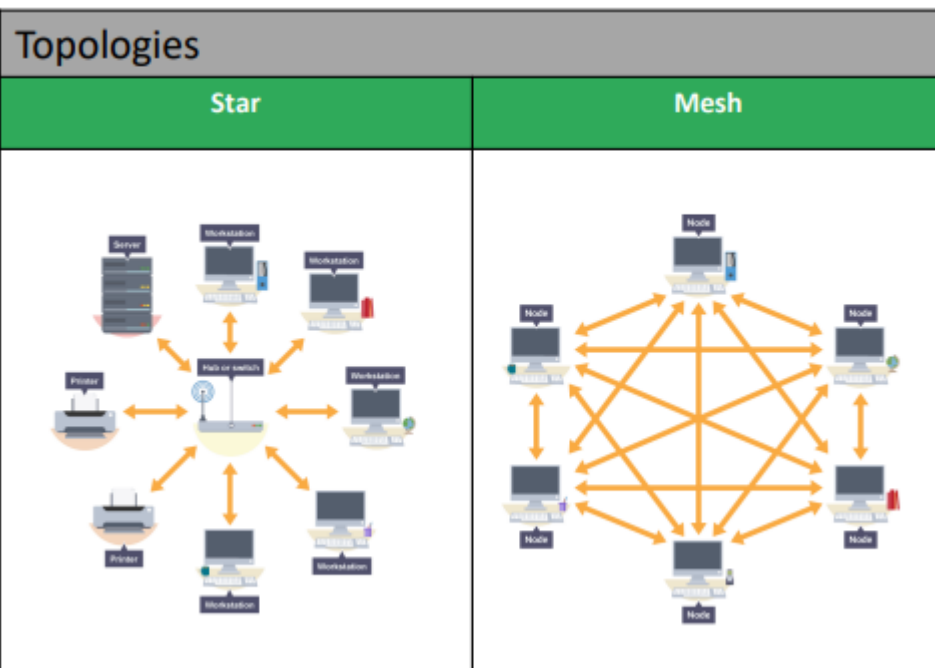
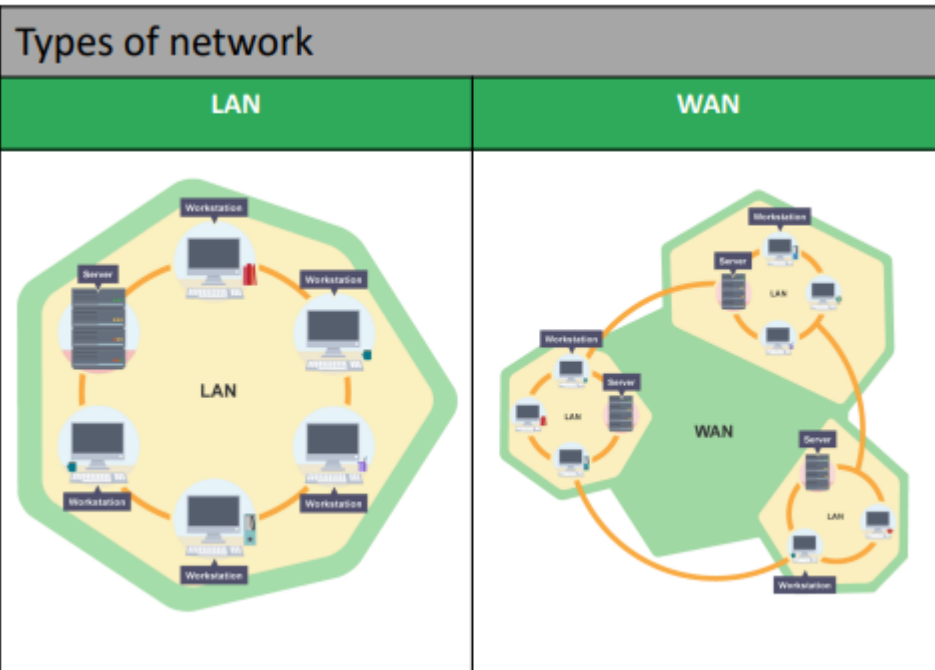




Key vocabulary	
Network	A group of interconnected computers/devices.
LAN	Local area network. A network of computers that covers a small area, eg a school or college.
WAN	Wide area network. A network that spans across a building, buildings or even countries, eg the internet.
Client-server	A relationship in which data or web application is hosted on a server and accessed by client computers.
Peer to peer	A relationship where all computers on the network share responsibility and there is no one central server.
WAP	A device that connects computers to a network using Wi-Fi.
Switch	A device for connecting computers and other network capable devices together to form a network.
NIC	Network Interface Controller -A circuit board that is installed in a computer so it can be connected to a network.
Transmission media	How data is carried from point A to point B physically, either by cable or wirelessly.
Ethernet	A set of protocols used in a wired local area network that describes how data is transmitted within it.
Wi-Fi	A method of connecting to the internet wirelessly using radio waves.
Bluetooth	Wireless technology used for transmitting data over short distances.
DNS	Domain name server - an internet service that translates IP addresses into website domain names. All websites have equivalent IP addresses.
Host	A server that stores files for other computers to access.
Cloud	A term often used to describe a location on the internet from which software applications are run and where data is stored.

Key vocabulary	
Encryption	Files that are encrypted have been altered using a secret code and are unreadable to unauthorised parties.
IP address	A unique address for each computer device on a network.
MAC address	Media access control - each unique piece of hardware on a network has a MAC address.
Standard	An agreed way of doing things.
Protocol	A set of rules for how messages are turned into data packets and sent across networks.

Layers
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. Layering allows standards to be developed, but also to be adapted to new hardware and software over time. For example, different software packages (applications) may use the same transport, network and link layers but have their own application layer. The way the program encodes the message changes - the rest of communication method remains the same.

Common protocols	
TCP/IP	Transmission Control Protocol/Internet Protocol - enables communication over the internet.
HTTP	Hypertext Transfer Protocol - governs communication between a webserver and a client.
HTTPS	HTTPS (secure) includes secure encryption to allow transactions to be made over the internet.
FTP	File Transfer Protocol - governs the transmission of files across a network and the internet.
POP	Post Office Protocol – governs the transmission of emails to devices. Once downloaded to the device is deleted from the server.
IMAP	Internet Message Access Protocol – governs the transmission of emails. Stored on server and accessed by devices.
SMTP	Simple Mail Transfer Protocol - governs the sending of email over a network to a mail server.
Layering	In networking, the concept of breaking up communication into separate components or activities.

Encryption																																																							
A simple method of encryption requires the use of a technique known as the Caesar cipher. The cipher works by giving a number value to a key. Each plaintext letter is replaced by a new letter, the one found at the original letter's position in the alphabet plus the value of the key. The example uses a key value of 3.	<table><tr><td>Plaintext</td><td>a</td><td>b</td><td>c</td><td>d</td><td>e</td><td>f</td><td>g</td><td>h</td><td>i</td><td>j</td><td>k</td><td>l</td><td>m</td><td>n</td><td>o</td><td>p</td><td>q</td><td>r</td><td>s</td><td>t</td><td>u</td><td>v</td><td>w</td><td>x</td><td>y</td><td>z</td></tr><tr><td>Ciphertext</td><td>d</td><td>e</td><td>f</td><td>g</td><td>h</td><td>i</td><td>j</td><td>k</td><td>l</td><td>m</td><td>n</td><td>o</td><td>p</td><td>q</td><td>r</td><td>s</td><td>t</td><td>u</td><td>v</td><td>w</td><td>x</td><td>y</td><td>z</td><td>a</td><td>b</td><td>c</td></tr></table>	Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	Ciphertext	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z																													
Ciphertext	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c																													

Protecting networks	
Form of attack	Prevention
Malware	Anti-Malware software.
Phishing	Training of user to detect scams as well as the filtering of emails.
Brute-force attacks	Use of different strong passwords. A limit on the number of incorrect attempts.
Denial of service attacks	Block IP addresses which send too many requests. Increase capacity.
Data interception and theft	Encryption of data.
SQL injection	Ensuring that all data input is sanitized. (Forcing data to be in the format you want it such as a date, text or integer.)

Key vocabulary	
Malware	Software that is designed to cause harm or damage to a computer. This includes viruses that might damage files, adware that causes pop-ups, and spyware that collects and shares login details.
Social Engineering	Tricking people into giving sensitive data such as PINs or passwords.
Phishing	An attempt to gain personal information about someone by way of deception, eg sending an email pretending to be from their bank asking them for their bank details.
Brute-force attack	Attempting every combination of a password or encryption key until it is correct.
Denial of service attack	An attack designed to render online services inaccessible. One type of this attack involves many computers simultaneously flooding a target with network traffic.
Data interception	Where data is intercepted during transmission. This is done using software called a packet sniffer, which examines data packets as they are sent around a network.
SQL Injection	Where SQL code is entered as a data input. Many databases use SQL code to interrogate the data and maintain the structure. SQL code can be inputted as data, which can cause errors or unintended operations.
Penetration testing	Systems are tested for vulnerabilities to reveal any weaknesses in the system which can be fixed.
Anti-malware	A type of computer program which detects, prevents and removes malware on a system.
Firewall	An application that prevents unauthorised connections to and from the Internet.
User-access level	These are the permissions given to a user to access facilities on a computer.
Encryption	Files that are encrypted have been altered using a secret code and are unreadable to unauthorised parties.