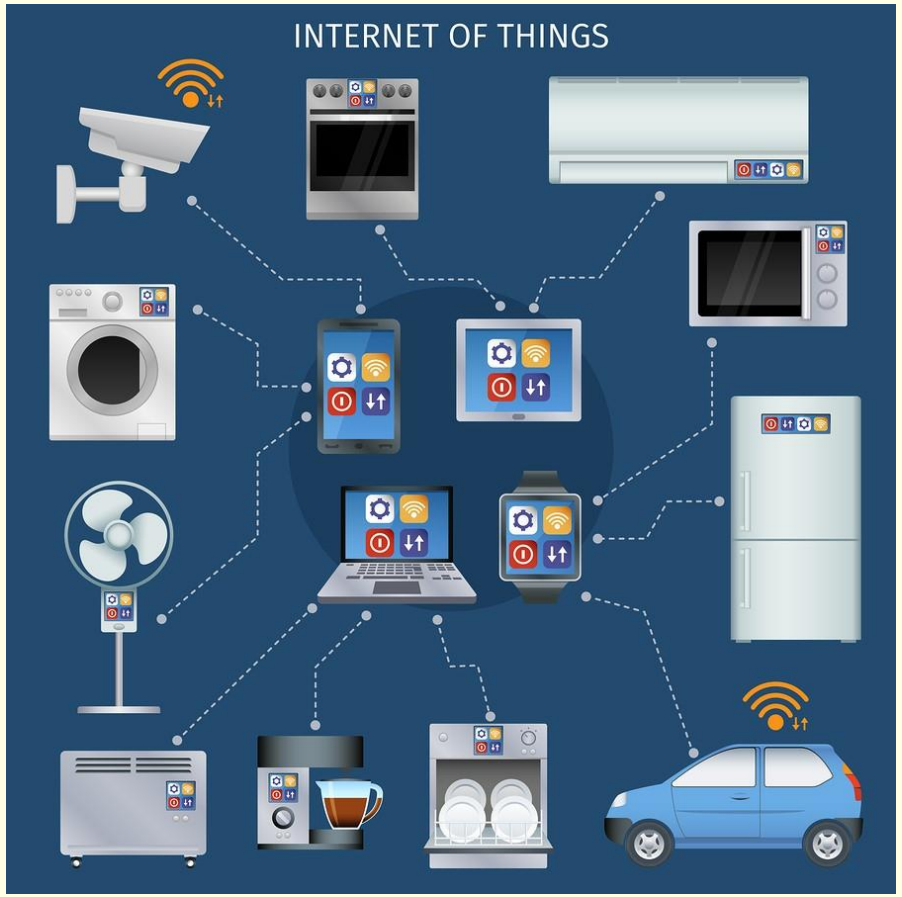
Learning Aims

In this lesson you will learn to:

- Define what is meant by the term ‘Internet of Things’ (IoT)
- Explain the role of embedded systems in the IoT
- Outline security and privacy issues associated with the IoT
- Explain why power is an important consideration for many IoT devices.

Internet of Things (IoT)

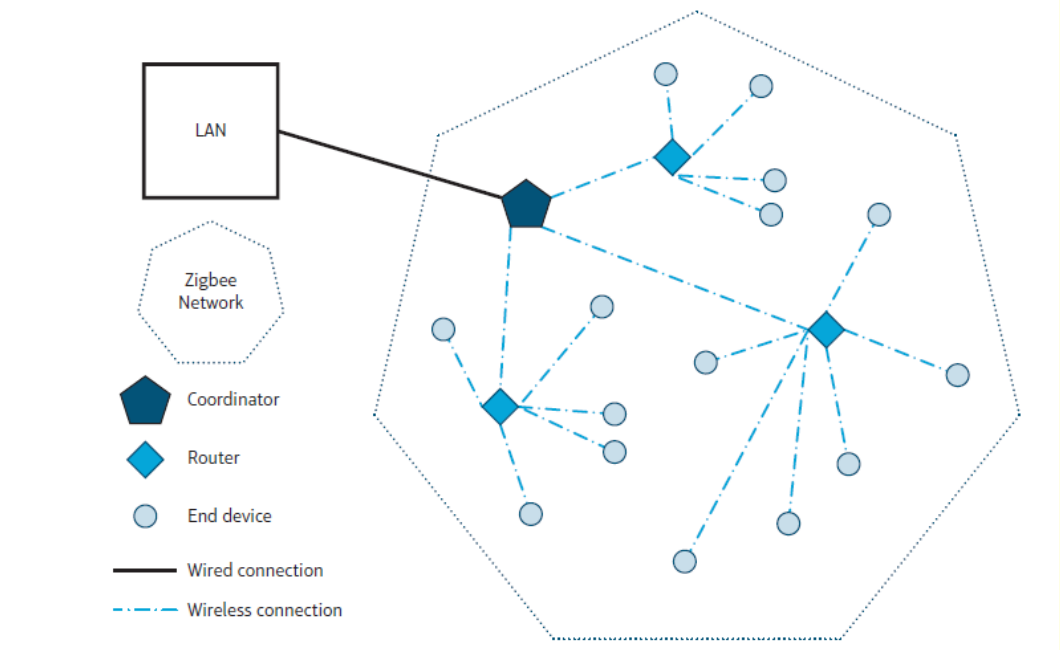


The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data

The Internet of Things

The **Internet of Things** (IoT) is the name given to the everyday devices which are increasingly being given network connectivity.

Hundreds of devices can now be connected to a network, both in public spaces and in your own home.



Embedded systems and the IoT

In order for devices to be connected to the IoT, they need to be made "smart".

- Any device that can be connected in this way will contain an embedded system. Without it, connection to the IoT is impossible.
- Many of these devices can be found in our homes, but there are commercial applications as well.
- Most IoT devices are low-powered, have reduced-memory and a slow-processor and are designed to accomplish a single task.
- For the data they generate to be useful, it must be passed on to a platform that can store and analyse it.
- Power consumption is an important design consideration when developing IoT devices.
- Many IoT devices are battery powered, which means a balance between power use and performance needs to be struck in order to maximise battery life.

Security

The more devices we have in our homes, offices and public spaces, the more **attack vectors** hackers have to access networks and data.

Security concerns include:

- Packet sniffing – accessing unsecured wireless traffic to potentially obtain sensitive data
- Hijacking and ransomware
- Home invasion – compromised IoT home security systems could make it easy for people to break in
- Vehicle theft – keyless entry and other such technologies might make it easier for cars to be stolen
- Counterfeit devices containing security back doors.

attack vectors - is a pathway or method used by a hacker to illegally access a network

Privacy

An additional concern that people have about IoT devices is personal privacy.

Increasingly devices are listening to us, monitoring the environment in and around our homes and tracking our location using our smartphones.

This leads to concerns about who is able to see this data, what is done with the data that is collected and what other actions are being carried out based on this data.

Issues of personal data privacy are covered in detail in a future lesson.

IoT and security issues

- Horizon clp.bbcrewind.co.uk/284e2724458fb8930970fcdf89c471da Go to 50:56 in the video to find out about IoT and security issues.

Privacy vs Safety

Who?
Government agencies & police

Criminals can access your data

Devices controlled remotely

If regularly updated not an issue.

Monthly software upgrades will be needed to fix safety issues without having to recall vehicles.

Cars and medical devices, are now online and could go wrong, or be made to go wrong, and harm people.

Issue of liability. Legislation must be created to ensure that if a manufacturer creates a device that harms people, then they are liable.

Large devices, such as cars, are made from components produced by many different manufacturers using many different types of software is another problem that could make these devices more difficult to patch.