

The “Black Box” of the computer is a mystery to lots of people who are interested only in using a mouse or keyboard to get the desired result. Like the engine in a car or the inside of a television, what happens inside the box is of no interest so long as it works.

So far, so good; there is no danger of confusion between a car, a TV or a computer. Alas, times are changing. More people are using several computers at home and need to link them together for convenience.

This makes sense because all the computers can then talk to a single printer or use the same gateway to the internet. That they can also talk to each other means that files can be backed up easily to a central storage device or onto another computer. They can be linked by cable or wirelessly to form a home network.

To control the traffic another black box is necessary and could be a hub, a switch or a router. Because they form the links in a network and seem to do the same sort of thing the names are sometimes (wrongly) used interchangeably. These black boxes are all communication devices, but they have different levels of ability.

A Google search will quickly turn up lots of information and use words like ‘protocols’ and ‘IP addresses’. That’s fine if you feel you need to know all that stuff, but the distinction can be put into simple terms.

A HUB is the simplest. A hub will take a signal from any device capable of sending it and forward it to all other devices connected to it. If it gets a reply from any device, it will also send the reply to all other devices connected to it.

A SWITCH will start like a hub, but immediately learn the identities assigned automatically to each device. Signals carry information about the originating device and any response will be forwarded to the appropriate device ONLY. That reduces traffic and makes the network more efficient.

A ROUTER is a more complex beast. It notes the source of a signal it receives from the home network, but forwards the signal to the internet as if it was the originator, using its own address. It adds to each signal a code unique to that signal. If the code is contained in a response signal from elsewhere, the router remembers which device on the local network initiated the original signal and routes the response accordingly.

Any unwanted incoming signal such as spam cannot contain such a unique code and cannot be passed to anywhere on the local network. This security is referred to as a Firewall.

As a network grows a dedicated computer can be added as a SERVER to handle it all - a bigger Black Box.

