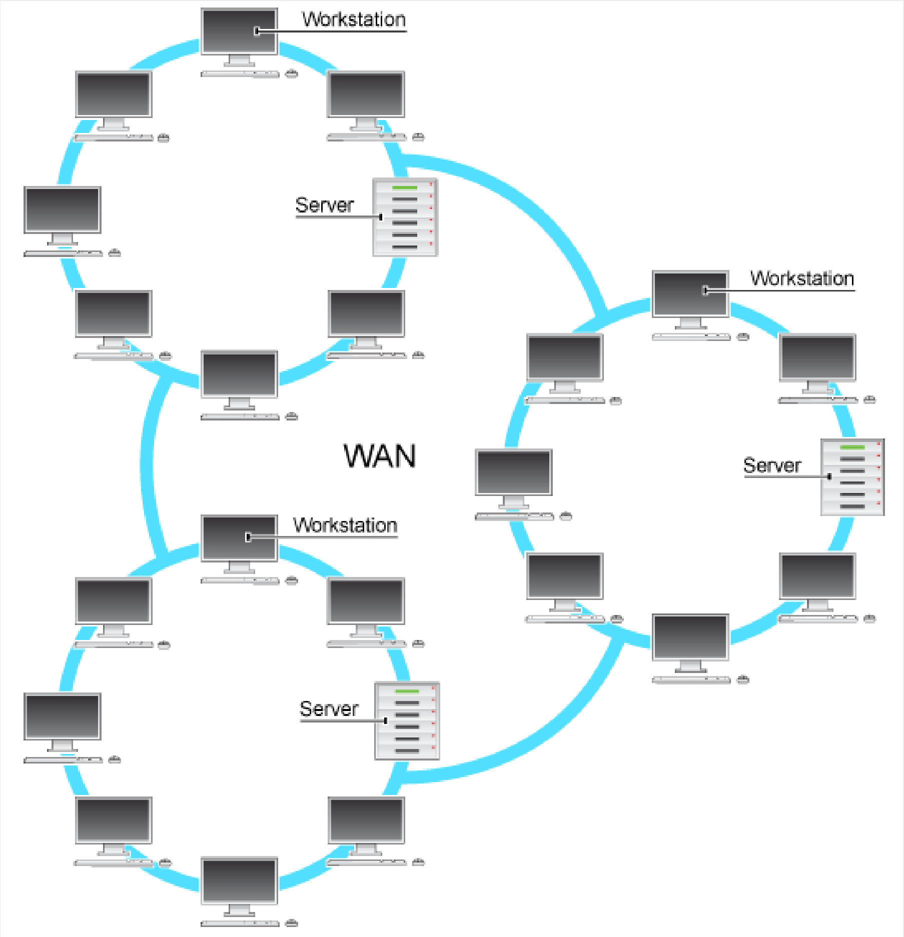
Networking infrastructure

Wide Area Networks (WANs)

A Wide Area Network (WAN) = a network relying on third-party carriers or connections such as those provided by British telecom and are spread over large geographical areas, even continents.

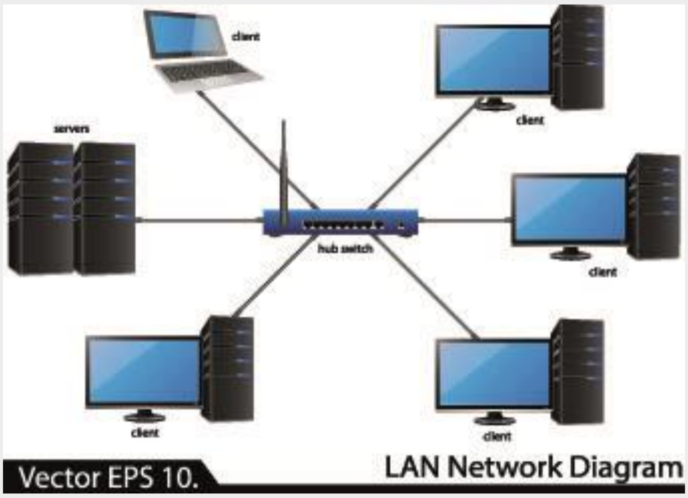
As a network of inter-connected networks, the Internet comprises of millions, if not billions of Local Area Networks and individual users to form the world's largest Wide Area Network.



Local Area Networks (LANs)

A Local Area Network = a network consisting of multiple computing devices connected together via cables on a single site. Devices can communicate, share data and hardware resources with each other.

LANs can generally transmit data at **high speeds** but over **short distances**. In most cases, there will be a **central server**.



PC with (wireless) network interface card → (Wireless access point WAP) → Router → Modem → ISP → Internet

Modem: A modulator, it is needed to convert digital signal from the computer to an analogue signal used by telecom lines. A second modem at the receiving end converts the signal back to digital.

Router (Particular detail is A-level not required)

A router is very similar to a switch. Its function is to route packets of data to their correct port.

Router = Network hardware device that is **used to connect different segments of a Local area network together and allow the devices access to wider outside networks (like the Internet).**

The router is responsible for routing the packet data to and from different network devices and possibly a WAN they are connecting to. They perform routing on IP addresses rather than MAC addresses. Sections of the network (sub-domains) are assigned ranges similar to IP address ranges, which provide the router with more information to help it direct the packet.

The act of traversing across a network to another (between nodes/routers) is known as a hop. The job of the router is to read the recipient's IP (destination) and route it to the next router along the fastest and least congested route. The next router does the same until the packet reaches its destination.

When a router is connected to the internet, the IP address of the port connecting it must be registered with the Internet Registry because this IP address must be unique over the whole internet.

Today many routers have a built-in WAP (wireless access point) allowing devices to connect wirelessly and reducing the need and cost for multiple cables. However, WIFI signal is affected by interference, bad weather, distance and is less secure. With a low wireless signal, the packets may contain errors and the data will need to be resent.

Gateways

When the protocols between networks differ, a gateway is used rather than a router to translate between them. All of the protocol specific information such as the header data is stripped off to leave just the raw data. New data is then added in the format of the new network before the gateway sends the packet on its way to its destination again.
Gateways basically do the same job as a router but are for routing packets between networks with different protocols.

Media Access Control (MAC) addresses

Every computing device that connects to the internet requires a Network Interface Card. This sometimes may be a wireless NIC. Each NIC has a unique Media Access Control address (MAC address), which is assigned and hand-coded by the manufacturer. This uniquely identifies the device, unlike an IP which may be dynamic and vary depending on location.

MAC addresses are 48 bits long and are written with 12 hex digits.
e.g. 00-09-5D-E3-F7-62
The MAC address is also sometimes called a physical address.

The network interface card is commonly built onto the motherboard. NICs produce electrical signals based on the physical protocol being used – one of the most common being Ethernet. This piece of hardware is responsible for placing packets onto network cables in the form of electrical or optical signals. Wireless network cards (WICs) are also common and use the physical protocol 802.11x rather than Ethernet. This transfers data using electromagnetic waves.

What is WIFI?

WIFI is a **local area wireless access technology** that enables devices with wireless interface cards (WICs) to be connected to the **LAN and or internet** via a **wireless network access point** (WAP).
The range of the typical WAP is around 20m indoors and further outdoors.

Standards on device connectivity are enforced. For example, the physical protocol used tends to be 802.11x compared to using Ethernet.

A firewall

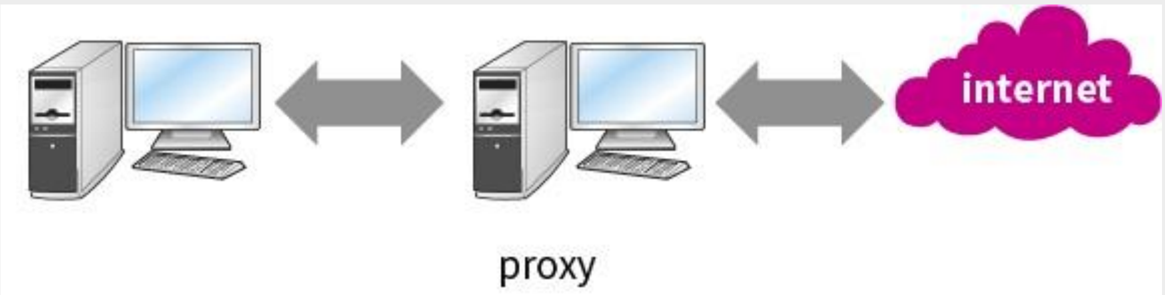
This can either be a piece of software or hardware depending on the network size. It acts as a barrier between a local area network and the internet, protecting computers from unauthorised access and filtering inbound/outbound connections.

Firewalls operate by enforcing rules:

1. The protocol used by the packet.
2. The port it is designed for.
3. Which applications are allowed to communicate with the internet.

Proxies

These act as a go-between in packet switching. A proxy server sits between the end user and the client. Any data requests are sent to the proxy, which in turn will forward the request to the intended destination. The response packets are received by the proxy server and are forwarded back to the user. This in effect hides the details of the end user and so proxies may be used to bypass filters set up in a local network.



Network topologies

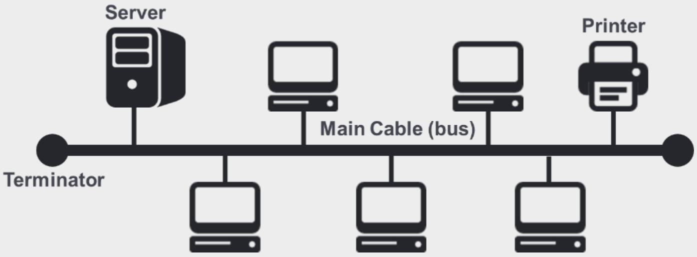
We network computers in order to save money as resources can be shared such as storage servers and printers. File sharing is also much easier and central servers offer an easy way to backup data.

However, purchasing network hardware is expensive, managing large networks can become complicated and viruses can infiltrate the network infecting all of the machines.

1. Physical bus topology

In a bus topology, all computers are connected to a single backbone cable that. The ends of the cable are connected to terminators to prevent signal reflections. Printers, storage drives and central servers can be connected to the backbone so that data transfer is managed are sharing resources is easy.

This topology is typical for a LAN that needs a budget solution and there are a small number of machines on the network.



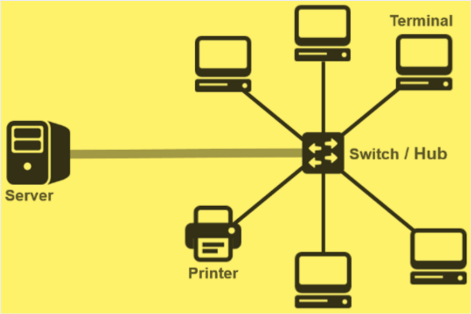
Advantages	Disadvantages
Inexpensive to install as it requires less cable than a star topology and does not require any additional hardware.	If the main cable fails then the whole network fails as data can't be transmitted between the nodes.
New nodes can easily be added without disturbing the rest of the network, unlike a ring network.	Performance degrades with heavy traffic as all data transfer occurs on the same bus.
It is easiest to install as it only requires cabling (no server/switch)	Low security as all the computers on the network can see all other data transmissions.

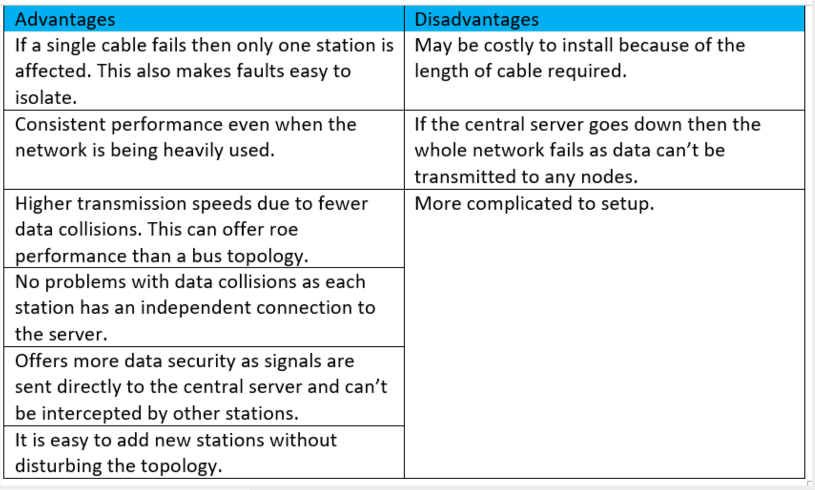
2. Star topology

A star network uses a central node, which may be a **switch** or **computer acting as a router** to transmit messages.

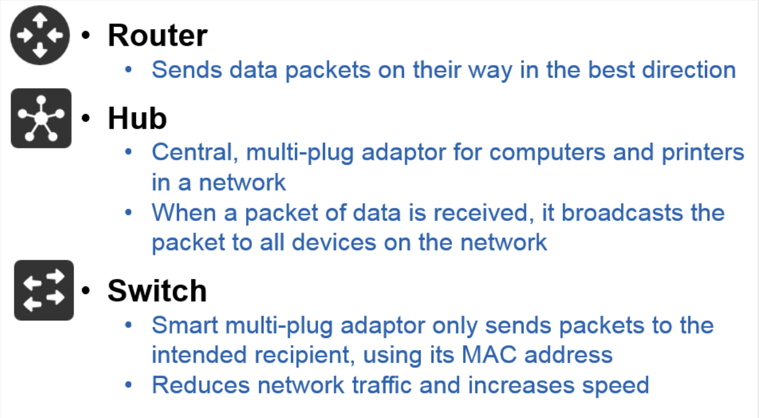
A switch keeps a record of the **unique MAC addresses of each device** on the network and can **identify which particular computer** on a network it should **send data to.**

The central switch may, in turn, be connected to one or more central servers that at as routers.





Advantages	Disadvantages
If a single cable fails then only one station is affected. This also makes faults easy to isolate.	May be costly to install because of the length of cable required.
Consistent performance even when the network is being heavily used.	If the central server goes down then the whole network fails as data can't be transmitted to any nodes.
Higher transmission speeds due to fewer data collisions. This can offer roe performance than a bus topology.	More complicated to setup.
No problems with data collisions as each station has an independent connection to the server.	
Offers more data security as signals are sent directly to the central server and can't be intercepted by other stations.	
It is easy to add new stations without disturbing the topology.	

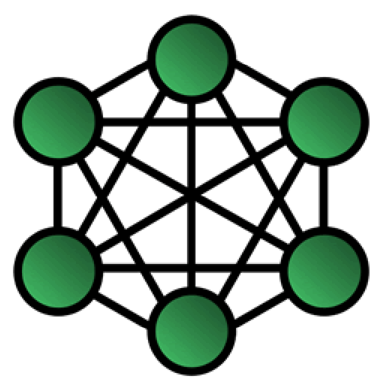


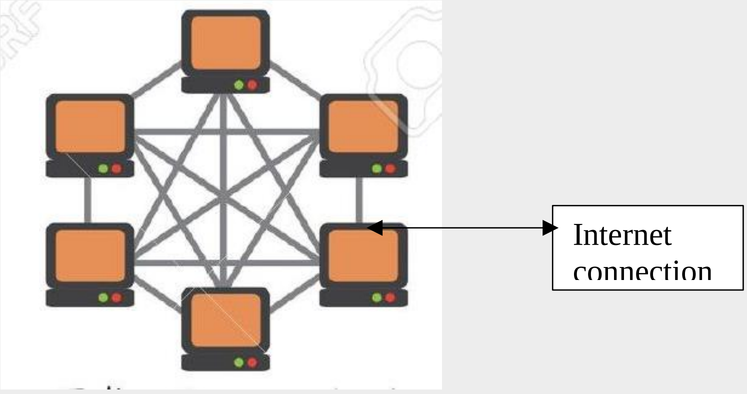
- **Router**
  - Sends data packets on their way in the best direction
- **Hub**
  - Central, multi-plug adaptor for computers and printers in a network
  - When a packet of data is received, it broadcasts the packet to all devices on the network
- **Switch**
  - Smart multi-plug adaptor only sends packets to the intended recipient, using its MAC address
  - Reduces network traffic and increases speed

3. Mesh topology

Mesh networks consist of computing devices (or nodes) that are connected to every other node by transmitting data across any intermediate nodes.

Only one node needs to have a connection to the internet and all the others can share this connection. Mesh networks can quickly become large enough to cover whole cities, they are becoming more common with the widespread use of wireless technology.
Each device on the network here has an equal status.

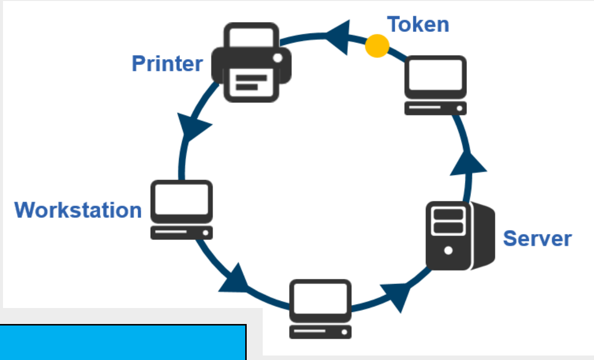




Advantages	Disadvantages
No cabling costs	Less secure as data is passed between different nodes where it can be intercepted before it reaches the destination.
The more nodes that are installed, the faster and more reliable the network becomes since one blocked or broken connection can easily be circumvented by another route. It can be described as “**self-healing”**	Viruses can easily be sent across the network and infiltrate all devices
New nodes are automatically incorporated into the network.	Data recovery and backup is harder as there is no central server.
Faster communication without the need for packets to travel via a central switch	

4. Ring topology

Data is **passed through each node**, carried in **data units called tokens** until it reaches the **intended recipient**. **Traffic** is directed **one way** to **prevent collisions. Devices are connected** in a **circular fashion** with each device having an inbound and outbound connection to the next.

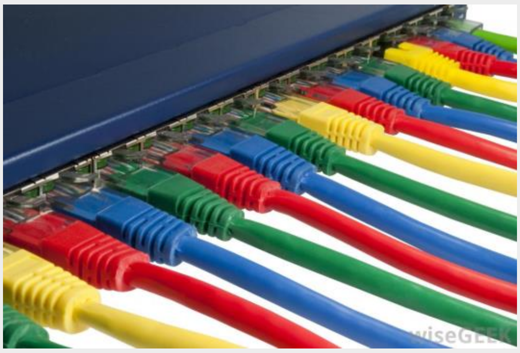


Advantages	Disadvantages
Data does not have collisions as it is one way so can travel quickly.	If any cable fails then the network fails as transmission can’t occur through this node.
Not affected by heavy traffic.	Less secure as workstations could intercept communications not intended for their receipt
More workstations can be added without degrading the performance.	If there are any problems with the network it can be difficult to identify.

Physical vs logical topology

The physical topology is the actual network hardware layout (design), which is important to consider when a wiring scheme is set up for a new building's network.

The logical topology is the shape of the path that the data travels in and describes how components communicate across the physical topology.

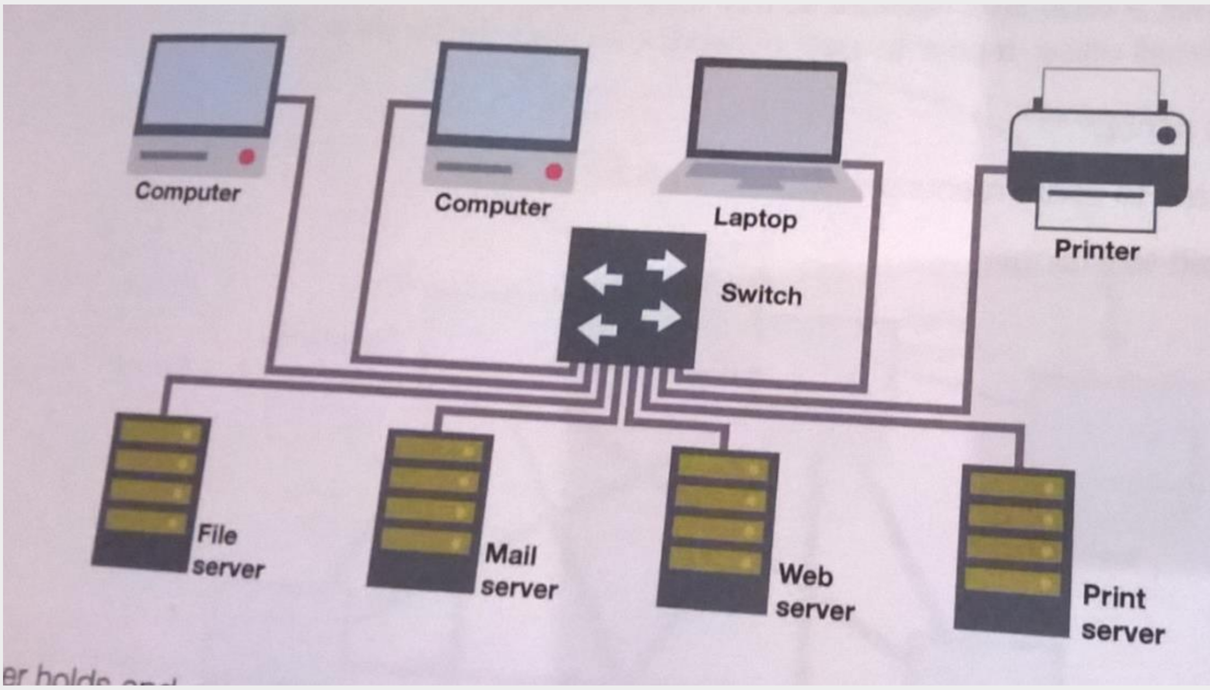


Physical and logical topologies are **independent of each other**. A network physically wired in a star topology can behave logically like a bus network by using a bus protocol and appropriate physical switching.

For example, any variety of Ethernet uses a logical bus topology when components communicate, regardless of the physical layout.

Client-Server and Peer-to-Peer networks

In a client network, one or more computers known as clients are connected to a powerful central computer known as a server.
Each client may hold some of its own data and applications locally and maybe some local connected resources such as storage/printing facilities.
The server will have a larger store of data (and possibly software) and more resources as well as offering the interconnect ability between multiple devices.
In a large network, there may be several servers that each perform different tasks.



- A file server holds and manages data for clients
- Printer servers manage print requests
- Web servers manage requests to access the Web
- Mail servers manage email systems
- Database servers manage database applications.

In a client-server network, the client makes a request to the server which then processes that request.

***In a client-server model, data may be processed on either side*.**

Cloud computing

Cloud computing refers to the growing service-based industry providing access to software or files via the internet using the client-server model.
File storage companies like Dropbox and OneDrive offer file storage facilities where users' files are kept on remote servers.
Other companies offer software via the cloud as a provision known as Software as a Service (SaaS).

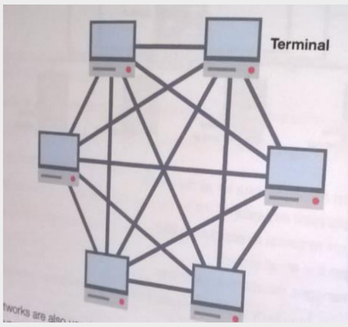
Peer-to-Peer networking

In a peer-to-peer network, there is no central server. Individual computers are connected to each other (like a mesh network), either locally or over a wide area network, so that they can share files.
In a small local area network, such as in a home or small office, a peer-to-peer network is a good choice.

Peer-to-peer networking is also used by companies providing say a video on demand. A problem arises when thousands of people want to simultaneously download the latest episode of a TV program. Using a Peer-to-peer network, hundreds of computers can be used to hold parts of the video and so share the load (uploading sections).

This is the main principle behind dozens of torrent websites that enable sharing of files, often containing copyrighted material.

BitTorrent™



Peer-to-peer

Advantages	Downsides
Cheap to set up	Widely used for online piracy. Often used by torrent websites and allows distribution of copyrighted material illegally – causing negative impacts on media industry profits/resources. It is impossible to trace the files which are being illegally downloaded.
Enables users to share resources such as a printer or router	May not be as fast for sharing/downloading small files compared to a direct download form a server
It is not difficult to maintain	
Reduces need for a central server with a large bandwidth connection as multiple computers a specific piece of software and upload small parts of it (acting as seeders).	

Client-server

Advantages	Downsides
Lightens the load on servers and their bandwidth connection. Reducing internet traffic to ISPs (spreads out traffic)	Expensive to install and manage
Security is better since all files stored on the central server location are managed by the server and have access rights.	Professional IT staff are needed to maintain the servers and run the network
Backups are done centrally so there is no need for individual user backups. Recovery procedures often in place to prevent data loss.	An internet connection of large bandwidth is needed on the server side to upload vast amounts of data and process lots of internet traffic.
Data and other resources can be shared	Internet traffic along one route can become congested for that ISP
Serve provides more processing power and can carry out more strenuous tasks for the benefit of many clients	

Client-side processing:

Describes situations when **data is processed on the client computer**, rather than on the server. This may happen because the **client computer has specific software** that can **process the information**, or to **lighten the load on the server's processor**.
Processing data on the client side can also **increase security as** it avoids **unnecessary data transfer.**

JavaScript is a client-side language and is frequently used to **provide interactivity on a web** page. Client-side processing can also **adjust styles for different platforms and screen sizes.**

Server-side processing:

Servers often process enormous volumes of data on **behalf of multiple clients**. They can also process the **data much faster than a client computer**.

There are **specific languages** that are used for server-side processing such as **SQL and PHP. Search requests** (e.g. on a **search engine** or company database) may be **sent to the server** where they may be **applied to a database using SQL**.

Database search results are sent back to the client browser. **Validation** may also be carried out **on the server** where an **invalid entry must be compared to data already** in the database of the server.
e.g. Looking up an airport location

Client-side processing	Server-side processing
Applies styles (CSS)	Provides further validation
Initial data validation	Used to query a Database
Manipulates user interface elements	Updates server databases
Provides web page interactivity (JavaScript)	Performs complex calculations
Reduces the load on the server	Encodes data to readable HTML
Reduces the amount of web traffic	Keep organisational data secure