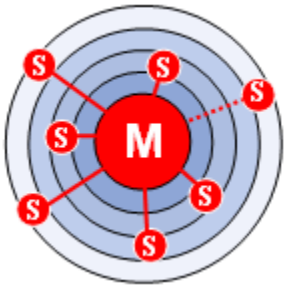
Bluetooth - How it works

How Bluetooth works

The Bluetooth standard, like WiFi, uses the FHSS technique (*Frequency-Hopping Spread Spectrum*), which involves splitting the frequency band of 2.402-2.480 GHz into 79 channels (called *hops*) each 1MHz wide, then transmitting the signal using a sequence of channels known to both the sending and receiving stations.
Thus, by switching channels as often as 1600 times a second, the Bluetooth standard can avoid interference with other radio signals.

Communication principle

The Bluetooth standard is based upon a master/slave operational mode. The term "**piconet**" is used to refer to the network formed by one device and all devices found within its range. Up to 10 piconets can coexist within a single coverage area. A master can be simultaneously connected to as many as 7 active slave devices (255 when in *parked* mode). Devices in a piconet have a logical address of 3 bits, for a maximum of 8 devices. Devices in *parked* mode are synchronized, but do not have their own physical address in the piconet.



In reality, at a given moment, the master device can only be connected to a single slave at once. Therefore, it quickly switches between slaves in order to make it seem as if it is simultaneously connected to all the slave devices.
Bluetooth enables two piconets to be linked to one another in order to form a wider network, called a "**scatternet**", using certain devices which act as a bridge between the two piconets.

Establishing connections

Establishing a connection between two Bluetooth devices follows a relatively complicated procedure meant to ensure a certain amount of security, as follows:

- Passive mode
- Inquiry: Finding access points
- Paging: Synchronizing with access points
- Access point service discovery
- Creating a channel with access point
- Pairing using PIN (security)
- Using the network

During normal use, a device operates in "**passive mode**", meaning that it is listening to the network.
Establishing a connection begins with a phase called "**inquiry**", during which the master device sends an inquiry request to all devices found within its range, called *access points*. All devices which receive the query reply with their address.
The master device chooses an address and synchronizes with the access point using a technique called **paging**, which primarily involves synchronizing its clock and frequency with the access point.
A link with the access point is then established, allowing the master device to enter an access point **service discovery** phase, using a protocol called *SDP*(*Service Discovery Protocol*).
At the end of this service discovery phase, the master device is ready to created a **communication channel** with the access point, using the protocol *L2CAP*.
Depending on the service's needs, an additional channel, called *RFCOMM* and operating over the *L2CAP* channel, may be established in order to provide a virtual serial port. Indeed, some applications have been designed to connect to a standard port, independent of the hardware used. For example, certain highway navigation programs have been designed to connect to any GPS Bluetooth device (GPS stands for *Global Positioning System*, a satellite-based geolocation system for finding the geographic coordinates of a mobile device or vehicle).

The access point may include a security mechanism called **pairing**, which restricts access to authorized users only, in order to give the piconet a certain measure of protection. Pairing is done with an encryption key commonly known as a "PIN"

(*PIN* stands for *Personal Information Number*). To do so, the access point sends a pairing request to the master device. Most of the time, this may prompt the user to enter the access point's PIN. If the PIN received is correct, the connection is made.
In secure mode, the PIN will be sent encrypted, using a second key, in order to prevent the signal from being compromised.

When the pairing becomes active, the master device is free to use the communication channel thereby established.

Bluetooth profiles

The Bluetooth standard defines a certain number of application profiles (called *Bluetooth profiles*) in order to define which kinds of services are offered by a Bluetooth device. Thus, each device can support multiple profiles. Here is a list of the main Bluetooth profiles:

- Advanced Audio Distribution Profile (A2DP)
- Audio Video Remote Control Profile (AVRCP)
- Basic Imaging Profile (BIP)
- Basic Printing Profile (BPP)
- Cordless Telephony Profile (CTP)
- Dial-up Networking Profile (DUNP)
- Fax Profile (FAX)
- File Transfer Profile (FTP)
- Generic Access Profile (GAP)
- Generic Object Exchange Profile (GOEP)
- Hardcopy Cable Replacement Profile (HCRP)
- Hands-Free Profile (HFP)
- Human Interface Device Profile (HID)
- Headset Profile (HSP)
- Intercom Profile (IP)
- LAN Access Profile (LAP)
- Object Push Profile (OPP)
- Personal Area Networking Profile (PAN)
- SIM Access Profile (SAP)
- Service Discovery Application Profile (SDAP)

- Synchronization Profile (SP): used to synchronize the device with a personal information manager (or *PIM* for short).
- Serial Port Profile (SPP)

Source: http://en.kioskea.net/contents/69-bluetooth-how-it-works