Network hardware

In order for a computer to operate on a network, there are ranges of different hardware components that are required.

Local area networks, need Ethernet cables/ Land Cable to connect devices to each other.

Ethernet cables resembles a phone cable but are larger and feature more wires. It consists of four twisted pair of coper wires. Ethernet cables normally support one or more industry standards including Category 5 and Category 6.

## Differences between Cat5 and Cat6 cables

### **Bandwidth of Cat5 and Cat6** The main difference between the two is total bandwidth available on the cable. While Cat5 is limited to 100 Mbps transfer speed, Cat6 can go all the way up to 10 Gbps, which is a more reliable specification for residential installments.

### **Safety Margins:** Cat6 utilizes a thick-gauge plastic casing which is able to traverse longer distances without interfering with the signal, thereby reducing crosstalk issues which would limit the previous Cat5 configurations. Cat5 is not the ideal cabling system to tackle crosstalk issues. Plus, the speeds are maintained at longer distances without affecting speed. **What is Crosstalk?** Electronic equipment (including cat cables) emits electromagnetic signals. When lots of cables are near one another, these cables can interfere with one another. This interference is referred to as “crosstalk”. Crosstalk increases errors and lost packets. The newer versions of cat cables (i.e., Cat6 and Cat6A cables) reduce the impact of crosstalk by using improved shielding and twisted cable design.

### **Backward Compatibility:** Cat6 is backward compatible with Cat5 and Cat5e standards, so there will be no compatibility issues with Cat6, which accounts for almost 90 percent of cable installations of modern-day networking infrastructure.

### **Future of Data :** Cat6 is the future of network infrastructure, which adheres to the highest industry-standard specifications to future proof any business establishment for years to come. Cat5, on the other hand, is an outdated cabling system, which was once the backbone of residential infrastructure. Large scale, applications require a more stringent network configuration and Cat6 delivers.

## Hubs

A hub is a device that connects a number of computers together to make a LAN.   
  
The typical use of a hub is at the centre of a star network (or as part of a hybrid network) - the hub has cables plugged into it from each computer which allows the computers to share data packets.

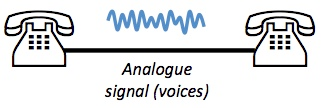
The number of ports on the hub will determine how many computers will be connected. With an '8 port hub', you will be able to connect up to eight computers together.

A hub is a ‘**dumb**’ device: if it receives a message, it sends it to **every computer** on the network. This means that hub-based networks are **not very secure** - everyone can listen in to communications.

## Switches

A switch, like a hub, is a device that **connects** a number of computers together to make a **LAN**.   
The typical use of a switch is at the **centre of a star network** (or as part of a hybrid network) - the switch has cables plugged into it from each computer.  
A switch is a more ‘**intelligent**’ device than a hub: if it receives a message, it checks who it is **addressed** to, and only sends it to that **specific computer**. Because of this, networks that use switches are **more secure** than those that use hubs, but also a little more **expensive**.

## Modem

Before the days of broadband Internet connections, most computers connected to the Internet via telephone lines (dial-up connections).   
  
The problem with using telephone lines is that they are designed to carry voices, which are [analogue](https://www.igcseict.info/theory/5/anadig/index.html) signals. They are not designed for digital data.

The solution was to use a special device to join the digital computer to the analogue telephone line. This device is known as a modem. A modem contains a [DAC and an ADC](https://www.igcseict.info/theory/5/anadig/index.html).  
  
The DAC in the modem is required so that the digital computer can send data down the analogue telephone line (it converts digital data into noises which is exactly what the telephone line is designed to carry.) The ADC in the modem is required so that the analogue signals (noises) that arrive via the telephone line can be converted back into digital data.

So, simply put, a **modem** is required because **computers are digital** devices, and the **telephone system is analogue**. The modem **converts** from digital to analogue and from analogue to digital.

## NIC Network interface card (NIC)

NICs enable desktop and laptop computers to connect to a network. NICs are small circuit boards that connect to the motherboard. Smartphones also use a GSM chip to connect to the telephone network. Games consoles contain a NIC card so users can access the internet, download games and play online.

Some computers, such as laptops, have two NICs: one for **wired** connections, and one for **wireless** connections (which uses radio signals instead of wires)

A wireless access point (WAP) is a hardware device or configured node on a local area network (LAN) that allows wireless capable devices and wired networks to connect through a wireless standard, including Wi-Fi or Bluetooth. WAPs feature radio transmitters and antennae, which facilitate connectivity between devices and the Internet or a network

A WAP is also known as a hotspot.

Wireless access points (WAP) may be used to provide network connectivity in office environments, allowing employees to work anywhere in the office and remain connected to a network. In addition, WAPs provide wireless Internet in public places, like coffee shops, airports and train stations.

Wireless access points are most commonly thought of in the context of the 802 series of wireless standards, commonly known as Wi-Fi. While there are other wireless standards, the vast majority of the time the terms Wi-Fi hotspot and WAP are synonymous.

## Router

A Router is a device that transfers data from one network to another in an intelligent way. It can be wireless or cabled. It has the task of forwarding data packets to their destination by the most efficient route. In order to do this, the router has a microcomputer inside it.

The router holds a table in memory that contains a list of all the networks it is connected to, along with the latest information on how busy each path in the network is. **This is called the 'routing table'.**

[Routers](https://searchnetworking.techtarget.com/definition/router) send data to a specific location based on an address for the network segment.

Routers has the ability to search routing tables and find the shortest path to the destination..

**Here's how a router works:**

* When a router receives a packet and sees a MAC address (hardware address) that is not on the local segment(network), it discards the MAC address, then looks at the IP address (software address).
* It then searches its routing table, and then sends the packet based on the IP address to the fastest and least congested path, to the router that's connected to the segment that contains that address.

**Gateways**  
A gateway is a combination of hardware and software that acts as a "gate" between two [networks](https://techterms.com/definition/network). It may be a router, firewall, server, or other device that enables traffic to flow in and out of the network. It connects two networks that use **different protocols**.

Where two networks use different protocols, packets must be modified so as to conform to both protocols. The gateway does this modification it transforms the packets but leaves its contents and then gives the packets a new sender and receiver addresses which comply to the new protocol.

The router and the gateway have similar function in that they regulate network traffic between two or more separate networks, however, Gateways regulate traffic **between two dissimilar** networks, while routers regulate traffic **between similar** networks.

Examples of a gateway on an e-mail system allows different e-mail systems to exchange data.

Bridge

A network bridge, also known as a layer 2 switch, is a hardware device used to create a connection between two separate computer networks or to divide one network into two.

* A bridge joins two separate computer networks.
* It enables communication between the two networks and provides a way for them to work as a single network.
* Bridges extend local area networks to cover a larger physical area than the LAN can reach
* The joined networks usually use the same protocol

Repeater

Network repeaters (also called signal boosters and range extenders) are small devices that receive incoming electrical, wireless, and optical signals and retransmit them to spots that Ethernet and Wi-Fi data transmissions can't reach. Repeaters attempt to preserve signal integrity and extend the distance over which data can travel. Repeater – A repeater operates at the physical layer and is a 2-port device

Proxy Server:

Proxy server is an intermediary server between client and the internet. Proxy servers offers the following basic functionalities:

* Firewall and network data filtering.
* Network connection sharing
* Data caching

Purpose of Proxy Servers

* Monitoring and Filtering such as content filtering, filtering encrypted data, bypass filters, logging and eavesdropping.
* Improving performance. It gives quick service by retrieving contents/information from cache.
* Translation; It helps to customize the source site for local users by excluding source content or substituting source content with original local content. In this the traffic from the global users is routed to the source website through Translation proxy
* Accessing services anonymously : The destination server receives the request from the proxy server (anonymously) and thus does not receive information about the end user
* Security: It hides the identity of the user therefore it protects the user network from spam and the hacker attacks.

Firewall

A firewall is a security device — computer hardware or software — that can help protect your network by filtering traffic and blocking outsiders from gaining unauthorized access to the private data on your computer. Not only does a firewall block unwanted traffic, it can also help block malicious software from infecting your computer.

It monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

## Types of firewalls

There are many types of firewalls. Your choice of firewall will depend on the type and sized of network you have and the amount and type of security that is needed. The two main types

### Packet-filtering firewalls

A packet-filtering firewall is a management program that can block network traffic IP protocol, an IP address, and a port number. This type of firewall is the most basic form of protection and is meant for smaller networks. While packet-filtering firewalls can be helpful, they also have limitations. Because all web traffic is allowed, a packet-filtering firewall doesn’t block web-based attacks. So, you need additional protection to distinguish between friendly and malicious web traffic.

### Proxy service firewalls

The proxy service firewall is a system that can help protect your network security by filtering messages at the application layer. It essentially serves as a gateway or middle man between your internal network and outside servers on the web. Also known as a gateway firewall, it is more secure in its use of stateful and deep packet inspection technology to analyze incoming traffic.

Comparison between hardware and software firewalls

* A single hardware firewall can protect your entire network
* They run on their own dedicated CPU and memory not taking away computer resources
* Hardware firewalls cannot be disabled by malware as easily as software firewalls can
* A single hardware firewall can protect multiple computers not needing a license for each computer
* Hardware firewalls still protect the computer when the operating system crashes
* A single router firewall is considerably more expensive than a license for a single software firewall
* Hardware firewalls are more difficult to configure than software firewalls
* Hardware firewalls need physical space where to install it and cable layout
* A hardware firewall protecting the whole network will affect multiple computers if it fails