# Wireless Technology

In today's hi-tech world, wireless connections are extremely common. Let's see how four of them work: **WiFi**, **Bluetooth, cellular phones** and **NFC**.

## 1. WiFi (invented in 1997)

WiFi uses the same principal as other wireless devices – it uses **radio waves** to send signals between devices. The radio frequencies are completely different from those used for walkie-talkies, car radios or cell phones. For example, your car radio receives frequencies in the Kilohertz (KHz) and Megahertz (MHz) range (AM and FM stations), whereas WiFi transmits and receives data in the Gigahertz (GHz) range. Since each technology uses different frequency ranges, there is no possibility of them interfering with each other.

One **Hertz** is a frequency of **one** wave per second.
One **KHz** is a frequency of one **thousand** waves per second.
One **MHz** is a frequency of one **million** waves per second.
One **GHz** is a frequency of one **billion** waves per second.

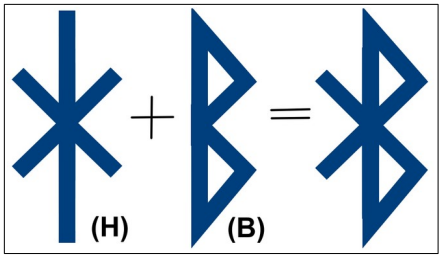
The higher the frequency, the greater the volume of data transmitted. Many WiFi routers use a frequency of **2.4 GHz**. A microwave oven uses the frequency 2.45 GHz to heat food, so if you have an old or faulty microwave oven, you could experience problems with your WiFi signal while using your oven. Modern routers use a frequency of **5 GHz**. The two possible WiFi frequencies are split into multiple channels to prevent traffic problems. These channels use slightly different frequencies and they allow multiple routers to communicate in the same area without causing problems. An analogy is driving on the highway – if there was only one lane, there would be traffic problems, but with many lanes, traffic flows more easily. The frequency channels are set up automatically when you connect to your router. A 2.4 Ghz frequency device has about 12 channels, the exact number of channels differs in each country, for example: USA – 11 channels, Europe – 13 channels, Brazil – 13 channels. A 5 GHz device can use 30 channels.

When you access the internet on your device, it converts your information to binary code (0s and 1s). These 0s and 1s are converted into radio waves by the WiFi chip in your device. These radio waves travel through the air and are received by your WiFi router. The router then re-converts the radio waves to binary code again and passes it to the internet using a cable (usually copper or fiber optic). Most routers operate at 54 Mbps (megabits per second), meaning that when your router transmits binary data, 54 million 0s and 1s are sent or received in 1 second. That would be about 13,000 sheets of A4 paper full of text. The high frequency radio waves easily pass through walls and furniture. The high speed and high capacity are what allow you to watch Netflix on your TV, phone, tablet or laptop from anywhere in your house.

## 2. Bluetooth (invented in 1994)

### Why is it called "Bluetooth"?

Harald Bluetooth was the King of Denmark in the 10th century. He had a dead tooth, which was a blue/grey colour, and so he was given the nickname "Bluetooth". During his reign, he successfully united Denmark and Norway. So, in the same way that Harald Bluetooth united two countries, Bluetooth technology unites two devices. The symbol for Bluetooth technology is a combination of two Nordic rune symbols for 'H' and 'B' (from "**H**arald **B**luetooth") called "Hagalaz" and "Berkana"; see image below.




Bluetooth is a wireless technology which connects mouses and keyboards to computers, phones to cars, smartwatches to smartphones and headphones to tablets. Bluetooth devices communicate directly with each other, instead of sending data through "man-in-the-middle" devices such as a router. This direct communication keeps power usage extremely low and so extends battery life.

Bluetooth devices communicate using radio waves in the frequency range **2.4 GHz to 2.483 GHz**. This is a range, agreed internationally, for the use of industrial, scientific and medical devices. Many devices, that you may already have, also use this radio-frequency range, such as baby monitors, garage-door controls and cordless phones.

Sometimes Bluetooth and WiFi connections can interfere with each other. When these two technologies are used together, you can sometimes have problems. Both connections could be using a similar radio frequency range to transfer data. The more congested the frequency range, the more connection problems you might have. Symptoms could be an unreliable WiFi connection or a Bluetooth device repeatedly disconnecting. To fix this, you can:

- Disconnect and reconnect your WiFi – on reconnection, your router will search for a channel with little or no traffic.
- Re-pair all your Bluetooth devices. This will remove old connections which could be causing interference.
- Replace your Bluetooth device with a newer version. Most modern Bluetooth devices are designed to "hop" (jump) along the channels to alleviate interference issues. This is called "frequency hopping".
- Reduce the distance between your device and your router to get a stronger signal.

Bluetooth devices must always be "paired" and this procedure results in the two devices "trusting" each other and exchanging data in a secure way, using encryption. Bluetooth is a short-range technology, typically just a few centimeters or meters. There are two types of Bluetooth connection – automatic pairing and authenticated pairing. With automatic pairing, two Bluetooth devices which are close automatically connect and can then exchange data. When this happens, you usually hear some phrases, spoken in a Chinese accent, like "*The Bluetooth device is ready to pair*". Other devices, like your car entertainment system, require authentication before connection is made. Usually you need to enter a code or password into one of the devices in order to allow pairing between them. Some devices are designed to connect to only one other device, like headphones, while others are designed to connect to multiple devices, like computers.

## 3. Cellular Phones (invented in 1973)

| | |
|---|---|
| USA: | cell phone |
| UK: | mobile |
| France: | téléphone portable |
| Sweden: | mobiltelefon |
| Spain: | teléfono móvil |
| Brazil: | celular |
| Germany: | handy |
| South Africa: | selfoon |


With around 10 billion cell phones in the world (2024), they have become a universal and indispensable tool for modern life. With a cell phone, you can talk to anybody in any country at any time.

A cell phone is essentially a two-way radio, consisting of a radio transmitter and a radio receiver. When you chat with somebody on your cell phone, your phone converts your voice into an electrical signal, which is then transmitted via radio waves to the nearest cell tower. The network of cell towers then relays the radio wave to your friend's cell phone, which converts it to an electrical signal and then back to sound again. In the United States, there are four cell phone operators – AT&T, Verizon, Sprint and T-Mobile. In Brazil, there are also four – Claro, Oi, Tim and Vivo.

**3G vs 4G vs 5G**

On highways and in small towns, operators usually use 4G in the 700 MHz range since lower frequencies deliver a greater coverage area, which reduces the number of antennas needed to cover a region. However, the capacity for concurrent users is less and speeds are slower than 5G.

5G uses higher radio frequencies than 4G, so it can carry more information, but it is easily blocked by physical objects such as trees and buildings. In order to overcome these difficulties, 5G uses many more antennas than for 4G. The transmitters for 5G are much smaller, so can be placed on buildings and street posts (4G transmitters use huge masts). 5G technology can support up to 1,000 times as many devices per meter than 4G.The biggest advantage of 5G is speed, being approximately 100 times faster than 4G.

| Technology | Time to download a high quality movie |
|---|---|
| 3G | 1 day |
| 4G | 30 minutes |
| 5G | 4 seconds |

5G will eventually enable the "Internet of Things" (IoT) and will allow any device in your home to connect to the internet (TV, fridge, microwave, printer, security cameras, doors, windows, etc.) allowing you to control them remotely. Transport will also be revolutionized, with car-to-car communication and autonomous vehicles.

**Potential Risks and Concerns**

Long-term exposure to RF radiation (associated with Wi-Fi, Bluetooth and mobile phones) has raised concerns about potential effects on the human body, but large-scale studies have not shown any conclusive evidence of harm. RF radiation does not directly affect DNA, unlike ionizing radiation such as X-rays and gamma rays. Health agencies such as WHO, the CDC and the FDA state that there is no evidence of harm from RF exposure experienced from common, everyday devices. Hearing aids use BLE (Bluetooth Low Energy) and there is no evidence linking Bluetooth use in hearing aids to any health issues. In fact, Bluetooth hearing aids are considered to be one of the safest wireless devices.

Even though current evidence doesn't show any dangers, you can reduce exposure to RF radiation by:

- Using speakerphone to limit phone contact with your head;
- Avoiding carrying your phone in your pocket for long periods;
- Keeping routers away from bedrooms;
- Limiting screen time for kids.

**4. NFC (Near Field Communication)**

NFC is a very short-range radio conversation between two devices that can communicate only when they are within about 4cm of each other.

Typical uses include:

- Payments (Apple Pay, Google Pay): your phone emulates a bank card;
- Travel passes: your card or phone talks to a gate reader;
- Pairing devices: like touching a phone to a speaker to connect via Bluetooth;
- Access control: ID badges or tags to unlock doors or turnstiles;
- Phone to phone file sharing.

NFC is based on RFID (Radio Frequency Identification) technology, operating at 13.56 MHz. One device generates a tiny oscillating magnetic field (using an antenna coil) and if another NFC device enters the field, the two coils couple electromagnetically, allowing them to transfer data or even power wirelessly. They can only exchange small amounts of data, typically up to 424 kbit/s, which is sufficient for payments, ticketing, or pairing devices. Because the range is so short, NFC is very difficult to hack, unlike Bluetooth or Wi-Fi, but encryption is still used for security.

Active mode: Both devices generate their own RF fields and take turns transmitting. This is used for phone-to-phone file sharing.

Passive mode: One device (like a contactless card) has no power source of its own. It's powered by the field from the other device (like a phone or payment terminal). This is used in "tap-to-pay" cards (in Portuguese, "aproximação") and travel passes.