Paper 1 | GCSE Computer Science | **Networks**

Factors that affect the performance of networks

Bandwidth- amount of data that can be transferred in a give time. Measured in bits per second (bps). This indicates the number of bits of information that can travel down the line in 1 second. The greater the bandwidth the better the network.
Wired connections faster and more reliable than wireless.

Latency is a measure of delay. The time it takes for some data to get to its destination across the network. It is usually measured as a round trip delay - the time taken for information to get to its destination and back again. Latency is usually measured in milliseconds (ms).

Hardware

NICs-
- Allows device to connect to a network.
- Built into motherboard.

Routers
- Transmits data between networks- they're always connected to two networks- ADSL port connects to internet & Ethernet is connected to LAN.

Switches-
- Connect devices on a LAN.
- Receive data (in units called frames).
- Transmit the data on the network with the correct **MAC address.**

Wireless Access Point (WAP)
- This is a switch that allows devices to connect wirelessly.
- **A hotspot is a location **where** you can connect to a WAP**

Cables-
- Ethernet- connect devices in LAN e.g. CAT 5e and CAT 6. Made of twisted copper wires.
- Coaxial- single copper wire surrounded by plastic and metallic mesh to stop interference.
- Fibre optic- transmit data as light, no interference, transmits large distances.

Wi-Fi is the standard for Wireless Network
- 2.4 GHz- greater range and better at getting through walls.
- 5 GHz is faster over shorter distances.
- Bands are split into numbered channels that each cover a small frequency range.

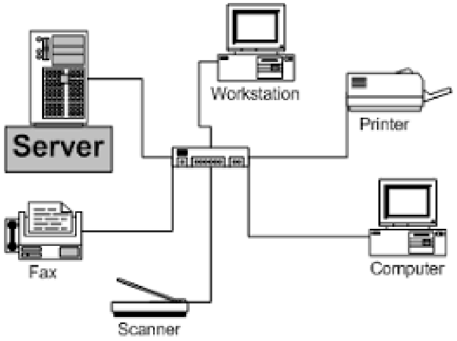
LAN
- Connects computers, peripherals, and other devices in a single building or other small geographic area.
- Typically owned by the company that uses them.
- **Advantages-** Can install and update software on all computers at once, rather than one by one. Can share files & work collaboratively. Can share hardware e.g. printers.

WAN
- Allows the transmission of data across greater geographic distance.
- Organisations hire infrastructure from telecommunications companies who own and manage the WAN.
- Connected using fibre or copper telephone lines, satellite links or radio links.

Client server-
- Managed by server.
- Devices called clients.
- Clients send requests to server. Server processes the request and responds.
- Server stores profiles, passwords and access information.

Pros-
- Central storage of files.
- Easy to back up.
- Easy to install software.
- Easy to manage security.
- Reliable

Cons-
- Expensive
- Needs specialists
- If server down, all clients lose access.

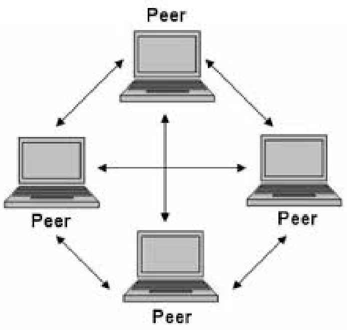


Peer to peer networks-
- NO server.
- All devices equal.
- Files stored on each device.

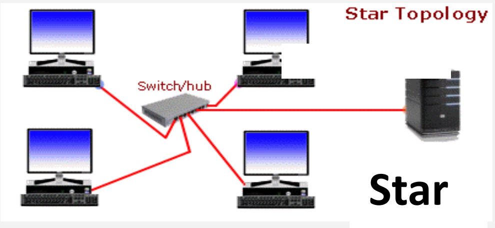
Pros-
- Easy to maintain.
- No dependence on server.

Cons-
- No centralised management so all updates done on each device.
- Copying files causes duplicate files.
- Less reliable.
- Machines prone to slowing down when other devices access them.

Skype is an example of a P2P



Network Topologies



Star

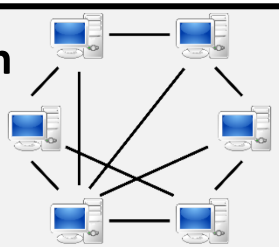
Pros of STAR topologies-

- If device fails the rest of the network is unaffected.
- Simple to add more devices.
- Better performance as data goes straight to device.

Cons-

- All devices needs a cable to connect to main switch or server.
- Can be expensive.
- If switch or server breaks whole network affected.

Mesh



- Decentralised- networking devices are either directly or indirectly connected to each other.
- No need for a switch or a server.
- **Works by sending the data along the fastest route possible.**

Pros of Mesh topologies-

- No single point where network can fail.
- If one device fails the data will be sent along another route.

Cons of Mesh topologies

- Used to be expensive with lots of cables. HOWEVER with the use of wireless technology this has become more practical.

The Internet

- Network of networks.
- It's a WAN connecting devices and networks over the world.
- Based around the protocol TCP/IP.

World Wide Web

- Collection of website hosted on web ser
- Accessed through the **<u>http</u>** protocol.

URLs

- Addresses used to access web servers and resources on them.

Domain Name Server (DNS)

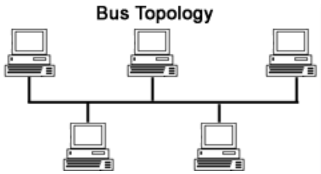
- Websites domain name into its IP address.

<u>Virtual networks</u>

- Network that is software based. Partitioning off some physical network bandwidth to form separate network.
- Several virtual networks can exist on the same physical network.
- Share the same hardware.
- Has their own security.

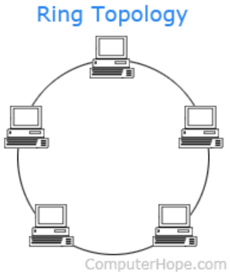
- **<u>A Virtual private network</u>** is a type of virtual network that can be used to send data securely over a large network, like a WAN or the internet. E.g. a VPN could be used to set up a school intranet that all the students access from home.

- **<u>Virtual LAN</u>** allows you to split a LAN into several separate networks using the same hardware.



Bus

- **Devices in a line.**
- **Connected with backbone cable.**
- **Data sent both ways which causes data collisions which slows the network.**



Ring

- **Data moves in one direction which prevents collisions.**
- **Only one device can send at a time.**
- **Data passes through many devices before destination.**

The cloud uses the internet to store files and applications.

- <u>Hosting-</u> a business users servers to store files for other organisations.

Pros of the cloud.

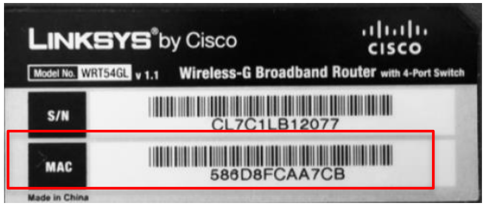
- Access from any device.
- No hardware or IT staff required.
- Can increase storage.
- Provides security.
- Updated automatically.

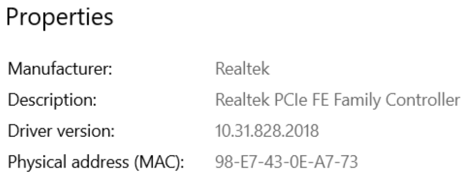
Cons of the cloud.

- Need to connect to the internet.
- Dependent on host for security.
- Data vulnerable to hackers.
- Unclear of ownership.
- Subscription costs.

Network protocols- *set of rules of how devices communicate & how data is transmitted across a network.*

MAC addresses-
- Unique identifiers.
- Assigned to all network enabled devices.
- 48 or 64 bit binary numbers **converted to HEX**.
- Used by Ethernet protocol on LANs. LAN switches read the MAC addresses and use them to direct data to the correct device.



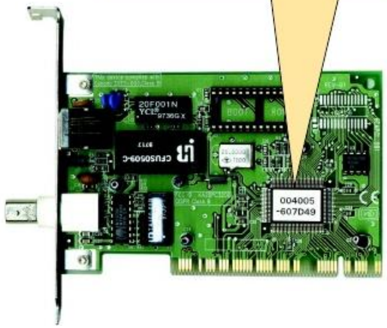


Properties

Manufacturer:	Realtek
Description:	Realtek PCIe FE Family Controller
Driver version:	10.31.828.2018
Physical address (MAC):	98-E7-43-0E-A7-73

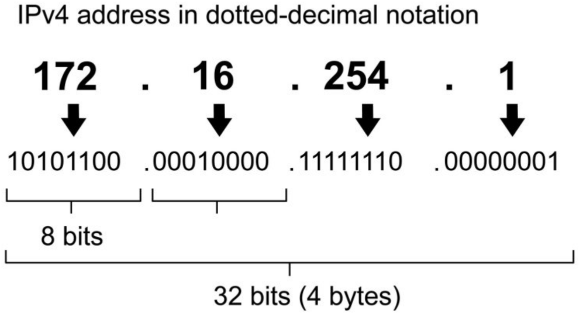
The NIC

- Each system must have a unique identifier
- Media Access Control (MAC) address
  - A unique address burned into a ROM chip on the network card
  - Each MAC address is 12 hex characters or 48 bits in length



MAC address printed on surface of chip – and burned inside the chip.

Communication between different networks uses IP Addresses
- Used when sending data between networks.
- IP addresses not linked to hardware.
- Assigned manually when before device can access the network.
- Static IP addresses are permanent and used to connect printers on a LAN & hosting websites on the internet.
- Dynamic IP addresses assigned to the device by a network server. Devices can have different IP addresses each time they log on.
- IP addresses can be 32-bit (converted to denary) or 128-bit (converted to HEX).



IPv4 address in dotted-decimal notation

172 . 16 . 254 . 1

10101100 .00010000 .11111110 .00000001

8 bits

32 bits (4 bytes)

File Transfer Protocol [FTP]
FTP is used to transfer large files. It is often used for organizing files on a web server for a website. You can have private access to an area on an FTP server where you can upload your files. You can then give another user access to download the documents that you have shared.

Hyper Text Transfer Protocol [HTTP]
HTTP transfers web pages from web servers to the client. All web page addresses start with http.

Hyper Text Transfer Protocol Secure [HTTPS]
An https address is a secure web address which has been encrypted. An https address is used for sites holding bank details and secure information.

Simple Mail Transfer Protocol [SMTP] and Post Office Protocol [POP]
Email uses these protocols to communicate with mail servers. SMTPis used to send the email; POP is used to receive email. Most email clients allow for transfers of up to 10 MB.

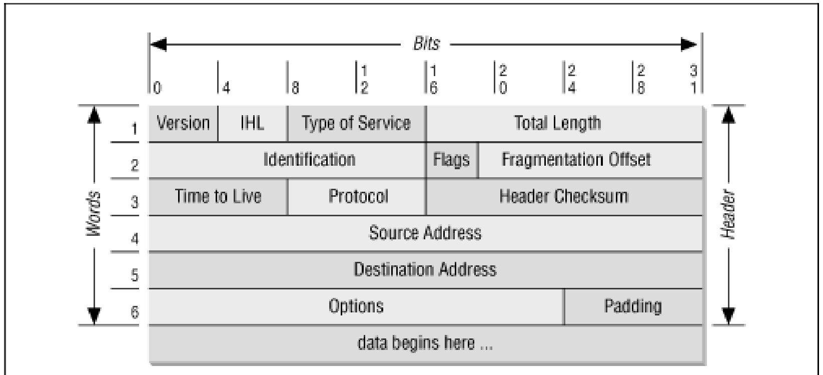
Voice Over Internet Protocol (VOIP)
VOIP is a set of protocols that enables people to have voice conversations over the internet. Used for Skype for example.

Internet Message Access Protocol (IMAP)
Used to retrieve emails from a server. Server holds the email until you actually delete it. You only download a copy.

Network protocols- Between networks (e.g. over the internet), data is sent in packets and directed by routers using TCP/ IP protocols.

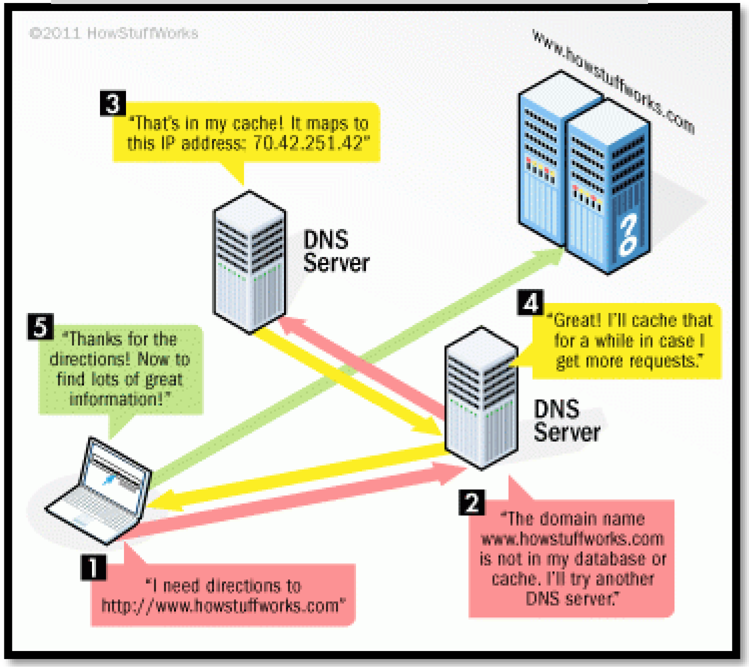
Packets

- Packet has <u>header </u>(control info) which includes the **<u>destination address, source address</u>** and <u>packet number.</u>
- **Payload-**the thing the person is to read e.g. the email or document or webpage.
- Packets include the **checksum number** which is a form of validation to check for corruption.
- Packet switching is used by routers to direct data packets on the internet & other IP networks.
- Sending device splits data into packets > Packet given packet number to show order of the data > router reads header and decides which way to send it next > packet can take different routes > packets can arrive in different orders but reassembled using the packet number > if packets are not received there is a timeout message > if all data is received & checksum matched a receipt confirmation is sent.

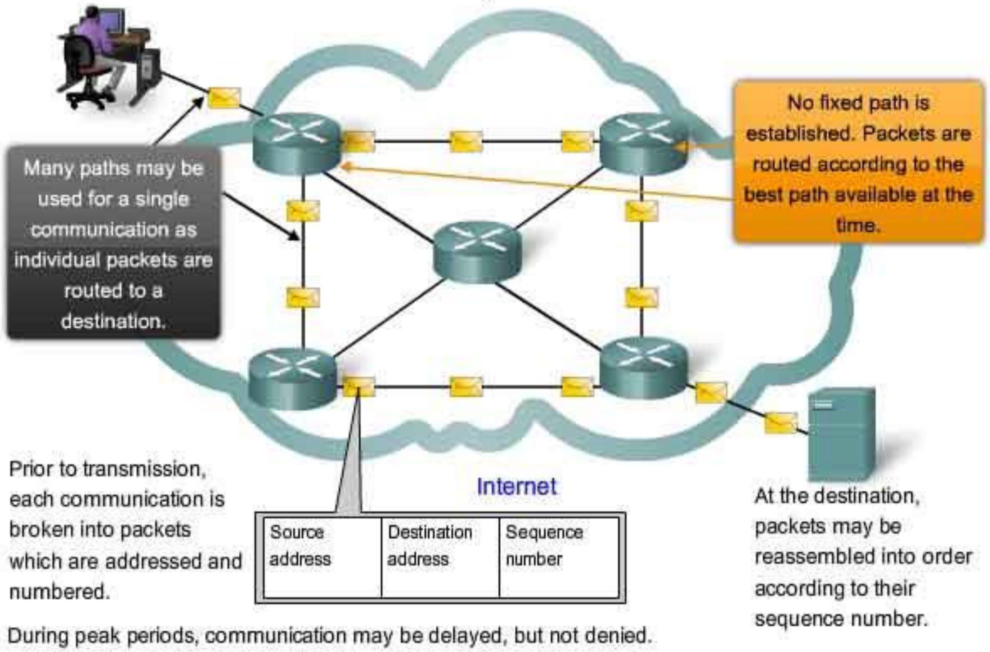


An example Packet

How do DNS servers work?


©2011 HowStuffWorks
www.howstuffworks.com
3 "That's in my cache! It maps to this IP address: 70.42.251.42"
DNS Server
4 "Great! I'll cache that for a while in case I get more requests."
DNS Server
5 "Thanks for the directions! Now to find lots of great information!"
2 "The domain name www.howstuffworks.com is not in my database or cache. I'll try another DNS server."
1 "I need directions to http://www.howstuffworks.com"

Packet Switching in a Data Network



Many paths may be used for a single communication as individual packets are routed to a destination.

No fixed path is established. Packets are routed according to the best path available at the time.

Prior to transmission, each communication is broken into packets which are addressed and numbered.

At the destination, packets may be reassembled into order according to their sequence number.

During peak periods, communication may be delayed, but not denied.

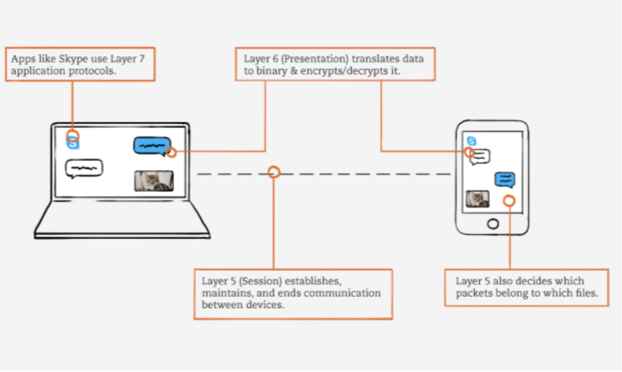
Network protocols & layers

Open Systems Interconnection (OSI)

Network protocols are divided into layers

- Layer- group of protocols with similar functions.
- Layers are self contained. They do their job and don’t worry about the other layers.
- Each layer serves the layer above.

Layer 7	Application Layer	Web browser, email, file management **e.g. SNMP, HTTP, FTP.**
Layer 6	Presentation Layer	**e.g. Encryption, ASCII, PNG, MIDI.**
Layer 5	Session layer	determines which data packets belong to which files, as well as where these packets go. Also establishes, maintains, and ends communication between devices **e.g. Syn/Ack**
Layer 4	Transport Layer	Creating and sequencing packets on a WAN. Error checking of packets **e.g. TCP, port numbers.**
Layer 3	Network Layer	Routing packets on a WAN **e.g. IP, routers.**
Layer 2	Data Link Layer	Creating and routing frames on a LAN. Error checking of frames **e.g. MAC, switches.**
Layer 1	Physical Layer	Methods of encoding bits onto wires and wireless. Frequencies and channels **e.g. cables, RJ45.**

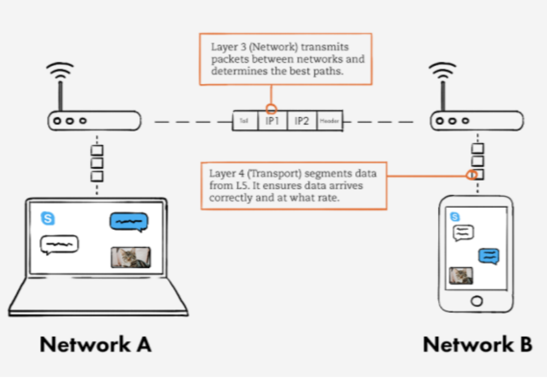


Apps like Skype use Layer 7 application protocols.

Layer 6 (Presentation) translates data to binary & encrypts/decrypts it.

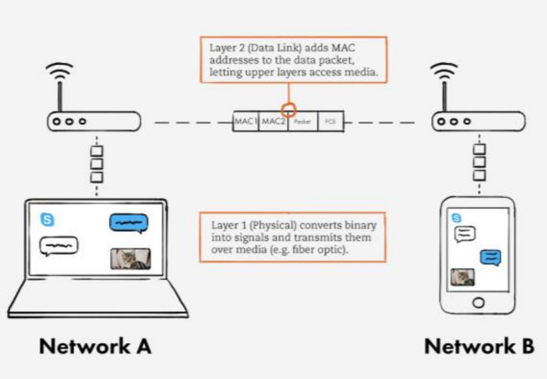
Layer 5 (Session) establishes, maintains, and ends communication between devices.

Layer 5 also decides which packets belong to which files.



Layer 3 (Network) transmits packets between networks and determines the best paths.

Layer 4 (Transport) segments data from L5. It ensures data arrives correctly and at what rate.



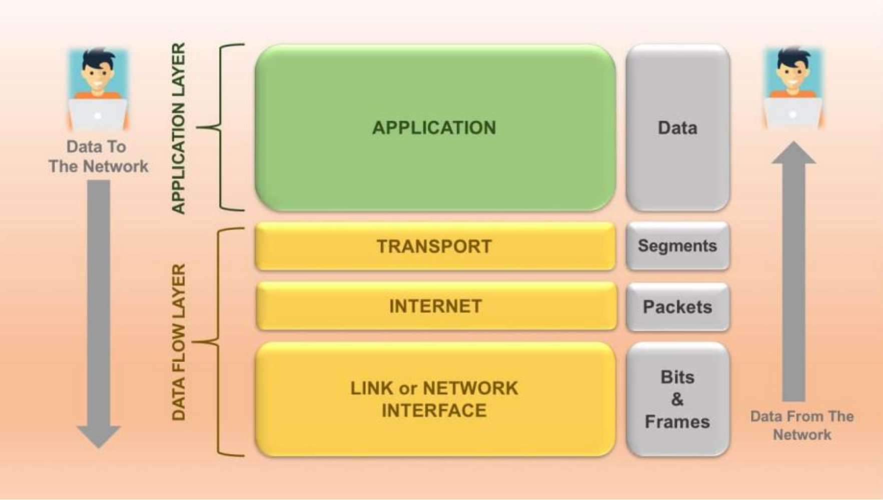
Layer 2 (Data Link) adds MAC addresses to the data packet, letting upper layers access media.

Layer 1 (Physical) converts binary into signals and transmits them over media (e.g. fiber optic).

One popular mnemonic, starting with Layer 1:
“Please Do Not Throw Sausage Pizza Away.”

Network protocols & layers

4 layer model- **This model is the one in the OCR exam **



Advantages of using layers

Breaks network communication into manageable pieces which helps developers concentrate on only one side of the network.

Layers are self contained, they can be changed without other layers being affected.

Standards for each layer forces companies to make compatible, universal hardware and software, so other brands with work with each other.

Layer	Protocols in this layer cover	Protocol examples
Layer 4- **Application layer**	Turning data into websites and other applications and vice versa	HTTP, FTP, SMTP
Layer 3- **Transport layer**	Controlling data flow- e.g. checking data is sent and delivered.	TCP
Layer 2- **Network or Internet Layer**	Making connections between networks and directing data.	IP
Layer 1- **Data link or Network interface**	Passing data (as electrical signals) over physical networks.	Ethernet

Each layer serves the layer above it- it does the hidden work needed for an action on the layer above . So in the example 4-layer model, when you send an email (on layer 4), this triggers actions in layer 3, which triggers actions in layer 2, all the way down to layer 1.

Network Attacks and Security threats

Malware is short for 'malicious software'.
A general term for any hostile or intrusive software. For example it may disrupt computer operations (virus), or it may seek to secretly monitor what the user is doing (spyware).
image

How do they access your computer?

- Computer Virus- attaches to files e.g. .exe. Spread by copying infected files and activate by opening files.
- Trojan- malware disguised as legitimate software. Users install them.
- Worms- like viruses but they self-replicate and spread very quickly.

What are the typical actions of malware?

- Spyware- Secretly monitors users actions e.g. key presses.
- Adware-
- Pharming-
- Click fraud
- Ransomware
- Rootkits- alter permissions, giving malware & hackers administration level access.
- Scareware- tells user computer is infected- scares them into opening malicious links or paying for solutions.

Network attacks comes in different forms

Passive attack- monitoring data travelling on a network and intercepts information. Use **network- monitoring** hardware & software such as **packet sniffers.**

Active attack- someone attacks a network with **malware.** Defence against it is using **firewalls.**

Insider attack- someone in an organization exploits the **network access** to steal information.

Brute force attack- cracking passwords through trial and error. Uses **automated software** producing hundreds of passwords.

Denial-of-service attack- DoS- hacker tries to stop users from accessing a park of network or website. Floods network with useless traffic, slowing it down.

Social engineering.

- People can make mistakes; they can be tricked, fooled, bribed, or threatened. All of these threats to a network are labeled together as 'social attacks'.
- Bribing a user into allowing an attacker access to a system
- Putting a thumb-drive full of malware somewhere a user might pick it up, and labelling it like "Salary Records" or "Staff redundancies".
- Phoning up a user at work and convincing them to break policy and give them the information they want directly, like patient information records.

SQL injections (structured query language).

- SQL is one of the main coding languages used to access information in databases.
- SQL injections are pieces of SQL typed into a website input box to reveal sensitive information.

Network policies to prevent vulnerabilities

Good network policies will….

- **Test** the network to find and fix security weaknesses and investigate problems.
- Use **passwords** to prevent unauthorized access.
- Enforce **user access levels** to limit the number of people with access to sensitive information.
- Install **anti-malware** and **firewall** software to prevent and destroy malicious software.
- **Encrypt** sensitive data.

Penetration testing- Staff simulate potential attacks on the network. Identifies weakness in the security. Results reported back.

Network forensics- Investigations to find the cause of attacks on a network. They capture the data packets as they enter the network. The packets are analysed. Decisions made on how to prevent future attacks.

Passwords- Help prevent unauthorised users accessing the network. Combination of letters, numbers and symbols. Changed regularly.

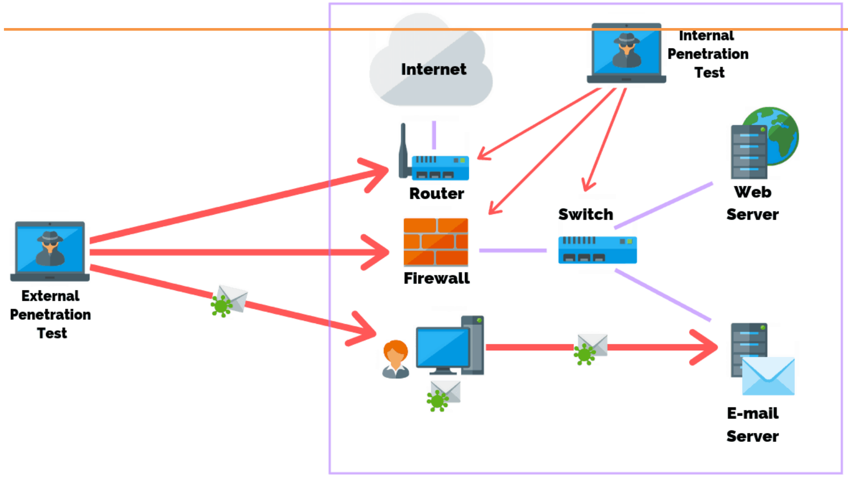
User access levels.

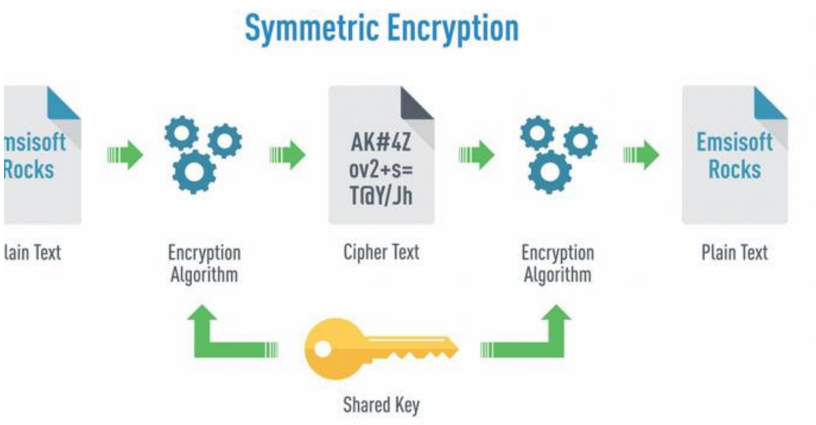
- E.g. a Business manager has a higher access level allowing them to access more sensitive data e.g. salaries.
- Limits the amount of people with access to important data therefore helping to prevent **insider attacks.**

Anti malware software-

- Designed to find and stop malware from damaging an organisations network and the devices on it.
- **Firewalls** examine all data entering and leaving the network and block any potential threats.

Encryption- Data translated into a code which only someone with the correct key can access. Encrypted text is called cipher text. Data not encrypted is called plain text. Allows data to be sent securely.





LANs, WANs and Hardware- Exam questions

Describe 2 differences between a LAN and WAN?	Explain one advantage of a wired network over a wireless network.
Describe some of the advantages of using a LAN?	What is the difference between a WAP and a Hot spot?
How does bandwidth affect the performance of a network?	What is the difference between 2.4GHz and 5GHz radio frequency bands.
How does latency affect the performance of a network?	Draw a client server and a peer to peer network
How is a switch used in a network?	Explain the differences between a client server network and a peer to peer network.
What is a NIC? What is it used for?	What type of network work a small business use?
What is a router used for in a network?	Give three advantages and two disadvantages of using a star network.
What is the difference between an ethernet cable and a fibre optic cable?	Describe the key features of a mesh network.
What is a DNS server? What is its purpose?	What is the difference between a bus topology and a ring topology?

Network protocols, the internet and Network Security- Exam questions

What is the definition of a protocol?	Can you give examples of what happens at each layer of the OSI network protocols.
What is the difference between a MAC address and an IP address?	*Describe each part of the 4 layer network model and how they interlink*
What is the difference between a static and a dynamic IP address.	Can you give examples of the advantages and disadvantages of using the cloud..
Can you write step by step how packet switching is used to direct data?	What is a virtual network?
List some of the things that a data packet contains	What is social engineering and who could it affect?
What is a packet number used for?	What is encryption?
What is a checksum? How and when is it used?	Describe 5 different types of network attacks.
Write a sentence explaining what each of the following **stands** for and **what they do**: TCP, IP, FTP, HTTP, HTTPS, SMTP, POP3, IMAP	Describe three examples of a good network policy.
What is the mnemonic to remember the 7 layers of the OSI network model?	How does a firewall work?