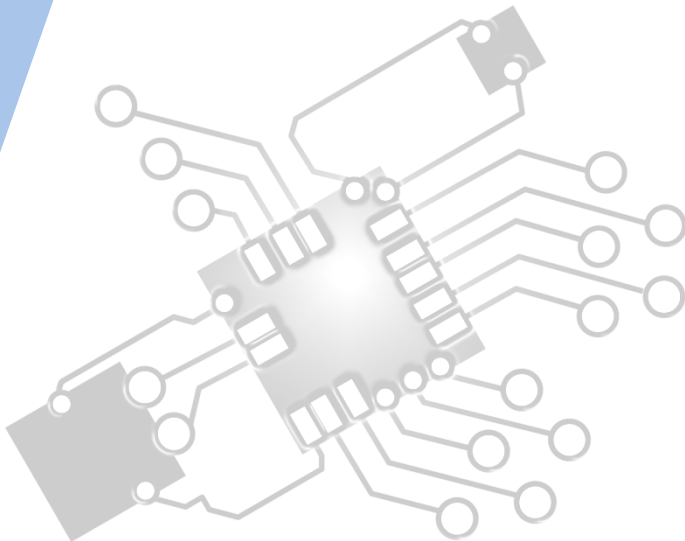# *Network fundamentals*

IB Computer Science

Content developed by
Dartford Grammar School
Computer Science Department

HL Topics 1-7, D1-4

1: System design

2: Computer Organisation

3: Networks

4: Computational thinking

5: Abstract data structures

6: Resource management

7: Control

D: OOP

HL & SL 3 Overview

Network fundamentals

3.1.1 Identify different types of networks

3.1.2 Outline the importance of standards in the construction of networks

3.1.3 Describe how communication over networks is broken down into different layers

3.1.4 Identify the technologies required to provide a VPN

3.1.5 Evaluate the use of a VPN

Data transmission

3.1.6 Define the terms: protocol, data packet

3.1.7 Explain why protocols are necessary

3.1.8 Explain why the speed of data transmission across a network can vary

3.1.9 Explain why compression of data is often necessary when transmitting across a network

3.1.10 Outline the characteristics of different transmission media

3.1.11 Explain how data is transmitted by packet switching

Wireless networking

3.1.12 Outline the advantages and disadvantages of wireless networks

3.1.13 Describe the hardware and software components of a wireless network

3.1.14 Describe the characteristics of wireless networks

3.1.15 Describe the different methods of network security

3.1.16 Evaluate the advantages and disadvantages of each method of network security
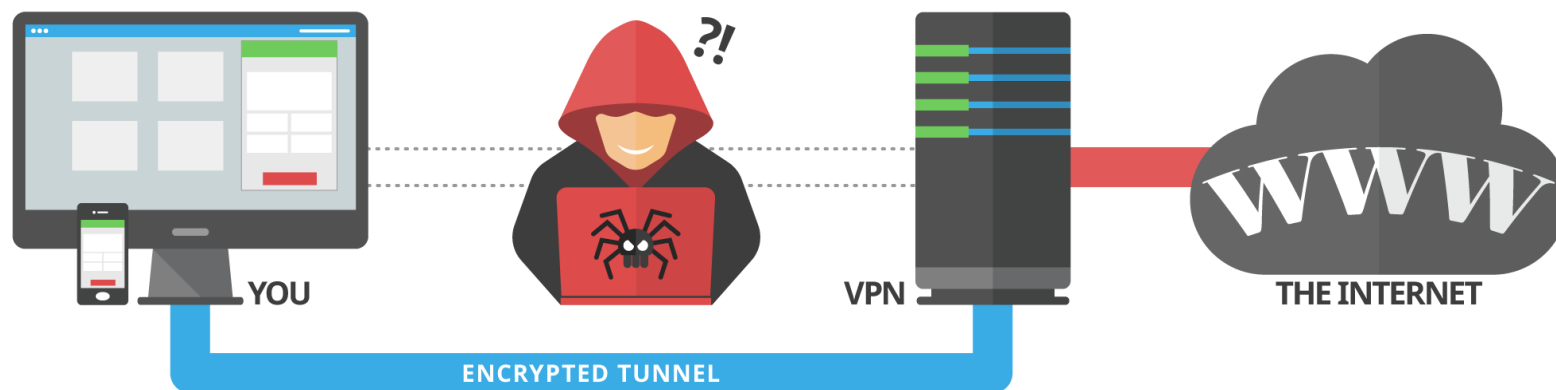
Topic 3.1.4

Identify the **technologies** required to provide a **VPN**

VPN = Virtual Private Network

- It uses the internet to allow people to **log into a network remotely** and access its resources, but **encrypts** the connection to thwart eavesdroppers.

- If your company sets you up with a VPN, you can access your corporate intranet, file servers or email from home or a coffee shop – **just as if you were using it in your office**.

- This makes VPN a popular way to support **remote workers**, especially in fields where **privacy** is paramount, such as health care.

VPN
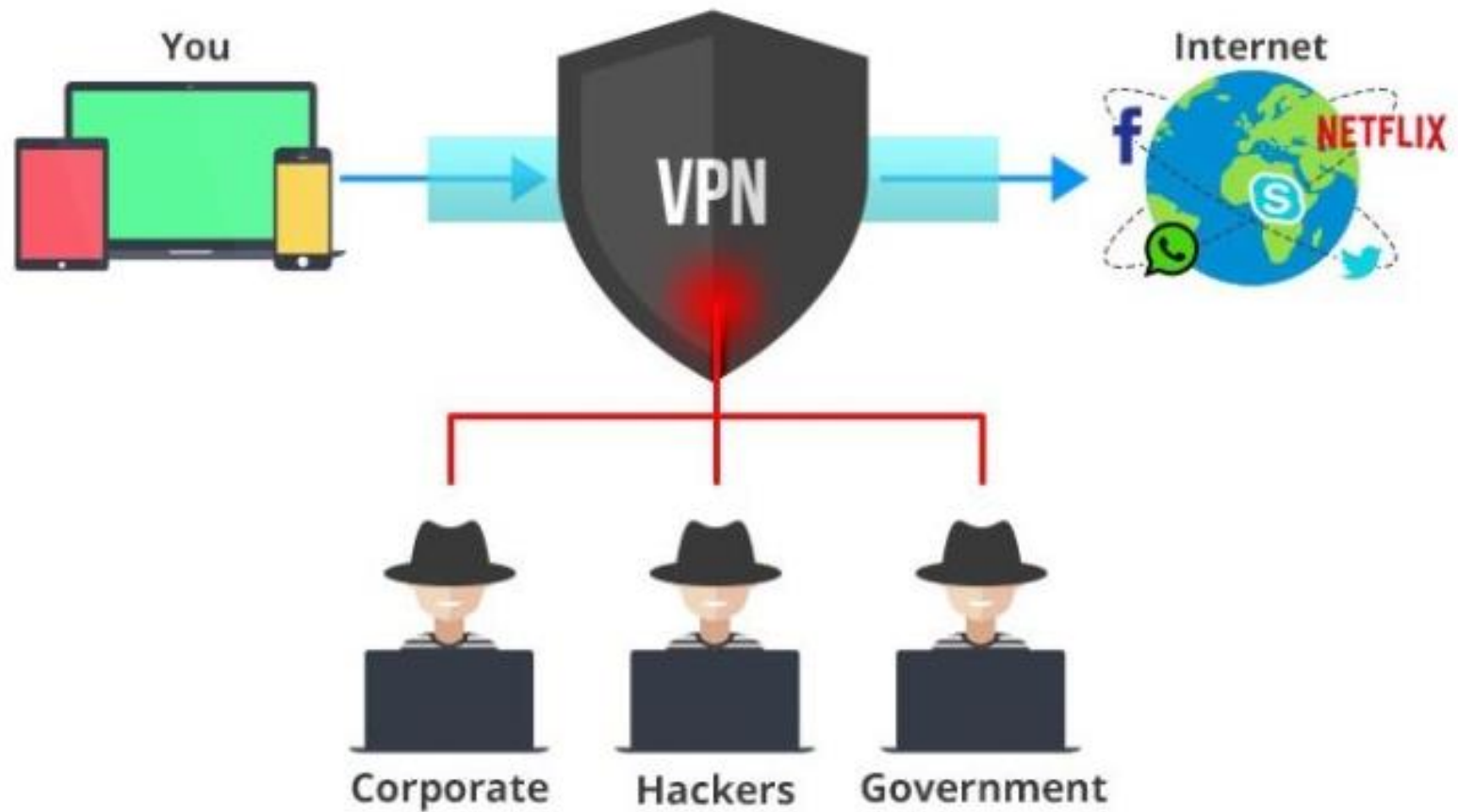
Two fundamental VPN technologies

- **Encryption** is the process of encoding data so that only a computer with the right decoder will be able to read and use it.

- **Tunnelling** involves establishing and maintaining a logical network connection (that may contain intermediate hops). On this connection, packets constructed in a specific VPN protocol format are encapsulated within some other base or carrier protocol, then transmitted between VPN client and server, and finally de-encapsulated on the receiving side

In a VPN, the computers at each end of the tunnel encrypt the data entering the tunnel and decrypt it at the other end.

Tunnelling
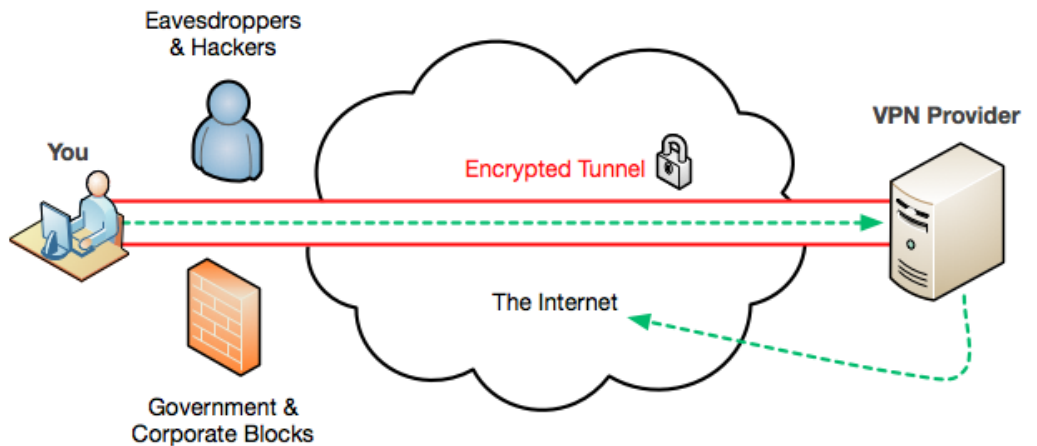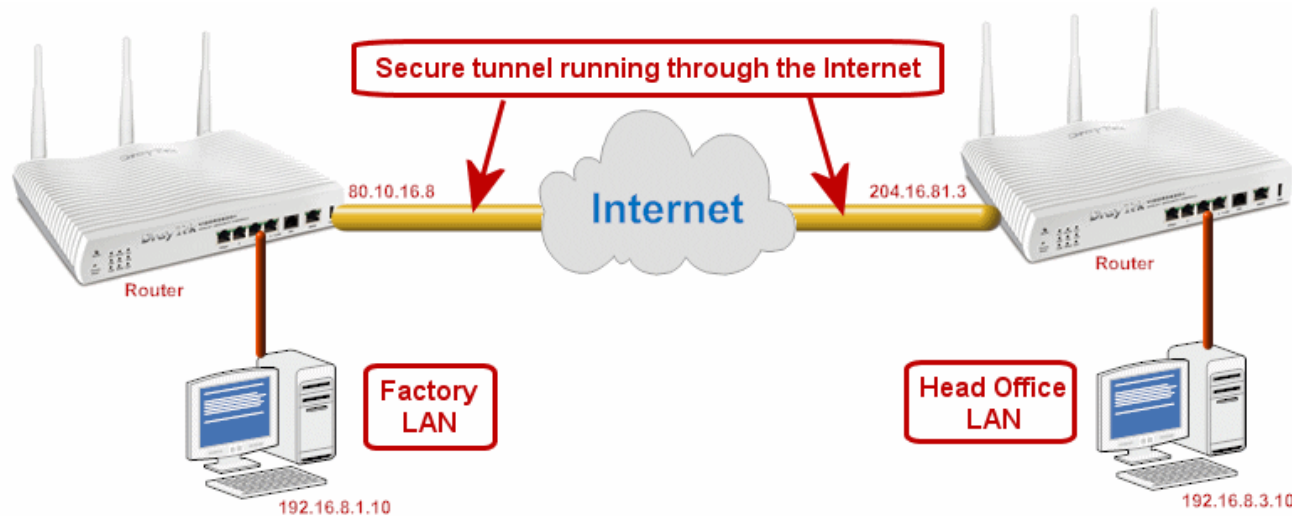
Video: How VPNs work

YouTube link: https://youtu.be/_wQTRMBAvzg

Basic checklist for VPN

- ✓ A LAN that is connected to the internet.
- ✓ One computer outside of the LAN that is also connected to the internet.
- ✓ VPN client and server running on the lone machine and the original LAN
- ✓ Internet connection