Tiverton High School Year 11
J277 GCSE Computer Science
Knowledge Organiser / Recap
Part 6: Protocols, Addressing and the Internet

Unit 1.3.2 Data Packets and IP Addressing

Data is transmitted in short bursts called **data packets**. When transmitting large files, they are split into **sequences** of packets. Each packet travels across one or more **communication links** in a network

Data packets must be sent and recieved in a very **precise** way to ensure successful communication between devices.
A **network protocol** is **a set of rules or conventions which control the communication between devices on a network**.
Protocols provide **strict definitions** about the **structure** of data packets and **how** they should be sent.
They also determine what to do when data packets have been **lost** or **corrupted** during transmission.

When recieving data, protocol software **puts the data packets back together in the correct order** to reconstruct the original data that was sent. The protocol **automatically detects errors** and **lost-packets**, requesting them to be re-sent.

Structure of a data packet

IP address of the **sender**	**IP address** of **destination** device	**Sequence number**	**Total packets**	**Payload** actual data that you want to send	**Checksum** to detect errors
124.63.0.5	182.45.0.60	3	10	Your password has been accepted.	38

Every device on a network has a unique **Internet Protocol address** (**IP address**). which is **32 bits long**.

IP v4 addresses must consist of **4 numbers**, separated by a **dot**. Each part uses **8-bits**, allowing values between **0** and **255**.
Example IP v4 addresses: `168.0.192.1` `255.70.12.65`

IPv6 addresses use 128 bits, which means many more IP addresses are possible than when using 32 bit IPv4 addresses.
An **IP v6 address** is represented uaing **eight groups of four hexadecimal digits**, each group representing **16 bits**.
The groups are separated by **colon** symbols **:**
Example IP v6 address: `1805:0ca8:85f3:0000:0000:8b5a:0420:3741`

IP addresses can be changed, but **every device on a network must have a different IP address**.
If two devices have the **same** IP address it will be unclear which of them is meant to recieve each particular data packet.

Unit 1.3.2 MAC Addressing

MAC address means **Media Access Contol address**.

A MAC address **uniquely identifies a device on a network** by identifying the **network adapter** hardware that the device is using.
It is a **unique code** which is built into the **Network Interface Controller** (**NIC**) hardware.

The MAC address is used to make sure that **devices never get mixed up** during network communications.

Each MAC address is made up of **48 binary digits**.
`000101001101001011001110100101101101101001011001`

...but they are usually written in **hexadecimal** (easier for humans to read and write down.
`14-D2-CE-96-DA-59`

MAC addresses cannot ever be changed because **they are built into the hardware of each device when it is manufactured**.

Because each MAC address is **unique**, no two hardware devices in the world have the **same** MAC address.
Criminals can be traced using MAC addresses - the MAC addresses proves which device was used when breaking the law.

Units 1.3.1 and 1.3.2 The internet

"**Internet**" means "**Inter-Networking**" – **communication BETWEEN networks**.

The Internet is a way of **connecting networks together**. It joins Local Area Networks and Wide Area Networks from many different countries. To connect a network to the internet, most people connect through an **Internet Service Provider** (**ISP**).
An ISP provides a **gateway router** for your network to connect to.

Packets can travel across the Internet using **different routes** to get to their destination. **Backbone internet routers** receive data packets. Each router examines the destination IP address that shows where the packet is trying to get to. The router then decides which communications link to use and sends the packet on the next stage of it's journey, towards it's intended destination.

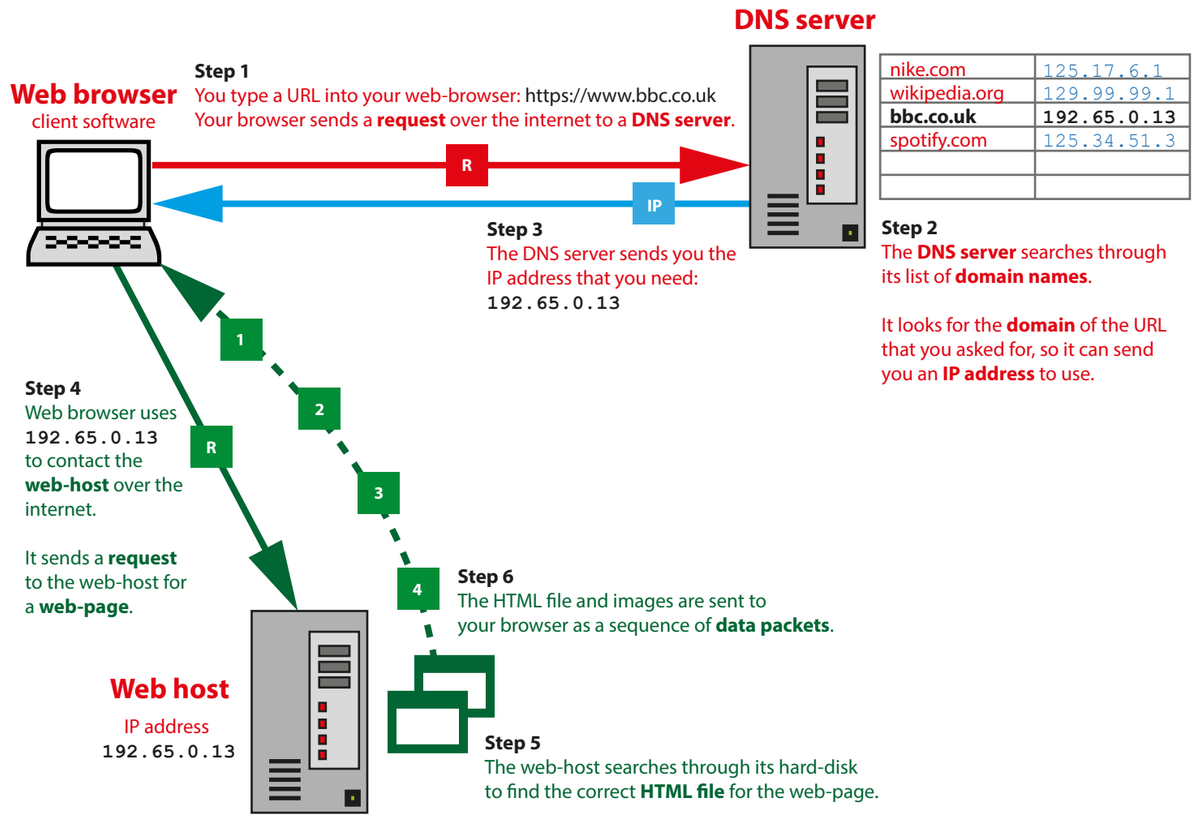
This **packet switching** process needs to happen really quickly so that packets are not kept waiting. If a queue of packets waiting to be routed fills up, the router may no longer cope with the traffic, leading to slow network performance.

The internet uses **redundant links** to allow data packets to take **different** routes to their destination as efficiently as possible.
Because of the redundant links, it is very difficult to **censor** parts of the internet - there are many routes through between devices.

When communicating across the Internet, a **collection** of inter-related protocols needs to be used, called the **protocol stack**.
The protocol stack defines all of the different processes and protocols that will be used to send and receive data.

The internet uses the **TCP (Transmission Control Protocol)** and **IP (Internet Protocol)** to split data into packets and route it.

Unit 1.3.1 Domain Name System (DNS)



The numbers in an IP address can be difficult for people to remember e.g. `255.70.12.65`

We can use **text aliases** instead which are equivalent to the numbers. These are called **domain names**. e.g. `bbc.co.uk`

Special computer servers on the Internet called the **Domain Name System (DNS)** **translate text domain names to IP addresses**.