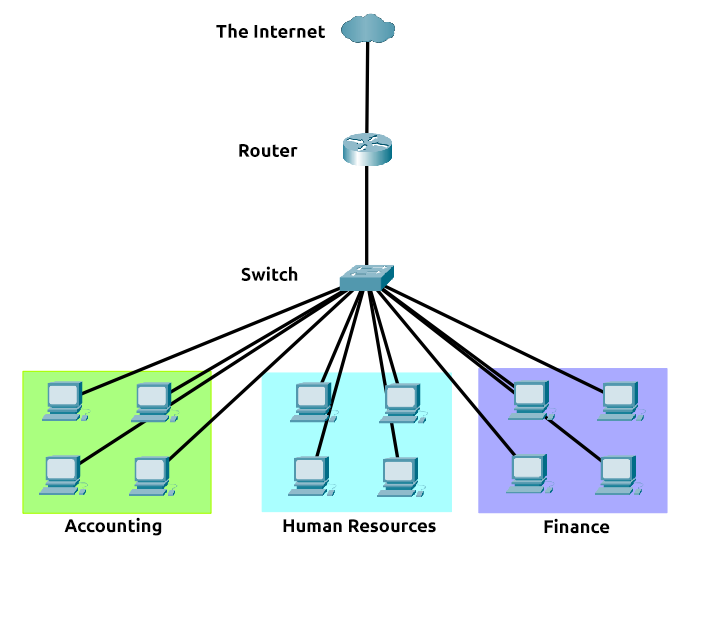
As we've previously discussed throughout the module so far, Networks can be found in all shapes and sizes - ranging from small to large. Subnetting is the term given to splitting up a network into smaller, miniature networks within itself. Think of it as slicing up a cake for your friends. There's only a certain amount of cake to go around, but everybody wants a piece. Subnetting is you deciding who gets what slice & reserving such a slice of this metaphorical cake.

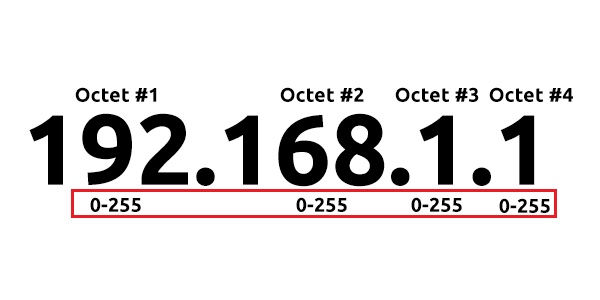
Take a business, for example; You will have different departments such as:

* Accounting
* Finance
* Human Resources



Whilst you know where to send information in real life to the correct department, networks need to know as well. Network administrators use subnetting to categorise and assign specific parts of a network to reflect this.

Subnetting is achieved by splitting up the number of hosts that can fit within the network, represented by a number called a subnet mask. Let's refer back to our diagram from the first room in this module:



As we can recall, an IP address is made up of four sections called octets. The same goes for 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

Let's split these three up to understand their purposes into the table below:

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Purpose** | **Explanation** | **Example** |
| Network Address | This address identifies the start of the actual network and is used to identify a network's existence. | For example, a device with the IP address of 192.168.1.100 will be on the network identified by 192.168.1.0 | 192.168.1.0 |
| Host Address | An IP address here is used to identify a device on the subnet | For example, a device will have the network address of 192.168.1.1 | 192.168.1.100 |
| Default Gateway | The default gateway address is a special address assigned to a device on the network that is capable of sending information to another network | Any data that needs to go to a device that isn't on the same network (i.e. isn't on 192.168.1.0) will be sent to this device. These devices can use any host address but usually use either the first or last host address in a network (.1 or .254) | 192.168.1.254 |

Now, in small networks such as at home, you will be on one subnet as there is an unlikely chance that you need more than 254 devices connected at one time.

However, places such as businesses and offices will have much more of these devices (PCs, printers, cameras and sensors), where subnetting takes place.

Subnetting provides a range of benefits, including:

* Efficiency
* Security
* Full control

We'll come on to explore exactly how subnetting provides these benefits at a later date; however, for now, all we need to understand is the security element to it. Let's take the typical café on the street. This cafe will have two networks:

1. One for employees, cash registers, and other devices for the facility
2. One for the general public to use as a hotspot

Subnetting allows you to separate these two use cases from each other whilst having the benefits of a connection to larger networks such as the Internet.

***Answer the questions below***

What is the technical term for dividing a network up into smaller pieces?



Correct Answer

How many **bits**are in a subnet mask?



Correct Answer

 Hint

What is the range of a section (octet) of a subnet mask?



Correct Answer

 Hint

What address is used to identify the start of a network?



Correct Answer

 Hint

What address is used to identify devices within a network?



Correct Answer

 Hint

What is the name used to identify the device responsible for sending data to another 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).

This process is illustrated in the diagram below: