

# Bluetooth

From Wikipedia, the free encyclopedia

**Bluetooth** is a proprietary open wireless technology standard for exchanging data over short distances (using short-wavelength radio transmissions in the ISM band from 2400–2480 MHz) from fixed and mobile devices, creating personal area networks (PANs) with high levels of security. Created by telecoms vendor Ericsson in 1994,<sup>[1]</sup> it was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization.



Bluetooth is managed by the Bluetooth Special Interest Group, which has more than 15,000 member companies in the areas of telecommunication, computing, networking, and consumer electronics.<sup>[2]</sup> The SIG oversees the development of the specification, manages the qualification program, and protects the trademarks.<sup>[3]</sup> To be marketed as a Bluetooth device, it must be qualified to standards defined by the SIG. A network of patents is required to implement the technology<sup>[citation needed]</sup> and are only licensed to those qualifying devices; thus the protocol, whilst open, may be regarded as proprietary.

## Contents

- 1 Name and logo
- 2 Implementation
  - 2.1 Communication and connection
- 3 Uses
  - 3.1 Bluetooth profiles
  - 3.2 List of applications
  - 3.3 Bluetooth vs. Wi-Fi (IEEE 802.11)
  - 3.4 Devices
- 4 Computer requirements
  - 4.1 Operating system support
- 5 Mobile phone requirements
- 6 Specifications and features
  - 6.1 Bluetooth v1.0 and v1.0B
  - 6.2 Bluetooth v1.1
  - 6.3 Bluetooth v1.2
  - 6.4 Bluetooth v2.0 + EDR
  - 6.5 Bluetooth v2.1 + EDR
  - 6.6 Bluetooth v3.0 + HS
    - 6.6.1 Ultra-wideband
  - 6.7 Bluetooth v4.0
- 7 Technical information
  - 7.1 Bluetooth protocol stack
    - 7.1.1 LMP
    - 7.1.2 AVRCP
    - 7.1.3 L2CAP
    - 7.1.4 SDP
    - 7.1.5 RFCOMM
    - 7.1.6 BNEP
    - 7.1.7 AVCTP
    - 7.1.8 AVDTP
    - 7.1.9 TCS
    - 7.1.10 Adopted protocols
  - 7.2 Baseband error correction
  - 7.3 Setting up connections
  - 7.4 Pairing/Bonding
    - 7.4.1 Motivation
    - 7.4.2 Implementation
    - 7.4.3 Pairing mechanisms
    - 7.4.4 Security Concerns
  - 7.5 Air interface
- 8 Security
  - 8.1 Overview
  - 8.2 Bluejacking

- 8.3 History of security concerns
  - 8.3.1 2001 - 2004
  - 8.3.2 2005
  - 8.3.3 2006
  - 8.3.4 2007
- 9 Health concerns
- 10 Bluetooth Innovation World Cup marketing initiative
- 11 See also
- 12 References
- 13 External links

## Name and logo

The word "Bluetooth" is an anglicised version of the Scandinavian *Blåtand/Blåtann*, the epithet of the tenth-century king Harald I of Denmark and parts of Norway who united dissonant Danish tribes into a single kingdom. The implication is that Bluetooth does the same with communications protocols, uniting them into one universal standard.<sup>[4][5][6]</sup>

The Bluetooth logo is a bind rune merging the Younger Futhark runes ᚺ (Hagall) (  ) and ᚷ (Bjarkan) (  ), Harald's initials.

## Implementation

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 bands (1 MHz each; centered from 2402 to 2480 MHz) in the range 2,400–2,483.5 MHz (allowing for guard bands). This range is in the globally unlicensed Industrial, Scientific and Medical (ISM) 2.4 GHz short-range radio frequency band.

Originally Gaussian frequency-shift keying (GFSK) modulation was the only modulation scheme available; subsequently, since the introduction of Bluetooth 2.0+EDR,  $\pi/4$ -DQPSK and 8DPSK modulation may also be used between compatible devices. Devices functioning with GFSK are said to be operating in basic rate (BR) mode where an instantaneous data rate of 1 Mbit/s is possible. The term Enhanced Data Rate (EDR) is used to describe  $\pi/4$ -DPSK and 8DPSK schemes, each giving 2 and 3 Mbit/s respectively. The combination of these (BR and EDR) modes in Bluetooth radio technology is classified as a "BR/EDR radio".

Bluetooth is a packet-based protocol with a master-slave structure. One master may communicate with up to 7 slaves in a piconet; all devices share the master's clock. Packet exchange is based on the basic clock, defined by the master, which ticks at 312.5  $\mu$ s intervals. Two clock ticks make up a slot of 625  $\mu$ s; two slots make up a slot pair of 1250  $\mu$ s. In the simple case of single-slot packets the master transmits in even slots and receives in odd slots; the slave, conversely, receives in even slots and transmits in odd slots. Packets may be 1, 3 or 5 slots long but in all cases the master transmit will begin in even slots and the slave transmit in odd slots.

Bluetooth provides a secure way to connect and exchange information between devices such as faxes, mobile phones, telephones, laptops, personal computers, printers, Global Positioning System (GPS) receivers, digital cameras, and video game consoles.

## Communication and connection

A master Bluetooth device can communicate with a maximum of seven devices in a piconet (an ad-hoc computer network using Bluetooth technology), though not all devices support this limit. The devices can switch roles, by agreement, and the slave can become the master (for example, a headset initiating a connection to a phone will necessarily begin as master, as initiator of the connection; but may subsequently prefer to be slave).

The Bluetooth Core Specification provides for the connection of two or more piconets to form a scatternet, in which certain devices simultaneously play the master role in one piconet and the slave role in another.

At any given time, data can be transferred between the master and one other device (except for the little-used broadcast mode). The master chooses which slave device to address; typically, it switches rapidly from one device to another in a round-robin fashion. Since it is the master that chooses which slave to address, whereas a slave is (in theory) supposed to listen in each receive slot, being a master is a lighter burden than being a slave. Being a master of seven slaves is possible; being a slave of more than one master is difficult. The specification is vague as to required behaviour in scatternets.

Many USB Bluetooth adapters or "dongles" are available, some of which also include an IrDA adapter. Older (pre-2003) Bluetooth dongles, however, have limited capabilities, offering only the Bluetooth Enumerator and a less-powerful Bluetooth Radio incarnation. Such devices can link computers with Bluetooth with a distance of 100 meters, but they do not offer as many services as modern adapters do.

## Uses

Bluetooth is a standard wire-replacement communications protocol primarily designed for low power consumption, with a short range (power-class-dependent, but effective ranges vary in practice; see table below) based on low-cost transceiver microchips in each device.<sup>[7]</sup> Because the devices use a radio (broadcast) communications system, they do not have to be in visual line of sight of each other, however a *quasi optical* wireless path must be viable.<sup>[2]</sup>

Class	Maximum permitted power		Range (m)
	(mW)	(dBm)	
<b>Class 1</b>	100	20	~100
<b>Class 2</b>	2.5	4	~10
<b>Class 3</b>	1	0	~5

The effective range varies due to propagation conditions, material coverage, production sample variations, antenna configurations and battery conditions. In most cases the effective range of class 2 devices is extended if they connect to a class 1 transceiver, compared to a pure class 2 network. This is accomplished by the higher sensitivity and transmission power of Class 1 devices.<sup>[8]</sup>

Version	Data rate	Maximum application throughput
<b>Version 1.2</b>	1 Mbit/s	0.7 Mbit/s
<b>Version 2.0 + EDR</b>	3 Mbit/s	2.1 Mbit/s
<b>Version 3.0 + HS</b>	See Version 3.0+HS.	
<b>Version 4.0</b>	See Version 4.0LE.	

While the Bluetooth Core Specification does mandate minimums for range, the range of the technology is application specific and is not limited. Manufacturers may tune their implementations to the range needed to support individual use cases.

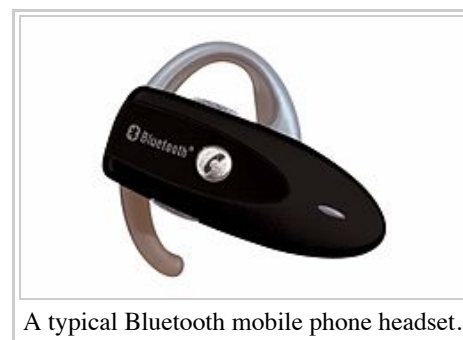
## Bluetooth profiles

*Main article: Bluetooth profile*

To use Bluetooth wireless technology, a device has to be able to interpret certain Bluetooth profiles, which are definitions of possible applications and specify general behaviors that Bluetooth enabled devices use to communicate with other Bluetooth devices. These profiles include settings to parametrize and to control the communication from start. Adherence to profiles saves the time for transmitting the parameters anew before the bi-directional link becomes effective. There are a wide range of Bluetooth profiles that describe many different types of applications or use cases for devices.<sup>[9]</sup>

## List of applications

- Wireless control of and communication between a mobile phone and a handsfree headset. This was one of the earliest applications to become popular.
- Wireless control of and communication between a mobile phone and a Bluetooth compatible car stereo system
- Wireless Bluetooth headset and Intercom.
- Wireless networking between PCs in a confined space and where little bandwidth is required.
- Wireless communication with PC input and output devices, the most common being the mouse, keyboard and printer.
- Transfer of files, contact details, calendar appointments, and reminders between devices with OBEX.
- Replacement of previous wired RS-232 serial communications in test equipment, GPS receivers, medical equipment, bar code scanners, and traffic control devices.
- For controls where infrared was often used.
- For low bandwidth applications where higher USB bandwidth is not required and cable-free connection desired.
- Sending small advertisements from Bluetooth-enabled advertising hoardings to other, discoverable, Bluetooth devices.<sup>[10]</sup>
- Wireless bridge between two Industrial Ethernet (e.g., PROFINET) networks.
- Three seventh-generation game consoles, Nintendo's Wii<sup>[11]</sup> and Sony's PlayStation 3 and PSP Go, use Bluetooth for their respective wireless controllers.
- Dial-up internet access on personal computers or PDAs using a data-capable mobile phone as a wireless modem.
- Short range transmission of health sensor data from medical devices to mobile phone, set-top box or dedicated telehealth



A typical Bluetooth mobile phone headset.

devices.<sup>[12]</sup>

- Allowing a DECT phone to ring and answer calls on behalf of a nearby cell phone
- Real-time location systems (RTLS), are used to track and identify the location of objects in real-time using “Nodes” or “tags” attached to, or embedded in the objects tracked, and “Readers” that receive and process the wireless signals from these tags to determine their locations<sup>[13]</sup>
- Personal security application on mobile phones for prevention of theft or loss of items. The protected item has a Bluetooth marker (e.g. a tag) that is in constant communication with the phone. If the connection is broken (the marker is out of range of the phone) then an alarm is raised. This can also be used as a man overboard alarm. A product using this technology has been available since 2009.<sup>[14]</sup>

## Bluetooth vs. Wi-Fi (IEEE 802.11)

Bluetooth and Wi-Fi (the brand name for products using IEEE 802.11 standards) have some similar applications: setting up networks, printing, or transferring files. Wi-Fi is intended as a replacement for cabling for general local area network access in work areas. This category of applications is sometimes called wireless local area networks (WLAN). Bluetooth was intended for portable equipment and its applications. The category of applications is outlined as the wireless personal area network (WPAN). Bluetooth is a replacement for cabling in a variety of personally carried applications in any setting and can also support fixed location applications such as smart energy functionality in the home (thermostats, etc.).

Wi-Fi is a wireless version of a common wired Ethernet network, and requires configuration to set up shared resources, transmit files, and to set up audio links (for example, headsets and hands-free devices). Wi-Fi uses the same radio frequencies as Bluetooth, but with higher power, resulting in higher bit rates and better range from the base station. The nearest equivalents in Bluetooth are the DUN profile, which allows devices to act as modem interfaces, and the PAN profile, which allows for ad-hoc networking.<sup>[citation needed]</sup>

## Devices

Bluetooth exists in many products, such as the iPod Touch, Lego Mindstorms NXT, PlayStation 3, PSP Go, telephones, the Nintendo Wii, and some high definition headsets, modems, and watches.<sup>[15]</sup> The technology is useful when transferring information between two or more devices that are near each other in low-bandwidth situations. Bluetooth is commonly used to transfer sound data with telephones (i.e., with a Bluetooth headset) or byte data with hand-held computers (transferring files).

Bluetooth protocols simplify the discovery and setup of services between devices.<sup>[citation needed]</sup> Bluetooth devices can advertise all of the services they provide.<sup>[16]</sup> This makes using services easier because more of the security, network address and permission configuration can be automated than with many other network types.<sup>[citation needed]</sup>

## Computer requirements

A personal computer that does not have embedded Bluetooth can be used with a Bluetooth adapter that will enable the PC to communicate with other Bluetooth devices (such as mobile phones, mice and keyboards). While some desktop computers and most recent laptops come with a built-in Bluetooth radio, others will require an external one in the form of a dongle.

Unlike its predecessor, IrDA, which requires a separate adapter for each device, Bluetooth allows multiple devices to communicate with a computer over a single adapter.

## Operating system support

*For more details on this topic, see Bluetooth stack.*

Apple has supported Bluetooth since Mac OS X v10.2 which was released in 2002.<sup>[17]</sup>

For Microsoft platforms, Windows XP Service Pack 2 and SP3 releases have native support for Bluetooth 1.1, 2.0 and 2.0+EDR.<sup>[18]</sup> Previous versions required users to install their Bluetooth adapter's own drivers, which were not directly supported by Microsoft.<sup>[19]</sup> Microsoft's own Bluetooth dongles (packaged with their Bluetooth computer devices) have no external drivers and thus require at



A Bluetooth USB dongle with a 100 m range. The MacBook Pro, shown, also has a built in Bluetooth adaptor.



A typical Bluetooth USB dongle.

least Windows XP Service Pack 2. Windows Vista RTM/SP1 with the Feature Pack for Wireless or Windows Vista SP2 support Bluetooth 2.1+EDR.<sup>[18]</sup> Windows 7 supports Bluetooth 2.1+EDR and Extended Inquiry Response (EIR).<sup>[18]</sup>

The Windows XP and Windows Vista/Windows 7 Bluetooth stacks support the following Bluetooth profiles natively: PAN, SPP, DUN, HID, HCRP. The Windows XP stack can be replaced by a third party stack which may support more profiles or newer versions of Bluetooth. The Windows Vista/Windows 7 Bluetooth stack supports vendor-supplied additional profiles without requiring the Microsoft stack to be replaced.<sup>[18]</sup>

Linux has two popular Bluetooth stacks, BlueZ and Affix. The BlueZ stack is included with most Linux kernels and was originally developed by Qualcomm.<sup>[20]</sup> The Affix stack was developed by Nokia. FreeBSD features Bluetooth support since its 5.0 release. NetBSD features Bluetooth support since its 4.0 release. Its Bluetooth stack has been ported to OpenBSD as well.

## Mobile phone requirements

A Bluetooth-enabled mobile phone is able to pair with many devices. To ensure the broadest support of feature functionality together with legacy device support, the Open Mobile Terminal Platform (OMTP) forum has published a recommendations paper, entitled "Bluetooth Local Connectivity".<sup>[21]</sup>

## Specifications and features

The Bluetooth specification was developed as a cable replacement in 1994 by Jaap Haartsen and Sven Mattisson, who were working for Ericsson in Lund, Sweden.<sup>[22]</sup> The specification is based on frequency-hopping spread spectrum technology.

The specifications were formalized by the Bluetooth Special Interest Group (SIG). The SIG was formally announced on May 20, 1998. Today it has a membership of over 14,000 companies worldwide. It was established by Ericsson, IBM, Intel, Toshiba and Nokia, and later joined by many other companies.

All versions of the Bluetooth standards are designed for downward compatibility. That lets the latest standard cover all older versions.

### Bluetooth v1.0 and v1.0B

Versions 1.0 and 1.0B had many problems, and manufacturers had difficulty making their products interoperable. Versions 1.0 and 1.0B also included mandatory Bluetooth hardware device address (BD\_ADDR) transmission in the Connecting process (rendering anonymity impossible at the protocol level), which was a major setback for certain services planned for use in Bluetooth environments.

### Bluetooth v1.1

- Ratified as IEEE Standard 802.15.1-2002<sup>[23]</sup>
- Many errors found in the 1.0B specifications were fixed.
- Added support for non-encrypted channels.
- Received Signal Strength Indicator (RSSI).

### Bluetooth v1.2

This version is backward compatible with 1.1 and the major enhancements include the following:

- Faster Connection and Discovery
- *Adaptive frequency-hopping spread spectrum (AFH)*, which improves resistance to radio frequency interference by avoiding the use of crowded frequencies in the hopping sequence.
- Higher transmission speeds in practice, up to 721 kbit/s,<sup>[24]</sup> than in v1.1.
- Extended Synchronous Connections (eSCO), which improve voice quality of audio links by allowing retransmissions of corrupted packets, and may optionally increase audio latency to provide better support for concurrent data transfer.
- Host Controller Interface (HCI) support for three-wire UART.
- Ratified as IEEE Standard 802.15.1-2005<sup>[25]</sup>
- Introduced Flow Control and Retransmission Modes for L2CAP.



An internal notebook Bluetooth card (14×36×4 mm).

## Bluetooth v2.0 + EDR

This version of the Bluetooth Core Specification was released in 2004 and is backward compatible with the previous version 1.2. The main difference is the introduction of an Enhanced Data Rate (EDR) for faster data transfer. The nominal rate of EDR is about 3 Mbit/s, although the practical data transfer rate is 2.1 Mbit/s.<sup>[24]</sup> EDR uses a combination of GFSK and Phase Shift Keying modulation (PSK) with two variants,  $\pi/4$ -DQPSK and 8DPSK.<sup>[26]</sup> EDR can provide a lower power consumption through a reduced duty cycle.

The specification is published as "Bluetooth v2.0 + EDR" which implies that EDR is an optional feature. Aside from EDR, there are other minor improvements to the 2.0 specification, and products may claim compliance to "Bluetooth v2.0" without supporting the higher data rate. At least one commercial device states "Bluetooth v2.0 without EDR" on its data sheet.<sup>[27]</sup>

## Bluetooth v2.1 + EDR

Bluetooth Core Specification Version 2.1 + EDR is fully backward compatible with 1.2, and was adopted by the Bluetooth SIG on July 26, 2007.<sup>[26]</sup>

The headline feature of 2.1 is secure simple pairing (SSP): this improves the pairing experience for Bluetooth devices, while increasing the use and strength of security. See the section on Pairing below for more details.<sup>[28]</sup>

2.1 allows various other improvements, including "Extended inquiry response" (EIR), which provides more information during the inquiry procedure to allow better filtering of devices before connection; and sniff subrating, which reduces the power consumption in low-power mode.

## Bluetooth v3.0 + HS

Version 3.0 + HS of the Bluetooth Core Specification<sup>[26]</sup> was adopted by the Bluetooth SIG (<https://www.bluetooth.org/apps/content/>) on April 21, 2009. Bluetooth 3.0+HS supports theoretical data transfer speeds of up to 24 Mbit/s, though not over the Bluetooth link itself. Instead, the Bluetooth link is used for negotiation and establishment, and the high data rate traffic is carried over a collocated 802.11 link.

The main new feature is AMP (Alternate MAC/PHY), the addition of 802.11 as a high speed transport. The High-Speed part of the specification is not mandatory, and hence only devices sporting the "+HS" will actually support the Bluetooth over 802.11 high-speed data transfer. A Bluetooth 3.0 device without the "+HS" suffix will not support High Speed, and needs to only support a feature introduced in Core Specification Version 3.0<sup>[29]</sup> or earlier Core Specification Addendum 1.<sup>[30]</sup>

### L2CAP Enhanced modes

Enhanced Retransmission Mode (ERTM) implements reliable L2CAP channel, while Streaming Mode (SM) implements unreliable channel with no retransmission or flow control. Introduced in Core Specification Addendum 1.

### Alternate MAC/PHY

Enables the use of alternative MAC and PHYs for transporting Bluetooth profile data. The Bluetooth radio is still used for device discovery, initial connection and profile configuration, however when large quantities of data need to be sent, the high speed alternate MAC PHY 802.11 (typically associated with Wi-Fi) will be used to transport the data. This means that the proven low power connection models of Bluetooth are used when the system is idle, and the faster radio is used when large quantities of data need to be sent. AMP links require enhanced L2CAP modes.

### Unicast Connectionless Data

Permits service data to be sent without establishing an explicit L2CAP channel. It is intended for use by applications that require low latency between user action and reconnection/transmission of data. This is only appropriate for small amounts of data.

### Enhanced Power Control

Updates the power control feature to remove the open loop power control, and also to clarify ambiguities in power control introduced by the new modulation schemes added for EDR. Enhanced power control removes the ambiguities by specifying the behaviour that is expected. The feature also adds closed loop power control, meaning RSSI filtering can start as the response is received. Additionally, a "go straight to maximum power" request has been introduced. This is expected to deal with the headset link loss issue typically observed when a user puts their phone into a pocket on the opposite side to the headset.

## Ultra-wideband

The high speed (AMP) feature of Bluetooth v3.0 was originally intended for UWB, but the WiMedia Alliance, the body responsible for the flavor of UWB intended for Bluetooth, announced in March 2009 that it was disbanding, and ultimately UWB was omitted from the Core v3.0 specification.<sup>[31]</sup>

On March 16, 2009, the WiMedia Alliance announced it was entering into technology transfer agreements for the WiMedia Ultra-wideband (UWB) specifications. WiMedia has transferred all current and future specifications, including work on future high speed and power optimized implementations, to the Bluetooth Special Interest Group (SIG), Wireless USB Promoter Group and the USB Implementers Forum. After the successful completion of the technology transfer, marketing and related administrative items, the WiMedia Alliance will cease operations.<sup>[32][33][34][35][36][37]</sup>

In October 2009 the Bluetooth Special Interest Group suspended development of UWB as part of the alternative MAC/PHY, Bluetooth v3.0 + HS solution. A small, but significant, number of former WiMedia members had not and would not sign up to the necessary agreements for the IP transfer. The Bluetooth SIG is now in the process of evaluating other options for its longer term roadmap.<sup>[38]</sup>

## Bluetooth v4.0

The Bluetooth SIG completed the Bluetooth Core Specification version 4.0, which includes *Classic Bluetooth*, *Bluetooth high speed* and *Bluetooth low energy* protocols. Bluetooth high speed is based on Wi-Fi, and Classic Bluetooth consists of legacy Bluetooth protocols. This version has been adopted as of June 30, 2010.

Bluetooth low energy (BLE), previously known as WiBree,<sup>[39]</sup> is a subset to Bluetooth v4.0 with an entirely new protocol stack for rapid build-up of simple links. As an alternative to the Bluetooth standard protocols that were introduced in Bluetooth v1.0 to v3.0, it is aimed at very low power applications running off a coin cell. Chip designs allow for two types of implementation, dual-mode, single-mode and enhanced past versions.<sup>[40]</sup> The provisional names *Wibree* and *Bluetooth ULP* (Ultra Low Power) were abandoned and the BLE name was used for a while. In late 2011, new logos “Bluetooth Smart Ready” for hosts and “Bluetooth Smart” for sensors were introduced as the general-public face of BLE.<sup>[41]</sup>

- In a single mode implementation the low energy protocol stack is implemented solely. CSR,<sup>[42]</sup> Nordic Semiconductor<sup>[43]</sup> and Texas Instruments<sup>[44]</sup> have released single mode Bluetooth low energy solutions.
- In a dual-mode implementation, Bluetooth low energy functionality is integrated into an existing Classic Bluetooth controller. Currently (2011-03) the following semiconductor companies have announced the availability of chips meeting the standard: Atheros, CSR, Broadcom<sup>[45][46]</sup> and Texas Instruments. The compliant architecture shares all of Classic Bluetooth’s existing radio and functionality resulting in a negligible cost increase compared to Classic Bluetooth.

Cost-reduced single-mode chips, which enable highly integrated and compact devices, feature a lightweight Link Layer providing ultra-low power idle mode operation, simple device discovery, and reliable point-to-multipoint data transfer with advanced power-save and secure encrypted connections at the lowest possible cost.

General improvements in version 4.0 include the changes necessary to facilitate BLE modes, as well the Generic Attribute Profile (GATT) and Security Manager (SM) services with AES Encryption.

Core Specification Addendum 2 was unveiled in December 2011; it contains improvements to the audio Host Controller Interface and to the High Speed (802.11) Protocol Adaptation Layer.

## Technical information

### Bluetooth protocol stack

*Main articles: Bluetooth stack and Bluetooth protocols*

"Bluetooth is defined as a layer protocol architecture consisting of core protocols, cable replacement protocols, telephony control protocols, and adopted protocols."<sup>[47]</sup> Mandatory protocols for all Bluetooth stacks are: LMP, L2CAP and SDP. Additionally, these protocols are almost universally supported: HCI and RFCOMM.

#### LMP

The *Link Management Protocol* (LMP) is used for control of the radio link between two devices. Implemented on the controller.

#### AVRCP

A/V Remote Control Profile. Commonly used in car navigation systems to control streaming Bluetooth audio. Adopted versions (<https://www.bluetooth.org/Technical/Specifications/adopted.htm>) 1.0, 1.3 & 1.4

#### L2CAP

**L2CAP**  
The *Logical Link Control and Adaptation Protocol* (L2CAP) Used to multiplex multiple logical connections between two devices using different higher level protocols. Provides segmentation and reassembly of on-air packets.

In *Basic* mode, L2CAP provides packets with a payload configurable up to 64kB, with 672 bytes as the default MTU, and 48 bytes as the minimum mandatory supported MTU.

In *Retransmission and Flow Control* modes, L2CAP can be configured for reliable or isochronous data per channel by performing retransmissions and CRC checks.

Bluetooth Core Specification Addendum 1 adds two additional L2CAP modes to the core specification. These modes effectively deprecate original Retransmission and Flow Control modes:

- **Enhanced Retransmission Mode** (ERTM): This mode is an improved version of the original retransmission mode. This mode provides a reliable L2CAP channel.
- **Streaming Mode** (SM): This is a very simple mode, with no retransmission or flow control. This mode provides an unreliable L2CAP channel.

Reliability in any of these modes is optionally and/or additionally guaranteed by the lower layer Bluetooth BDR/EDR air interface by configuring the number of retransmissions and flush timeout (time after which the radio will flush packets). In-order sequencing is guaranteed by the lower layer.

Only L2CAP channels configured in ERTM or SM may be operated over AMP logical links.

## **SDP**

The *Service Discovery Protocol* (SDP) allows a device to discover services supported by other devices, and their associated parameters. For example, when connecting a mobile phone to a Bluetooth headset, SDP will be used for determining which Bluetooth profiles are supported by the headset (Headset Profile, Hands Free Profile, Advanced Audio Distribution Profile (A2DP) etc.) and the protocol multiplexer settings needed to connect to each of them. Each service is identified by a Universally Unique Identifier (UUID), with official services (Bluetooth profiles) assigned a short form UUID (16 bits rather than the full 128).

## **RFCOMM**

*Radio Frequency Communications* (RFCOMM) is a cable replacement protocol used to create a virtual serial data stream. RFCOMM provides for binary data transport and emulates EIA-232 (formerly RS-232) control signals over the Bluetooth baseband layer, i.e. it is a serial port emulation.

RFCOMM provides a simple reliable data stream to the user, similar to TCP. It is used directly by many telephony related profiles as a carrier for AT commands, as well as being a transport layer for OBEX over Bluetooth.

Many Bluetooth applications use RFCOMM because of its widespread support and publicly available API on most operating systems. Additionally, applications that used a serial port to communicate can be quickly ported to use RFCOMM.

## **BNEP**

The *Bluetooth Network Encapsulation Protocol* (BNEP) is used for transferring another protocol stack's data via an L2CAP channel. Its main purpose is the transmission of IP packets in the Personal Area Networking Profile. BNEP performs a similar function to SNAP in Wireless LAN.

## **AVCTP**

The *Audio/Video Control Transport Protocol* (AVCTP) is used by the remote control profile to transfer AV/C commands over an L2CAP channel. The music control buttons on a stereo headset use this protocol to control the music player.

## **AVDTP**

The *Audio/Video Distribution Transport Protocol* (AVDTP) is used by the advanced audio distribution profile to stream music to stereo headsets over an L2CAP channel. Intended to be used by video distribution profile in the bluetooth transmission.

## **TCS**

The *Telephony Control Protocol – Binary* (TCS BIN) is the bit-oriented protocol that defines the call control signaling for the

establishment of voice and data calls between Bluetooth devices. Additionally, "TCS BIN defines mobility management procedures for handling groups of Bluetooth TCS devices."

TCS-BIN is only used by the cordless telephony profile, which failed to attract implementers. As such it is only of historical interest.

## Adopted protocols

Adopted protocols are defined by other standards-making organizations and incorporated into Bluetooth's protocol stack, allowing Bluetooth to create protocols only when necessary. The adopted protocols include:

Point-to-Point Protocol (PPP)

Internet standard protocol for transporting IP datagrams over a point-to-point link.

TCP/IP/UDP

Foundation Protocols for TCP/IP protocol suite

Object Exchange Protocol (OBEX)

Session-layer protocol for the exchange of objects, providing a model for object and operation representation

Wireless Application Environment/Wireless Application Protocol (WAE/WAP)

WAE specifies an application framework for wireless devices and WAP is an open standard to provide mobile users access to telephony and information services.<sup>[47]</sup>

## Baseband error correction

Depending on packet type, individual packets may be protected by error correction, either 1/3 rate forward error correction (FEC) or 2/3 rate. In addition, packets with CRC will be retransmitted until acknowledged by automatic repeat request (ARQ).

## Setting up connections

Any Bluetooth device in *discoverable mode* will transmit the following information on demand:

- Device name
- Device class
- List of services
- Technical information (for example: device features, manufacturer, Bluetooth specification used, clock offset)

Any device may perform an inquiry to find other devices to connect to, and any device can be configured to respond to such inquiries. However, if the device trying to connect knows the address of the device, it always responds to direct connection requests and transmits the information shown in the list above if requested. Use of a device's services may require pairing or acceptance by its owner, but the connection itself can be initiated by any device and held until it goes out of range. Some devices can be connected to only one device at a time, and connecting to them prevents them from connecting to other devices and appearing in inquiries until they disconnect from the other device.

Every device has a unique 48-bit address. However, these addresses are generally not shown in inquiries. Instead, friendly Bluetooth names are used, which can be set by the user. This name appears when another user scans for devices and in lists of paired devices.

Most phones have the Bluetooth name set to the manufacturer and model of the phone by default. Most phones and laptops show only the Bluetooth names and special programs are required to get additional information about remote devices. This can be confusing as, for example, there could be several phones in range named T610 (see Bluejacking).

## Pairing/Bonding

### Motivation

Many of the services offered over Bluetooth can expose private data or allow the connecting party to control the Bluetooth device. For security reasons it is necessary to be able to recognize specific devices and thus enable control over which devices are allowed to connect to a given Bluetooth device. At the same time, it is useful for Bluetooth devices to be able to establish a connection without user intervention (for example, as soon as they are in range).

To resolve this conflict, Bluetooth uses a process called *bonding*, and a bond is created through a process called *pairing*. The pairing process is triggered either by a specific request from a user to create a bond (for example, the user explicitly requests to "Add a Bluetooth device"), or it is triggered automatically when connecting to a service where (for the first time) the identity of a device is required for security purposes. These two cases are referred to as dedicated bonding and general bonding respectively.

Pairing often involves some level of user interaction; this user interaction is the basis for confirming the identity of the devices. Once

Pairing often involves some level of user interaction, this user interaction is the basis for confirming the identity of the devices. Once pairing successfully completes, a bond will have been formed between the two devices, enabling those two devices to connect to each other in the future without requiring the pairing process in order to confirm the identity of the devices. When desired, the bonding relationship can later be removed by the user.

## Implementation

During the pairing process, the two devices involved establish a relationship by creating a shared secret known as a *link key*. If a link key is stored by both devices they are said to be *paired* or *bonded*. A device that wants to communicate only with a bonded device can cryptographically authenticate the identity of the other device, and so be sure that it is the same device it previously paired with. Once a link key has been generated, an authenticated Asynchronous Connection-Less (ACL) link between the devices may be encrypted so that the data that they exchange over the airwaves is protected against eavesdropping.

Link keys can be deleted at any time by either device. If done by either device this will implicitly remove the bonding between the devices; so it is possible for one of the devices to have a link key stored but not be aware that it is no longer bonded to the device associated with the given link key.

Bluetooth services generally require either encryption or authentication, and as such require pairing before they allow a remote device to use the given service. Some services, such as the Object Push Profile, elect not to explicitly require authentication or encryption so that pairing does not interfere with the user experience associated with the service use-cases.

## Pairing mechanisms

Pairing mechanisms have changed significantly with the introduction of Secure Simple Pairing in Bluetooth v2.1. The following summarizes the pairing mechanisms:

- **Legacy pairing:** This is the only method available in Bluetooth v2.0 and before. Each device must enter a PIN code; pairing is only successful if both devices enter the same PIN code. Any 16-byte UTF-8 string may be used as a PIN code; however, not all devices may be capable of entering all possible PIN codes.
  - **Limited input devices:** The obvious example of this class of device is a Bluetooth Hands-free headset, which generally have few inputs. These devices usually have a *fixed PIN*, for example "0000" or "1234", that are hard-coded into the device.
  - **Numeric input devices:** Mobile phones are classic examples of these devices. They allow a user to enter a numeric value up to 16 digits in length.
  - **Alpha-numeric input devices:** PCs and smartphones are examples of these devices. They allow a user to enter full UTF-8 text as a PIN code. If pairing with a less capable device the user needs to be aware of the input limitations on the other device, there is no mechanism available for a capable device to determine how it should limit the available input a user may use.
- **Secure Simple Pairing (SSP):** This is required by Bluetooth v2.1. A Bluetooth v2.1 device may only use legacy pairing to interoperate with a v2.0 or earlier device. Secure Simple Pairing uses a form of public key cryptography, and has the following modes of operation:
  - **Just works:** As implied by the name, this method just works. No user interaction is required; however, a device may prompt the user to confirm the pairing process. This method is typically used by headsets with very limited IO capabilities, and is more secure than the fixed PIN mechanism which is typically used for legacy pairing by this set of limited devices. This method provides no man in the middle (MITM) protection.
  - **Numeric comparison:** If both devices have a display and at least one can accept a binary Yes/No user input, they may use Numeric Comparison. This method displays a 6-digit numeric code on each device. The user should compare the numbers to ensure they are identical. If the comparison succeeds, the user(s) should confirm pairing on the device(s) that can accept an input. This method provides MITM protection, assuming the user confirms on both devices and actually performs the comparison properly.
  - **Passkey Entry:** This method may be used between a device with a display and a device with numeric keypad entry (such as a keyboard), or two devices with numeric keypad entry. In the first case, the display is used to show a 6-digit numeric code to the user, who then enters the code on the keypad. In the second case, the user of each device enters the same 6-digit number. Both cases provide MITM protection.
  - **Out of band (OOB):** This method uses an external means of communication, such as Near Field Communication (NFC) to exchange some information used in the pairing process. Pairing is completed using the Bluetooth radio, but requires information from the OOB mechanism. This provides only the level of MITM protection that is present in the OOB mechanism.

SSP is considered simple for the following reasons:

- In most cases, it does not require a user to generate a passkey.
- For use-cases not requiring MITM protection, user interaction has been eliminated.
- For *numeric comparison*, MITM protection can be achieved with a simple equality comparison by the user.
- Using OOB with NFC enable pairing when devices simply get close, rather than requiring a lengthy discovery process.

- Using GOB with NFC enable pairing when devices simply get close, rather than requiring a lengthy discovery process.

## Security Concerns

Prior to Bluetooth v2.1, encryption is not required and can be turned off at any time. Moreover, the encryption key is only good for approximately 23.5 hours; using a single encryption key longer than this time allows simple XOR attacks to retrieve the encryption key.

- Turning off encryption is required for several normal operations, so it is problematic to detect if encryption is disabled for a valid reason or for a security attack.
- Bluetooth v2.1 addresses this in the following ways:
  - Encryption is required for all non-SDP (Service Discovery Protocol) connections
  - A new Encryption Pause and Resume feature is used for all normal operations requiring encryption to be disabled. This enables easy identification of normal operation from security attacks.
  - The encryption key is required to be refreshed before it expires.

Link keys may be stored on the device file system, not on the Bluetooth chip itself. Many Bluetooth chip manufacturers allow link keys to be stored on the device; however, if the device is removable this means that the link key will move with the device.

## Air interface

The protocol operates in the license-free ISM band at 2.402-2.480 GHz.<sup>[48]</sup> To avoid interfering with other protocols that use the 2.45 GHz band, the Bluetooth protocol divides the band into 79 channels (each 1 MHz wide) and changes channels, generally 800 times per second. Implementations with versions 1.1 and 1.2 reach speeds of 723.1 kbit/s. Version 2.0 implementations feature Bluetooth Enhanced Data Rate (EDR) and reach 2.1 Mbit/s. Technically, version 2.0 devices have a higher power consumption, but the three times faster rate reduces the transmission times, effectively reducing power consumption to half that of 1.x devices (assuming equal traffic load).

## Security

### Overview

Bluetooth implements confidentiality, authentication and key derivation with custom algorithms based on the SAFER+ block cipher. Bluetooth key generation is generally based on a Bluetooth PIN, which must be entered into both devices. This procedure might 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 the E22 algorithm.<sup>[49]</sup> The E0 stream cipher is used for encrypting packets, granting confidentiality and is based on a shared cryptographic secret, namely a previously generated link key or master key. Those keys, used for subsequent encryption of data sent via the air interface, rely on the Bluetooth PIN, which has been entered into one or both devices.

An overview of Bluetooth vulnerabilities exploits was published in 2007 by Andreas Becker.<sup>[50]</sup>

In September 2008, the National Institute of Standards and Technology (NIST) published a Guide to Bluetooth Security that will serve as reference to organizations on the security capabilities of Bluetooth and steps for securing Bluetooth technologies effectively. While Bluetooth has its benefits, it is susceptible to denial of service attacks, eavesdropping, man-in-the-middle attacks, message modification, and resource misappropriation. Users/organizations must evaluate their acceptable level of risk and incorporate security into the lifecycle of Bluetooth devices. To help mitigate risks, included in the NIST document are security checklists with guidelines and recommendations for creating and maintaining secure Bluetooth piconets, headsets, and smart card readers.<sup>[51]</sup>

Bluetooth v2.1 - finalized in 2007 with consumer devices first appearing in 2009 - makes significant changes to Bluetooth's security, including pairing. See the #Pairing mechanisms section for more about these changes.

## Bluejacking

*Main article: Bluejacking*

Bluejacking is the sending of either a picture or a message from one user to an unsuspecting user through *Bluetooth* wireless technology. Common applications include short messages (e.g., "You've just been bluejacked!").<sup>[52]</sup> Bluejacking does not involve the removal or alteration of any data from the device. Bluejacking can also involve taking control of a mobile wirelessly and phoning a premium rate line, owned by the bluejacker.

## History of security concerns

## 2001 - 2004

In 2001, Jakobsson and Wetzel from Bell Laboratories discovered flaws in the Bluetooth pairing protocol and also pointed to vulnerabilities in the encryption scheme.<sup>[53]</sup> In 2003, Ben and Adam Laurie from A.L. Digital Ltd. discovered that serious flaws in some poor implementations of Bluetooth security may lead to disclosure of personal data.<sup>[54]</sup> In a subsequent experiment, Martin Herfurt from the trifinite.group was able to do a field-trial at the CeBIT fairgrounds, showing the importance of the problem to the world. A new attack called BlueBug was used for this experiment.<sup>[55]</sup> In 2004 the first purported virus using Bluetooth to spread itself among mobile phones appeared on the Symbian OS.<sup>[56]</sup> The virus was first described by Kaspersky Lab and requires users to confirm the installation of unknown software before it can propagate. The virus was written as a proof-of-concept by a group of virus writers known as "29A" and sent to anti-virus groups. Thus, it should be regarded as a potential (but not real) security threat to Bluetooth technology or Symbian OS since the virus has never spread outside of this system. In August 2004, a world-record-setting experiment (see also Bluetooth sniping) showed that the range of Class 2 Bluetooth radios could be extended to 1.78 km (1.11 mi) with directional antennas and signal amplifiers.<sup>[57]</sup> This poses a potential security threat because it enables attackers to access vulnerable Bluetooth devices from a distance beyond expectation. The attacker must also be able to receive information from the victim to set up a connection. No attack can be made against a Bluetooth device unless the attacker knows its Bluetooth address and which channels to transmit on.

## 2005

In January 2005, a mobile malware worm known as Lasco.A began targeting mobile phones using Symbian OS (Series 60 platform) using Bluetooth enabled devices to replicate itself and spread to other devices. The worm is self-installing and begins once the mobile user approves the transfer of the file (velasco.sis) from another device. Once installed, the worm begins looking for other Bluetooth enabled devices to infect. Additionally, the worm infects other .SIS files on the device, allowing replication to another device through use of removable media (Secure Digital, Compact Flash, etc.). The worm can render the mobile device unstable.<sup>[58]</sup>

In April 2005, Cambridge University security researchers published results of their actual implementation of passive attacks against the PIN-based pairing between commercial Bluetooth devices, confirming the attacks to be practicably fast and the Bluetooth symmetric key establishment method to be vulnerable. To rectify this vulnerability, they carried out an implementation which showed that stronger, asymmetric key establishment is feasible for certain classes of devices, such as mobile phones.<sup>[59]</sup>

In June 2005, Yaniv Shaked (<http://www.eng.tau.ac.il/~shakedy>) and Avishai Wool (<http://www.eng.tau.ac.il/~yash/>) published a paper describing both passive and active methods for obtaining the PIN for a Bluetooth link. The passive attack allows a suitably equipped attacker to eavesdrop on communications and spoof, if the attacker was present at the time of initial pairing. The active method makes use of a specially constructed message that must be inserted at a specific point in the protocol, to make the master and slave repeat the pairing process. After that, the first method can be used to crack the PIN. This attack's major weakness is that it requires the user of the devices under attack to re-enter the PIN during the attack when the device prompts them to. Also, this active attack probably requires custom hardware, since most commercially available Bluetooth devices are not capable of the timing necessary.<sup>[60]</sup>

In August 2005, police in Cambridgeshire, England, issued warnings about thieves using Bluetooth enabled phones to track other devices left in cars. Police are advising users to ensure that any mobile networking connections are de-activated if laptops and other devices are left in this way.<sup>[61]</sup>

## 2006

In April 2006, researchers from Secure Network and F-Secure published a report that warns of the large number of devices left in a visible state, and issued statistics on the spread of various Bluetooth services and the ease of spread of an eventual Bluetooth worm.<sup>[62]</sup>

## 2007

In October 2007, at the Luxemburgish Hack.lu Security Conference, Kevin Finistere and Thierry Zoller demonstrated and released a remote root shell via Bluetooth on Mac OS X v10.3.9 and v10.4. They also demonstrated the first Bluetooth PIN and Linkkeys cracker, which is based on the research of Wool and Shaked.

## Health concerns

*Main article: Wireless electronic devices and health*

Bluetooth uses the microwave radio frequency spectrum in the 2.402 GHz to 2.480 GHz range.<sup>[40]</sup> Maximum power output from a Bluetooth radio is 100 mW, 2.5 mW, and 1 mW for Class 1, Class 2, and Class 3 devices respectively, which puts Class 1 at roughly the same level as mobile phones, and the other two classes much lower.<sup>[63]</sup> Accordingly, Class 2 and Class 3 Bluetooth devices are considered less of a potential hazard than mobile phones, and Class 1 may be comparable to that of mobile phones : the maximum for a Class 1 is 100 mW for Bluetooth but 250 mW for UMTS W-CDMA, 1 W for GSM1800/1900 and 2 W for GSM850/900 for instance.

## Bluetooth Innovation World Cup marketing initiative

The *Bluetooth* Innovation World Cup, a marketing initiative of the Bluetooth Special Interest Group (SIG), is an international competition encouraging the development of innovations for applications leveraging the *Bluetooth* low energy wireless technology in sports, fitness and health care products. The aim of the competition is to stimulate new markets. The initiative will take three years, having started June 1, 2009.<sup>[64]</sup>

### **Bluetooth Innovation World Cup 2009**

The first international *Bluetooth* Innovation World Cup 2009 drew more than 250 international entries, including Nokia, Freescale Semiconductor, Texas Instruments, Nordic Semiconductor, STMicroelectronics and Brunel.

### **Bluetooth Innovator of the Year 2009**

On February 8, 2010, Edward Sazonov, Physical Activity Innovations LLC, was awarded the title of *Bluetooth* Innovator of the Year for 2009. Sazonov received this recognition at a ceremony held at the Wearable Technologies Show at ispo 2010, a trade show for sporting goods. The award includes a cash prize of €5,000 and a *Bluetooth* Qualification Program voucher (QDID) valued at up to US\$ 10,000. Sazonov's idea, The Fit Companion, is a small, unobtrusive sensor that, when clipped-on to a user's clothing or integrated into a shoe, provides feedback about physical activity. The data, transmitted via Bluetooth, can help individuals to lose weight and achieve optimal physical activity. Intended for use in both training and daily activities like walking or performing chores, this simple measuring device may offer a solution for reducing obesity.

### **Bluetooth Innovation World Cup 2010**

The Bluetooth Special Interest Group (SIG) announced the start of the second Innovation World Cup on 1 June 2010, with a focus on applications for the sports & fitness, health care, and home information and control markets. The competition will close for registration on September 15, 2010.

## See also

- Bluesniping
- BlueSoleil - Proprietary driver
- Continua Health Alliance
- DASH7
- Java APIs for Bluetooth
- MyriaNed
- Near Field Communication
- Tethering
- ZigBee - low power lightweight wireless protocol in the ISM band.
- RuBee- secure wireless protocol alternative
- Bluetooth wireless headsets
- Li-Fi

## References

- <sup>1</sup> <sup>^</sup> "Bluetooth traveler" ([http://www.hoovers.com/business-information/--pageid\\_\\_13751--/global-hoov-index.xhtml](http://www.hoovers.com/business-information/--pageid__13751--/global-hoov-index.xhtml)) . www.hoovers.com. [http://www.hoovers.com/business-information/--pageid\\_\\_13751--/global-hoov-index.xhtml](http://www.hoovers.com/business-information/--pageid__13751--/global-hoov-index.xhtml). Retrieved 9 April 2010.
- <sup>2</sup> <sup>^</sup> <sup>a</sup> <sup>b</sup> Newton, Harold. (2007). *Newton's telecom dictionary*. New York: Flatiron Publishing.
- <sup>3</sup> <sup>^</sup> "Bluetooth.org" ([https://www.bluetooth.org/About/bluetooth\\_sig.htm](https://www.bluetooth.org/About/bluetooth_sig.htm)) . Bluetooth.org. [https://www.bluetooth.org/About/bluetooth\\_sig.htm](https://www.bluetooth.org/About/bluetooth_sig.htm). Retrieved 2011-05-03.
- <sup>4</sup> <sup>^</sup> Monson, Heidi (1999-12-14). "Bluetooth Technology and Implications" (<http://www.sysopt.com/features/network/article.php/3532506>) . SysOpt.com. <http://www.sysopt.com/features/network/article.php/3532506>. Retrieved 2009-02-17.
- <sup>5</sup> <sup>^</sup> "About the Bluetooth SIG" (<http://www.bluetooth.com/Bluetooth/SIG/>) . Bluetooth SIG. <http://www.bluetooth.com/Bluetooth/SIG/>. Retrieved 2008-02-01.
- <sup>6</sup> <sup>^</sup> Kardach, Jim (2008-05-03). "How Bluetooth got its name" ([http://www.eetimes.eu/scandinavia/206902019?cid=RSSfeed\\_eetimesEII\\_scandinavia](http://www.eetimes.eu/scandinavia/206902019?cid=RSSfeed_eetimesEII_scandinavia)) . [http://www.eetimes.eu/scandinavia/206902019?cid=RSSfeed\\_eetimesEII\\_scandinavia](http://www.eetimes.eu/scandinavia/206902019?cid=RSSfeed_eetimesEII_scandinavia)

- Retrieved 2009-02-24.
7. ^ "How Bluetooth Technology Works" (<http://web.archive.org/web/20080117000828/http://bluetooth.com/Bluetooth/Technology/Works/>) . Bluetooth SIG. Archived from the original (<http://www.bluetooth.com/Bluetooth/Technology/Works/>) on 2008-01-17. <http://web.archive.org/web/20080117000828/http://bluetooth.com/Bluetooth/Technology/Works/>. Retrieved 2008-02-01.
  8. ^ "Class 1 Bluetooth Dongle Test" (<http://www.amperordirect.com/pc/r-electronic-resource/z-reference-bluetooth-class1-myth.html>) . Amperordirect.com. <http://www.amperordirect.com/pc/r-electronic-resource/z-reference-bluetooth-class1-myth.html>. Retrieved 2010-09-04.
  9. ^ "Profiles Overview" ([http://www.bluetooth.com/English/Technology/Works/Pages/Profiles\\_Overview.aspx](http://www.bluetooth.com/English/Technology/Works/Pages/Profiles_Overview.aspx)) . Bluetooth.com. [http://www.bluetooth.com/English/Technology/Works/Pages/Profiles\\_Overview.aspx](http://www.bluetooth.com/English/Technology/Works/Pages/Profiles_Overview.aspx). Retrieved 2010-09-04.
  10. ^ "Hypertag.com" (<http://www.hypertag.com/company1/what-is-proximity-or-bluetooth-marketing/>) . Hypertag.com. <http://www.hypertag.com/company1/what-is-proximity-or-bluetooth-marketing/>. Retrieved 2010-09-04.
  11. ^ "Wii Controller" ([http://web.archive.org/web/20080220080315/http://bluetooth.com/Bluetooth/Products/Products/Product\\_Details.htm?ProductID=2951](http://web.archive.org/web/20080220080315/http://bluetooth.com/Bluetooth/Products/Products/Product_Details.htm?ProductID=2951)) . Bluetooth SIG. Archived from the original ([http://bluetooth.com/Bluetooth/Products/Products/Product\\_Details.htm?ProductID=2951](http://bluetooth.com/Bluetooth/Products/Products/Product_Details.htm?ProductID=2951)) on February 20, 2008. [http://web.archive.org/web/20080220080315/http://bluetooth.com/Bluetooth/Products/Products/Product\\_Details.htm?ProductID=2951](http://web.archive.org/web/20080220080315/http://bluetooth.com/Bluetooth/Products/Products/Product_Details.htm?ProductID=2951). Retrieved 2008-02-01.
  12. ^ "Telemedicine.jp" (<http://www.telemedicine.jp/>) . Telemedicine.jp. <http://www.telemedicine.jp/>. Retrieved 2010-09-04.
  13. ^ "Real Time Location Systems" ([http://www.clarinix.com/docs/whitepapers/RealTime\\_main.pdf](http://www.clarinix.com/docs/whitepapers/RealTime_main.pdf)) . clarinix. [http://www.clarinix.com/docs/whitepapers/RealTime\\_main.pdf](http://www.clarinix.com/docs/whitepapers/RealTime_main.pdf). Retrieved 2010-08-04.
  14. ^ "Tenbu's nio is kind of like a car alarm for your cellphone" (<http://www.ohgizmo.com/2009/03/30/tenbu-nio-is-kind-of-like-a-car-alarm-for-your-cellphone/>) , *OhGizmo.com*, March 2009.
  15. ^ "Watch" (<http://www.bluetooth.com/English/Products/Pages/Watch.aspx>) . Bluetooth.com. <http://www.bluetooth.com/English/Products/Pages/Watch.aspx>. Retrieved 2010-09-04.
  16. ^ "Specification Documents" (<http://www.bluetooth.com/Specification%20Documents/AssignedNumbersServiceDiscovery.pdf>) . Bluetooth.com. 2010-06-30. <http://www.bluetooth.com/Specification%20Documents/AssignedNumbersServiceDiscovery.pdf>.
  17. ^ "Apple Introduces "Jaguar," the Next Major Release of Mac OS X" (<http://www.apple.com/pr/library/2002/jul/17jaguar.html>) (Press release). Apple. 2002-07-17. <http://www.apple.com/pr/library/2002/jul/17jaguar.html>. Retrieved 2008-02-04.
  18. ^ *a b c d* "Bluetooth Wireless Technology FAQ - 2010" ([http://download.microsoft.com/download/9/c/5/9c5b2167-8017-4bae-9fde-d599bac8184a/Bth\\_FAQ.docx](http://download.microsoft.com/download/9/c/5/9c5b2167-8017-4bae-9fde-d599bac8184a/Bth_FAQ.docx)) . [http://download.microsoft.com/download/9/c/5/9c5b2167-8017-4bae-9fde-d599bac8184a/Bth\\_FAQ.docx](http://download.microsoft.com/download/9/c/5/9c5b2167-8017-4bae-9fde-d599bac8184a/Bth_FAQ.docx). Retrieved 2010-09-04.
  19. ^ "Network Protection Technologie" (<http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2netwk.mspx>) . *Changes to Functionality in Microsoft Windows XP Service Pack 2*. Microsoft Technet. <http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2netwk.mspx>. Retrieved 2008-02-01.
  20. ^ "Official Linux Bluetooth protocol stack" (<http://www.bluez.org/>) . BlueZ. <http://www.bluez.org/>. Retrieved 2010-09-04.
  21. ^ OMTp.org (<http://www.omtp.org/Publications/Display.aspx?Id=8f152a02-4120-4933-a1e5-74c7ad472bc8>)
  22. ^ "The Bluetooth Blues" ([http://web.archive.org/web/20071222231740/http://www.information-age.com/article/2001/may/the\\_bluetooth\\_blues](http://web.archive.org/web/20071222231740/http://www.information-age.com/article/2001/may/the_bluetooth_blues)) . Information Age. 2001-05-24. Archived from the original ([http://www.information-age.com/article/2001/may/the\\_bluetooth\\_blues](http://www.information-age.com/article/2001/may/the_bluetooth_blues)) on 2007-12-22. [http://web.archive.org/web/20071222231740/http://www.information-age.com/article/2001/may/the\\_bluetooth\\_blues](http://web.archive.org/web/20071222231740/http://www.information-age.com/article/2001/may/the_bluetooth_blues). Retrieved 2008-02-01.
  23. ^ "IEEE Std 802.15.1-2002 – IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)" (<http://ieeexplore.ieee.org/servlet/opac?punumber=7932>) . Ieeexplore.ieee.org. doi:10.1109/IEEESTD.2002.93621 (<http://dx.doi.org/10.1109%2FIEEESTD.2002.93621>) . <http://ieeexplore.ieee.org/servlet/opac?punumber=7932>. Retrieved 2010-09-04.
  24. ^ *a b* Guy Kewney (2004-11-16). "High speed Bluetooth comes a step closer: enhanced data rate approved" (<http://www.newswireless.net/index.cfm/article/629>) . Newswireless.net. <http://www.newswireless.net/index.cfm/article/629>. Retrieved 2008-02-04.
  25. ^ "IEEE Std 802.15.1-2005 – IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (W Pans)" (<http://ieeexplore.ieee.org/servlet/opac?punumber=9980>) . Ieeexplore.ieee.org. doi:10.1109/IEEESTD.2005.96290 (<http://dx.doi.org/10.1109%2FIEEESTD.2005.96290>) . <http://ieeexplore.ieee.org/servlet/opac?punumber=9980>. Retrieved 2010-09-04.
  26. ^ *a b c* "Specification Documents" (<http://www.bluetooth.com/Bluetooth/Technology/Building/Specifications/>) . Bluetooth SIG. <http://www.bluetooth.com/Bluetooth/Technology/Building/Specifications/>. Retrieved 2008-02-04.
  27. ^ "HTC TyTN Specification" ([http://www.europe.htc.com/z/pdf/products/1766\\_TyTN\\_LFLT\\_OUT.PDF](http://www.europe.htc.com/z/pdf/products/1766_TyTN_LFLT_OUT.PDF)) (PDF). HTC. [http://www.europe.htc.com/z/pdf/products/1766\\_TyTN\\_LFLT\\_OUT.PDF](http://www.europe.htc.com/z/pdf/products/1766_TyTN_LFLT_OUT.PDF). Retrieved 2008-02-04.
  28. ^ (PDF) *Simple Pairing Whitepaper* ([http://web.archive.org/web/20061018032605/http://www.bluetooth.com/NR/rdonlyres/0A0B3F36-D15F-4470-85A6-F2CCFA26F70F/0/SimplePairing\\_WP\\_V10r00.pdf](http://web.archive.org/web/20061018032605/http://www.bluetooth.com/NR/rdonlyres/0A0B3F36-D15F-4470-85A6-F2CCFA26F70F/0/SimplePairing_WP_V10r00.pdf)) . Version V10r00. Bluetooth SIG. 2006-08-03. Archived from the original ([http://bluetooth.com/NR/rdonlyres/0A0B3F36-D15F-4470-85A6-F2CCFA26F70F/0/SimplePairing\\_WP\\_V10r00.pdf](http://bluetooth.com/NR/rdonlyres/0A0B3F36-D15F-4470-85A6-F2CCFA26F70F/0/SimplePairing_WP_V10r00.pdf)) on October 18, 2006. [http://web.archive.org/web/20061018032605/http://www.bluetooth.com/NR/rdonlyres/0A0B3F36-D15F-4470-85A6-F2CCFA26F70F/0/SimplePairing\\_WP\\_V10r00.pdf](http://web.archive.org/web/20061018032605/http://www.bluetooth.com/NR/rdonlyres/0A0B3F36-D15F-4470-85A6-F2CCFA26F70F/0/SimplePairing_WP_V10r00.pdf). Retrieved 2007-02-01.
  29. ^ "Bluetooth Core Version 3.0 + HS specification" ([https://www.bluetooth.org/docman/handlers/DownloadDoc.ashx?doc\\_id=40560](https://www.bluetooth.org/docman/handlers/DownloadDoc.ashx?doc_id=40560)) . [https://www.bluetooth.org/docman/handlers/DownloadDoc.ashx?doc\\_id=40560](https://www.bluetooth.org/docman/handlers/DownloadDoc.ashx?doc_id=40560).
  30. ^ "Bluetooth Core Specification Addendum (CSA) 1" ([https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc\\_id=119993](https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=119993)) . [https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc\\_id=119993](https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=119993).
  31. ^ David Meyer (2009-04-22). "Bluetooth 3.0 released without ultrawideband" (<http://news.zdnet.co.uk/communications/0,1000000085,39643174,00.htm>) . zdnet.co.uk. <http://news.zdnet.co.uk/communications/0,1000000085,39643174,00.htm>. Retrieved 2009-04-22.

32. ^ "Wimedia.org" (<http://www.wimedia.org/>) . Wimedia.org. 2010-01-04. <http://www.wimedia.org/>. Retrieved 2010-09-04.
33. ^ "Wimedia.org" (<http://www.wimedia.org/imwp/download.asp?ContentID=15508>) . Wimedia.org. <http://www.wimedia.org/imwp/download.asp?ContentID=15508>. Retrieved 2010-09-04.
34. ^ "Wimedia.org" (<http://www.wimedia.org/imwp/download.asp?ContentID=15506>) . <http://www.wimedia.org/imwp/download.asp?ContentID=15506>. Retrieved 2010-09-04.
35. ^ Bluetooth.com ([http://www.bluetooth.com/Bluetooth/Technology/Technology\\_Transfer/](http://www.bluetooth.com/Bluetooth/Technology/Technology_Transfer/))
36. ^ "USB.org" ([http://www.usb.org/press/WiMedia\\_Tech\\_Transfer/](http://www.usb.org/press/WiMedia_Tech_Transfer/)) . USB.org. 2009-03-16. [http://www.usb.org/press/WiMedia\\_Tech\\_Transfer/](http://www.usb.org/press/WiMedia_Tech_Transfer/). Retrieved 2010-09-04.
37. ^ "Incisor.tv" (<http://www.incisor.tv/2009/03/what-to-make-of-bluetooth-sig-wimedia.html>) . Incisor.tv. 2009-03-16. <http://www.incisor.tv/2009/03/what-to-make-of-bluetooth-sig-wimedia.html>. Retrieved 2010-09-04.
38. ^ Bluetooth group drops ultrawideband, eyes 60 GHz (<http://www.eetimes.com/showArticle.jhtml;jsessionid=J5E0PN3NQ5BNLQE1GHPSKH4ATMY32JVN?articleID=221100170>) , Report: Ultrawideband dies by 2013 (<http://www.eetimes.com/showArticle.jhtml;jsessionid=J5E0PN3NQ5BNLQE1GHPSKH4ATMY32JVN?articleID=217201265>) , Incisor Magazine November 2009 (<http://www.incisor.tv/download.php?file=140november2009.pdf>)
39. ^ "Wibree forum merges with Bluetooth SIG" ([http://www.wibree.com/press/Wibree\\_pressrelease\\_final\\_1206.pdf](http://www.wibree.com/press/Wibree_pressrelease_final_1206.pdf)) (PDF) (Press release). Nokia. 2007-06-12. [http://www.wibree.com/press/Wibree\\_pressrelease\\_final\\_1206.pdf](http://www.wibree.com/press/Wibree_pressrelease_final_1206.pdf). Retrieved 2008-02-04.
40. ^ "Bluetooth.com" ([http://www.bluetooth.com/Bluetooth/Press/SIG/SIG\\_INTRODUCES\\_BLUETOOTH\\_LOW\\_ENERGY\\_WIRELESS\\_TECHNOLOGY\\_THE\\_NEXT\\_GENERATION\\_OF\\_BLUETOOTH\\_WIRELESS\\_TE.htm](http://www.bluetooth.com/Bluetooth/Press/SIG/SIG_INTRODUCES_BLUETOOTH_LOW_ENERGY_WIRELESS_TECHNOLOGY_THE_NEXT_GENERATION_OF_BLUETOOTH_WIRELESS_TE.htm)) . Bluetooth.com. [http://www.bluetooth.com/Bluetooth/Press/SIG/SIG\\_INTRODUCES\\_BLUETOOTH\\_LOW\\_ENERGY\\_WIRELESS\\_TECHNOLOGY\\_THE\\_NEXT\\_GENERATION\\_OF\\_BLUETOOTH\\_WIRELESS\\_TE.htm](http://www.bluetooth.com/Bluetooth/Press/SIG/SIG_INTRODUCES_BLUETOOTH_LOW_ENERGY_WIRELESS_TECHNOLOGY_THE_NEXT_GENERATION_OF_BLUETOOTH_WIRELESS_TE.htm). Retrieved 2010-09-04.
41. ^ <http://www.engadget.com/2011/10/25/bluetooth-sig-unveils-smart-marks-explains-v4-0-compatibility-w/>
42. ^ "CSR.com" (<http://www.csr.com/products/45/csr-energy>) . CSR. <http://www.csr.com/products/45/csr-energy>. Retrieved 2011-04-07.
43. ^ "Nordicsemi.com" (<http://www.nordicsemi.com/eng/Products/Bluetooth-R-low-energy/nRF8001>) . Nordic Semiconductor. <http://www.nordicsemi.com/eng/Products/Bluetooth-R-low-energy/nRF8001>. Retrieved 2011-04-07.
44. ^ "TI.com" (<http://focus.ti.com/docs/prod/folders/print/cc2540.html>) . Texas Instruments. <http://focus.ti.com/docs/prod/folders/print/cc2540.html>. Retrieved 2011-04-07.
45. ^ "iFixit MacBook Air 13" Mid 2011 Teardown" (<http://www.ifixit.com/Teardown/MacBook-Air-13-Inch-Mid-2011-Teardown/6130/1>) . iFixit.com. <http://www.ifixit.com/Teardown/MacBook-Air-13-Inch-Mid-2011-Teardown/6130/1>. Retrieved 2011-07-27.
46. ^ "Broadcom.com - BCM20702 - Single-Chip Bluetooth® 4.0 HCI Solution with Bluetooth Low Energy (BLE) Support" (<http://www.broadcom.com/products/Bluetooth/Bluetooth-RF-Silicon-and-Software-Solutions/BCM20702>) . Broadcom. <http://www.broadcom.com/products/Bluetooth/Bluetooth-RF-Silicon-and-Software-Solutions/BCM20702>. Retrieved 2011-07-27.
47. ^ <sup>a</sup> <sup>b</sup> Stallings, William. (2005). *Wireless communications & networks.* Upper Saddle River, NJ: Pearson Prentice Hall.
48. ^ <sup>a</sup> <sup>b</sup> D. Chomienne, M. Eftimakis (2010-10-20). "Bluetooth Tutorial" (<http://www.newlogic.com/products/Bluetooth-Tutorial-2001.pdf>) (PDF). <http://www.newlogic.com/products/Bluetooth-Tutorial-2001.pdf>. Retrieved 2009-12-11.
49. ^ Juha T. Vainio (2000-05-25). "Bluetooth Security" (<http://www.iki.fi/jiitv/bluesec.pdf>) . Helsinki University of Technology. <http://www.iki.fi/jiitv/bluesec.pdf>. Retrieved 2009-01-01.
50. ^ Andreas Becker (2007-08-16) (PDF). *Bluetooth Security & Hacks* ([http://gsec.es/~anto/ubicuos2/bluetooth\\_security\\_and\\_hacks.pdf](http://gsec.es/~anto/ubicuos2/bluetooth_security_and_hacks.pdf)) . Ruhr-Universität Bochum. [http://gsec.es/~anto/ubicuos2/bluetooth\\_security\\_and\\_hacks.pdf](http://gsec.es/~anto/ubicuos2/bluetooth_security_and_hacks.pdf). Retrieved 2007-10-10.
51. ^ Scarfone, K., and Padgett, J. (September 2008) (PDF). *Guide to Bluetooth Security* (<http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf>) . National Institute of Standards and Technology. <http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf>. Retrieved 2008-10-03.
52. ^ "What is bluejacking?" (<http://www.bluejackq.com/what-is-bluejacking.shtml>) . Helsinki University of Technology. <http://www.bluejackq.com/what-is-bluejacking.shtml>. Retrieved 2008-05-01.
53. ^ "Security Weaknesses in Bluetooth" (<http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.23.7357>) . RSA Security Conf. – Cryptographer's Track. <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.23.7357>. Retrieved 2009-03-01.
54. ^ "Bluetooth" (<http://web.archive.org/web/20070126012417/http://www.thebunker.net/resources/bluetooth>) . The Bunker. Archived from the original (<http://www.thebunker.net/resources/bluetooth>) on January 26, 2007. <http://web.archive.org/web/20070126012417/http://www.thebunker.net/resources/bluetooth>. Retrieved 2007-02-01.
55. ^ "BlueBug" ([http://trifinite.org/trifinite\\_stuff\\_bluebug.html](http://trifinite.org/trifinite_stuff_bluebug.html)) . Trifinite.org. [http://trifinite.org/trifinite\\_stuff\\_bluebug.html](http://trifinite.org/trifinite_stuff_bluebug.html). Retrieved 2007-02-01.
56. ^ John Oates (2004-06-15). "Virus attacks mobiles via Bluetooth" ([http://www.theregister.co.uk/2004/06/15/symbian\\_virus/](http://www.theregister.co.uk/2004/06/15/symbian_virus/)) . The Register. [http://www.theregister.co.uk/2004/06/15/symbian\\_virus/](http://www.theregister.co.uk/2004/06/15/symbian_virus/). Retrieved 2007-02-01.
57. ^ "Long Distance Snarf" ([http://trifinite.org/trifinite\\_stuff\\_lds.html](http://trifinite.org/trifinite_stuff_lds.html)) . Trifinite.org. [http://trifinite.org/trifinite\\_stuff\\_lds.html](http://trifinite.org/trifinite_stuff_lds.html). Retrieved 2007-02-01.
58. ^ "F-Secure Malware Information Pages: Lasco.A" ([http://www.f-secure.com/v-descs/lasco\\_a.shtml](http://www.f-secure.com/v-descs/lasco_a.shtml)) . F-Secure.com. [http://www.f-secure.com/v-descs/lasco\\_a.shtml](http://www.f-secure.com/v-descs/lasco_a.shtml). Retrieved 2008-05-05.
59. ^ Ford-Long Wong, Frank Stajano, Jolyon Clulow (2005-04) (PDF). *Repairing the Bluetooth pairing protocol* (<http://web.archive.org/web/20070616082657/http://www.cl.cam.ac.uk/~fw242/publications/2005-WongStaClu-bluetooth.pdf>) . University of Cambridge Computer Laboratory. Archived from the original (<http://www.cl.cam.ac.uk/~fw242/publications/2005-WongStaClu-bluetooth.pdf>) on 2007-06-16. <http://web.archive.org/web/20070616082657/http://www.cl.cam.ac.uk/~fw242/publications/2005-WongStaClu-bluetooth.pdf>. Retrieved 2007-02-01.
60. ^ Yaniv Shaked, Avishai Wool (2005-05-02). *Cracking the Bluetooth PIN* (<http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/>) . School of Electrical Engineering Systems, Tel Aviv University. <http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/>. Retrieved 2007-02-01.
61. ^ "Phone pirates in seek and steal mission" ([http://web.archive.org/web/20070717035938/http://www.cambridge-news.co.uk/news/region\\_wide/2005/08/17/06967453-8002-45f8-b520-66b9bed6f29f.lpf](http://web.archive.org/web/20070717035938/http://www.cambridge-news.co.uk/news/region_wide/2005/08/17/06967453-8002-45f8-b520-66b9bed6f29f.lpf)) . Cambridge Evening News. Archived from the

- original ([http://www.cambridge-news.co.uk/news/region\\_wide/2005/08/17/06967453-8002-45f8-b520-66b9bed6f29f.lpf](http://www.cambridge-news.co.uk/news/region_wide/2005/08/17/06967453-8002-45f8-b520-66b9bed6f29f.lpf)) on 2007-07-17. [http://web.archive.org/web/20070717035938/http://www.cambridge-news.co.uk/news/region\\_wide/2005/08/17/06967453-8002-45f8-b520-66b9bed6f29f.lpf](http://web.archive.org/web/20070717035938/http://www.cambridge-news.co.uk/news/region_wide/2005/08/17/06967453-8002-45f8-b520-66b9bed6f29f.lpf). Retrieved 2008-02-04.
62. ^ (PDF) *Going Around with Bluetooth in Full Safety* ([http://www.securenetwork.it/bluebag\\_brochure.pdf](http://www.securenetwork.it/bluebag_brochure.pdf)) . F-Secure. 2006-05. [http://www.securenetwork.it/bluebag\\_brochure.pdf](http://www.securenetwork.it/bluebag_brochure.pdf). Retrieved 2008-02-04.
63. ^ M. Hietanen, T. Alanko (2005-10). "Occupational Exposure Related to Radiofrequency Fields from Wireless Communication Systems" ([http://web.archive.org/web/20061006124651/http://www.ursi.org/Proceedings/ProcGA05/pdf/K03.7\(01682\).pdf](http://web.archive.org/web/20061006124651/http://www.ursi.org/Proceedings/ProcGA05/pdf/K03.7(01682).pdf)) (PDF). *XXVIIIth General Assembly of URSI - Proceedings*. Union Radio-Scientifique Internationale (<http://www.ursi.org/>) . Archived from the original ([http://www.ursi.org/Proceedings/ProcGA05/pdf/K03.7\(01682\).pdf](http://www.ursi.org/Proceedings/ProcGA05/pdf/K03.7(01682).pdf)) on October 6, 2006. [http://web.archive.org/web/20061006124651/http://www.ursi.org/Proceedings/ProcGA05/pdf/K03.7\(01682\).pdf](http://web.archive.org/web/20061006124651/http://www.ursi.org/Proceedings/ProcGA05/pdf/K03.7(01682).pdf). Retrieved 2007-04-19.
64. ^ "Bluetooth Innovation World Cup" ([http://www.bluetooth.com/Bluetooth/Press/Bluetooth\\_World\\_Innovation\\_Cup.htm](http://www.bluetooth.com/Bluetooth/Press/Bluetooth_World_Innovation_Cup.htm)) . Bluetooth.com. [http://www.bluetooth.com/Bluetooth/Press/Bluetooth\\_World\\_Innovation\\_Cup.htm](http://www.bluetooth.com/Bluetooth/Press/Bluetooth_World_Innovation_Cup.htm). Retrieved 2010-09-04.

## External links

- Official website (<http://www.bluetooth.org/>)
- Bluetooth Specifications (<https://www.bluetooth.org/Technical/Specifications/adopted.htm>)

Retrieved from "<http://en.wikipedia.org/w/index.php?title=Bluetooth&oldid=482521513>"

Categories: Channel access methods | Bluetooth | Mobile computers | Networking standards | Wireless

- 
- This page was last modified on 19 March 2012 at 05:48.
  - Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. See Terms of use for details.

<sup>w</sup>ikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

page