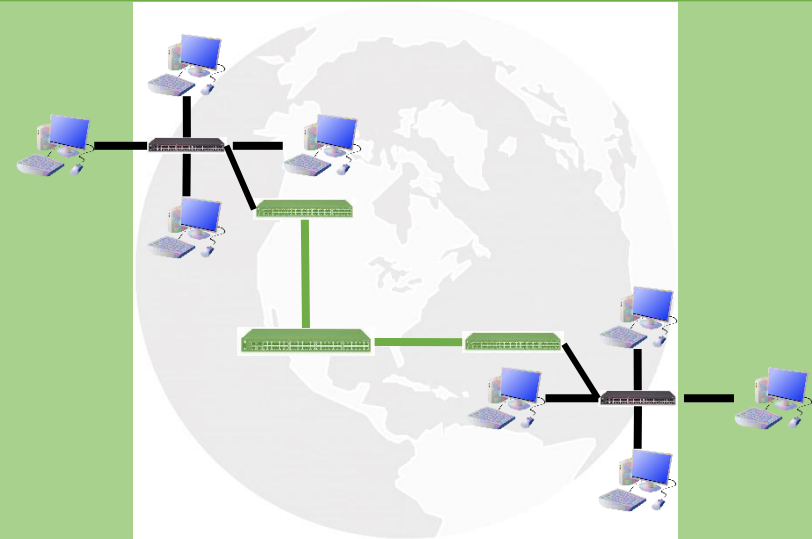- There is a danger of **hacking**, particularly with wide area networks.

Types of networks

Representation of a local area network (LAN):
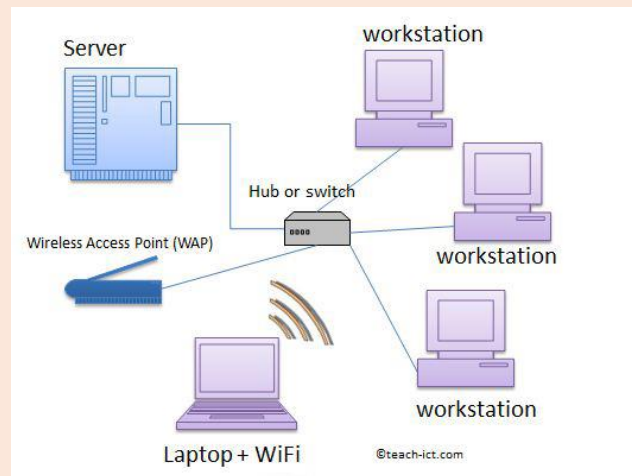
Description of a local area network:
- Covers a small geographic area located on a single site.
- All the hardware for the LAN is owned by the organisation using it.
- LANs are wired or wireless.

Representation of a wide area network (WAN):

Description of a wide area network:
- Covers a large geographic area that connects LANs together.
- Infrastructure between the LANs is hired from telecommunication companies who own and manage it.
- WANs are connected with telephone lines, fibre optic cables or satellite links.

1.3 – Computer networks, connections and protocols

Sub topic	Guidance
1.3.1 Networks and topologies	

☐ Types of network:
   o LAN (Local Area Network)
   o WAN (Wide Area Network)
 	
☐ Factors that affect the performance of networks
☐ The different roles of computers in a client-server and a peer-to-peer network
 	
☐ The hardware needed to connect stand-alone computers into a Local Area Network:
   o Wireless access points
   o Routers
   o Switches
   o NIC (Network Interface Controller/Card)
   o Transmission media
 	
☐ The Internet as a worldwide collection of computer networks:
   o DNS (Domain Name Server)
   o Hosting
   o The Cloud
   o Web servers and clients
 	
☐ Star and Mesh network topologies
	Required
	✓ The characteristics of LANs and WANs including common examples of each
	✓ Understanding of different factors that can affect the performance of a network, e.g.:
	   ▪ Number of devices connected
	   ▪ Bandwidth
	✓ The tasks performed by each piece of hardware
	✓ The concept of the Internet as a network of computer networks
	✓ A DNS's role in the conversion of a URL to an IP address
	✓ Concept of servers providing services (e.g. Web server → Web pages, File server → file storage/retrieval)
	✓ Concept of clients requesting/using services from a server
	✓ The Cloud: remote service provision (e.g. storage, software, processing)
	✓ Advantages and disadvantages of the Cloud
	✓ Advantages and disadvantages of the Star and Mesh topologies
	✓ Apply understanding of networks to a given scenario

Some of the factors which affect network performance are:

Bandwidth refers to the maximum amount of data that can be transmitted over a network in a given amount of time.

Higher bandwidth allows for faster data transfer rates, resulting in improved network performance.

The bandwidth of the network

The number of users on the network

Too many users or devices on the same network can cause the network to slow down if there is insufficient bandwidth for the data.

Less reliable connections increase the number of errors that occur when data is being transferred, resulting in data having to be resent.

The error rate

The transmission media used

Wired connections give better performance than wireless connections.

Fibre optic cables have a higher bandwidth than copper cables.

Latency

The delay from transmitting data to receiving it.

Lower latency is desirable as it reduces the delay in data transmission, resulting in quicker response times.

1.3 – Computer networks, connections and protocols

| Sub topic	Guidance
1.3.1 Networks and topologies	

☐ Types of network:
   ○ LAN (Local Area Network)
   ○ WAN (Wide Area Network)
 	
☐ Factors that affect the performance of networks
 	
☐ The different roles of computers in a client-server and a peer-to-peer network
 	
☐ The hardware needed to connect stand-alone computers into a Local Area Network:
   ○ Wireless access points
   ○ Routers
   ○ Switches
   ○ NIC (Network Interface Controller/Card)
   ○ Transmission media
 	
☐ The Internet as a worldwide collection of computer networks:
   ○ DNS (Domain Name Server)
   ○ Hosting
   ○ The Cloud
   ○ Web servers and clients
 	
☐ Star and Mesh network topologies
	Required
	✓ The characteristics of LANs and WANs including common examples of each
	✓ Understanding of different factors that can affect the performance of a network, e.g.:
	   ▪ Number of devices connected
	   ▪ Bandwidth
	✓ The tasks performed by each piece of hardware
	✓ The concept of the Internet as a network of computer networks
	✓ A DNS's role in the conversion of a URL to an IP address
	✓ Concept of servers providing services (e.g. Web server → Web pages, File server → file storage/retrieval)
	✓ Concept of clients requesting/using services from a server
	✓ The Cloud: remote service provision (e.g. storage, software, processing)
	✓ Advantages and disadvantages of the Cloud
	✓ Advantages and disadvantages of the Star and Mesh topologies
	✓ Apply understanding of networks to a given scenario

Network Topologies

Both local area networks and wide area networks can operate as either a client-server or a peer-to-peer approach when sharing data.
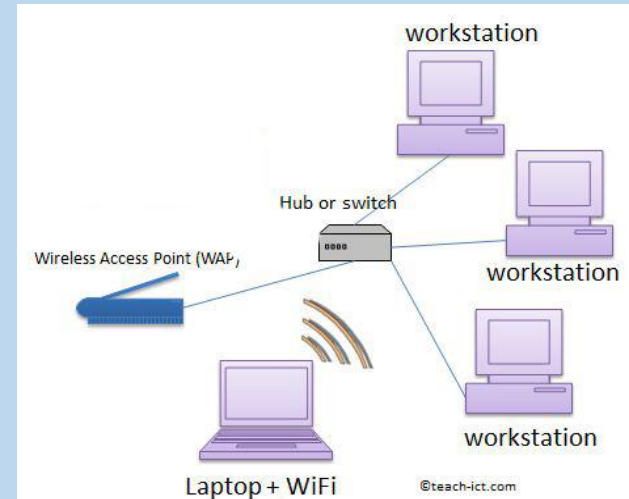
Client-server model
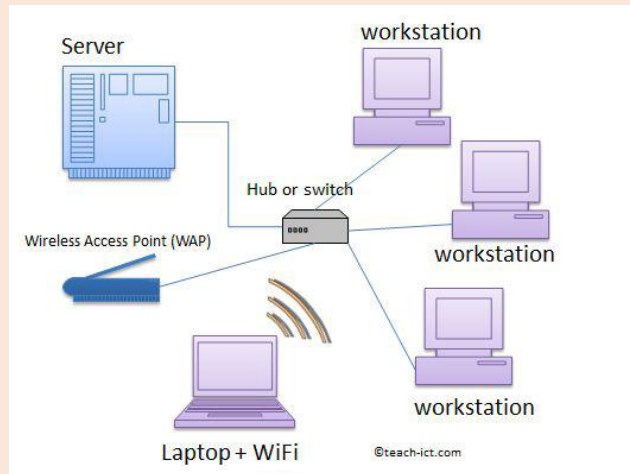
Description of a client-server network
- A server controls access and security to one shared file store.
- A server manages access to the internet.
- A server manages printing jobs.
- A server provides email services.
- A server runs a backup of data.
- A client makes requests to the server for data and connections.

Peer-to-peer model

- A peer is equal to all other peers, they serve their own files to each other.
- Each peer is responsible for its own security.
- Each peer is responsible for its own backup.
- Peers usually have their own printers. You can send print jobs to another peer to process, but that peer would need to be switched on to be able to communicate with the connected printer.

Advantages and disadvantages of client-server and peer-to-peer networks.

Client-server model	Peer-to-peer model

Advantages:

Resource sharing.

Easier to take backups of all shared data.

Easier to install software updates.

Security – Passwords & access levels.

Advantages:

Very easy to maintain without expertise employed.

No dependency on a single server.

Cheaper to set up. No expensive hardware required.

Disadvantages:

Expensive to set up and maintain.

Requires IT specialists to maintain.

A single point of failure. Users will lose access if the server fails.

Requires IT specialists to maintain.

Disadvantages:

The network is less secure.

Users will need to manage their own backups.

Can be complicated to update.

1.3 – Computer networks, connections and protocols

Sub topic	Guidance
1.3.1 Networks and topologies	

☐ Types of network:
   ○ LAN (Local Area Network)
   ○ WAN (Wide Area Network)
 	
☐ Factors that affect the performance of networks
☐ The different roles of computers in a client-server and a peer-to-peer network
 	
☐ The hardware needed to connect stand-alone computers into a Local Area Network:
   ○ Wireless access points
   ○ Routers
   ○ Switches
   ○ NIC (Network Interface Controller/Card)
   ○ Transmission media
 	
☐ The Internet as a worldwide collection of computer networks:
   ○ DNS (Domain Name Server)
   ○ Hosting
   ○ The Cloud
   ○ Web servers and clients
 	
☐ Star and Mesh network topologies
	Required
	✓ The characteristics of LANs and WANs including common examples of each
	✓ Understanding of different factors that can affect the performance of a network, e.g.:
	   ▪ Number of devices connected
	   ▪ Bandwidth
	✓ The tasks performed by each piece of hardware
	✓ The concept of the Internet as a network of computer networks
	✓ A DNS's role in the conversion of a URL to an IP address
	✓ Concept of servers providing services (e.g. Web server → Web pages, File server → file storage/retrieval)
	✓ Concept of clients requesting/using services from a server
	✓ The Cloud: remote service provision (e.g. storage, software, processing)
	✓ Advantages and disadvantages of the Cloud
	✓ Advantages and disadvantages of the Star and Mesh topologies
	✓ Apply understanding of networks to a given scenario

Network Hardware

Hardware	Function
Network Interface Controller (NIC)	A network interface controller (NIC) provides a method of connecting to a network.
Switch	Switches receive and transmits data between devices on a LAN using Mac addresses.
Transmission Media	Wired or wireless radio waves that carry data signals from one devices to another.
Wireless Access Point (WAP)	Allows devices to connect to a network wirelessly. Similar to a switch.
Router	Transmits data between networks by directing data as 'packets' to their destination.

1.3 – Computer networks, connections and protocols

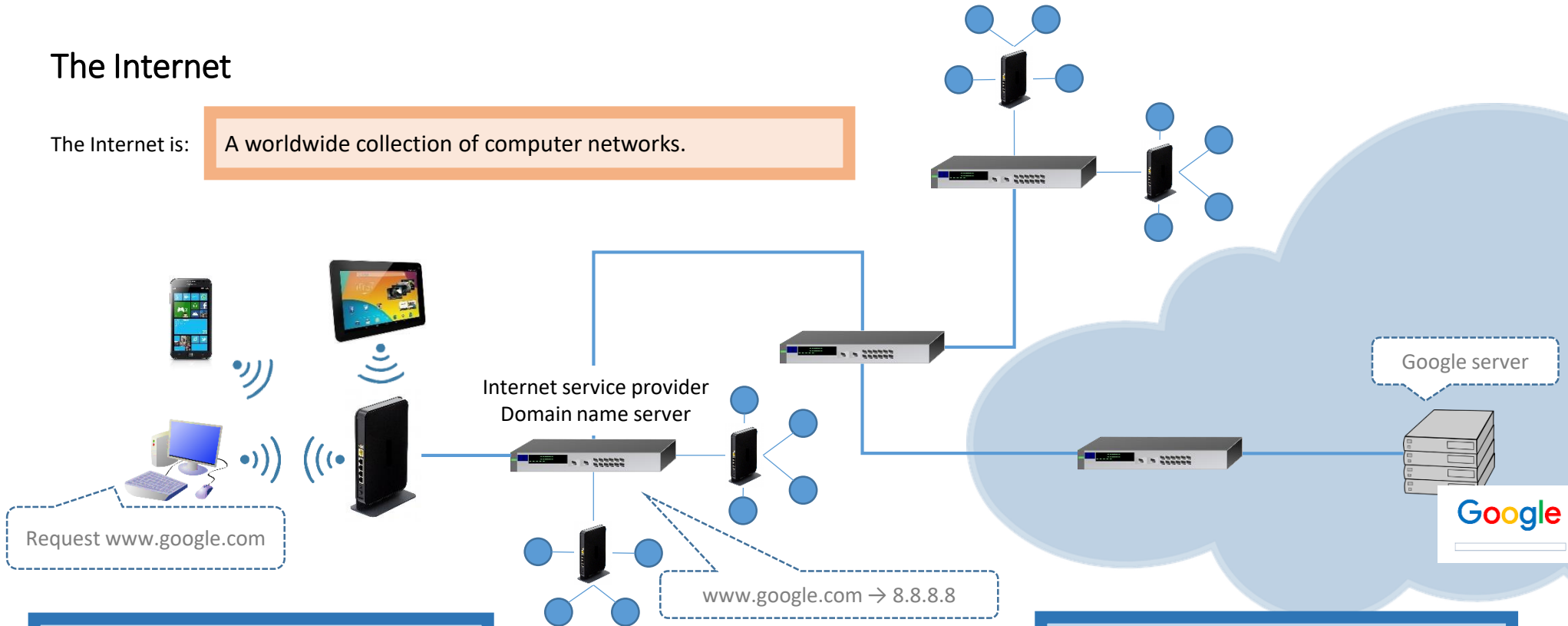| Sub topic	Guidance
1.3.1 Networks and topologies	

☐ Types of network:
   ○ LAN (Local Area Network)
   ○ WAN (Wide Area Network)
 	
☐ Factors that affect the performance of networks
☐ The different roles of computers in a client-server and a peer-to-peer network
☐ The hardware needed to connect stand-alone computers into a Local Area Network:
   ○ Wireless access points
   ○ Routers
   ○ Switches
   ○ NIC (Network Interface Controller/Card)
   ○ Transmission media
 	
☐ The Internet as a worldwide collection of computer networks:
   ○ DNS (Domain Name Server)
   ○ Hosting
   ○ The Cloud
   ○ Web servers and clients
 	
☐ Star and Mesh network topologies
	Required
	✓ The characteristics of LANs and WANs including common examples of each
	✓ Understanding of different factors that can affect the performance of a network, e.g.:
	   ▪ Number of devices connected
	   ▪ Bandwidth
	✓ The tasks performed by each piece of hardware
	✓ The concept of the Internet as a network of computer networks
	✓ A DNS's role in the conversion of a URL to an IP address
	✓ Concept of servers providing services (e.g. Web server → Web pages, File server → file storage/retrieval)
	✓ Concept of clients requesting/using services from a server
	✓ The Cloud: remote service provision (e.g. storage, software, processing)
	✓ Advantages and disadvantages of the Cloud
	✓ Advantages and disadvantages of the Star and Mesh topologies
	✓ Apply understanding of networks to a given scenario

J277 - 1.3 Computer networks, connections and protocols

The Internet

The Internet is: A worldwide collection of computer networks.

Internet service provider
Domain name server

Request www.google.com

www.google.com → 8.8.8.8

Google server

Google

Domain name server

A service made of many domain name servers that store domain names and matching IP addresses.
1. Browser sends URL to DNS.
2. DNS finds matching IP address and sends it back to the browser.
3. Browser requests web page from the web server at the IP address.
4. Web server processes the request and sends the web page back.

Hosting

- Web hosting services work by maintaining stable and secure storage spaces.
- While web hosts provide more than just simple data storage, it's a core part of their functionality.
- Hosts store data on hardware called web servers, which allows for easy maintenance and access by online users.

The cloud

Servers accessed over the Internet that offer a range of services including:
1. Storing and accessing data and files – Uses need less storage on their computers.
2. Running cloud applications – Users can access software without needing it on their own computer.
3. Providing increased processing power – Users don't need to have expensive hardware in their computer.

Web servers, clients and the cloud

The relationship between servers and clients on the Internet:

Files, software, user profiles and passwords are all stored centrally on the server.

Client sends a request to the server.

Server processes the request and responds.

Web server

In this example the mobile phone is the client. The user of the phone could be requesting a webpage via a browser, this request reaches the web server which returns the page for rendering on the mobile phone (client).

Client

File server

In this example a desktop computer is the client. The user of the computer could be requesting a file being held on a file server in a cloud storage data centre. The file server returns the file to the requesting computing (client).

The cloud

Pros:

Access files on any device.

No need for expensive hardware & staff as everything is hosted in the cloud.

Excellent backup, security and recovery options.

Easy to scale up and expand.

Cons:

Relies on host for backups and security.

Bandwidth issues can depend on speed of connection.

Ongoing subscription fees for hosting data and information.

Relies completely on a stable internet connection.

1.3 – Computer networks, connections and protocols

| Sub topic	Guidance
1.3.1 Networks and topologies	

☐ Types of network:
    ○ LAN (Local Area Network)
    ○ WAN (Wide Area Network)
 	
 ☐ Factors that affect the performance of networks
 ☐ The different roles of computers in a client-server and a peer-to-peer network
 ☐ The hardware needed to connect stand-alone computers into a Local Area Network:
    ○ Wireless access points
    ○ Routers
    ○ Switches
    ○ NIC (Network Interface Controller/Card)
    ○ Transmission media
 	
 ☐ The Internet as a worldwide collection of computer networks:
    ○ DNS (Domain Name Server)
    ○ Hosting
    ○ The Cloud
    ○ Web servers and clients
 	
 ☐ Star and Mesh network topologies
	Required
	 ✓ The characteristics of LANs and WANs including common examples of each
	 ✓ Understanding of different factors that can affect the performance of a network, e.g.:
	    ▪ Number of devices connected
	    ▪ Bandwidth
	 ✓ The tasks performed by each piece of hardware
	 ✓ The concept of the Internet as a network of computer networks
	 ✓ A DNS's role in the conversion of a URL to an IP address
	 ✓ Concept of servers providing services (e.g. Web server → Web pages, File server → file storage/retrieval)
	 ✓ Concept of clients requesting/using services from a server
	 ✓ The Cloud: remote service provision (e.g. storage, software, processing)
	 ✓ Advantages and disadvantages of the Cloud
	 ✓ Advantages and disadvantages of the Star and Mesh topologies
	 ✓ Apply understanding of networks to a given scenario

Star and Mesh Topologies

Star Topology

In a star topology, all of the devices connect to a central device – usually a router or switch.
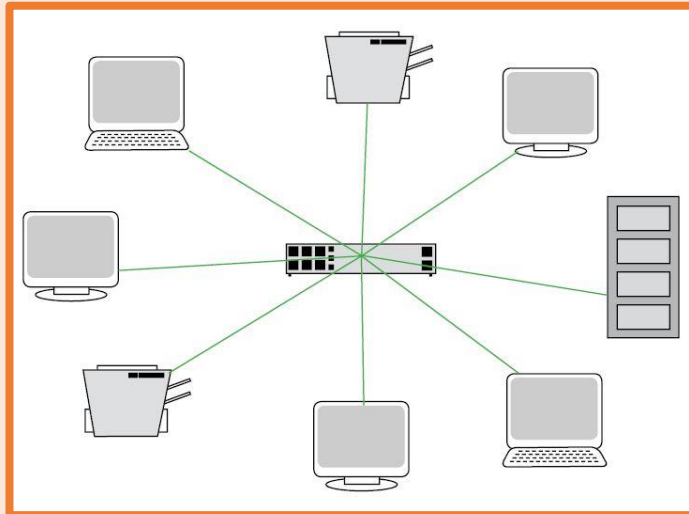
- A **star network**:
  - needs fewer cables
  - is easier to add or remove devices
  - is simple to understand and troubleshoot.
- But:
  - if the central switch fails, the whole network fails
  - causes a bottleneck in a busy network.

Mesh Topology

In a mesh topology, devices are connected to lots of other devices, with no central switch.
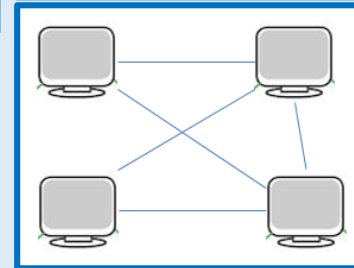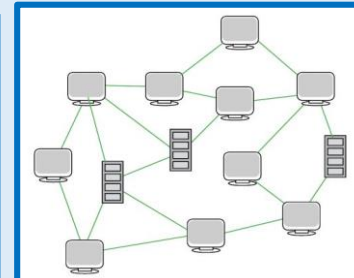
In a partial mesh, most devices are connected to several other devices.
In a full mesh, **every** device is connected to **all** other devices.

- A **mesh network**:
  - allows packets to be routed around bottlenecks
  - as more reliable as a single failure won't stop the rest of the network.
- But:
  - needs more cabling
  - is more complicated to add/remove devices
  - is more complicated to understand and troubleshoot.

1.3.2 Wired and wireless networks, protocols and layers

☐ Modes of connection:
  ○ Wired
    • Ethernet
  ○ Wireless
    • Wi-Fi
    • Bluetooth

☐ Encryption
☐ IP addressing and MAC addressing
☐ Standards
☐ Common protocols including:
  ○ TCP/IP (Transmission Control Protocol/Internet Protocol)
  ○ HTTP (Hyper Text Transfer Protocol)
  ○ HTTPS (Hyper Text Transfer Protocol Secure)
  ○ FTP (File Transfer Protocol)
  ○ POP (Post Office Protocol)
  ○ IMAP (Internet Message Access Protocol)
  ○ SMTP (Simple Mail Transfer Protocol)

☐ The concept of layers

Required
✓ Compare benefits and drawbacks of wired versus wireless connection
✓ Recommend one or more connections for a given scenario
✓ The principle of encryption to secure data across network connections
✓ IP addressing and the format of an IP address (IPv4 and IPv6)
✓ A MAC address is assigned to devices; its use within a network
✓ The principle of a standard to provide rules for areas of computing
✓ Standards allows hardware/software to interact across different manufacturers/producers
✓ The principle of a (communication) protocol as a set of rules for transferring data
✓ That different types of protocols are used for different purposes
✓ The basic principles of each protocol i.e. its purpose and key features
✓ How layers are used in protocols, and the benefits of using layers; for a teaching example, please refer to the 4-layer TCP/IP model

Not required
✘ Understand how Ethernet, Wi-Fi and Bluetooth protocols work
✘ Understand differences between static and dynamic, or public and private IP addresses
✘ Knowledge of individual standards
✘ Knowledge of the names and function of each TCP/IP layer

Modes of connection: <u>Wired - Ethernet</u>

Computers can be connected to networks using many different types of wires to transmit data.

The most common type of cable in a LAN is Ethernet. This uses wires to carry electrical signals between devices and is common in most offices and classrooms.

Fibre optic cables use beams of light instead of electrical signals and are used for high speed connections between switches and in many WANs.

+ Ethernet networks are more secure, as you need physical access to the cables to get into the network.

+ The connections are also more stable, faster and are less susceptible to interference.

- Ethernet networks require physical cables to be connected – this makes it much harder to change or move around.

- Cables can also be trip hazards, so should always be routed along walls, under floors or through the ceiling where possible.

Modes of connection: Wireless – Wi Fi and Bluetooth
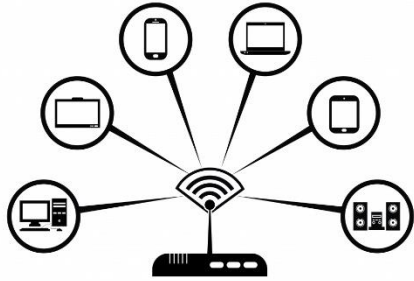
- Wireless connections use radio waves to transmit data through the air.

- The most common type of wireless used in LANs is Wi-Fi. Devices communicate with a wireless access point (WAP) – which can be a standalone device or built into a router or switch.

- Many people have one of these as the centre of their home network and many schools and offices have Wi-Fi access as well as wired Ethernet.

Max range: 40-100 metres.

Max range: 10 metres.

- Direct connection between two devices on wireless networks.

- Bluetooth is also a popular wireless connection method, though this has a much shorter range than Wi-Fi and is more typically used for a direct connection between two devices.

- Bluetooth headphones, mice and keyboards are very common.

- Wi-Fi networks are vulnerable to hacking as the radio waves can be intercepted by anyone within range, even if they are outside the building.
- Walls or obstructions will reduce the signal strength, and many electrical objects such as fridges and microwaves will cause interference.
- Transfer speeds over Wi-Fi are typically slower than Ethernet.

+ The main advantage of Wi-Fi is ease of movement.
+ You also don't need to purchase extra cables for each device and most devices come with a Wi-Fi adapter built in.

- Bluetooth signals can also be intercepted by anyone in range.
- Bluetooth only works over a very short range and transfer speeds are very slow.

+ Bluetooth is ideal for personal devices such as headphones, keyboards and mice as the small range makes it harder to intercept the data.
+ Bluetooth uses less power to send the data than Wi-Fi and is designed to quickly make ad-hoc connections.

Practice Questions

Dave has set up a new travel agency and needs you to set up a network for the shop. There will be four workstations for staff to book new holidays and take payments from clients, and each member of staff will also be issued with a tablet so they can show customers different destinations and hotels. Staff will use their PCs to phone customers and suppliers using headsets.

Describe how different types of network connection could be set up to support then new business

- The workstations should be connected using Ethernet because they won't need to be moved, they will allow for fast transfer speeds and it is more secure than Wi-Fi for sending customer data.

- The tablets should be connected using Wi-Fi so they can be moved around without cables and the signals won't have to go through walls.

- The headsets should be connected through Bluetooth so that staff don't get tangled in wires and they can connect just to their own workstation rather than needing full access to the network.

A brand new state of the art building is being designed for a large scale corporate business. It is essential that the business has a very reliable, fast and secure data transfer on its network. State whether you would recommend a wired, wireless or hybrid solution and provide reasons to back this up.

- A state of the art building will be build with modern technology as a consideration.

- As such there will be plenty of ceiling and floor crawl spaces to hide cabling required for a wired network.

- It is also stated that a very fast and secure network is required, this is another plus for a wired solution.

- That said, it is highly likely and workers / visiting clients with expect a wireless connection in a modern office…

- …so the network could be supplemented with wireless access points (WAP) in key locations such as conference rooms, assuming the appropriate steps have been taken to secure the network.

1.3.2 Wired and wireless networks, protocols and layers

☐ Modes of connection:
- ○ Wired
  - • Ethernet
- ○ Wireless
  - • Wi-Fi
  - • Bluetooth

☐ Encryption
☐ IP addressing and MAC addressing
☐ Standards
☐ Common protocols including:
- ○ TCP/IP (Transmission Control Protocol/Internet Protocol)
- ○ HTTP (Hyper Text Transfer Protocol)
- ○ HTTPS (Hyper Text Transfer Protocol Secure)
- ○ FTP (File Transfer Protocol)
- ○ POP (Post Office Protocol)
- ○ IMAP (Internet Message Access Protocol)
- ○ SMTP (Simple Mail Transfer Protocol)

☐ The concept of layers

Required
- ✓ Compare benefits and drawbacks of wired versus wireless connection
- ✓ Recommend one or more connections for a given scenario
- ✓ The principle of encryption to secure data across network connections
- ✓ IP addressing and the format of an IP address (IPv4 and IPv6)
- ✓ A MAC address is assigned to devices; its use within a network
- ✓ The principle of a standard to provide rules for areas of computing
- ✓ Standards allows hardware/software to interact across different manufacturers/producers
- ✓ The principle of a (communication) protocol as a set of rules for transferring data
- ✓ That different types of protocols are used for different purposes
- ✓ The basic principles of each protocol i.e. its purpose and key features
- ✓ How layers are used in protocols, and the benefits of using layers; for a teaching example, please refer to the 4-layer TCP/IP model
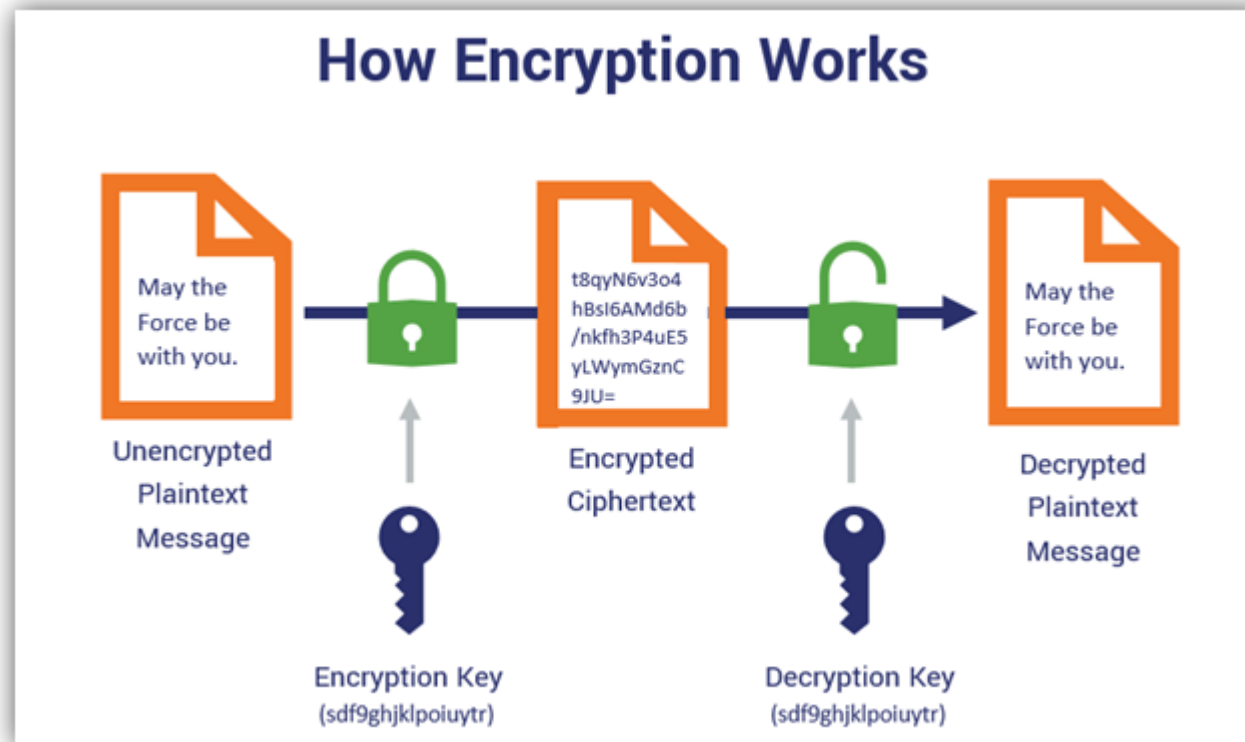
Not required
- ✘ Understand how Ethernet, Wi-Fi and Bluetooth protocols work
- ✘ Understand differences between static and dynamic, or public and private IP addresses
- ✘ Knowledge of individual standards
- ✘ Knowledge of the names and function of each TCP/IP layer

Wi-Fi encryption

- Encryption is a method of scrambling data with a key code such that it makes no sense.
- On an open or public Wi-Fi network anyone can join and sniff out packets of data from other users.
- Therefore encryption is used. If intercepted the data will have no meaning.
- In order to read the data the user is required to decrypt the data using the key.

How Encryption Works

May the
Force be
with you.

Unencrypted
Plaintext
Message

t8qyN6v3o4
hBsI6AMd6b
/nkfh3P4uE5
yLWymGznC
9JU=

Encrypted
Ciphertext

May the
Force be
with you.

Decrypted
Plaintext
Message

Encryption Key
(sdf9ghjklpoiuytr)

Decryption Key
(sdf9ghjklpoiuytr)

The uses of IP addressing (IPv4 & IPv6) and MAC addressing

There are two types of addressing used for local and wide area networks:

MAC address	Media Access Control address	Found on network interface cards. Routes frames on a local area network between network interface cards. Every address is completely unique.

Wi-Fi Properties

Networking | Sharing

Connect using:

Qualcomm Atheros AR9485WB-EG Wireless Network Ada

MAC Address: 18-67-B0-5D-3F-4A

This connection uses the following items:

IP address	Internet Protocol address	Routes packets on a wide area network between routers.

The reason we have IPv6 is:

- Due to the shortage of IPv4 addresses, IPv6 is now used as well, though some older devices don't support the new format.

- To solve this problem, new devices have both an IPv4 AND an IPv6 address so that they can work on any network.

IPv6 addresses are represented using 8 blocks of 4 hexadecimal digits, separated by colons
E.g. 6164:6120:6C6F:7665:6C61:6365:2043:4B4B

When displayed, an IPv6 address will often miss leading zeroes, so *... :6365:0001:2043: …* might appear as *… :6365:1:2043: …*

1.3.2 Wired and wireless networks, protocols and layers

☐ Modes of connection:
- ○ Wired
  - • Ethernet
- ○ Wireless
  - • Wi-Fi
  - • Bluetooth

☐ Encryption
☐ IP addressing and MAC addressing
☐ Standards
☐ Common protocols including:
- ○ TCP/IP (Transmission Control Protocol/Internet Protocol)
- ○ HTTP (Hyper Text Transfer Protocol)
- ○ HTTPS (Hyper Text Transfer Protocol Secure)
- ○ FTP (File Transfer Protocol)
- ○ POP (Post Office Protocol)
- ○ IMAP (Internet Message Access Protocol)
- ○ SMTP (Simple Mail Transfer Protocol)

☐ The concept of layers

Required
✓ Compare benefits and drawbacks of wired versus wireless connection
✓ Recommend one or more connections for a given scenario
✓ The principle of encryption to secure data across network connections
✓ IP addressing and the format of an IP address (IPv4 and IPv6)
✓ A MAC address is assigned to devices; its use within a network
✓ The principle of a standard to provide rules for areas of computing
✓ Standards allows hardware/software to interact across different manufacturers/producers
✓ The principle of a (communication) protocol as a set of rules for transferring data
✓ That different types of protocols are used for different purposes
✓ The basic principles of each protocol i.e. its purpose and key features
✓ How layers are used in protocols, and the benefits of using layers; for a teaching example, please refer to the 4-layer TCP/IP model

Not required
✘ Understand how Ethernet, Wi-Fi and Bluetooth protocols work
✘ Understand differences between static and dynamic, or public and private IP addresses
✘ Knowledge of individual standards
✘ Knowledge of the names and function of each TCP/IP layer

Standards and protocols

What are standards?

An agreed set of requirements for hardware and software that allows different manufacturers to make compatible products.

What are protocols?

Rules for how devices communicate, and how data is organised and transmitted across a network.

TCP/IP	**Transmission Control Protocol / Internet Protocol**	Provides an error free transmission between two routers (TCP) and routing of packets on a wide area network (IP).
HTTP	**Hypertext Transfer Protocol**	A client-server method of requesting and delivering HTML files.
HTTPS	**Hypertext Transfer Protocol Secure**	Encryption and authentication for client-server data.
FTP	**File Transfer Protocol**	Sending files between computers. Used for uploading web pages and associated files to a web server for hosting.
POP	**Post Office Protocol**	Used by email clients to retrieve email from a mail server.
IMAP	**Internet Message Access Protocol**	Used by email clients to retrieve email from a mail server, and to manage remote mail boxes. Better than POP.
SMTP	**Simple Mail Transfer Protocol**	Sends mail to a mail server.

1.3.2 Wired and wireless networks, protocols and layers

☐ Modes of connection:
- ○ Wired
  - • Ethernet
- ○ Wireless
  - • Wi-Fi
  - • Bluetooth

☐ Encryption
☐ IP addressing and MAC addressing
☐ Standards
☐ Common protocols including:
- ○ TCP/IP (Transmission Control Protocol/Internet Protocol)
- ○ HTTP (Hyper Text Transfer Protocol)
- ○ HTTPS (Hyper Text Transfer Protocol Secure)
- ○ FTP (File Transfer Protocol)
- ○ POP (Post Office Protocol)
- ○ IMAP (Internet Message Access Protocol)
- ○ SMTP (Simple Mail Transfer Protocol)

☐ The concept of layers

Required
- ✓ Compare benefits and drawbacks of wired versus wireless connection
- ✓ Recommend one or more connections for a given scenario
- ✓ The principle of encryption to secure data across network connections
- ✓ IP addressing and the format of an IP address (IPv4 and IPv6)
- ✓ A MAC address is assigned to devices; its use within a network
- ✓ The principle of a standard to provide rules for areas of computing
- ✓ Standards allows hardware/software to interact across different manufacturers/producers
- ✓ The principle of a (communication) protocol as a set of rules for transferring data
- ✓ That different types of protocols are used for different purposes
- ✓ The basic principles of each protocol i.e. its purpose and key features
- ✓ How layers are used in protocols, and the benefits of using layers; for a teaching example, please refer to the 4-layer TCP/IP model

Not required
- ✖ Understand how Ethernet, Wi-Fi and Bluetooth protocols work
- ✖ Understand differences between static and dynamic, or public and private IP addresses
- ✖ Knowledge of individual standards
- ✖ Knowledge of the names and function of each TCP/IP layer

The concept of layers

In networking, layering means to break up the sending of messages into separate components and activities.

Each component handles a different part of the communication.

This can be referred to as the Transmission Control Protocol/Internet Protocol (TCP/IP) model.

+ Reducing the complexity of the problem.

+ Devices can be manufactured to operate at a particular layer.

+ Products from different vendors will work together.

There are four layers to be considered:

• **Application layer** - encodes/decodes the message in a form that is understood by the sender and the recipient.

• **Transport layer** - breaks down the message into small chunks (packets). Each packet is given a packet number and the total number of packets. The recipient uses this information to assemble the packets together in the correct order. It also allows the recipient to see if there are any missing packets.

• **Network layer** - adds the sender's IP address and that of the recipient. The network then knows where to send the message, and where it came from.

• **Link layer** - enables the transfer of packets between nodes on a network, and between one network and another.