The DHCP and ARP Protocols

* The hardware address, known as the MAC address (Media Access Control) of a NIC or Wi-Fi chip is fixed at manufacturer time, and so therefore cannot be changed because it’s unique.
* A MAC address is 48 bits long (6 bytes) and is split into two different sections:
* 3 bytes = Organisationally Unique Identifier (OUI)
* 3 bytes = Set by manufacturer.
* The OUI is administered by the IEEE.
* The IP address of a device is managed in software and so it can be changed, and we do change it often.
* When you connect to an Ethernet / Wi-Fi access point, your computer will either:
* Be configured with a predefined address (Static address)
* Or request for an IP address from a resource on the network known as the DHCP server.

DHCP (Dynamic Host Configuration Protocol)

* For a computer to connect to a DHCP server to get an IP address, it first sends out a UDP packet onto the network. Seeing, as how the IP address of the server is also unknown, we set the source address as “0.0.0.0” and the destination address as “255.255.255.255”. If there is a DHCP server present then dialogue opposite follows.

Graphical user interface, text, application

Description automatically generated

* The DHCP server is configured with a block of addresses for example, your broadband access point may use the range 192.168.0.0 – 192.168.0.255 to allocate addresses. This operation is independent of the list of IP addresses and works on fixed line networks. The range could also potentially be public depending on whether or not it’s owned by the access provider.
* The IP address your given by the server will have a lease parameter (how long you have the address)
* What’s important to note is that the client only sends out a generic DHCP server request, as it doesn’t know the DHCP server address. Therefore, a spoof DHCP server could reply instead of the real one.
* UDP Port Number 68 = DHCP Client and UDP Port Number 67 = DHCP Server

ARP

* If your computer wishes to send a data packet to a known destination IP address on your LAN, the computer needs to know the MAC address of that computer (to build the layer 2 packet)
* Therefore, the computer asks the LAN, who has the following IP address, tell me their MAC address. This process is known as ARP or Address Resolution Protocol.
* In this process, an ARP packet format is created. This is then encapsulated within an IP packet, which is then encapsulated within an Ethernet packet which is then sent out onto the LAN.
* An ARP storm occurs when ARP packets are sent out and received, but due to a loop, this then gets repeated infinitely until the buffers on your device get full.
* Graphical user interface, text, application

  Description automatically generatedThe format of an ARP request is shown below:
* Network traffic can be increased by a lot due to ARP requests being sent out and then waiting for a response. Therefore, to reduce network traffic, ARP software extracts and saves the information from a response so that it can be used for subsequent packets. The information is only saved temporarily, ARP maintains a small table of bindings in memory as a cache, and so before using the network ARP searches the cache.
* However, ARP is also prone to exploitation by Hackers. If you can get a rogue server onto a network you can reply to ARP requests, and therefore you can force a client to send requests to your rouge server. This is known as ARP Poisoning (ARP Spoofing).
* Done by a malicious user or Man in the middle (MITM)