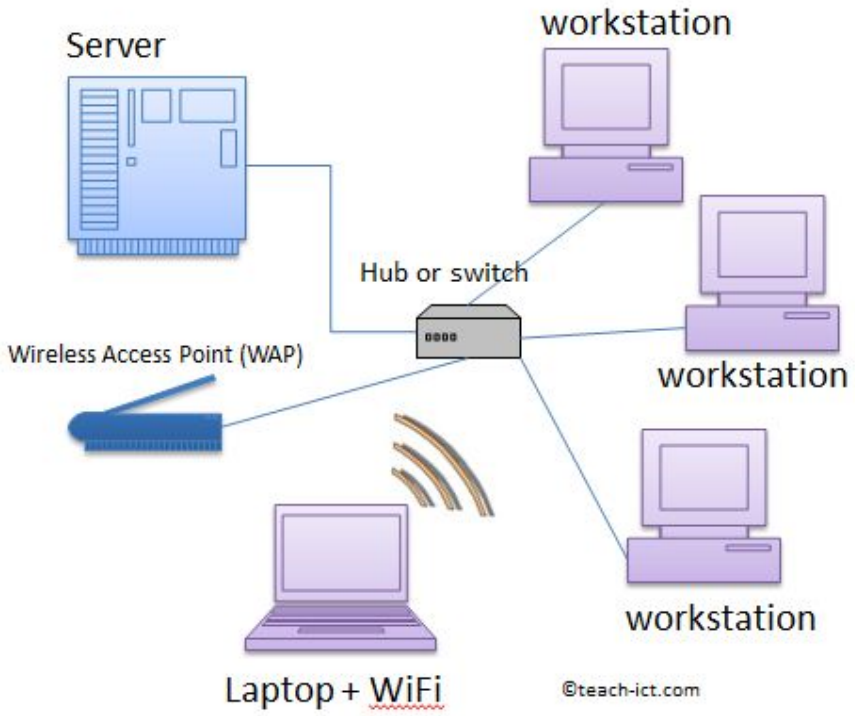
Client-Server and Peer-to-Peer Networks

Client-Server Network

With a client server network the files will not be stored on the hard drive of each workstation. Instead they will be stored on a computer which is known as a server.

If you are using a client server network then you will have a user account and you will have to log on with a user name and password.



There are a number of reasons why you do this. The first is to identify you to the server so that it knows which files belong to you and it can fetch them for you. The second is so that the security systems can check that you are actually who you say you are and that the account belongs to you.

On a large network there may be more than just the file server. There might also be an email server which deals with the internal email system. A web server controls access to the Internet and blocks access to any unsuitable sites and a print server which deals with all of the printing requests.

So that is the 'server' part of the client server network. The 'client' part is the workstations that are connected to the network. The 'clients' rely on servers to

- store and fetch networked files
- provide services that the users require

- manage network peripherals that the user wants to access.

Client-Server Networks

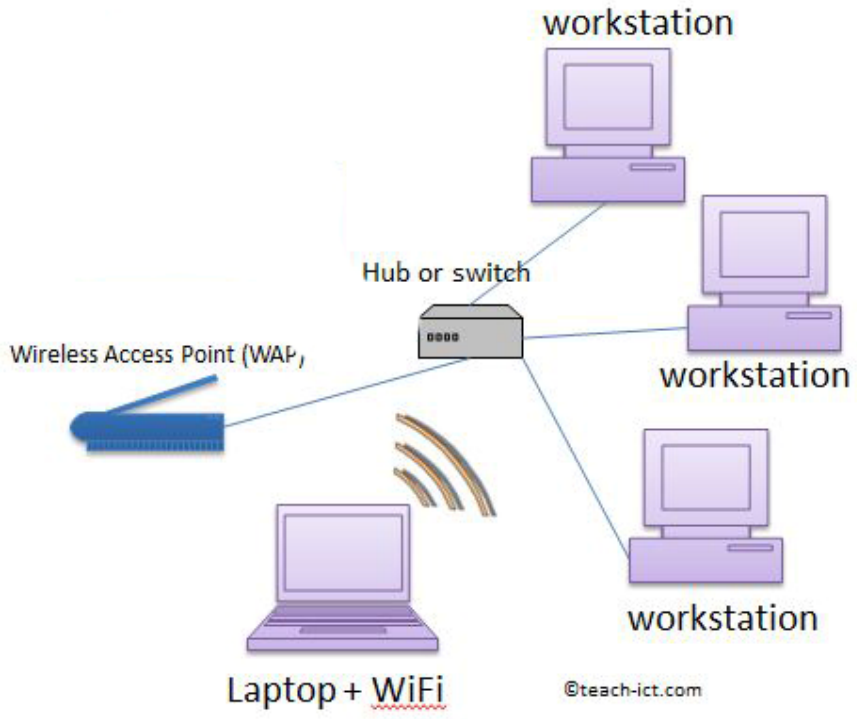
Advantages	Disadvantages
Files can be are stored in a central location (although each workstation can have its own files as well)	A specialist network operating system is needed
Network peripherals are controlled centrally	The server is expensive to purchase
Backups and network security is controlled centrally	Specialist staff such as a network manager is often needed
Users can access shared data which is centrally controlled	If key parts of the network fail such as the server or the switch, a lot of disruption can occur
Software licenses and installation for each workstation can be controlled centrally	

Peer-to-Peer Network

This type of network is where two or more computers are connected together without needing a file server to be part of the network.

A peer to peer network can be as simple as two people in the same room temporarily connecting their computers via a Universal Serial Bus to enable them to transfer or share files directly with one another.

It can also include a more permanent network where say half-a-dozen computers in a small office are connected together via a hub or switch.



This type of network means that every PC, once connected to the network is acting both as a server and a client. There is no need for a special network operating system. Access rights to files, folders and data is controlled by setting the sharing permissions on individual machines. So for example, if User A wants to access some files from User B's computer, User B must set their permissions to allow this. Otherwise, User A won't be able to see or access any of User B's work.

Permissions can be set to allow complete access to every file, folder and document stored on your system or just for particular things - perhaps a music library if at home.

This also works with a Wi-Fi connected laptop as long as the Wireless Access Point is also connected to the hub. In home networking systems, the hub / switch / WAP / ADSL modem are

all built into one unit that an ISP (Internet Service Provider) supplies. For example; BT supplies a 'Home Hub' unit for its customers that acts as a switch, WAP and a modem.

Peer-to-Peer Networks

Advantages	Disadvantages
No need for a network operating system	Because each computer might be being accessed by others it can slow down the performance for the user
Does not need an expensive server because individual workstations are used to access the files	Files and folders cannot be centrally backed up
No need for specialist staff such as network technicians because each user sets their own permissions as to which files they are willing to share.	Files and resources are not centrally organized into a specific 'shared area'. They are stored on individual computers and might be difficult to locate if the computer's owner doesn't have a logical filing system.
Much easier to set up than a client-server network - does not need specialist knowledge	Ensuring that viruses are not introduced to the network is the responsibility of each individual user
If one computer fails it will not disrupt any other part of the network. It just means that those files aren't available to other users at that time.	Although it is often the case that a password protected user account is set up on a machine, this does not have to be the case and so security is not as robust as a client server model.

Virtual Private Network (VPN)

A VPN or Virtual Private Network is a network connection that enables you to create a secure connection over the public Internet to private networks at a remote location. With a VPN, all network traffic (data, voice, and video) goes through a secure virtual tunnel between the host device (client) and the VPN provider’s servers, and is encrypted. VPN technology uses a combination of features such as encryption, tunneling protocols, data encapsulation, and

certified connections to provide you with a secure connection to private networks and to protect your identity.

Early VPNs were often set up to give individual employees secure remote access to their company networks, hence the name “virtual private network”. By connecting to the company’s network, an individual employee can access all the company’s resources and services as if the employee were inside the company.

Since then, VPNs have evolved to provide the same level of secure communication between any device on the internet. Today, using VPN is increasingly popular among consumers as a means to protect their privacy online, secure their browsing sessions, and get unrestricted access to content or websites that are otherwise blocked or censored