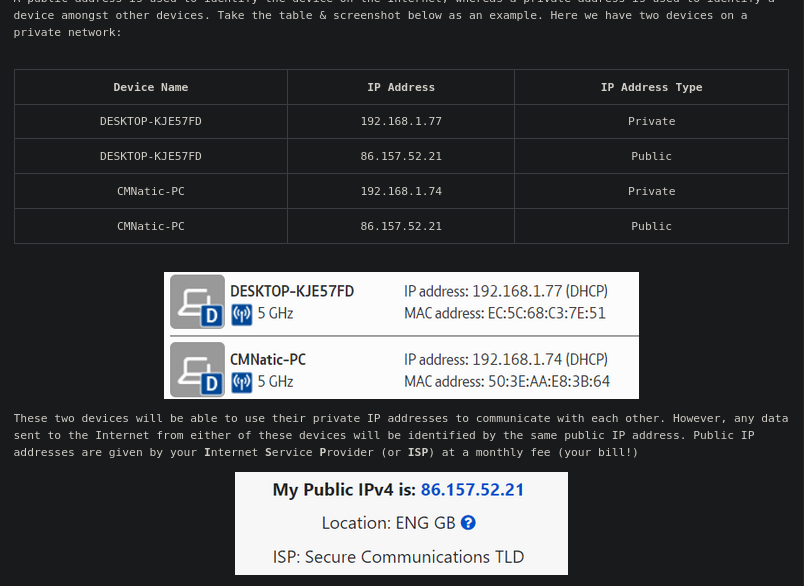
Devices have two means of identification, with one being permeable. These are:

1. Non-permeable----> An IP Address
2. Permeable-----> A Media Access Control (MAC) Address -- think of this as being similar to a serial number.

### **IP Addresses**

In **IP** address is a set of numbers that are divided into four octets.

A public address is used to identify the device on the Internet, whereas a private address is used to identify a device amongst other devices.



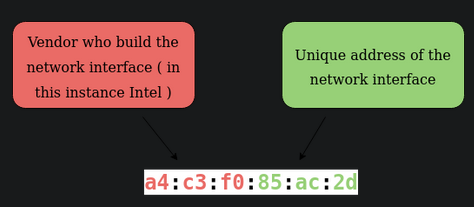
IPv4, uses a numbering system of 2^32 IP addresses (4.29 billion)

IPv6, supports up to 2^128 of IP addresses (340 trillion-plus), resolving the issues faced with Ipv4 and more efficient due to new methodologies

**MAC Addresses**

Devices on a network will all have a physical network interface, which is a microchip board found on the device's motherboard. This network interface is assigned a unique address at the factory it was built at, called a **MAC** (**M**edia **A**ccess **C**ontrol ) address.

The MAC address is a **twelve-character** hexadecimal number (*a base sixteen numbering system used in computing to represent numbers*) split into two's and separated by a colon. These colons are considered separators. For example, *a4:c3:f0:85:ac:2d*. The first six characters represent the company that made the network interface, and the last six is a unique number.



However, an interesting thing with MAC addresses is that they can be faked or "spoofed" in a process known as spoofing. This spoofing occurs when a networked device pretends to identify as another using its MAC address.

**Ping**

Ping is one of the most fundamental network tools available to us. Ping uses **ICMP** (**I**nternet **C**ontrol **M**essage **P**rotocol) packets to determine the performance of a connection between devices, for example, if the connection exists or is reliable.

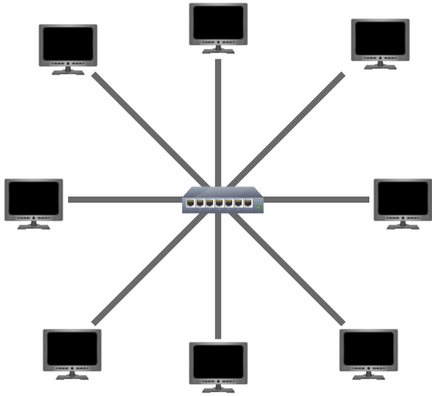
**Local Area Network (LAN) Topologies**

**Star Topology**

The main premise of a star topology is that devices are individually connected via a central networking device such as a switch or hub. This topology is the most commonly found today because of its reliability and scalability - despite the cost.

**Disadvantages:**

* If the centralised hardware that connects devices fails, these devices will no longer be able to send or receive data.
* It is more expensive than any of the other topologies.



**Bus Topology**

This type of connection relies upon a single connection which is known as a backbone cable. This type of topology is similar to the leaf off of a tree in the sense that devices (leaves) stem from where the branches are on this cable.

**Ring Topology**

The ring topology (also known as token topology) boasts some similarities. Devices such as computers are connected directly to each other to form a loop, meaning that there is little cabling required and less dependence on dedicated hardware such as within a star topology.

**What is a Switch?**

Switches are dedicated devices within a network that are designed to aggregate multiple other devices such as computers, printers, or any other networking-capable device using ethernet.

Switches are much more efficient than their lesser counterpart (hubs/repeaters). Switches keep track of what device is connected to which port. This way, when they receive a packet, instead of repeating that packet to every port like a hub would do, it just sends it to the intended target, thus reducing network traffic.

Both Switches and Routers can be connected to one another. The ability to do this increases the redundancy (the reliability) of a network by adding multiple paths for data to take. If one path goes down, another can be used. Whilst this may reduce the overall performance of a network because packets have to take longer to travel.

### **Wha**t is a Rou**ter?**

It's a router's job to connect networks and pass data between them. It does this by using routing (hence the name router!).

Routing is the label given to the process of data travelling across networks. Routing involves creating a path between networks so that this data can be successfully delivered.

Routing is useful when devices are connected by many paths.

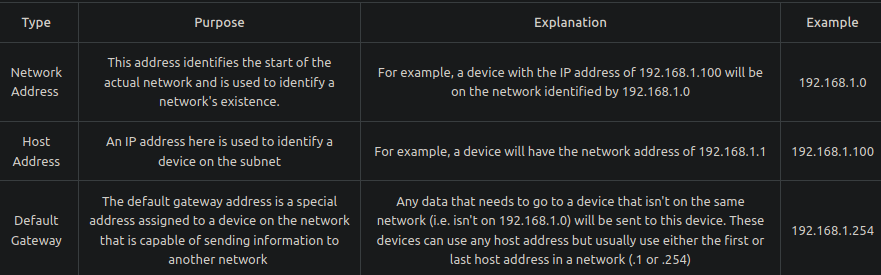
**Subnetting**

Subnetting is achieved by splitting up the number of hosts that can fit within the network, represented by a number called a subnet mask.

A subnet mask which is also represented as a number of four bytes (32 bits), ranging from 0 to 255 (0-255).

Subnets use IP addresses in three different ways:

* Identify the network address
* Identify the host address
* Identify the default gateway



Subnetting provides a range of benefits, including:

* Efficiency
* Security
* Full control

**The ARP Protocol**

The **ARP** protocol or **A**ddress **R**esolution **P**rotocol for short, is the technology that is responsible for allowing devices to identify themselves on a network.

Simply, the ARP protocol allows a device to associate its MAC address with an IP address on the network. Each device on a network will keep a log of the MAC addresses associated with other devices.

When devices wish to communicate with another, they will send a broadcast to the entire network searching for the specific device. Devices can use the ARP protocol to find the MAC address (and therefore the physical identifier) of a device for communication.

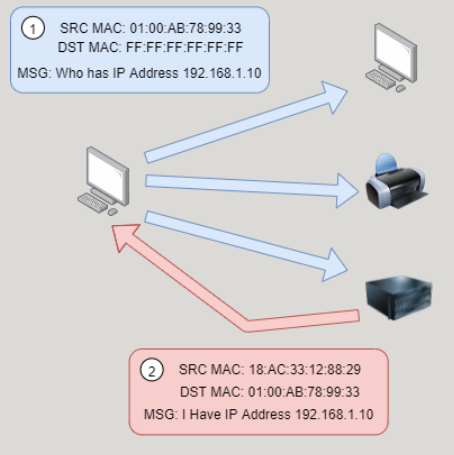
**How does ARP Work?**

Each device within a network has a ledger to store information on, which is called a cache. In the context of the ARP protocol, this cache stores the identifiers of other devices on the network.

In order to map these two identifiers together (IP address and MAC address), the ARP protocol sends two types of messages:

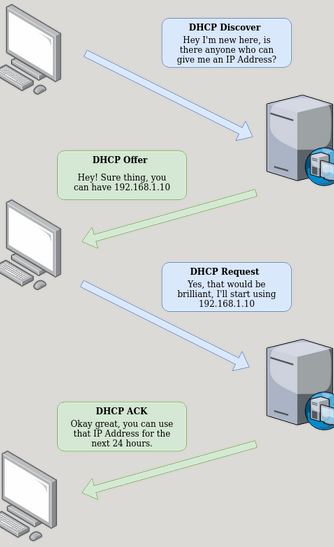
1. **ARP Request**
2. **ARP Reply**

When an **ARP request** is sent, a message is broadcasted to every other device found on a network by the device, asking whether or not the device's MAC address matches the requested IP address. If the device does have the requested IP address, an **ARP reply** is returned to the initial device to acknowledge this. The initial device will now remember this and store it within its cache (an ARP entry).



**The DHCP Protocol**

IP addresses can be assigned either manually, by entering them physically into a device, or automatically and most commonly by using a **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) server. When a device connects to a network, if it has not already been manually assigned an IP address, it sends out a request (DHCP Discover) to see if any DHCP servers are on the network. The DHCP server then replies back with an IP address the device could use (DHCP Offer). The device then sends a reply confirming it wants the offered IP Address (DHCP Request), and then lastly, the DHCP server sends a reply acknowledging this has been completed, and the device can start using the IP Address (DHCP ACK).

****