Types of networks

1. Introduction

The modern world now is now virtually dependent on the use of computer networks whether local or as part of the internet and other wide area networks.

Think of the things that need networks starting from the time you get up:

- Having a quick check on your smartphone - it needs the telephone network to work
- Switching on the television to catch the news, for satellite TV it needs the satellite network, for streaming it needs the internet
- Making an appointment say with the local surgery - it needs the network in the surgery
- Buying coffee in the local shop - it needs the point-of-sale network to take payment
- Ordering a taxi or buying a train ticket - it needs the internet or transport network
- In school, you will be using the school network

And so on. Therefore it is important that you understand computer networks.

Types of networks

2. What is a network

A **computer network** is two or more computing devices (such as a computer) connected together in order to share resources and exchange information.

A device is said to be 'network enabled' when it is capable of joining a network.

Network enabled devices include

- Network servers
- Personal computers
- Tablets
- Smart phones
- E-readers
- Smart televisions
- Printers

There are two types of networks that you need to understand, Local Area Networks (LANs) and Wide Area Networks (WANs).

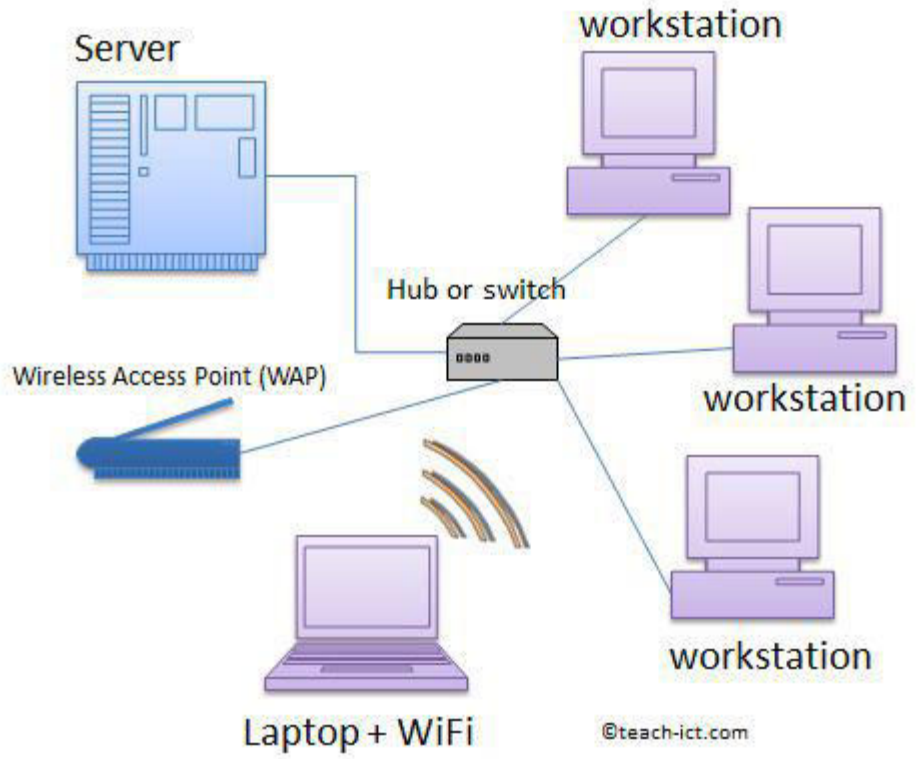
Types of networks

3. LAN - in a business

A Local Area Network is one that has two or more network-enabled devices connected within a fairly close geographical area.

For example the LAN may be located within a single building such as a home or business office or it may cover a few nearby buildings as well, such as an University campus, hospital, library or school.

The diagram below shows a typical business LAN with a network server connected to a number of computers. A wireless access point is also connected to the network so that Wi-Fi devices such as laptops can connect to the network.



This network has a central server connected to a switch. A number of workstations and wi-fi enabled devices are connected.

Computers and devices can be connected by physical Ethernet cables, which are usually owned by the organisation. They can also be connected wirelessly by using Wi-Fi connections.

To log onto a LAN, you usually need a user name and password, just like you do at school. The user name identifies you to the file server so that it can 'serve' you the correct files. The password ensures that the user name really does belong to you.

Types of networks

4. LAN - in the home

Many homes now have LANs where many devices other than workstations can connect together in order to share data. Here is an example of what a LAN within a home might look like:

The key device at the centre of a home LAN is the 'home hub', this connects the house to an ISP providing internet services. The home hub always contains a router to allow connection to the internet, it may also contain a hub or switch allowing up to 4 wired connections. It also contains a WAP (wireless access point) to allow Wi-Fi connections. By default, a secure password is needed to connect to it.

This means that while sitting on your sofa using your laptop you could select your playlist from an internet streaming service and at the same time send a document that you have been working on to the printer.

A wired connection is faster and provides high bandwidth (e.g. Gigabit 1000 Mb/s) use but it could be awkward to wire up the connection, whereas the Wi-Fi link is much slower (54Mb/s) but it does offer convenience.

Types of networks

5. Advantages of using a LAN network

A LAN usually offers the following benefits :

- A user can log on from any workstation and still access all of their files.
- Peripherals such as printers and photocopiers can be shared between many users, thus reducing costs
- Resources and files can be shared by users, this means that they can collaborate on a project.
- Backups of files and documents can be done centrally rather than needing to do it from each machine
- When software needs to be installed it can be done centrally rather than having to go to each individual workstation.
- An anti-virus and malware check can be carried out from the server to all workstations.
- Data can be transmitted very quickly between networked computers
- A LAN at home allows many devices to connect to one another, such as a smart TV or a media server

Types of networks

6. Downsides of a LAN network

There are no doubt plenty of advantages for a

business in having a network. However, they also need to take into consideration some of the disadvantages:

- **Network failure**. If there is a problem with the file server then no one will be able to access their files. If the internet server has an issue no one will be able to get onto the internet.
- **Slow service.** If there are a lot of users logged into the network requesting files and jobs then the network can start to slow down. There is only a limited amount of bandwidth in any network and the more data that is being used the slower things will become.
- **Viruses and malware**. Although these are dealt with centrally, if someone does install a virus on the local workstation it could easily spread around the network
- **Cost** - large business networks can be expensive to set up and keep running. The cost of the physical components can be very high.
- **Expert support required.** Many business networks will require specialist staff such as network managers or technicians who can deal with problems as they arise and keep the network running smoothly.
- **Security.** Although users have their own user names, giving them access to just their files, users can be careless and not log out when they leave their workstation. This could give an unauthorised person access to their files or to sensitive documents stored centrally on the network.

Types of networks

7. Measures to improve security on a LAN

Although there are various security issues that can arise through the use of a LAN, there are measures that can be put in place to counteract these:

- **Passwords**. Strong passwords should be required and users encouraged to change their passwords frequently - at least once per month.
- **Access rights.** Each user is assigned to a group e.g. students, teachers, admin etc. This is done via the user name. Each group is given different permissions to view folders and files. For

example, when students log in they cannot see all of the admin and finance documents whereas office staff cannot view students' work. Access rights can also govern what you can do on a network, for example, install software, delete files etc.

- **Audit log.** This means the computer will record every important event in an 'audit file. It records who saved what and when. Who deleted records or changed them.
- **Backups**. Central backups should be made regularly, at a minimum once a day. This way a rollback or restore of files can be made if an issue occurs.
- **Encryption.** Data travelling around the network should be encrypted, especially if hubs and Wi-Fi are being used. This is because data is broadcast to all devices on the network.
- **Installing software**. Users should not be able to install software or run .exe files because of the risk of introducing malware and viruses into the network.

Types of networks

8. WAN - Wide Area Network

A wide area network (WAN) connects two or more local area networks (LAN) that are in different geographical locations.

For example, a company might have offices in London and also New York, but they want to share a common work area so they can collaborate. In this case the LAN in London is connected to the LAN in New York by a Wide Area Network.

A WAN can also connect offices that are a bit closer together, such as estate agent offices in different towns. In this case a 'leased line' from a telecom company can be used.

A company normally hires the WAN from a major telecom company because it is so expensive and complicated to set up and maintain.

The WAN involves long distance communications and this can be achieved using

- Fibre optic lines, including laying undersea cables
- Satellite communication links
- Leased telephone lines
- Microwave links

The largest WAN of all is of course the internet. No single organisation owns the internet itself.

Types of networks

9. WAN Pros and Cons

Advantages

- Allows LANs to connect to one another.
- Allows workers to collaborate over a wide area, even across continents..
- Allows files and data to be shared between LANs. A WAN also allows direct person-to-person contact by methods such video conference virtually anywhere across the planet.

Disadvantages

- Can be expensive to hire a WAN service from the telecom operator.
- With a LAN, a company often has its own experts to maintain the network so any problems which arise can be addressed quickly. However with a WAN, it is owned by a number of external suppliers and so a failure of the WAN is usually beyond the control of the company to fix. For example, when an external DNS server fails, this immediately affects web access in the company.

Network performance

1. Introduction

Although networks are made up of similar hardware - servers, cable, hubs and so on. Their performance can be very different. Some of the factors are physical such as cable quality, some are environmental such as radio interference and others are to do with the people using the network

These factors will be discussed in the next few pages.

Network performance

2. Bandwidth

Any network has a limit in *how much* data can be moved across it in a given time. This quantity is called the **bandwidth** of the network.
Bandwidth is measured in **bits per second** also called the **bit rate**.

As you would expect, the higher the bandwidth the more expensive the network becomes to put together because of the cost of the cables and equipment.

Designing a network is a matter of balancing cost to the required performance.

Typical bit rates are:

- Kilobits per second (Kbps), a thousand bits per second.
- Megabits per second (Mbps), a million bits per second.
- Gigabits per second (Gbps), a thousand million bits per second.

The table below shows the bandwidth of various networks

You do not have to memorise all these numbers, it is just to show that networks come in a range of bandwidths:

Network bandwidths

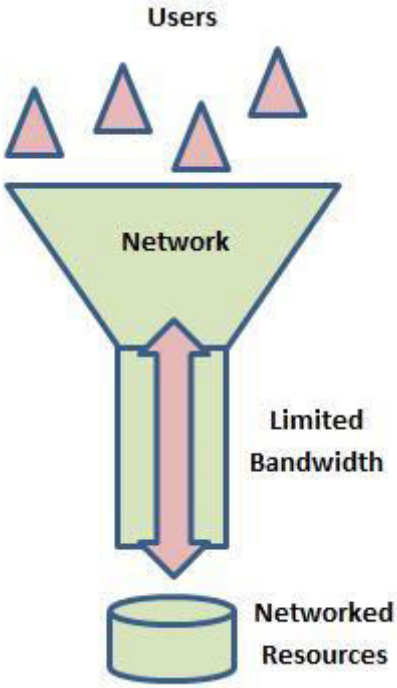
Bandwidth	Decription
56Kbps	Bandwidth of a non-broadband dial-up modem
2 to 10 Mbps	Basic copper wire based broadband (download bandwidth)
10 to 75 Mbps	Fibre-Optic based broadband (download bandwidth)
10 - 100 Mbps	Ethernet wired network using Cat-5 cable
1 Gbps - 10 Gbps	Ethernet wired network using Cat-6 cable
54 - 150 Mbps	Standard Wi-Fi connection
900 Mbps	Fast Wi-Fi

Network performance

3. Number of users

Even the most impressive network can be slowed down if too many people are using it at the same time because the bandwidth has to be shared between all users.

The more bandwidth each person uses, the less is available for everyone else.



So while theoretically a network with 100 Mbps of bandwidth should be sufficient for 50 people, if one of those users hogs the network by streaming video files, the network will seem to slow down for everyone else.

In a wired network the maximum number of people that can connect is simply the number of workstations connected to the network. However, this does not mean that bandwidth is shared equally amongst them.

In a Wi-Fi network the same thing applies - the more people or devices connecting to the network the slower the performance becomes.

There is also a limit in how many connections a Wi-Fi WAP accepts at any given time.

Network performance

4. Transmission media

These are the physical cables used within the network. They too have a performance limit in terms of bandwidth and allowed cable lengths.

A very popular choice for a wired network is copper Ethernet cables to carry data.

They have a length limit because the signal gets weaker and weaker the more it has to travel along the cable. Eventually it becomes too weak to be useful.

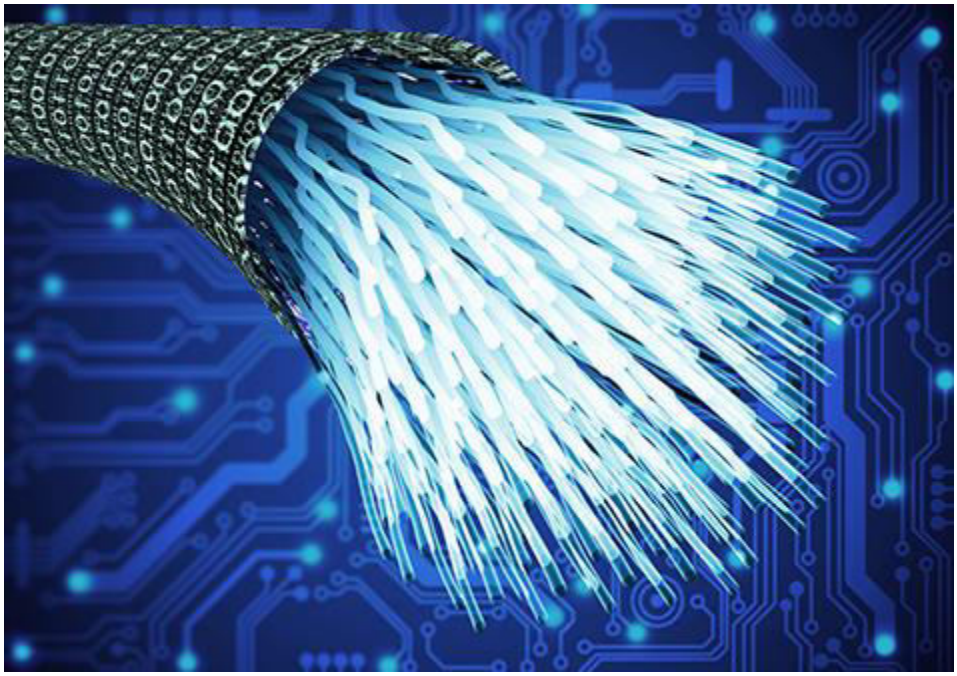
Ethernet cables come in two main performance categories called Cat-5 (slower) and Cat-6 (faster). The photo below shows ethernet cables plugged into a switch.

Choosing the type of cable will affect performance.

Cat-5 cable is cheaper per metre and is an excellent choice for a 100Mbps network. However, if a 1Gbps network or higher is required then the more expensive Cat-6 cable is recommended.

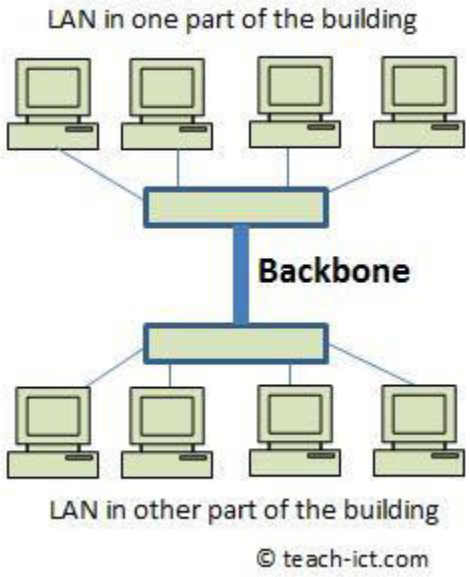
Fibre optic cable

Fibre optic cables transfer data using light which is reflected along the inside of the cable. Fibre optic offers extremely high bandwidth - in fact the bandwidth is actually limited by the equipment connected to it rather than the cable itself. But fibre optic is expensive compared to standard ethernet copper cable.



Many of the larger networks use both types - copper cable for local connections and a high-bandwidth fibre optic cable to handle the heaviest traffic such as between two LANS

A **backbone** joins together a number of LANs in the same building or as part of a WAN and the backbone is expected to carry heavy data traffic and so a fibre optic cable is preferred,.



Network performance

5. Wi-Fi performance

Wi-Fi is a very convenient way to connect to a network but there are performance limits

Range

The further away the user is from the Wi-Fi WAP then the weaker the signal becomes. Eventually the signal is too weak to make a connection.

Radio Interference

Wi-Fi is a radio technology and so it is directly affected by radio interference in the vicinity. The more interference the poorer the performance.

Blocked by walls and floors

Wi-Fi signals may be blocked by thick walls or floors, so in some places in the building you may not be able to get a connection.

Limited connections

Wi-Fi works by allocating radio channels to users logging in and there are only so many channels available. This limits how many people can use the network at the same time.

Each of these factors can reduce the bandwidth available to each user.

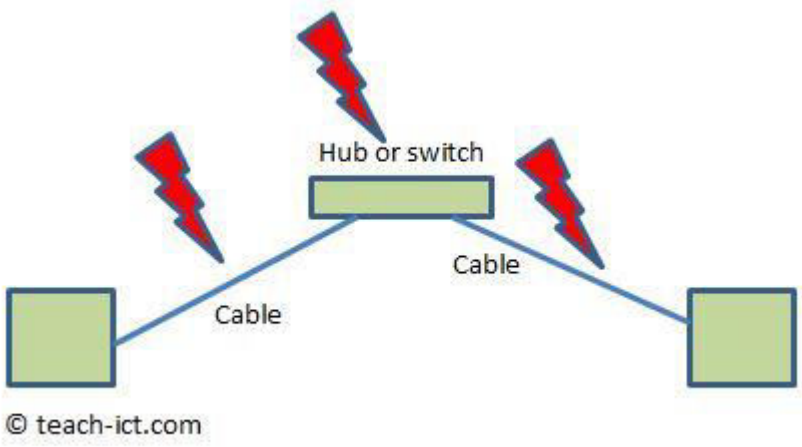
Network performance

6. Errors

A factor in measuring network performance is how many data errors happen over a given time.

An 'error' happens when a binary 1 was sent, but a binary 0 was actually received or the other way around.

On a wired network, data is moved along copper or fibre-optic cable.



There are two main reasons for errors happening:

- Interference
- Signal is too weak

If a cable or switch is too near heavy equipment such as electric motors or other power equipment then interference may cause bits to flip randomly. This is why shielded cables are used to try and reduce this problem, and network cable run layouts are thought through carefully to avoid problems.

The other factor is length of cable - the longer the cable, the weaker the signal. For example the longest recommended length of Cat-5 cable is 100 meters. If the signal gets too weak, then errors begin to creep in.

On a wireless network, radio interference can introduce errors. And if the Wi-Fi signal is too weak, then again errors creep in.

Network performance

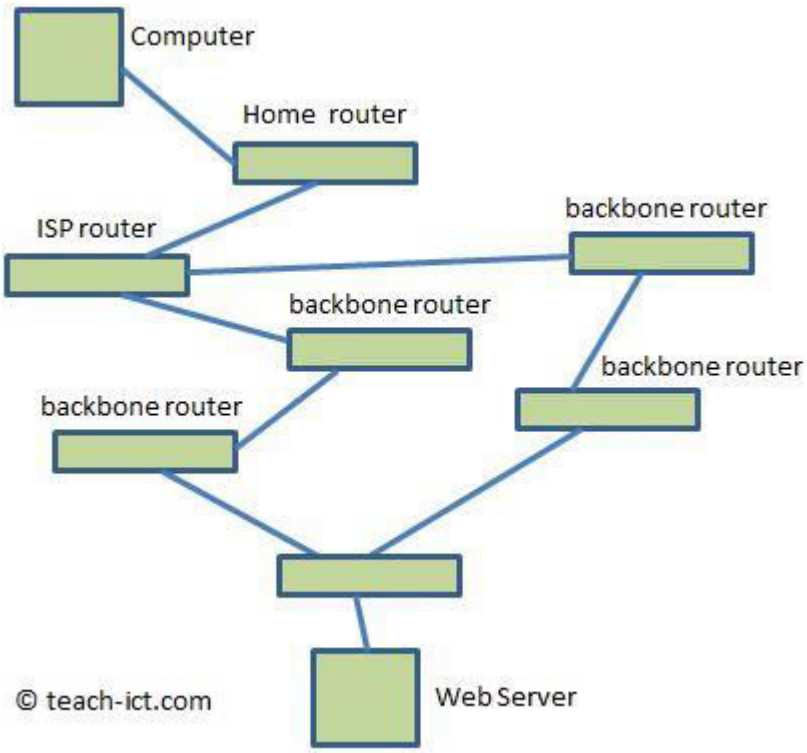
7. Latency

Latency is the technical word for 'delay'. The larger the network, then the longer it takes for a bit to travel from one point to another.

On a small local area network, latency is not much of a problem as everything is quite close to one another.

But on large networks such as a WAN (e.g the Internet), latency becomes much more important.

The picture below shows the connections between a home computer and a web server, with lots of routers in-between.



Every switch, cable and router is adding delay (latency) to the connection. And to make it worse, the actual connection changes second by second as the routers decide which path to use at that instant. This will cause bits to arrive in a different order to what was sent.

A high performance network should have low latency.

Network performance

8. Comparison of wired and wi-fi networks

Performance of wired networks is affected by:

- Type of cable connection (Ethernet or fibre optic)
- Bandwidth available
- Number of users
- Error rates
- Latency

Performance of wireless (wi-fi) networks is affected by:

- The number of connections available
- Range from WAP
- Radio interference
- Physical layout; solid walls and floors block signals

It is important to remember, though, that there are other comparisons to make between types of network. Here is a comparison of some of the factors affecting each type:

Comparison	
Wired network	**Wi-Fi network**
It is more costly than Wi-Fi to install in a building.	Only needs a Wireless Access Point to set up, so is cheaper.

Comparison	
Wired network	**Wi-Fi network**
Allows hundreds of people to log in at the same time.	Can only allow a limited number of people to connect at any one time
It is immune to radio interference	Affected by radio interference
High bandwidth, more than 10 Gbps is common	Lower bandwidth
Excellent security as a computer needs to be physically connected to the network	Not so secure as connection is by radio. So the WAP needs a strong password and encryption to disguise data being transmitted
Not affected by building layout	Signal is affected by walls and floors
Not portable as each computer needs to have a network socket available.	Very mobile, an user can carry their laptop from office to office and not lose a connection.

Roles of computers

1. Introduction

A Local Area Network allows computers to share resources and data with each other.

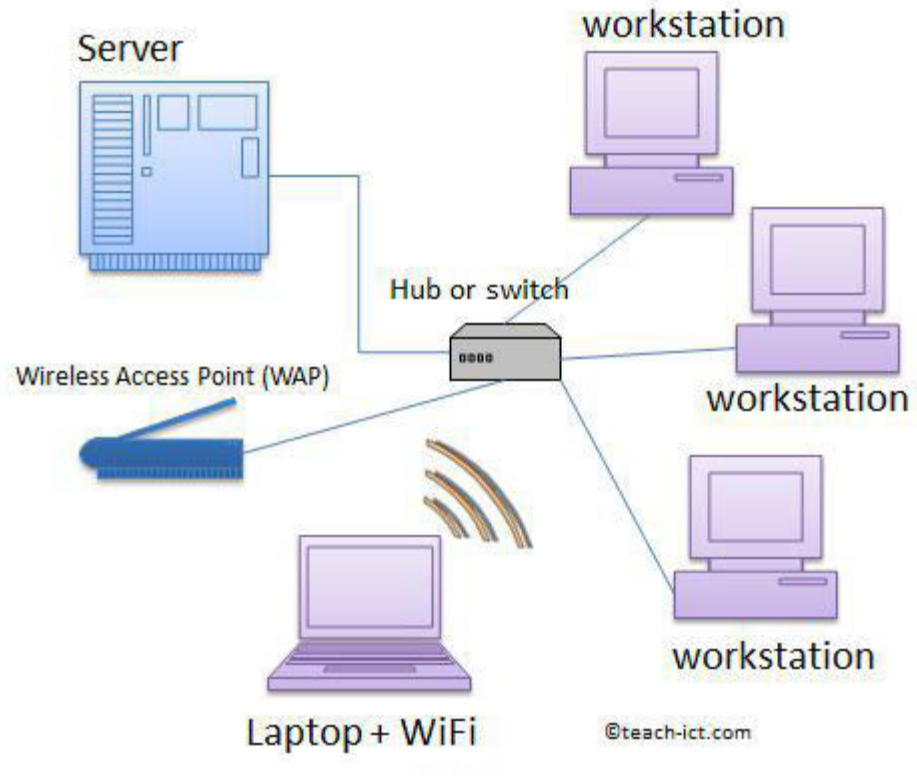
There are two main ways to connect computers on a LAN. These are

- Client-Server
- Peer-to-Peer

Client-Server and Peer-to-Peer are discussed over the next few pages.

2. Client-Server LAN

The network arrangement for a client-server local area network is shown below.



In a Client-Server LAN arrangement, most files and data are stored on a server. All computers on the network connect to this server through a central hub or switch.

The other computers on the network are called 'workstations' or 'clients'.

Users can access files and data from the server using any workstation. They just need to log into their account using their username and password. These accounts are managed by the server. Once they log in, they will see their work area or 'desktop' appear on the workstation screen.

Workstations cannot normally 'see' or share data with each other directly over the network. If people need to share data then a 'shared network folder' is created on the server by the network manager in order to share files.

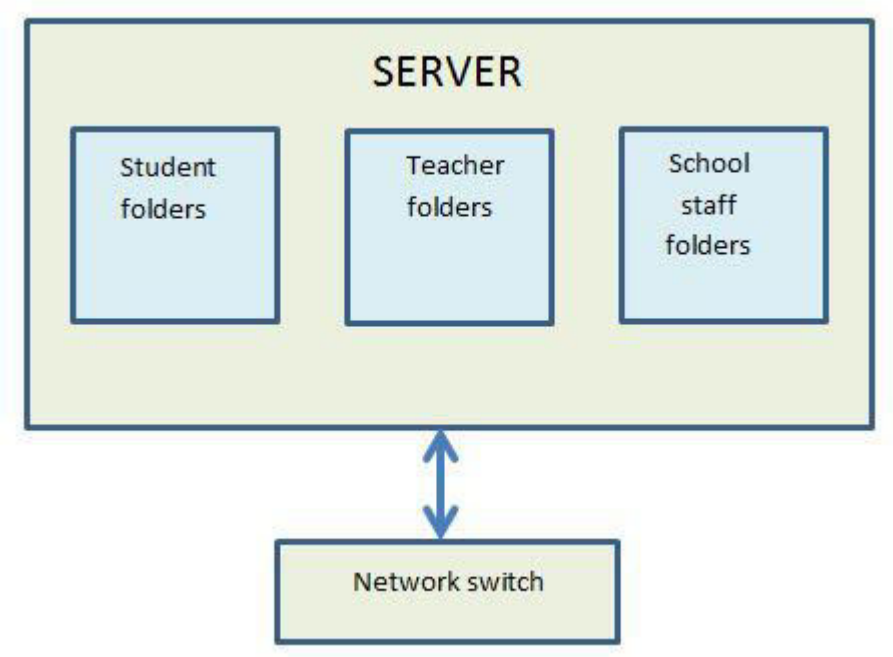
There may be multiple shared folders on a server with different access rights.

For example, in a school network there will be a shared folder for students where your teacher will store files and resources that you need. There will be another shared folder for office staff, perhaps containing copies of letters sent

to parents and other adminstrative documents. All students can see the student shared folder but not the office shared folder. And likewise the office staff can see their shared folder but not the student one.

This is because when your account and login are set up by the network manager you will be given permission to view and use only certain folders.

A typical arrangement is shown below:



Users will have their own private area on the network where they can save their files and documents. No one else can access this area (except the network manager and staff).

A client server network requires a specialist network operating system.

As files are stored on the server and they can be backed up centrally.

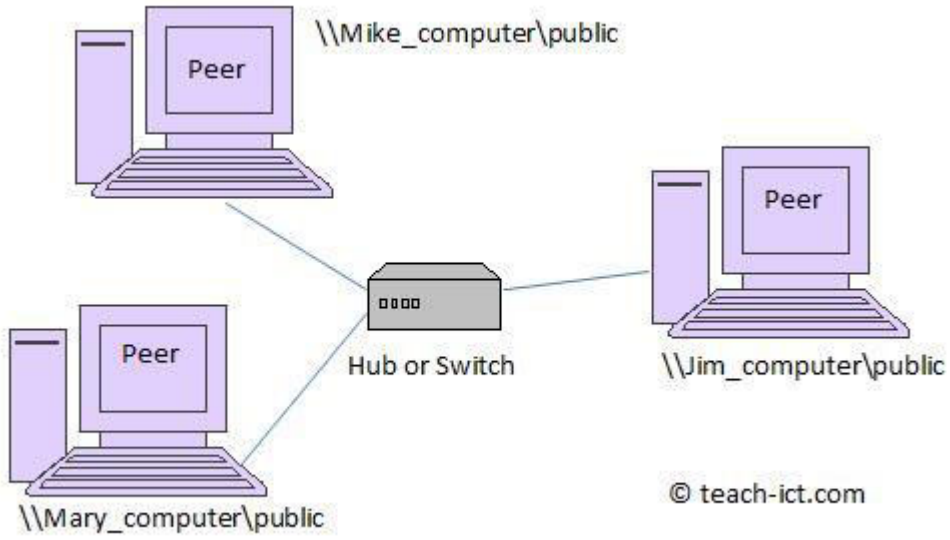
3. Peer to Peer

Peer to peer networks are very common in small offices or at home where there are only a few computers connected together.

With a peer-to-peer network a central server is not required because the files are stored on the hard disks of individual network machines.

Each computer on the network has equal importance and no more privileges than any other.

Each computer is both a client and a server - it acts as a 'host'. And users can access files and peripherals directly from all the other peers on the network.



Each computer has a name - in the diagram above they are 'Mike_computer', 'Jim_computer' and 'Mary_computer'. Of course they can be named anything the network manager chooses.

Each peer computer can be set up to share folders with other peers.

So let's assume that Mike has a folder on his computer which he has created and named 'public'. He wants to allow Jim to be able to view the documents in the folder and also to be able to add new documents. To do this, Mike has to set the 'public' folder as a 'network share' and then Jim is given 'read / write access' to the folder. The shared folder appears as a network share on the 'Jim' computer.

However, Mike doesn't want Mary to see the folder. Although the folder has been set as 'network share', because Mary hasn't been given 'read/write' access she will not be able to see or use it.

In addition to small LANs, the internet also supports huge peer-to-peer networks, where there is no single peer in control. The online peers can share files, or can be used for massive parallel computing tasks such as SETI@home, with each peer carrying out a small part of the overall computing task.

4. Compare Peer-Peer and Client-Server

Compare

Client-Server	Peer-Peer
It has one or more servers	There is no central server
A workstation computer or 'client' is used to log in to the server	Each peer may have its own local user accounts (or just a single account)
The network administrator sets up shared folders on the server	Each peer can be set to share folders (or no folders at all)
Needs technical skill to maintain a client-server network	Needs little technical skill as operating systems such as Windows and Linux have built-in support of network sharing
Files and data are stored centrally on the server	Files and data are stored locally or in a shared folder hosted by a specific peer computer
A broken workstation has no effect on the overall network. You just log in to a different workstation. A broken server, though, takes down the entire network.	A broken or disconnected peer computer has an effect on all peers because their shared folder(s) are no longer available.
Commonly used in organisations that need to connect many workstations / computers together e.g. school	Commonly used in small LANs such as at home or a small office with few computers

Compare	
Client-Server	**Peer-Peer**
network.	
Requires a network operating system	Can use a standard operating system

Advantages of a Client-server network

- With a single central server, files can be backed up more easily
- Installation of new software to the network is easier and faster
- Software only has to be licensed to the server itself
- Client machines (workstations) do not need much software or file storage of their own.
- Simpler to manage security and permissions for large networks

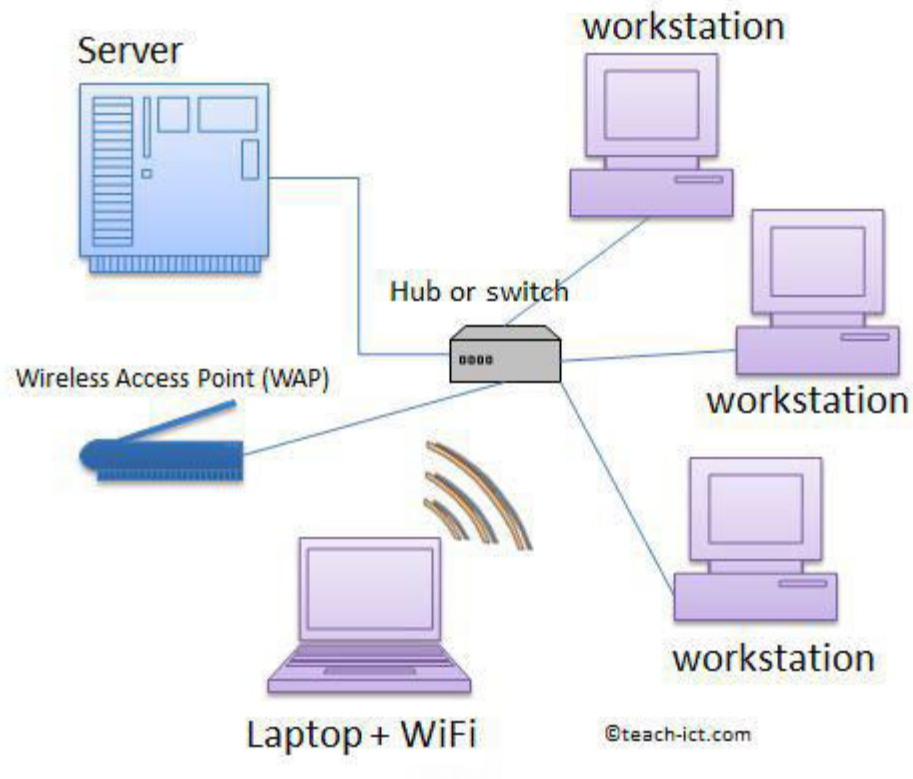
Advantages of a peer-to-peer network

- No single central point of failure. If one peer goes down, the others can continue to function.
- Easier to manage with small networks, for example two or three computers in a small office

Network hardware

1. Introduction

The arrangement of a typical Local Area Network (LAN) is shown below



This section will discuss the actual hardware required to set up such a network.

Network hardware

2. Network Interface Card

Networks need a method of telling connected devices apart from one another. The most commonly used method is the **Network Interface Card** (**NIC**).
This is an electronic chip built into the motherboard of the device. It is hard-wired with a unique 'address', called a **Media Access Control** address (or **MAC address**).

No two MAC addresses are the same.
So networks can use them to uniquely identify the connected devices.

In addition to holding the MAC address, the NIC is responsible for converting data on the computer into the format used by the network, and vice versa. Each network has its own set of rules, called a **network protocol**, and it's the NIC's job to ensure that the connected device follows these rules.

Image courtesy of Wikipedia

Network hardware

3. Hub

Hubs are a piece of hardware used to connect computers on the same network together. Every device gets plugged into the hub via cables. The hub has a socket, or 'port' available for each device. Larger networks might need a bigger hub with more ports.

To communicate across the network, devices send data in chunks called 'packets'. When a hub receives a data packet from any computer, it immediately copies it and broadcasts it to all connected devices. The packet includes a destination address, so the receiving computer knows to open it and all other computers discard it.

This is a cheap and effective way of transmitting data, but it is a little inefficient. Even if the data is meant to go to only a single computer, the hub will send it to all of them at once.

Network hardware

4. Issues with hubs

Data collisions

A network cable can only have one data packet in it at any instant.

So if two or more computers want to place a data packet on to the network at *exactly* the same time, then a 'data collision' will take place. If this happens,

the collided data is marked as unusable and the two computers are forced to send their data packets again, at slightly different times.

This is fine for a network with only a few computers. You will not notice the small delay caused by data collisions.

But imagine what happens when a hundred PCs are sharing the same network and they are all wanting to send their data packets. This will most likely result in thousands of data collisions per second - each one costing a small amount of time. You will certainly notice the network 'slowing down'.

Security

Using a hub to connect a network can be a security problem.

This is because when a hub receives data it will forward it to every device it connects to, regardless of whether the data was only meant to be sent to just one. This means that there is the potential for any computer connected to the hub to read data that was not intended for it.

Network hardware

5. Switches

Although hubs provide an inexpensive solution for small LANs, the two issues highlighted on the previous page means that it is often worth considering another, more expensive, alternative i.e. a switch.

A switch looks the same as a hub externally but the way it works is different. Unlike a hub, it does not broadcast every data packet to every device which means there is improved security. It knows which port is connected to the destination device by its MAC address and so it only sends the data packet to that port alone. This makes it more secure than a hub.

Switches also reduce the impact of data collisions and so help speed up the running of the network.

On the other hand, a switch is more expensive than a simple hub. So it tends to be used in high bandwidth, high performance networks.

Network hardware

6. Hubs Vs Switches

Comparison	
Hub	**Switch**
A hub connects nodes on the network together. It is not intelligent.	An intelligent device which connects nodes on the network together
Data packets are transmitted to every node on the network	Data packets are transmitted only to the node for which it is intended
Higher risk of data collisions leading to slower network performance	Less risk of data collisions leading to improved network performance

Comparison	
Hub	**Switch**
Security risks because data sent to all nodes	Better security as data only sent to the correct node.
Less expensive than a switch	More expensive than a hub

Network hardware

7. Router

A router is a device that transfers data packets, by the most efficient route, from one network to another i.e. between networks.

When a data packet arrives, the router does the following:-

- Reads the data packet's destination address
- Looks up all the paths it has available to get to that address
- Checks on how busy each path is at the moment
- Sends the packet along the least congested (fastest) path

Other tasks the router can perform:

- Exchange protocol information across networks
- Filter traffic - helps prevent unauthorised intrusion by malware

You are probably familiar with a home router, such as the one shown below. This connects a home network to the largest network of all - the internet.

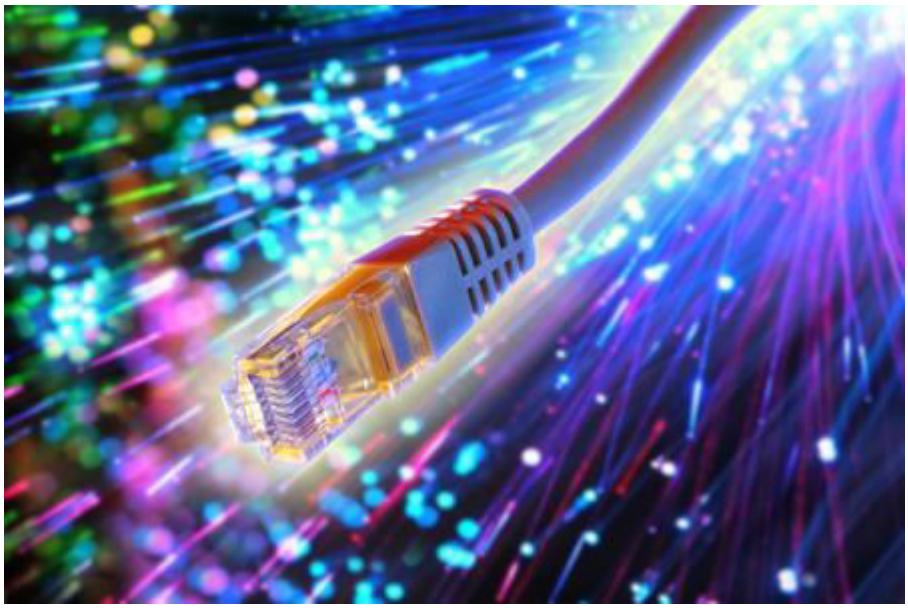
Network hardware

8. Transmission Media

Ethernet cables

An ethernet cable is made up of a set of four 'twisted pair' copper wires enclosed in a plastic sleeve with a standard network plug on the end.

Data is carried through the cables by means of electrical signals.



Fibre optic cable

For truly high bandwidth connections, then fibre optic cable is used.

Fibre optic cables are made up of many glass fibres held together inside a sheath. They use light signals to transport the data, often over a long distance.

Fibre-optic cables can be used to connect two or more local area networks, for example, two buildings on an university campus.

Also, the main data routes for the internet (known as the 'backbone') use fibre-optic cables to carry data.

The downside of this technology is that fibre optic cable is a lot more expensive than Ethernet cable.

Network hardware

9. Wireless Access Point (WAP)

If you want to connect Wi-Fi devices to a wired network, you need a wireless access point (WAP).

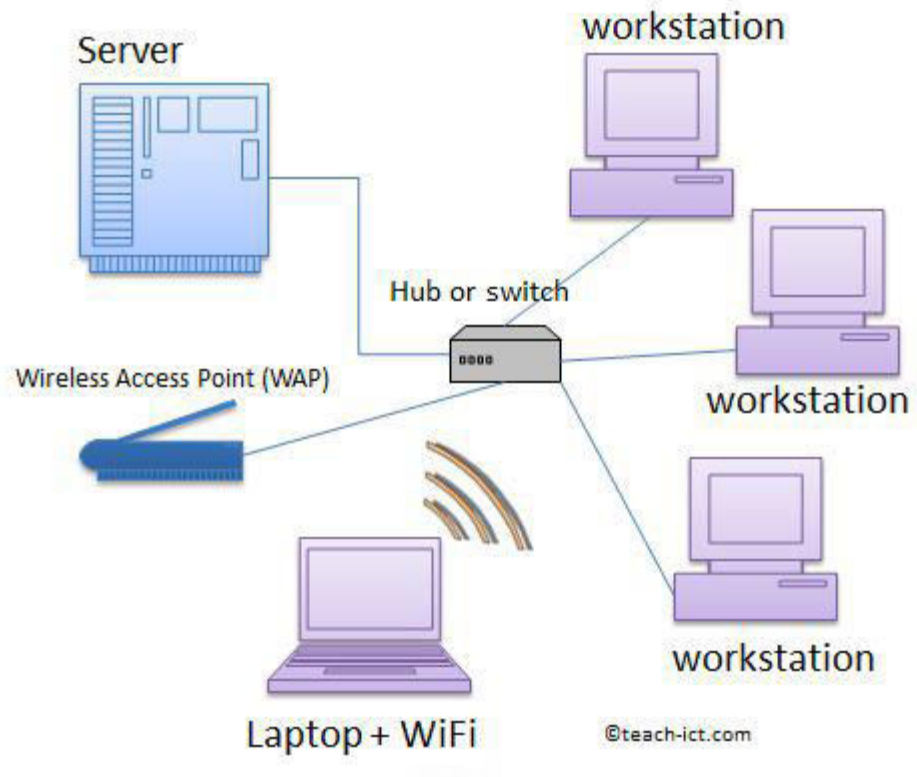
Wireless technolgy makes it easy for people to access a network and transmit data without being physically connected i.e. with wires. It gives people freedom of movement wherever the Wi-Fi signal is available.

Extra nodes can easily be added enabling more people to use the network. And unlike a wired network, no building work is required to add those extra nodes i.e. no holes need to be drilled in walls for cables.

WAPs are very commonly found in public areas such as airports, cafes and offices.

To access the Wi-Fi 'hotspot' you normally need a password.

In the diagram below, you can see that a Wireless Access Point device (WAP) is connected to the network.



The WAP has a cable connecting it to the network hub or switch.

A WAP is able to pick up Wi-Fi data packets and convert them into data packets for the wired network, and also the other way around - wired data packets back into Wi-Fi packets.

A WAP is similar to a hub in that it does not read the destination MAC address of a data packet and so the data is broadcast to everyone connected to it.

This is why it is a bad idea to connect to a sensitive web site such as your bank or savings site as all your data packets can potentially be read by another computer connected to the same wireless access point.

Network hardware

10. Summary

- The Network Interface Controller / Card provides a connection to the network.
- A hub allows nodes to be linked together and exchange data.
- A switch is an intelligent device which connects network nodes together and directs a data packet to its correct destination.

- A Wireless Access Point (WAP) allows Wi-Fi devices to connect to a wired network.
- A router is a device that transfers data from one network to another in an intelligent way.
- Transmission media includes Ethernet cables, fibre optic cables and Wi-Fi

1. Introduction

To make a website available to the general public, various things need to be in place:

- An ISP to provide access to the internet
- A unique URL for each website and page
- An IP address for the device where the website is being hosted
- A DNS to look up the URL and find the correct IP address
- Somewhere to host the website, either locally or externally
- Cloud services to provide alternative options

Over the next few pages we will be taking a closer look at these things.

2. ISP

ISP stands for 'Internet Service Provider'.

An ISP is a company that provides access to the internet for business and individuals.

They usually charge a monthly fee for this service.

They will issue you with a user name and password and very often an email address.

For individuals, the ISP normally provides a modem through which you can log in and access the internet via one of the ISPs servers.

Examples of ISPs in the UK are (in no particular order):

- Sky.
- Virgin Media
- Plus Net
- BT Infinity

3. URL

URL stands for Uniform Resource Locator. It is pronounced "you-are-ell".

A URL is the unique web address for every webpage on the internet. For example 'www.teach-ict.com' is the unique url for the home page of this website.

Other examples of URLs are:

- www.youtube.com
- www.amazon.com
- www.bbc.co.uk

IP Address

There are literally billions of devices using the internet, computers, laptops,

smart phones, tablets etc.

When you request some data from a webpage there has to be a way of getting that data delivered directly to your computer.

This is done by giving every single device connected to the internet its own unique address, a bit like you have a unique address for letters to be delivered to your home.

This unique address for digital devices is called an IP address.

IP is short for Internet Protocol. An Internet Protocol is a set of rules that govern the activity on the internet and WWW.

An IP address is made up of a set of four numbers, each of which contains one to three digits, and is separated by a dot (.)

An example of an IP address might look something like this:

76.215.67.190

Each part of the IP address is presented as a denary number ranging from 0 to 255 - unlike MAC addresses which are presented in Hex format. (Extra fact: An IP address is actually *stored* as a binary number).

Those numbers may not look like much but they are the key to being able to send and receive data over the internet.

They provide information such as your devices location in the world, right down to the city. It is possible to use a look-up service to find out where people are based through their IP addresses.

IP addresses can be either static or dynamic.

As the name suggests, static IP addresses are permenant and never change.

Whereas dynamic IP addresses are temporary and are assigned to the device every time it accesses the internet. If you are using a dynamic IP address then your device will have a different IP address each time it joins a network to access the internet.

5. DNS

Websites are hosted on servers. A server is simply a computer and as we discussed earlier, every computer or device on the internet has its own unique IP address.

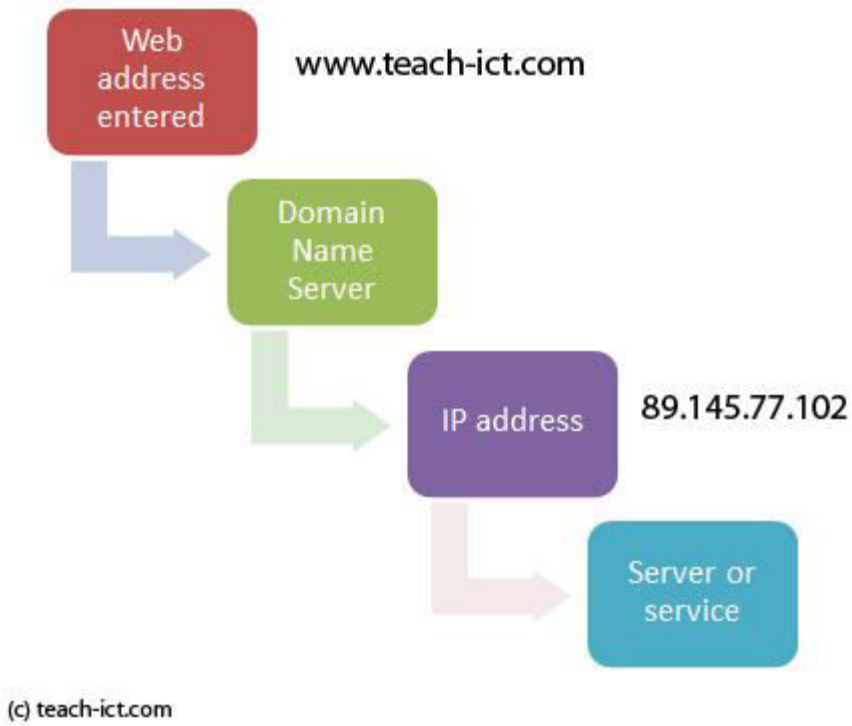
Now, imagine that you have been asked to look at a web page on teach-ict.com. Would you know the IP address to find the server where the web page is stored?

What about if you wanted to watch a video on YouTube - do you know the IP address of that server?

Luckily you don't need to know the IP address of every computer which hosts a website. This is because there is the Domain Name System (DNS).

The task of the Domain Name System is to translate a web address into the correct IP address for the server or service that you have requested.

DNS servers have a database of IP addresses and they are constantly updated by other DNS servers.



It works something like this:

- You type in the name of the website or web page that you wish to visit e.g. www.teach-ict.com.
- Your browser makes contact with a DNS server. The server contains a database that matches the domain name up with its registered IP

address. (if it cannot find the address then it searches other DNS servers)

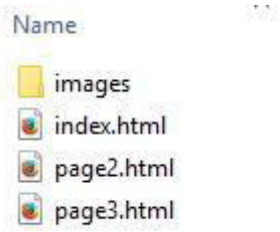
- The DNS sends this information back to your computer.
- Your computer attaches the IP address to the data packet to be sent.
- The data packet travels over the internet to its destination
- The server where the website is stored sends back the data which you requested

Advantages of DNS

- You do not need to remember any IP addresses of websites
- So long as you are connected to a DNS server you can access any website for which there is a stored IP address

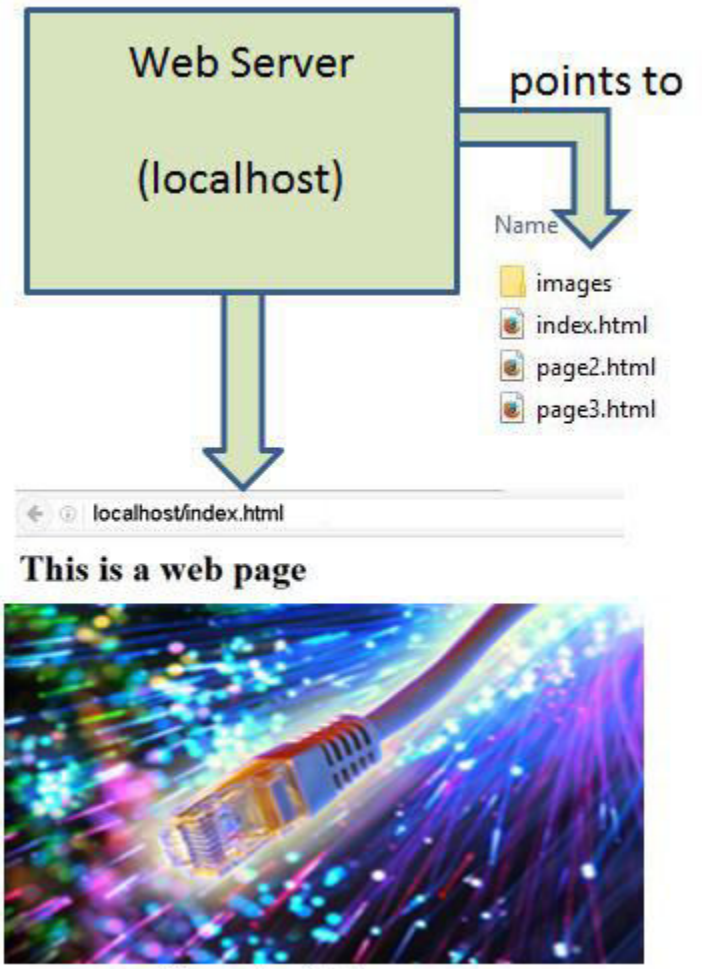
6. What is a web site

- A web site is made up of one or more web pages along with any images or other media such as video embedded within each web page.
- All of these are saved as files, arranged just like any other set of related files - in folders.
- For example a simple web site might have a folder organisation as shown below.



- The home page is the index.html file. The others are extra pages reached by some kind of navigation from the home page. Images are kept in their own folder to keep things tidy.
- So a web site is a set of files and folders, with each web page file containing html markup code. This means that the web site can be stored on any computer or storage media. You can even store it in your own computer's normal file system, but that would make it difficult for others to access it.
- For a web site to work correctly, it needs to be 'hosted' on a web server. Websites can be hosted either locally or externally - see the next few pages.

- # 7. Local hosting
- It is possible to host a website on your home PC. This is called 'local hosting'.
- To do this you would need to set up your PC as a web server and allow others to connect to it and access the web files that you store.
- The diagram below shows such an arrangement



(c) www.teach-ict.com

- As shown on the diagram, the web server is given a default address called 'localhost'.
- Why might someone decide to host their website locally? One reason is to save money, it costs less than using an external web host, and if the site is only for your own use or local network users, it is a good solution. There are a number of free, open source web server packages available that you can install.
- You can also run a local database that is attached to the web server, so it is easy to set up your own personal blog if you want to. Packages like 'WordPress' is a free open source package that can do this.
- If you are a web developer, then it is common to host a local copy of your site so you can test and update it properly before the site is uploaded to a public server.

8. Issues with local hosting

Although a localhost web server might work well for your own personal use, there are things that you would need to consider if you were going to make your website available for others:

- **Bandwidth:** Your bandwidth from the local web server will be that of your broadband connection. This is unlikely to be enough for practical connections
- **Always on**: Your computer would need to be on all the time - not even sleep mode could be used.
- **Technical knowledge:** Although setting up a web server is straightforward, if things go wrong, it can take a lot of technical knowledge to find the problem.
- **Firewall:** It can be difficult to protect a web site from deliberate intrusion attempts and malware.
- **Payments:** If you are going to sell anything from your website then you would need to set up a payment gateway (not easy) and have very strong encryption and security in place.
- **Dynamic IP:** The IP address for your home internet connection is usually supplied by your Internet Service Provider (ISP). This is usually a dynamic IP address meaning that it changes every time the router connects to the ISP. This means there is no permanent IP address that can be used to connect to the server.

For all these reasons, it generally is a better option to host websites using an external host as they have the infrastructure and expertise to address all of these issues.

9. External web hosting

External hosting is where you pay a web hosting company to host your website on one of their servers.

There are many companies who specialise in providing web hosting services, owning vast banks of servers (powerful computers).

As part of the monthly charge they will:

- provide hard disk space on their server to host your site
- ensure that your site remains running and available at all times
- provide the bandwidth required to allow users to access your site

- provide maintenance of the server
- regular backups of your site and if necessary provide a rollback
- provide security to protect your sites from malicious attack
- provide technical help

10. Types of external web hosting

If you want to have your website hosted externally you will need to think about the type of service that you need.

There are several types of hosting:

Shared web hosting

This is where many sites are hosted on the same web server.

The costs of running the server are shared between all of the users and so it is often the most economical way of having your website hosted.

The downsides are that all of the websites being hosted on the server have to share the same resources e.g. RAM, CPU time, bandwidth. So if one particular site on the server has a lot of web traffic or uses a lot of the CPU cycles then your site might experience poor performance.

Another downside is that you might have to accept advertising on your site. This sometimes happens with very low cost web hosting as the company offsets its lower charges with the advertising revenue.

Also they may only allow you to use the services supported by the web host. You may not be allowed to install specific modules or scripts that you want to run on your site.

Dedicated server

This is where the website is hosted on its own server, it does not share a server with any other sites.

Dedicated servers are often used by companies who have a lot of website traffic. They may want to be sure that their website's performance is not affected by having to share with other sites.

Also, paying for a dedicated server means that you get faster, better quality support from the web hosts. Backups and server patching are carried out on a daily basis.

The downside is that this is an expensive option as you cannot share the costs of renting the server with other users.

Virtual server

This is a powerful server that runs specialist software allowing it to create many 'virtual servers' within itself. These are then rented out to customers to host their web site.

This sharing of a single physical server to host many web sites means everyone shares the cost of it and so prices are kept low. It overcomes many of the issues of using the standard shared hosting service.

11. The Cloud

The 'cloud' or 'cloud computing' refers to a range of software and services that run on the internet rather than on your PC.

Examples of cloud services are:

- online hosting of web page data
- online file and media storage (Dropbox, GoogleDrive)
- streaming services of films and other media (Netflix, Spotify, Amazon)
- online backups of your files (Carbonite)
- online applications e.g. Office 365, Adobe Creative Cloud, GoogleDocs
- Email services such as Yahoo Mail

To access cloud services you need to use a web browser or a mobile app.

There is usually a charge for accessing services provided by these companies although some remain free to use, for example, GoogleDrive

The advantages of cloud computing are:

- you can access your data from any device with an internet connection
- documents and files can be worked on simultaneously by different people e.g. GoogleDocs

- you can store large files online and reduce the amount of storage space needed on your home device.
- you can access the latest versions of software - it won't ever become outdated
- online applications e.g. Office 365, Adobe Creative Cloud, GoogleDocs
- your work is automatically backed up, you don't have to remember to save it

The disadvantages of cloud computing are:

- if you don't have an internet connection you can't access any of the services
- if you forget your login details you can't access the services
- most of the services incur a cost, either a one-off payment or an ongoing monthly fee
- your files and personal data might not be stored in the UK and so won't be subject to the UK data laws
- there is a risk of online hackers being able to access your private data and files

12. Summary

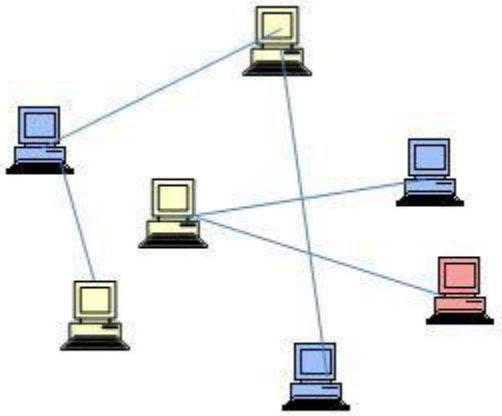
- An ISP provides access to the internet for a monthly fee
- A URL is the unique web address for every webpage on the internet
- An IP address uniquely identifies every device connected to the internet
- DNS translate a web address into the correct IP address
- A web site is a set of files and folders. With each web page file containing html markup code.

- A web server is required to host a web site.
- A web site can be hosted on a local web server or on an external host
- The 'cloud' is a general term for an organisation delivering some kind of service to you over the Internet.

Star and mesh networks

1. Network topology

This is a technical term that describes the layout of connections in a network.



Each device within a network is called a '**node**'. A node could be a workstation, a printer, a server etc.

Each of these nodes is connected to other nodes either by cable or Wi-Fi.

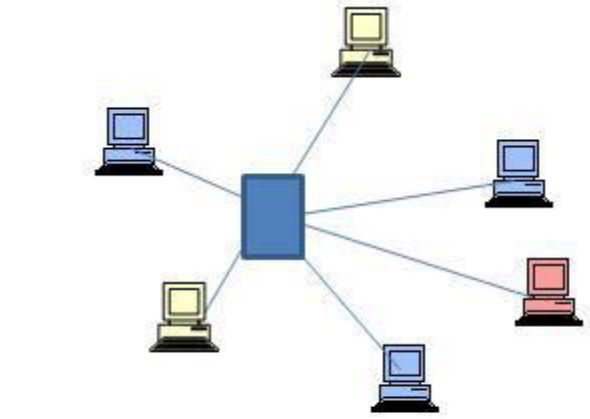
There are a number of different network topologies (layouts) for example, bus, ring, star and mesh. However for the OCR syllabus you only need to know about the star and mesh topologies.

Star and mesh networks

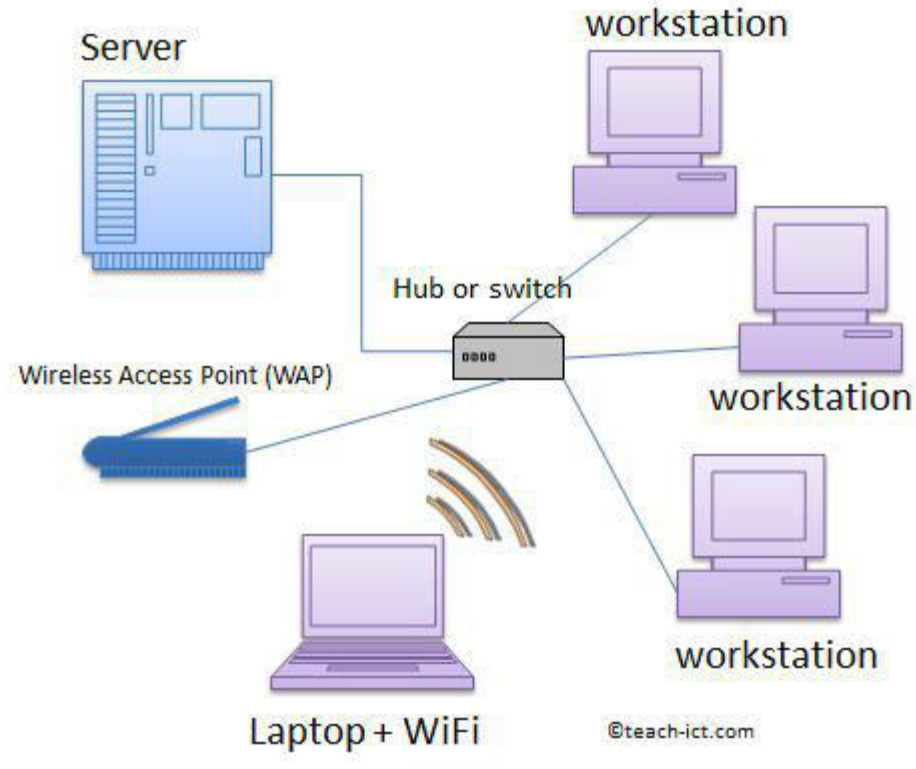
2. Star topology

The star network topology has a central device directly connected to all other nodes. Just like a star shape.

The central node could be a hub, a switch or a server.



A typical star network is shown below.



Uses of a star network

The star topology is very popular in an office or small company because it is very efficient, relatively low cost, and fairly simple to set up.

Star and mesh networks

3. Features of a star topology

Advantages

- Star networks are very reliable. If one connection fails, it does not affect other users
- Very few data collisions as each node has its own cable to the server
- Good security - no workstation can interact with another without going through the server first
- Simple to add or remove a node as it has no effect on any other node
- Scalability - can add many new nodes.

Disadvantages

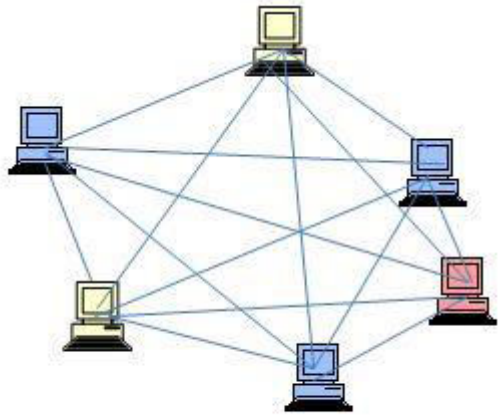
- The most expensive network layout to install because of the amount of cables needed
- Installing the network usually needs experts to set it up
- Extra hardware such as hubs and switches may be needed
- If the central switch or server fails, the whole network is down
- Requires a high performance switch or server in the centre as all traffic passes through it.

Star and mesh networks

4. Mesh network

In a mesh network, each node relays the data it receives to other nodes within reach. Unlike a star network, there is no central node in a mesh network.

A full mesh network looks like the diagram below

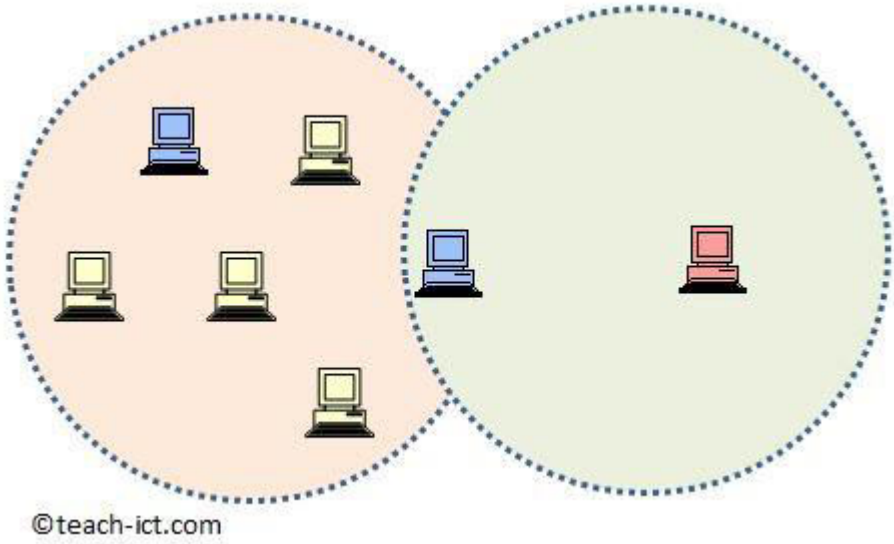


The diagram shows that each device connects to every other device.

NOTE: Peripherals such as a printer needs to be connected to a workstation or server and be in 'share' mode. This means other workstations can see the printer listed as available for use. If the server connected to the printer is switched off or offline, then so it the printer.

Using cables to connect the nodes means that a wired mesh network would rapidly become too expensive and complicated. However, when the connections are wireless, a mesh network offers significant advantages over a star topology. These are

Excellent wireless range: Look at this image of a wireless mesh network:



Most of the nodes are in the orange wireless range and so can easily exchange data with one another. But the red device is out of range of every node except the blue one. And yet, that is all that is needed to allow it to join the overall network.

Very Robust: If one node fails, then other nodes within range allow data transmission around the network to continue.

Star and mesh networks

5. Uses of a mesh network

The robustness and connectivity of a mesh network allows a number of interesting new applications:-

- *Music streaming* devices around the home can use mesh topology to maximise range within the house as each device relays music to other devices within range.
- *In factories.* Dozens of sensors on the assembly floor transmit data and relaying them into the factory network. If one sensor fails, the others just carry on.
- *The military* have battlefield mesh networks in place to allow soldiers to communicate with one another, again because it is such a robust technology.
- *Surveying.* A cluster of small drones can communicate with one another and act as a 'swarm'.
- *Rescue service.* There are also experiments underway for a cluster of small robots to communicate using a mesh network for use in rescue situations such as collapsed buildings.
- *Mobile hot-spots.* There are experiments underway to make a cars, taxis and buses mobile wi-fi hot-spots for citizens to use within a city.

Star and mesh networks

6. Features of a mesh topology

Advantages

- Very robust network. If one path fails, the rest can still be used
- There is no central node to fail
- Excellent for wireless networks as each node re-broadcasts all the data packets it receives.
- It can handle very high data traffic rates

- Data packets can be sent simultaneously
- Devices can join or leave the network without affecting the overall network.

Disadvantages

- The number of connections increase massively as more nodes are added
- Rapidly becomes an impractical topology for wired network as so many cables would be needed.
- Very expensive for a wired network due to cabling and switches needed
- Needs complex co-ordination to be effective