

An introduction to Bluetooth Technology



Table of Contents:

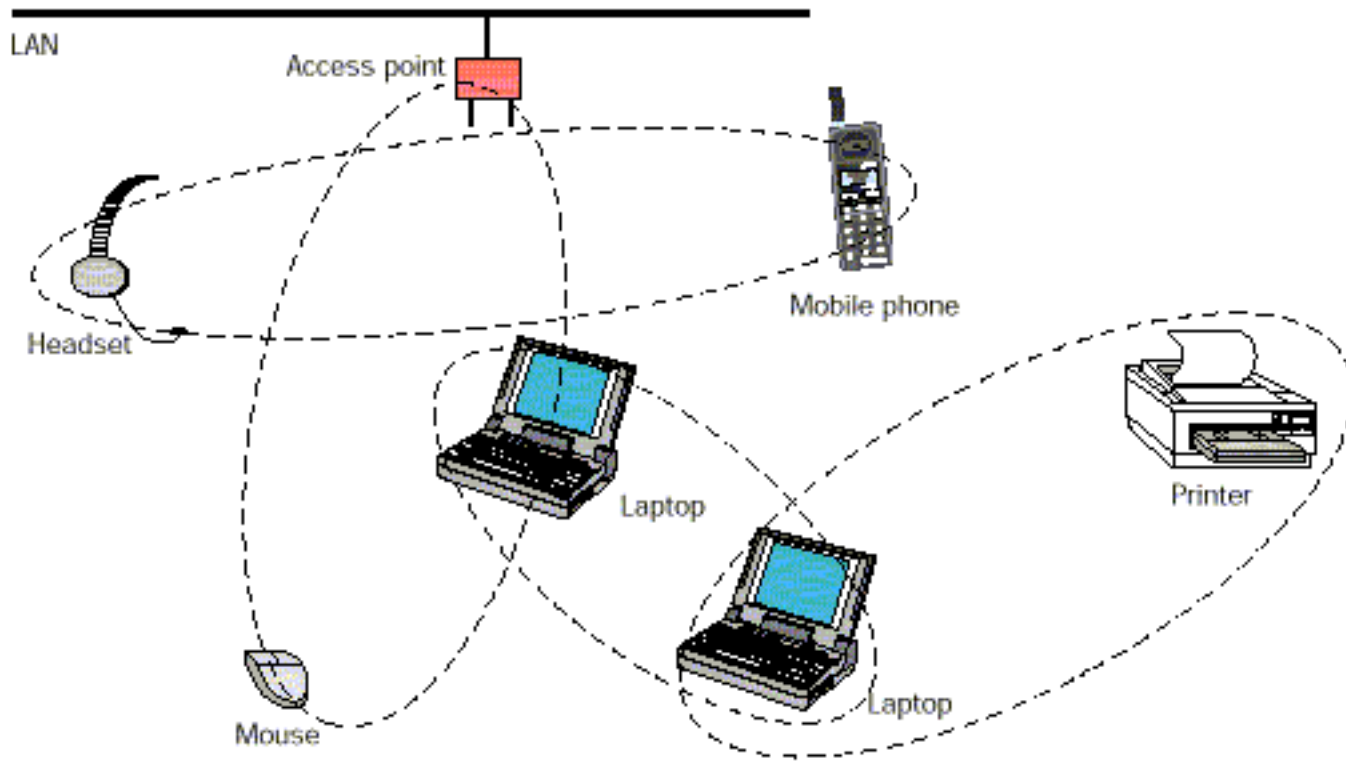
- 1. A little introduction to Bluetooth
- 2. The history of Bluetooth
- 3. How does it work?
- 4. Examples of Bluetooth devices
- 5. Security
- 6. Advertising via Bluetooth
- 7. Bibliography & Useful Links

1. What is Bluetooth?

Bluetooth is a wireless protocol for exchanging data over short distances from fixed and mobile devices, creating **personal area networks (PANs)**.

Bluetooth provides a way to connect and exchange information between devices such as mobile phones, telephones, laptops, personal computers, printers, Global Positioning System (GPS) receivers, digital cameras, and video game consoles through a secure, globally unlicensed Industrial, Scientific, and Medical (ISM) 2.4 GHz short-range radio frequency bandwidth.

1. What is Bluetooth?

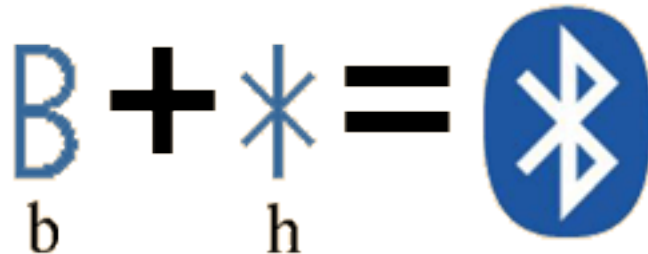


Bluetooth makes possible for these devices to communicate with each other when they are in range.

2. The History of Bluetooth

The word "Bluetooth" is an Anglicized version of the name of a tenth-century king, Harald Blaatand, king of Denmark and Norway, who united dissonant Scandinavian tribes into a single kingdom.

The Bluetooth logo design merges the Germanic runes analogous to the modern Latin letters H and B: (for Harald Bluetooth) (Hagall) and (Berkanan) merged together, forming a bind rune.



2. The History of Bluetooth

Founded in September 1998 by Ericsson, the **Bluetooth SIG** (Bluetooth Special Interest Group) is a unification of the leaders in the telecommunications, computing, network, industrial automation, and Automotive industries.

Today, the Bluetooth SIG is responsible for encouraging and supporting research and development in Bluetooth technology.

The Bluetooth SIG includes promoter member companies Microsoft, Sony Ericsson, IBM, Intel, Agere, Motorola, Nokia, and Toshiba, plus thousands of Associate and Adopter member companies.

2. The History of Bluetooth

Several Bluetooth specification versions have been released since Bluetooth technology was introduced in 1998.

BT 1.0/1.0B: First version of Bluetooth, not close to being interoperable, bluetooth Hardware Device Address's were sent during communication so there was no anonymity.

BT 1.1: Supports non-encrypted channels and fixes many 1.0 errors, can measure communicating signal strength, IEEE 802.15.1-2002 standard created for 1.1.

2. The History of Bluetooth

Many new Bluetooth devices, like the latest cell phones, are being sold with the newer Bluetooth specification version 1.2.

BT 1.2: Adds Adaptive Frequency Hopping, Higher practical speeds, better voice quality links, Host controller interface access to timing info.

BT 2.0: introducing of Enhanced Data Rate (3.0 Mbps), 100 meter range, even lower power usage, better error handling, IEEE 802.15.1-2005 standard created for 2.0.

2. The History of Bluetooth

Bluetooth version 2.0 + EDR also provides enhanced **multiple-connectivity**: users will be able to more efficiently run multiple Bluetooth devices at the same time.

For example, users will have the ability to synchronize a Bluetooth enabled computer with a Bluetooth PDA, and at the same time they can listen to music using a pair of Bluetooth wireless headphones.

Here is a listing of the main enhancements/features you will find with Bluetooth Specification Version 2.0 + EDR:

- Enhanced data rate of up to 3 Mbps
- Broadcast/multicast support
- Distributed media-access control protocols

3. How does it work?

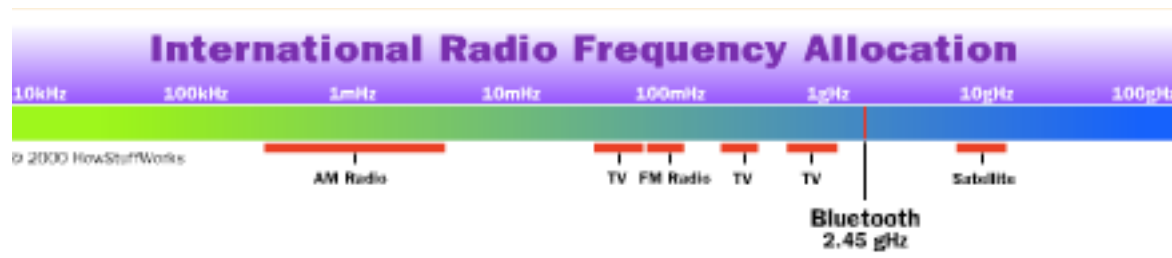
Bluetooth is a standard and communications protocol primarily designed for low power consumption, with a **short range (1 meter, 10 meters, 100 meters)** based on low-cost transceiver microchips in each device.

Bluetooth uses a radio technology called **frequency-hopping spread spectrum**, which chops up the data being sent and transmits chunks of it on up to 79 frequencies. In its basic mode, the modulation is Gaussian frequency-shift keying (GFSK). It can achieve a gross **data rate of 1-3 Mb/s**.

3. How does it work?

Bluetooth **transmits its information at a frequency of 2.45 GHz**. The frequency is located on the ISM operating band which is reserved for Industrial, Scientific, and Medical unlicensed signals.

Bluetooth signals could possibly interfere with other devices on the same band if they were more powerful. But **the signals are only 1 milliwatt** compared to the most powerful devices on the same band capable of transmitting 3 watts.



3. How does it work?

When two or more Bluetooth devices, sharing the same profile(s), come in range with each other, they establish a connection automatically. So, the user does not have to press any buttons or set anything up. Once the Bluetooth devices are all connected, a network is created.

Bluetooth devices create a Personal-area Network (PAN), or commonly called a **piconet**.

Bluetooth **piconets are designed to link up to eight different devices**. A piconet can be as small as a two foot connection between a keyboard and computer, or it can encompass several devices over an entire room.

4. Examples of Bluetooth devices



An example of a Bluetooth PAN: it's possible to connect Phones, Laptops, PDAs and many more devices all together.

4. Examples of Bluetooth devices

Bluetooth Headphone



Bluetooth Dongle



Bluetooth Remote



Bluetooth Keyboard

4. Examples of Bluetooth devices



← Sync your Mobile with Laptop

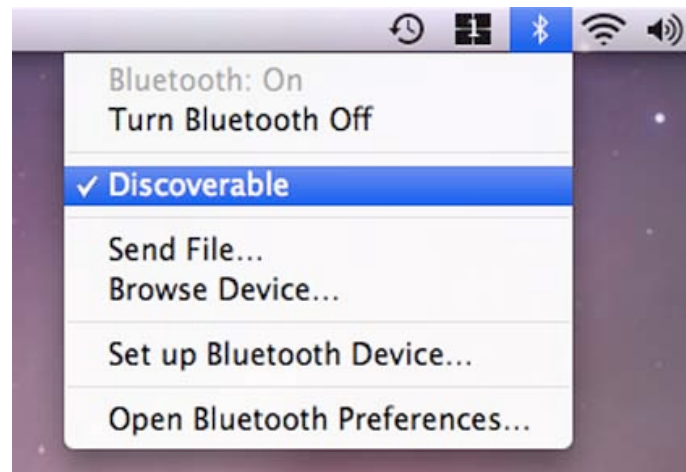
↓ Use your Mobile as a Remote



5. Security

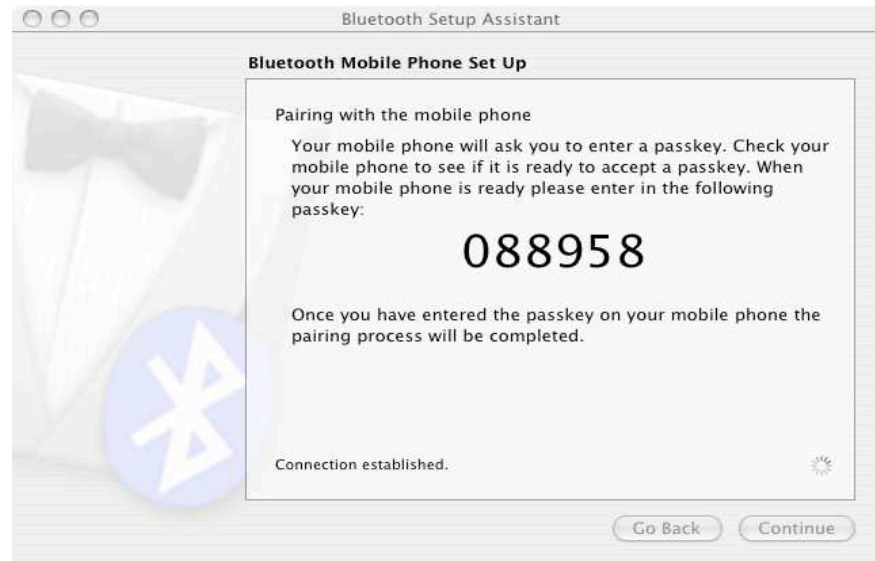
Bluetooth implements confidentiality, authentication and key derivation with custom algorithms based on the SAFER+ block cipher.

When a Bluetooth device is **discoverable**, it is very easy to scan for it using a PC and download private data. Setting Bluetooth to a "**non-discoverable**" mode prevents BT devices from appearing on the list during a BT device search process.



5. Security

In Bluetooth, key generation is generally based on a **Bluetooth PIN**, which must be entered into both devices. This procedure may be modified if one of the devices has a **fixed PIN**, e.g. for headsets or similar devices with a restricted user interface. During pairing, an initialization key or master key is generated, using an algorithm called E22.



5. Security

The **Bluejacking** is a technique that allows phone users to send business cards anonymously to one another using Bluetooth technology. **Bluejacking does NOT involve any alterations to your phone's data.** These business cards usually consist of some clever message or joke. Bluejackers are simply looking for a reaction from the recipient. To ignore bluejackers, simply reject the business card, or if you want to avoid them entirely, set your phone to non-discoverable mode.

Bluesnarfing refers to a hacker who has gained access to data, which is stored on a Bluetooth enabled phone. **Bluesnarfing allows the hacker to make phone calls,** send and receive text messages, read and write phonebook contacts, eavesdrop on phone conversations, and connect to the Internet.

5. Security

Bluebugging refers to a skilled hacker who has accessed a cell phone's commands using Bluetooth technology without the owner's permission or knowledge.

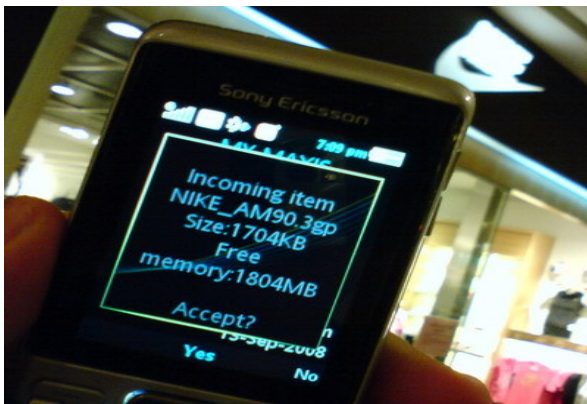
Bluebugging also allows the hacker to make phone calls, send messages, read and write contacts and calendar events, eavesdrop on phone conversations, and connect to the Internet.

Just like all Bluetooth attacks, the hacker must be within a 100 mt. range. Bluebugging and bluesnarfing are separate security issues, and phones that are vulnerable to one are not necessarily vulnerable to the other.

6. Advertising via Bluetooth

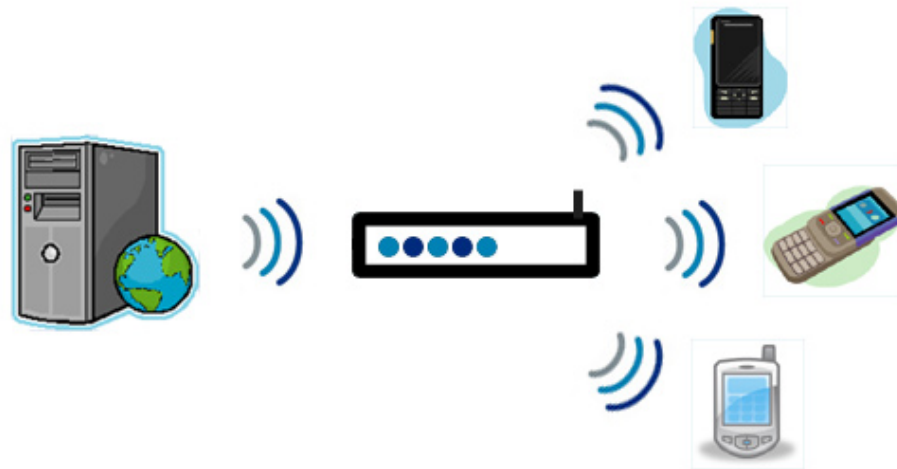
In 2005, a company called Wiremedia has announced that it will begin setting up the network and hardware infrastructure to deliver location-based, advertising and contextual information to cell phones via Bluetooth.

Wiremedia will use its **Bluetooth MediaServer** to distribute these ads. A Bluetooth MediaServer is a pocket-sized caching server that delivers customized content and applications directly to cell phones up to 300-1000 feet away.



6. Advertising via Bluetooth

When attached to billboards, poster sites, retail locations, etc, the Bluetooth **MediaServer will recognize your Bluetooth cell phone and deliver a message or advertisement.** You can expect to receive coupons, video, audio, photos, text messages, mms, sms, java-based applications, etc.



6. Advertising via Bluetooth



6. Advertising via Bluetooth

Advertising to Mobile phones using Bluetooth Marketing tools is one of the new ways to get ahead of your competitors, **Bluetooth Marketing will reduce costs** and increase the return on investment compared to your usual advertising techniques.

Bluetooth ads are made practical by the **growing density of Bluetooth in Western countries**. In all of Western Europe, 35 percent of cell phones will be Bluetooth-enabled by the end of this year.

A lot of people today wonder about whether Bluetooth Marketing, and proximity marketing in general is legal, as people claim it can be considered as **SPAM** and annoying!!!

7. Bibliography & Useful Links

- <http://en.wikipedia.org/wiki/Bluetooth>
- <http://www.bluetomorrow.com/>
- <http://www.ad2hand.co.uk/>
- <http://www.bluetooth.com/bluetooth/>
- <https://www.bluetooth.org/apps/content/>