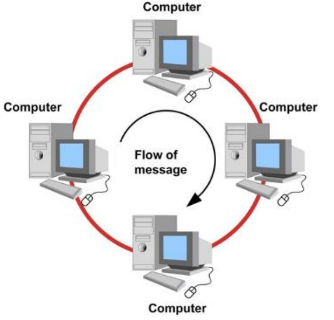
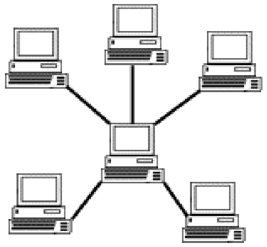
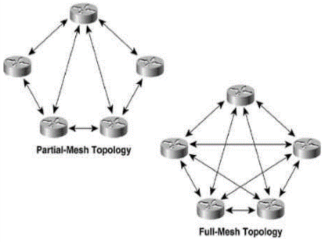
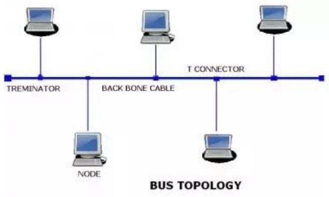
Computing GCSE – 1.5a

J276/01 – Network Topology

Topology means "how a network is laid out and the connections between computers"

NAME	DIAGRAM	DESCRIPTION	ADVANTAGES	DISADVANTAGES
Ring	 Computer Computer Computer Flow of message Computer	Each node is connected to 2 others, and packets tend to travel in 1 direction.	All data flow in 1 direction – greatly reduced chance of collisions. No need for network server High speed Additional nodes can be added without affecting performance	All data passes through every workstation on route If 1 node shuts down, then network collapses Hardware is more expensive than switches / NICs
Star		Each node connects to a hub or switch. A central machine acts as **server** whilst the outer nodes are **clients.**	Centralised management through the server Easy to add more machines to the network If 1 machine fails, the others are unaffected	Potentially higher set up costs, especially in server and switch set ups. Central server determines the speed of the network and the number of possible nodes If the server fails then the network fails
Mesh		Every nodes is interconnected with every other, allowing for distributed transmission. Mesh topology can be **FULL MESH** (where every possible connection is made) or **PARTIAL MESH** (at least 2 computers are connected with multiple links)	Multiple devices can transmit data at once, therefore can handle large amounts of data A failure of 1 device does not affect the rest of the network Adding devices does not impact on data transmission between existing devices	Cost is higher due to increased hardware requirements Building and maintaining a mesh network is costly and time consuming The chance of redundant connections is very high, which increases the cost, and makes the network cost inefficient
Bus	 T CONNECTOR TREMINATOR BACK BONE CABLE NODE BUS TOPOLOGY	Bus or Line topology is a network where all nodes are connected to a single cable (backbone).	Works well with small networks Easiest option for connecting nodes with shared peripherals Least costly in terms of hardware and cabling	Difficult to fault test because who network crashes when there are errors Additional devices slow down the network

Computing GCSE – 1.5b

J276/01 – Network Protocols

KEY VOCABULARY		
Protocol	The rules and standards that are agreed in order to make it possible for different devices to talk to one another	
IP Address	Each node on a network is given a unique 32 bit address (4x8bits) for example 192.168.0.1 There are 4 billion possible combinations.	
DHCP	Dynamic Host Configuration Protocol – this protocol allows the network server to control the allocation of IP addresses	
MAC Address	Media Access Control Unique addresses hard-coded into the network interface controller. Gives the manufacturer, NIC type and unique identifying number. 48 bits displayed as Hex (eg 01-23-45-67-89-ab-cd-ef)	
TCP/IP	Transmission Control Protocol / Internet Protocol	A set of protocols that governs the transfer of data over a network
HTTP	Hyper Text Transfer Protocol	Standards for writing webpages to display content for display
HTTPS	*Hyper Text Transfer Protocol Secure*	*Client-server protocol for requesting (client) and delivering (server) resources, such as HTML, securely*
FTP	*File Transfer Protocol*	*Used to directly send files from one node to another over the internet. Commonly used for uploading files to webservers*
POP	Post Office Protocol	Used by email clients to download email from the remote email server and save it onto the users computer. More or less redundant now, and has been replaced by IMAP
IMAP	Internet Message Access Protocol	An alternative to POP, allowing more control such as the complete control of remote mailboxes
SMTP	Simple Mail Transfer Protocol	An old standard for transmission of email. SMTP can only be used to *push* mail to client machines, whilst both POP and IMAP ae used by clients to *retrieve* mail.

ENCRYPTION

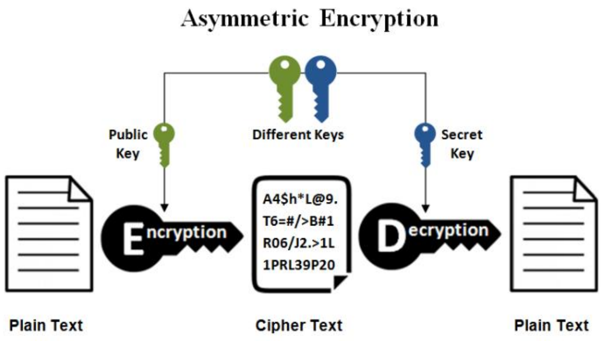
Encryption is taking a message and changing the letters in such a way that it is not readable. The correct recipient knows how to unscramble the message and can read the text.

Modern encryption is 128bit and secure against brute force attacks

PUBLIC KEY ENCRYPTION

Public Key Encryption is a method of securely sending data over the internet. The recipient's computer uses an algorithm to produce 2 linked keys: a public key and a private key.

1. Alice (the sender) requests Bob's (the recipient) public key. This is shared.
2. Alice uses Bob's public key to *encrypt* the message she wishes to send
3. The encrypted document is sent over the internet – it is secure.
4. When Bob receives the encrypted document he combines his public key with the secret private key. This allows the message to be decrypted and turned back into plain text



Computing GCSE – 1.5c

J276/01 – Network Layering

KEY VOCABULARY	
Protocol	The rules and standards that are agreed in order to make it possible for different devices to talk to one another
Layering	Rules organised into a distinct order in which they need to be applied
Interoperability	The ability for different systems and software to communicate, exchange data and use the information exchanged
Encapsulation	Enclosing data inside another data structure to form a single component
De-encapsulation	Removing data from inside and encapsulated item.

WHY LAYER?

Layering allows problems to be broken down into small chunks, and then smaller solutions created to specific parts of the problem. These small parts interact in an agreed manner, allowing the solution to be built by different teams or companies.

Layering is not unique to computing. In the car industry, a Ford engine might be used with a Jaguar gearbox in a Mazda car. By separating these 'layers', but agreeing on the interface between the layers, each company is free to develop their layer as they see fit, without affecting the other layers. It is also possible to swap one layer out, and replace it with another one – such as swapping an engine for a more powerful one.

This *interoperability* is important as it allows data (in computing) to be passed from one layer to the next.

TCP/IP Protocol Layers

LAYER 1: Application

This layer ensures data is produced in a form that is acceptable to the application that will use it, such as web-browsers or email clients. This is where IMAP or HTML protocols would be used.

LAYER 2: Transport

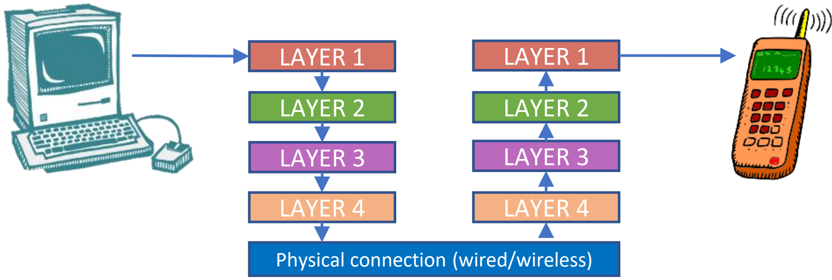
This layer establishes the connection across the network. The transmitting device agrees with the receiving device the speed or data transfer, the size and number of packets and any error checking to be used. This layer uses TCP protocols

LAYER 3: Internet

This layer is concerned with transmitting the data across different networks. It identifies the destination and establishes the path the data will take between nodes. It uses IP protocols

LAYER 4: Network

This layer deals with the physical transmitting of the data. It converts the data into binary electronic signal that can be understood by the network hardware. It uses protocols such as Ethernet or 802.11 (wireless) so the signal is hardware independent and can use any available compliant physical medium, such as UTP or fibre optic wire.



Data transfer occurs by breaking the file into small *packets*, adding each layer to the packet in order at the sending device, then decoding in reverse order at the receiving device before rebuilding the file.

Packet switching is the process that modern networks use to send large data between devices. The data is split into small ***packets*** and numbered. The packets can travel by any route to the destination where the receiving machine reassembles them into the correct order.