3.4 Network hardware

3.4.1 Network interface card (NIC)

A **network interface card (NIC)** is needed to allow a device to connect to a network (such as the internet). It is usually part of the device hardware and contains the **Media Access Control (MAC)** address generated at the manufacturing stage.

Wireless network interface cards/controllers (WNICs) are the same as NICs in that they are used to connect devices to the internet or other networks. However, they use wireless connectivity utilising an antenna to communicate with networks via microwaves. They would normally plug into the USB port or be part of an internal integrated circuit.

3.4.2 Media Access Control (MAC)

A MAC address is made up of 48 bits which are shown as six groups of hexadecimal digits with the general format:

$$\underbrace{\text{NN – NN – NN}}_{\text{manufacturer's code}} \text{ – } \underbrace{\text{DD – DD – DD}}_{\text{device serial number}}$$

For example, 00 – 1C – B3 – 4F – 25 – FF where the first six hex digits identify the device as made by, for example, Apple and the second set of six hex digits are the serial number of the device itself (this is unique). If the NIC card is replaced, the MAC address will also change.

Types of MAC address

It should finally be pointed out that there are two types of MAC address: the **Universally Administered MAC Address (UAA)** and the **Locally Administered MAC Address (LAA)**.

The UAA is by far the most common type of MAC address and this is the one set by the manufacturer at the factory. It is rare for a user to want to change this MAC address.

However, there are some occasions when a user or organisation wishes to change their MAC address. This is a relatively easy task to carry out, but it will cause big problems if the changed address isn't unique.

There are a few reasons why the MAC address needs to be changed using LAA:

- certain software used on mainframe systems need all the MAC addresses of devices to fall into a strict format; because of this, it may be necessary to change the MAC address of some devices to ensure they follow the correct format
- it may be necessary to bypass a MAC address filter on a router or a firewall; only MAC addresses with a certain format are allowed through, otherwise the devices will be blocked if their MAC address doesn't adhere to the correct format
- to get past certain types of network restrictions it may be necessary to emulate unrestricted MAC addresses; hence it may require the MAC address to be changed on certain devices connected to the network.

3.4.3 Internet protocol (IP) address

When a device connects to a private network, a router assigns a private IP address to it. That IP address is unique on that network, but might be the same as an IP address on a separate network. However, when a router connects to the internet it is given a unique public IP address. This is usually supplied by the internet service provider (ISP). No other device on the internet has the same public IP address. All the devices connected to that router have the same public IP address as the router but each have their own different private IP addresses on that network. Because the operation of the internet is based on a set of protocols (rules), it is necessary to supply an IP address. Protocols define the rules that must be agreed by senders and receivers of data communicating through the internet.

There are two versions of IP: IPv4 and IPv6. IPv4 is based on 32 bits and the address is written as four groups of eight bits (shown in denary format); for example,

254.25.28.77

Because the use of only 32 bits considerably reduces the potential number of devices and routers used on the internet at any one time, a newer version called IPv6 is now used. This uses 128-bit addresses that take the form of eight groups of hex digits; for example,

A8FB:7A88:FFF0:0FFF:3D21:2085:66FB:F0FA

Link

For more on packet routes see Section 2.1.1.

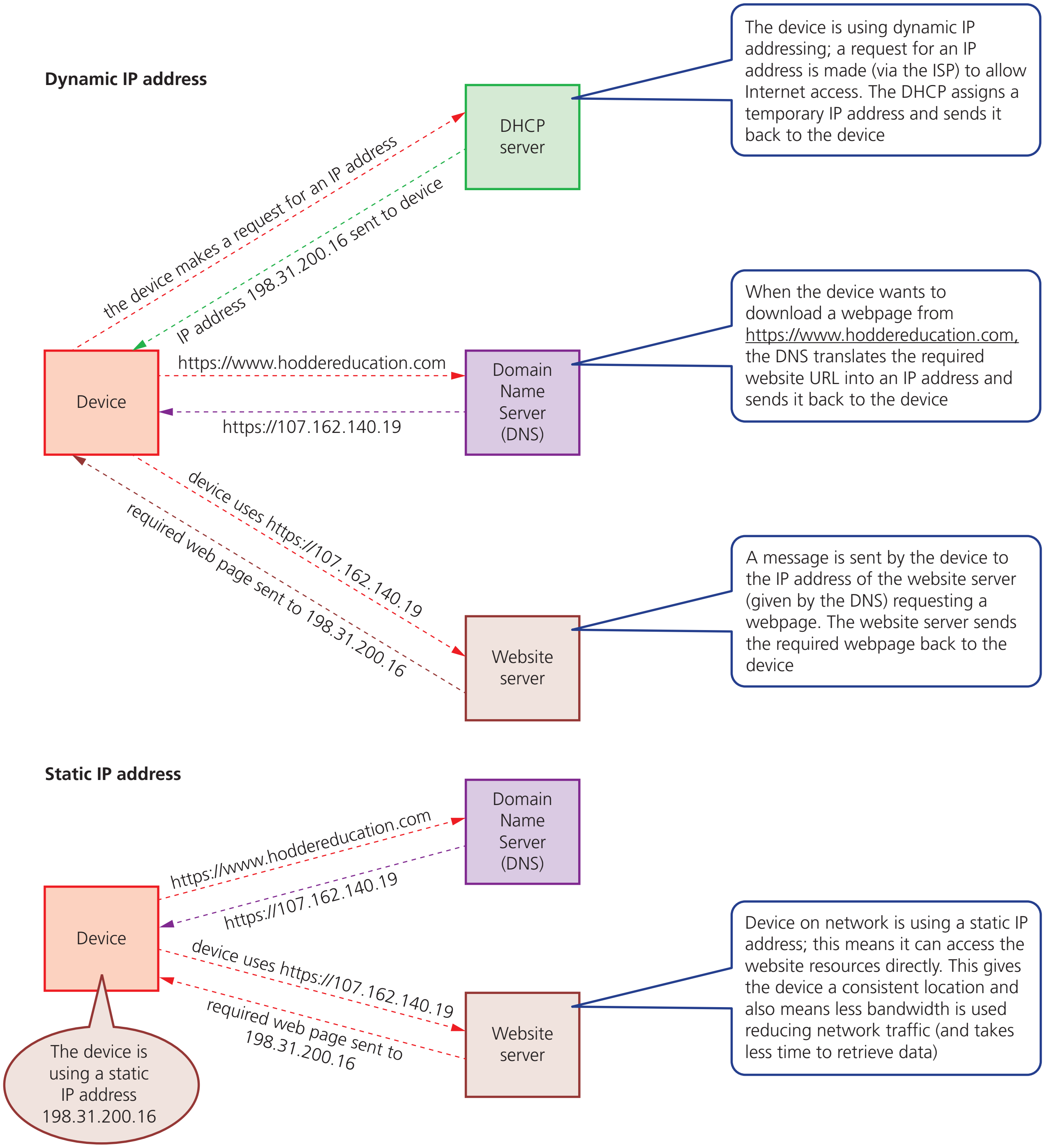
Note the use of colons (:) and hexadecimal numbering. IPv6 has been designed to allow the internet to grow in terms of the number of hosts and potential increase in the amount of data traffic. The main advantages of IPv6 compared to IPv4 are:

- removes the risk of IP address collisions
- has built-in authentication checks
- allows for more efficient packet routes.

Table 3.13 compares the features of MAC addresses and IP addresses:

▼ **Table 3.13** MAC addresses and IP addresses

MAC addresses	IP addresses
identifies the physical address of a device on the network	identifies the global address on the internet
unique for device on the network	may not necessarily be unique
assigned by the manufacturer of the device and is part of the NIC	dynamic IP addresses are assigned by ISP using DHCP each time the device connects to the internet (see later)
they can be universal or local	dynamic IP addresses change every time a device connects to the internet; static IP addresses don't change
when a packet of data is sent and received, the MAC address is used to identify the sender's and recipient's devices	used in routing operations as they specifically identify where the device is connected to the internet
use 48 bits	use either 32 bits (IPv4) or 128 bits (IPv6)
can be UAA or LAA	can be static or dynamic


Dynamic IP address
DHCP server
the device makes a request for an IP address
IP address 198.31.200.16 sent to device
Device
https://www.hoddereducation.com
https://107.162.140.19
Domain Name Server (DNS)
device uses https://107.162.140.19
required web page sent to 198.31.200.16
Website server
Static IP address
Domain Name Server (DNS)
https://www.hoddereducation.com
https://107.162.140.19
Device
device uses https://107.162.140.19
required web page sent to 198.31.200.16
Website server
The device is using a static IP address 198.31.200.16

The device is using dynamic IP addressing; a request for an IP address is made (via the ISP) to allow Internet access. The DHCP assigns a temporary IP address and sends it back to the device

When the device wants to download a webpage from https://www.hoddereducation.com, the DNS translates the required website URL into an IP address and sends it back to the device

A message is sent by the device to the IP address of the website server (given by the DNS) requesting a webpage. The website server sends the required webpage back to the device

Device on network is using a static IP address; this means it can access the website resources directly. This gives the device a consistent location and also means less bandwidth is used reducing network traffic (and takes less time to retrieve data)

▲ **Figure 3.71** Comparison of dynamic and static IP addressing

Static and dynamic IP addresses

IP addresses can be either **static** (don't change) or **dynamic** (change every time a device connects to the internet).

Static

Static IP addresses are permanently assigned to a device by the internet service provider (ISP); they don't change each time a device logs onto the internet. Static IP addresses are usually assigned to:

- remote servers which are hosting a website
- an online database
- a File Transfer Protocol (FTP) server. FTP servers are used when files need to be transferred to various computers throughout the network.

Dynamic

Dynamic IP addresses are assigned by the ISP each time a device logs onto the internet. This is done using **Dynamic Host Configuration Protocol (DHCP)**. A computer on the internet, configured as a DHCP server, is used by the ISP to automatically assign an IP address to a device. As the name suggests, a dynamic IP address could be different every time a device connects to the internet.

Table 3.14 compares static and dynamic IP addresses:

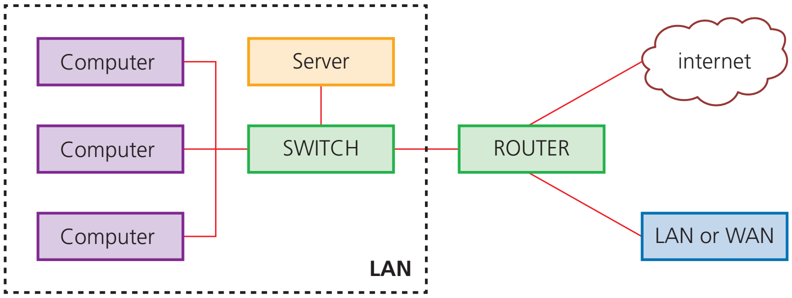
▼ **Table 3.14** Dynamic and static IP addresses

Dynamic IP addresses	Static IP addresses
greater privacy since they change each time a user logs on	since static IP addresses don't change, they allow each device to be fully traceable
dynamic IP addresses can be an issue when using, for example, VoIP since this type of addressing is less reliable as it can disconnect and change the IP address causing the VoIP connection to fail	allow for faster upload and download speeds (see Figure 3.71)
	more expensive to maintain since the device must be constantly running so that information is always available

Figure 3.71 shows the sequence of events when either a dynamic IP address or static IP address is assigned to a device using the internet. The diagram shows how a device contacts web servers that are also connected to the internet. A DHCP server supplies a dynamic IP address to the device, a DNS server looks up the domain name of the desired website into an IP address and a website server contains the web pages of the desired website.

3.4.4 Routers

Routers enable data packets to be routed between different networks, for example, to join a LAN to a WAN. The router takes data transmitted in one format from a network (which is using a particular protocol) and converts the data to a protocol and format understood by another network, thereby allowing them to communicate. A router would typically have an internet cable plugged into it and several cables connecting to computers and other devices on the LAN.



▲ **Figure 3.72** Router flow diagram

Broadband routers sit behind a firewall. The firewall protects the computers on a network. The router's main function is to transmit internet and transmission protocols between two networks and also allow private networks to be connected together.

Routers inspect the data package sent to it from any computer on any of the networks connected to it. Since every computer on the same network has the same part of an internet protocol (IP) address, the router is able to send the data packet to the appropriate switch, and the data will then be delivered to the correct device using the MAC destination address. If the MAC address doesn't match any device connected to the switch, it passes on to another switch on the same network until the appropriate device is found. Routers can be wired or wireless devices.

Activity 3.8

1 Explain each of the following terms:
   a Network interface card (NIC)
   b MAC address
   c IP address
   d Router
   e DHCP server.

2 a Give two features of dynamic IP addresses.
   b Give two features of static IP addresses.
   c Explain why we need both types of IP address.

3 Describe three differences between MAC addresses and IP addresses.

Extension

For those students considering the study of this subject at A Level, the following section gives some insight into further study of computer hardware and wireless networks.

Topic 1: Computer ports

Input and output devices are connected to a computer via ports. The interaction of the ports with connected input and output is controlled by the control unit. Here we will summarise some of the more common types of ports found on modern computers:

USB ports

The **Universal Serial Bus (USB)** is an **asynchronous serial** data transmission method. It has quickly become the standard method for transferring data between a computer and a number of devices. Essentially, the USB cable consists of:

- a 4-wired shielded cable
- 2 of the wires are used for power and the earth
- 2 of the wires are used in the data transmission.

When a device is plugged into a computer, using one of the USB ports, the computer:

- automatically detects that a device is present (this is due to a small change in the voltage level on the data signal wires in the cable)
- the device is automatically recognised, and the appropriate device driver is loaded up so that computer and device can communicate effectively
- if a new device is detected, the computer will look for the device driver which matches the device; if this is not available, the user is prompted to download the appropriate software.

Even though the USB system has become the industrial standard, there are still a number of benefits (✓) and drawbacks (X) to using this system:

✓	X
devices plugged into the computer are automatically detected; device drivers are automatically loaded up	the present transmission rate is limited to less than 500 megabits per second
the connectors can only fit one way; this prevents incorrect connections being made	the maximum cable length is presently about 5 metres
USB has become the industry standard; this means that considerable support is available to users	the older USB standard (1.1) may not still be supported in the near future
several different data transmission rates are supported	
newer USB standards are backward compatible with older USB standards	

High-definition Multimedia Interface (HDMI)

High-definition Multimedia Interface (HDMI) ports allow output (both audio and visual) from a computer to an HDMI-enabled monitor or other device. It will support high definition signals (enhanced or standard). HDMI was introduced as a digital replacement for the older VGA analogue system. Modern HD (high definition) televisions have the following features which are making VGA a redundant technology:

- they use a widescreen format (16:9 aspect ratio)
- the screens use a greater number of pixels (typically 1920 ×1080)
- the screens have a faster refresh rate (e.g. 120 Hz or 120 frames a second)
- the range of colours is extremely large (some companies claim up to 4 million different colour variations!).

This all means that modern HD televisions require more data and this data has to be received at a much faster rate than with older televisions (e.g. 10 gigabits per second). HDMI increases the bandwidth making it possible to supply the necessary data to produce high quality sound and visual effects.

Topic 2: Wired and wireless networks

Wireless

Wi-Fi and Bluetooth

Both Wi-Fi and Bluetooth offer wireless communication between devices. They both use electromagnetic radiation as the carrier of data transmission.

Bluetooth sends and receives radio waves in a band of 79 different frequencies (known as channels). These are all centred on a 2.45 GHz frequency. Devices using Bluetooth automatically detect and connect to each other; but they don't interfere with other devices since each communicating pair uses a different channel (from the 79 options).

When a device wants to communicate, it picks one of the 79 channels at random. If the channel is already being used, it randomly picks another channel. This is known as spread-spectrum frequency hopping. To further minimise the risks of interference with other devices, the communication pairs constantly change the frequencies (channels) they are using (several times a second). Bluetooth creates a secure wireless personal area network (WPAN) based on key encryption.

Essentially, Bluetooth is useful:

- when transferring data between two or more devices which are very close together (<30 metres distance)
- when the speed of data transmission is not critical
- for low bandwidth applications (e.g. when sending music files from a mobile phone to a headset).

Wi-Fi is best suited to operating full-scale networks since it offers much faster data transfer rates, better range and better security than Bluetooth. A Wi-Fi-enabled device (such as a computer or smartphone) can access the internet wirelessly at any wireless access point (WAP) or 'hot spot' up to 100 metres away.

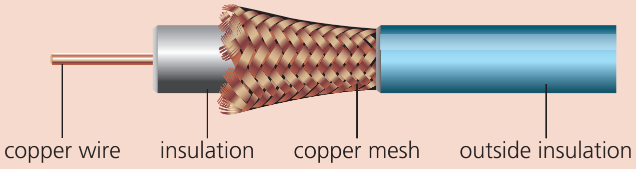
As mentioned above, wireless connectivity uses electromagnetic radiation: radio waves, microwaves or infrared. The scale of frequency and wavelength of magnetic radiation can be seen in the table below:

	Radio waves	Microwaves	Infrared	Visible light	Ultra violet	X-rays	Gamma rays
Wave length (m)	102	10^{-1}	10^{-5}	10^{-5}	10^{-7}	10^{-9}	10^{-11}
←							
Frequency (Hz)	3 MHz	3 GHz	300 GHz	30 THz	3 PHz	300 PHz	30 EHz

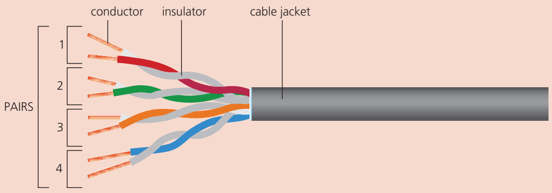
Wired

There are three main types of cable used in wired networks:

- twisted pair
- coaxial
- fibre optic.



Coaxial cable



Twisted pair cable

Fibre optic cable

Wired versus wireless

When deciding whether a network should use wired or wireless connectivity, the following factors should be considered:

Wireless networking	Wired networking
it is easier to expand the networks and it isn't necessary to connect the devices using cables	using cables produces a more reliable and stable network; wireless connectivity is often subject to interference
this gives devices increased mobility provided they are within range of the WAPs	data transfer rates tend to be faster and there won't be any 'dead spots'
there is an increased chance of interference from external sources	setting up cabled networks tends to be cheaper overall in spite of the need to buy and install cable
data is less secure than with wired systems; it is easier to intercept radio waves and microwaves than cables; it is essential to protect data transmissions using encryption (e.g. WEP, WPA2)	however, cabled networks lose the ability for devices to be mobile; they must be close enough to allow for cable connections
the data transmission rate is still slower than for cabled networks although it continues to improve	having lots of wires can lead to a number of hazards such as tripping hazards, overheating of connections (leading to potential fire risk) and disconnection of cables during routine office cleaning
it is possible for signals to be stopped by thick walls (e.g. in old houses) and there may be areas of variable signal strength leading to 'drop out'	

In this chapter, you have learnt about:

- ✔ the role of a CPU/microprocessor
- ✔ von Neumann architecture
- ✔ the Fetch–Decode–Execute cycle
- ✔ the function of a cache, (system) clock and multi-core core CPUs
- ✔ instruction sets
- ✔ embedded systems
- ✔ the operation of a number of input devices
- ✔ the operation of a number of output devices
- ✔ the use of sensors in a number of control and monitoring applications
- ✔ primary storage
- ✔ secondary storage (magnetic, optical and solid state)
- ✔ virtual memories
- ✔ cloud storage
- ✔ network interface card (NIC)
- ✔ MAC and IP addressing
- ✔ routers in networks.