Network Hardware

NIC | 3.4.2

A NIC (network interface card) is necessary for a device to connect to the internet. It is typically in the device's hardware. Additionally, **it contains the MAC address** assigned by the manufacturer. If the NIC changes, the MAC address will also be changed.

It is usually connected to a network cable. A wireless NIC or WNIC does this with microwaves.

MAC Addresses | 3.4.2

A MAC (Media Access Control) address is the **unique number** assigned by the manufacturer to any device that **accesses the internet**. It is a method of identifying the device. MAC addresses are **static**.

The first half identifies the manufacturing code of the device: N
The second half is the serial code allocated to the device: D

It is 48 bits long and is identified by:
6 hexadecimal pairs: NN:NN:NN:DD:DD:DD

Types of MAC addresses:

- UAA (Universally administered address)
    - The unique address is given to the physical device by the manufacturer
    - This is rarely changed
- LAA (Locally administered address)
    - This can override the UAA and is assigned by a network administrator or special software
    - May be necessary as:
        - Some systems have strict requirements on MAC addresses and the UAA must be changed
        - Needs to bypass a filter on a router or firewall
        - Bypass network restrictions

LAAs are relatively easy to get however it's risky as it must be a unique address.

IP addresses | 3.4.3

IP (Internet protocol) - a numeric address that uniquely identifies any device on a network so that data can be sent to accordingly.

When a device connects to a private network, a private IP address unique to that network is assigned by a router. This may be the same address as another device on a separate network.

When a router connects to a public network, a public IP assigned by an ISP (internet service provider) is given to the router, and all devices connected to that router share that IP address. This IP is different to every other IP address on the internet.

IPv4 - **32-bit system** (4 groups of 8 bits), not enough unique addresses for every device on the planet, around 4 billion address available (2^32), it is represented by **4 denary numbers** from 0-255 separated by dots: 254.25.28.77
IPv6 - **128-bit system** allowing for billions and billions (2^128) of unique addresses for each person, **eight groups** of **4 hexadecimal** digits separated by colons: A8FB:7A88:FFF0:0FFF:3D21:2085:66FB:F0FA

IPv6 addresses not only allow **more IP addresses** to be used, but due to their formatting they allow **more efficient packet routes**, reduces risk of collision, and has **built-in authentication checks.**

Static vs dynamic IP addresses
IP addresses are digital addresses that uniquely identify devices connected to a network. There are two types of IP addresses: static and dynamic. The main difference between them is that static addresses don't change, and dynamic addresses are temporary and change overtime.

A static IP address is a fixed address that is assigned to a device and does not change. It is typically used for servers, printers or other devices that need to have a consistent address on the internet. They are fully traceable and are typically very expensive to maintain as the device must always be running.

On the other hand, a dynamic IP address is assigned to a device temporarily by a service provider or a router. This IP address changes overtime and is recycled for use by other devices. They're usually used for personal devices like laptops, smartphones, and gaming consoles. Dynamic IP addresses are much easier to manage than static addresses; they don't require any configuration and the provider assigns the next available address. On top of this, they're more secure and the device has greater privacy.

IP addresses can be public or private. Private IP addresses are used for private networks, typically LAN. Public addresses are used when connecting globally or the public internet and must all be unique. Private IP addresses usually have a limited set of Ip addresses that can be used

Private IP addresses can be reused between different networks and are assigned by a router. Public IP addresses are all unique and are assigned by the ISP.

Everytime a device logs onto the internet, it requests a temporary IP address from a **Dynamic Host Configuration Protocol (DHCP)**. This can also be done by a router. It selects an IP address from a pool when a computer requests one as routers can act as simple DHCP servers.

Routers | 3.4.4

Routers are network devices that direct data packets to their destinations. They allow data to be transmitted to different networks converting data from one network to a different protocol that another network understands.

When handling data packets, the router looks at the IP address and MAC address of the destination and sends the packet to the right switch to be sent to the correct network. Every computer in one network shares a part of their IP addresses which is how the router knows which switch to send data to.

Routers can also act as proxy servers to protect devices from network traffic.

Routers can have an internal DNS (domain name server) and DHCP (Dynamic host configuration protocol)

DHCP is a network protocol that manages a collection of unique IP addresses and assigns them to devices when they connect to a network. This is how routers assign IP addresses.

All computers under the same network are connected to a network switch. All devices connected to the same switch share a part of their IP addresses, allowing routers to send packets to the correct switch.

(picture on the left is an example of a network switch where every device on a network is connected to its switch)