Introduction

At Plugable we love connecting things. Our USB products do that with reliable wired connections and we want to provide you with products that do the same for your Bluetooth wireless devices. We want to help connect your smartphone, computer and all of the Internet of Things (IoT) goodies coming to the marketplace.

All of us know Bluetooth; it has been around for well over a decade. As Sheldon Cooper says, "Everything is better with Bluetooth!"[1]. But most of us know the technology primarily for its role as an audio connection between smartphones and headsets. It is much more and now has two distinct 'flavors' to meet market needs ranging from audio to IoT.

In this article, we'll give a bit of background in wireless and Bluetooth technology, and then discuss the newer Bluetooth Low Energy version (also called Bluetooth Smart) of the standard.

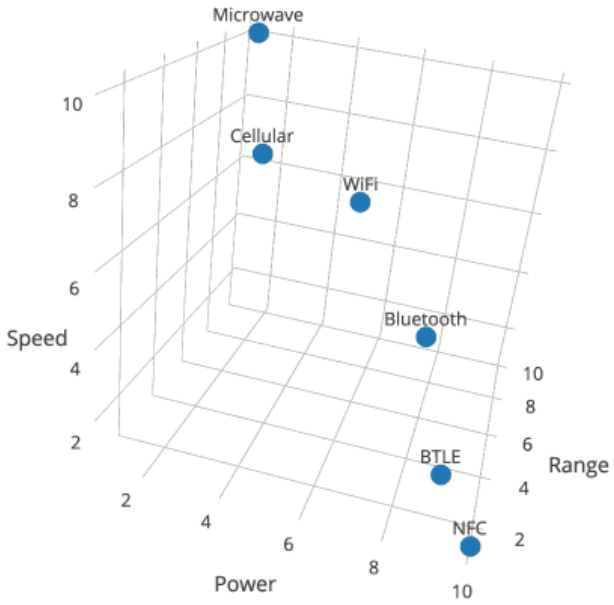
Wireless overview

Wireless technology

Wired connections are fantastic because they can transfer data and power at the same time. But our devices are mobile so that we can interact with them whenever and wherever we want, and it just doesn't make sense to connect cables all of the time.

All technologies have their tradeoffs; wireless technologies have three major factors that interact: speed, power and range. It turns out that like a lot of things in life, you can't have the best of all three. We just can't get around physics; it always wins. The chart below subjectively illustrates the tradeoffs between several commercially available wireless technologies.

[1] The Big Bang Theory: https://www.youtube.com/watch?v=H_lf8_pxg2Q



Interactive view: https://plot.ly/~billsalt/4/wireless-technology-attributes/

At Plugable, we focus on short-range technologies that don't have radar dishes or billing plans. We provide gear that works within your house or business and can easily connect devices that have the longer range and cloud connections.

While there seem to be several choices vying to be the short-range wireless technology that enables the IoT and mobile devices, right now WiFi® and Bluetooth are the clear choices for mobile products. Every handset and operating system today supports WiFi and Bluetooth, and both wireless technologies continue to improve and proliferate.

Bluetooth vs. WiFi

Why do we need *both* Bluetooth and Wifi? They serve two different purposes, and because of physics we can't have everything we want with just one.

WiFi is designed for high-speed large-scale network and internet connectivity for relatively stationary usage: *in one place*. This includes connecting your laptop at work and your smartphone at the coffee shop, airport or hotel. In these cases you want great speed while you are in that particular area and usually have a place to plug in your device if you want to connect for a longer time.

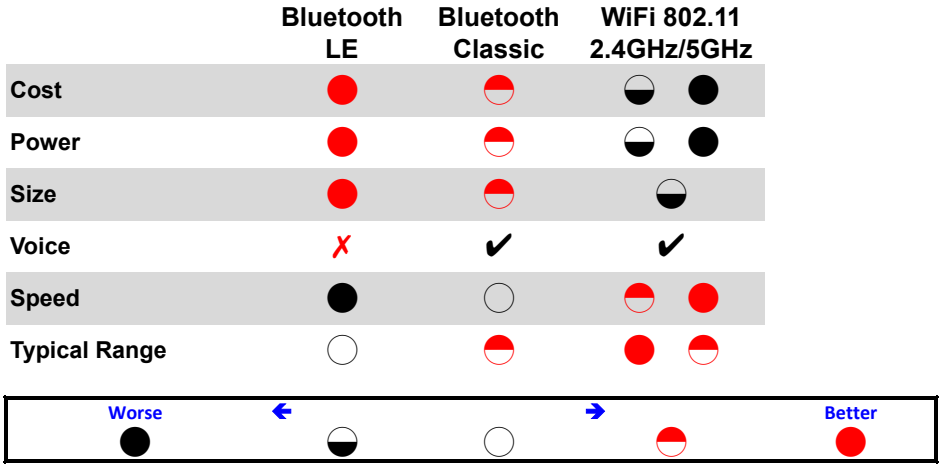
Bluetooth is designed for connections to battery-powered things around a personal device: *in a mobile environment*. In this environment we need a technology that supports devices running on batteries and without needing to plug them in and recharge frequently. The devices are used in places that wired infrastructure is prohibitive due to cost, power and mobility. Familiar examples include the headset

connected to your smartphone, connections to your car, and portable speakers on the beach.

Along with the trade-offs described above in power, range and speed, these technologies also have different cost and size factors that give Bluetooth a real advantage for devices that need to be both very low cost and powered by smaller batteries.

Bluetooth technology was specifically designed to support real-time audio as a native standard data stream, while WiFi requires the additional Voice over IP (VoIP) protocols including several proprietary implementations. WiFi also requires additional infrastructure that consumes even more power with higher data rate requirements. In addition to audio, Bluetooth technology also supports medium-speed data transfers of serial and IP data that is used in point-of-sale printers as well as other applications in consumer, industrial, and medical products.

The chart below subjectively illustrates this and also includes Bluetooth Low Energy (more on that later).



Brief Bluetooth history

Bluetooth[2] wireless technology formally began in a meeting proposed by Ericsson Mobile Communications in 1998 following their own work and discussions with Intel and included the other founding members: Nokia, IBM and Toshiba. It was designed to be an open standard in the unlicensed Industrial, Scientific and Medical (ISM) radio frequency band at 2.4GHz and above.

The group set out to develop a wireless connection technology to provide for communications between mobile phones and peripheral devices for short-term (ad-hoc) connections and initially replace serial (RS-232) cables. A company was created to hold the patents and provide for specification development and testing called the Bluetooth Special Interest Group (SIG)[3]. This group has the responsibility for providing approvals, promoting, and developing the specification.

Since the introduction of Bluetooth Low Energy, the original technology is now also called "Bluetooth BR/EDR" which references its Basic Rate/Enhanced Data Rate features.

Below is a brief history with high points of the evolution of the technology:

- Bluetooth 1.1 (2001)
  - First practical specification
  - Fixed errors in original specification that made it relatively unusable
  - Added RSSI (Received Signal Strength Indication)
  - Ratified as IEEE 802.15.1 (2002)
- Bluetooth 1.2 (2003)
  - Adaptive Frequency Hopping (AFH) greatly improves co-existence with WLAN
  - Improved voice quality
  - Improved data rates
  - Ratified as IEEE 802.15.1 - 2005
- Bluetooth 2.0 (2004)
  - Errata
  - Enhanced Data Rate (EDR) – 3x speed
- Bluetooth 2.1 (2007)
  - Quality of Service (QoS)
  - Secure Simple Pairing (SSP)
  - Security Improvements
- Bluetooth 3.0 (2009)
  - Bluetooth High Speed: Alternate MAC/PHY
  - Not widely implemented…

---

[2] The technology is named after King Harald Blåtand of Denmark from about 940 until about 986. King Harald was nicknamed Bluetooth, with at least two possible origins: he loved and ate lots of blueberries that stained his teeth, or (more likely) he fought a lot and had 'dead' front teeth that looked a bit blue.

[3] See www.bluetooth.com

What was Bluetooth missing?

Bluetooth got off to a good start and found its 'killer' market in the audio connections with headsets and cars. Initial thoughts were that the supported data profiles and protocols weren't quite right for applications that needed a higher data-rate connection and challenged WiFi, but those never seemed to be a good fit for Bluetooth, even with the increased data rates of the 2.0 and 3.0 specifications.[4]

While Bluetooth was and is used in many sensor and remote applications, it doesn't provide the ability to work in low data rate applications requiring small batteries and extended (for years) operation without charging batteries.

A new technology called WiBree was introduced by Nokia in 2006 that leveraged many aspects of Bluetooth technology and had a greatly simplified design. It allowed for the lower power operation in low data rate applications that Bluetooth was missing. After several years of discussion and several key changes to make it more compatible with the existing specification and technology, the Bluetooth SIG formally adopted this in version 4.0 as a feature called "Bluetooth Low Energy." It has since been formally named "Bluetooth Smart" for marketing purposes (though rumor has it that it will be changing back to "Bluetooth Low Energy" or "Bluetooth LE).

Bluetooth BR/EDR and Bluetooth LE devices can not directly connect with each other since there are fundamental differences between them. This issue has been minimized by one of the key features of Bluetooth LE that has allowed for its ease of implementation and wide proliferation: The low energy version is designed to allow implementation in integrated circuits with relatively small changes from their Bluetooth BR/EDR designs. IC manufacturers have quickly implemented dual-mode chips allowing computer, smartphone and tablet manufacturers to add Bluetooth Smart capability at almost no extra cost. These dual-mode devices are labeled as Bluetooth Smart Ready (meaning that they can talk to both types of Bluetooth devices).

A further bit of confusion is that the Bluetooth 4.x specifications and approvals include both types and so devices qualified for Bluetooth 4 can implement either BR/EDR, Low Energy (Smart), or both (Smart Ready).

A brief history of the Bluetooth low energy development:

- Bluetooth 4.0 (2011)
  - Added new Bluetooth low energy (Bluetooth Smart)
  - Provided for dual-mode implementations (Smart Ready)
- Bluetooth 4.1 (2013)
  - Multiple-role (Central/Peripheral, Master/Slave) devices

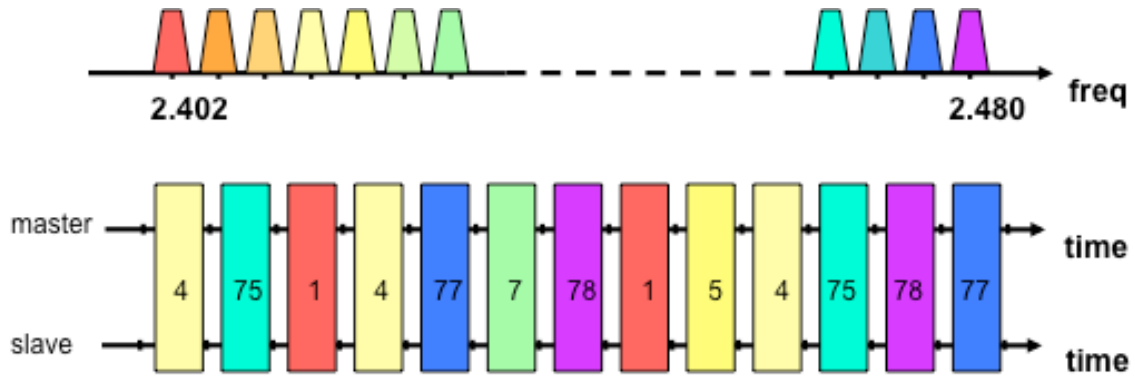
[4] Alternative implementations described in 3.0 included Bluetooth over 802.11 (WiFi) that was prototyped, but never widely utilized. The 3.0 revision also proposed a very high speed transport in conjunction with the Ultra-Wideband (UWB) group that never materialized.

    - IoT architectural enablers
    - Added hand-off between BR/EDR and Low Energy devices
- Bluetooth 4.2 (2014)
    - IoT, IPV6 enablers
    - Increased payload per connection interval (higher data rate)
    - Improved Bluetooth low energy security to match Bluetooth BR/EDR

Bluetooth BR/EDR overview

Let's take a quick overview of Bluetooth BR/EDR to give some context for our main discussion of Bluetooth Low Energy. Bluetooth BR/EDR technology utilizes a frequency hopping, spread spectrum (FHSS) radio at up to 20 dBM (100 mW) of power that allows operation up to about 100 meters.[5] Devices can implement differing power output and receive sensitivity, so 'your mileage may vary'. All Plugable devices are good for at least 10 meters.

Bluetooth BR/EDR divides radio bandwidth into 79 channels, each 1 MHz wide and hops in a pseudo-random sequence between them at 1600 times per second. All the data packets are error checked and provide varying levels of error correction, so that lost or damaged packets are corrected or automatically retransmitted. Since the radio hops so quickly, any lost or damaged data packets are retransmitted on a different channel (frequency), providing a great deal of tolerance of radio interference and making Bluetooth a very robust connection.



Devices are either Master or Slaves (or in some cases both) and are connected in a star configuration. One master can connect with up to 7 slaves simultaneously for data connections or a maximum of 3 audio connections, or a combination of both as the bandwidth allows.

Maximum raw data rates are 1 mbps for Basic Rate (BR) or 3 mbps for Enhanced Data Rate (EDR). Realizable throughput for data is roughly 75% (higher for audio

[5] Lots of people still remember the original 10mW, 10 dBM power giving10 meters, and some think that was 10 feet (Americans!). The reality is that even the low power BR/EDR Bluetooth devices often exceed this. It is also important to remember that range depends on *both* devices since Bluetooth is always a 2-way connection.

since it allows dropped packets), but also depends heavily on the hardware and software implementations.

Pairing and security

The device that wants to be the master starts out by performing a discovery to find devices that are advertising for a connection. Devices can simply connect using one of several methods. Historically, devices were connected securely by the exchange of a fixed 4-digit PIN (headsets used to use 0000, for example). Much better and more secure implementations have largely replaced that method (although a lot of previously designed devices are still shipping with fixed PIN security).

The current security implementation uses "Secure Simple Pairing" (introduced in Bluetooth 2.1) allowing several methods for setting up a secure connection. The appropriate method depends on the capabilities of each device (display, keyboard, etc.). These are shown below:

- Just works: As the name implies, this method just works, with no user interaction. However, a device may prompt the user to confirm the pairing process. This method is typically used by devices such as headsets with very limited capabilities, and is more secure than the fixed PIN mechanism this limited set of devices uses for legacy pairing. This method provides no man-in-the-middle (MITM) protection.
- Numeric comparison: If both devices have a display, and at least one can accept yes/no user input, they may use Numeric Comparison. This method displays a 6-digit numeric code on each device. The user compares the numbers to ensure they are identical. If the comparison succeeds, the user confirms 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 of these 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.

Profiles

Bluetooth BR/EDR connections depend on profiles. A profile is a collection of features and protocols that implement a particular type of connection. For example, the Headset profile allows a phone to connect and transfer real-time audio data

while the Serial Port Profile (SPP) allows for a data connection simulating an RS-232 cable between two devices.

Bluetooth BR/EDR requires operating system implementation for each profile supported by a device. This means that devices are limited to published profiles and constrained by the ones that are implemented; it is not possible to add new Bluetooth BR/EDR profiles without a complete update. A short excerpted (not complete) list of commonly used profiles is shown below:

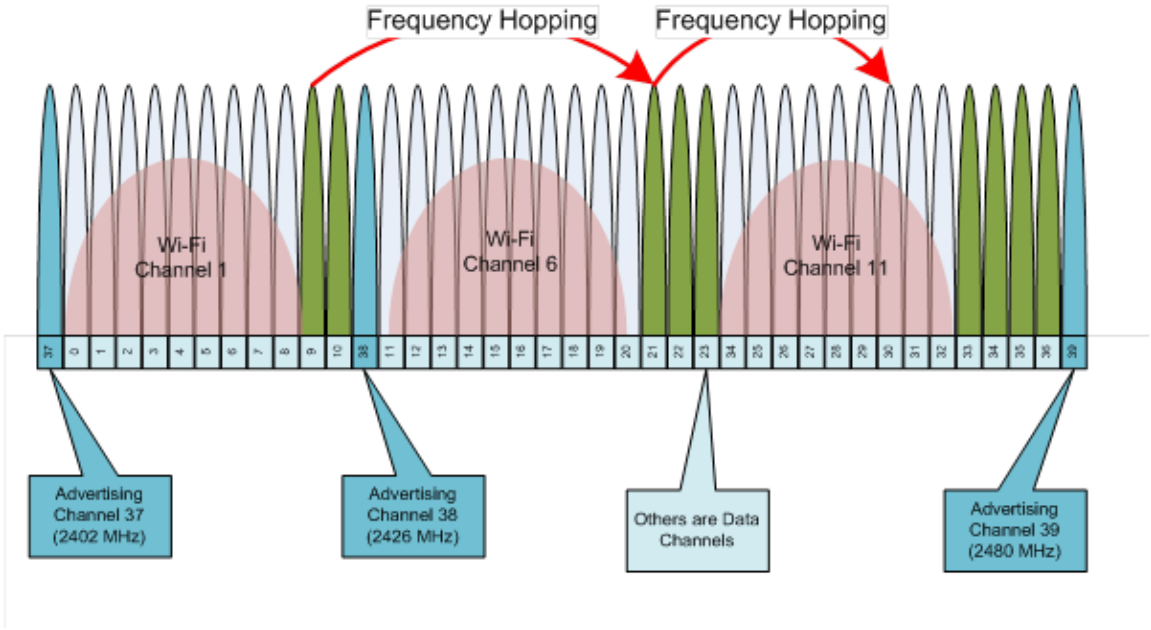
- Generic Access Profile (GAP) – the one profile required of all devices, it supports queries of device type and function and supports identification and setting up additional profiles
- Serial Port –functions required and methods for establishing a virtual serial connection between two devices; it is used in many of the higher level profiles
- Dial-up Networking –functions and methods required to establish a remote internet connection
- Handsfree –functionality to implement a hands-free headset for cell phones and computers
- Advanced Audio Distribution Profile (A2DP) – functionality for stereo headsets and players intended for music playback
- Human Interface Device (HID) – functionality to support keyboard, mouse, joystick
- File Transfer Profile (FTP) – functions to support transfer of files
- Object Push Profile (OPP) – another profile to facilitate transfer of files

Bluetooth Low Energy

Bluetooth Low Energy is "not your father's Bluetooth". While just as robust, it consumes much less power and can be implemented at lower cost. The table below compares the two; several of these features will be discussed below.

Feature	Bluetooth BR/EDR	Bluetooth LE	Notes
Power	AAA batteries for hours/days	Coin cells for months/years	Lower data rate, more efficient connections, fewer/wider channels
Data throughput	BR 720 kbps EDR 2200 kbps	4.x:125 kpbs 4.2:300 kbps	These are typical, realizable throughput figures. Mileage will vary with implementation.
Connections	7	Thousands	Low Energy is limited by implementation, not specification
Packet types	28	3	Mandatory plus optional
Protocols	9	1	
Frequency Channels	79	40	
Channel width	1 MHz	2 MHz	
Advertising	all channels	3 dedicated	
Adaptive Hopping	Yes	Yes	Same robust coexistence method

One of the basic differences, and one that shows immediately why the two kinds of Bluetooth cannot 'talk' with each other, is shown by the frequency diagram below. We discussed that Bluetooth BR/EDR has 79 channels, but shown below are the fewer, wider channels used by Bluetooth Low Energy.

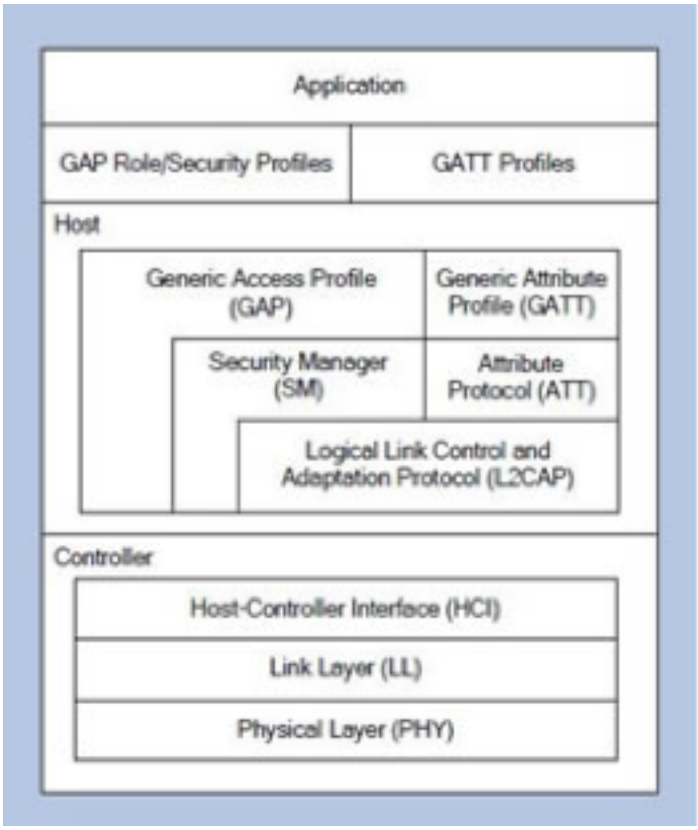


Note that for Bluetooth Low Energy, three of the channels are designated for dedicated advertising and are designed around WiFi channels 1, 6 and 11. The Bluetooth BR/EDR method is for a device to hop in a different sequence at a more rapid pace and look for advertisers. Hopping rapidly helps to increase the odds in the random process of hopping to the same channel to connect. The use of dedicated advertising channels allows Bluetooth Low Energy to connect much more quickly and to further reduce power consumption.

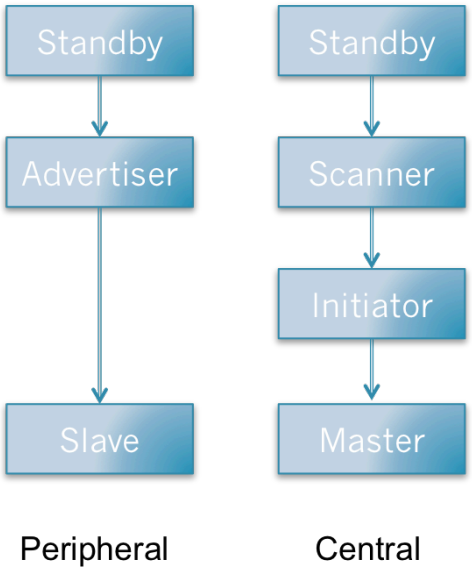
Creating connections

Both Bluetooth BR/EDR and Low Energy use the concept of profiles. Bluetooth Low Energy both simplifies and extends profiles, and allows for the creation and use of custom profiles, something not supported or allowed for in Bluetooth BR/EDR.

Profiles have been previously discussed for Bluetooth BR/EDR. Bluetooth Low Energy only has two required profiles: Generic Access Profile (GAP, similar to Bluetooth BR/EDR) and Generic ATTribute profile (GATT). All other profiles for Bluetooth Low Energy are based on GATT, so operating systems only need to support GATT to allow for a huge range of standard and customer profiles. A typical software implementation is shown in the block diagram below.



GAP defines the two roles of Central and Peripheral, and the two activities of Scanner and Advertiser (respectively). GAP is used to create the connection and is also responsible for security, pairing and bonding. The connection process implemented by GAP is shown below.



Bluetooth Low Energy uses only the Secure Simple Pairing discussed for Bluetooth BR/EDR above for authentication as well as establishing the keys for encryption and bonding. The terms 'bonding' and 'pairing' are often used interchangeably, but they are not: Pairing is the activity of authenticating and exchanging keys that are only good for the current connection[6].

To summarize the connection process for Bluetooth Low Energy:

- Devices with services (see below) advertise (GAP)
    - Uses selected advertising channels to speed discovery
- Devices wanting to use those services scan (GAP)
    - Collect advertising packets
    - (Optionally) ask for extended scan packets
    - Request connection
    - Pair (temporary)
    - Bond (optionally)
    - Set up connection parameters
- Read services, read/write characteristics, accept notifications (GATT)
- …
- Disconnect

Services and Profiles

GATT defines just two roles: Client and Server. One requests data and the other supplies it. The Central is the Scanner and usually becomes the client, but that role can be reversed. Usually the Advertiser is the Peripheral and becomes the Server of data.

Bluetooth Low Energy extends the profile concept by introducing services. A service implements one or more features and can be used as building blocks for profiles. Since services are based on GATT, custom services can be created and used with products that may not have any built-in support for them. Profile support can be (and often is) included in the application software, such as an app on a smartphone.

Examples of services are:

- Battery service – reports the state of charge of the battery
- Device ID service – reports information about a device such as the manufacturer, revisions, etc.
- Heart rate service – reports the current heart rate measurement

A profile can contain one or more services and the concept encourages re-use of services. For example, a hoverboard[7] profile might include:

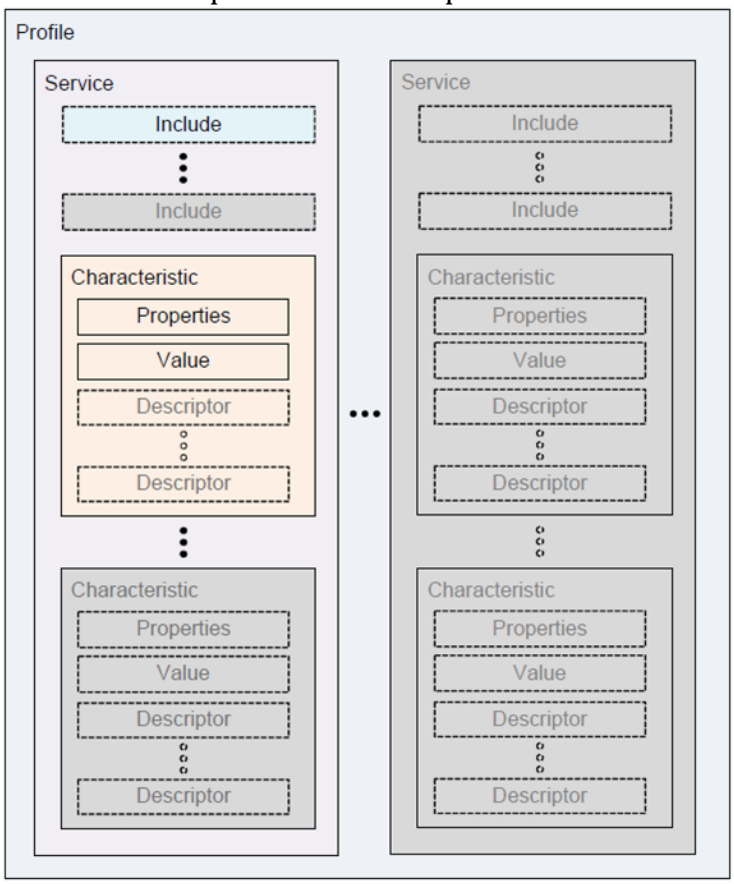
---

[6] If devices request to keep that information for future connections, the keys are stored to speed up the process by bonding. Thus bonding represents stored pairing information.

[7] Plugable does not endorse or condone the use of hoverboards. We just think they're cool looking and make a good example here.

- Battery service - standard
- Device ID service - standard
- Hoverboard service – custom. Reports speed, turns on/off lights and sets limits for 'catch fire' time[8].

The relationship of services and profiles is shown in the diagram below[9]:



GATT

GATT handles the exchange of data for Bluetooth Low Energy. The GATT server stores the data and accepts Attribute Protocol requests, commands, and confirmations from the GATT client.

The Characteristic is the basic building block for data exchange defined by GATT, and Services are defined as a set of Characteristics. In its simplest form, a Characteristic is a collection of bytes and properties. Characteristics can be read and written. In addition, a Characteristic's properties can be set so that it will notify the client upon events such as a change in value. These notifications are asynchronous so that the client does not need to poll for changes, which allows further power savings.

---

[8] Just kidding.

[9] Further information on Profiles and Services for both BR/EDR and Low Energy: https://developer.bluetooth.org/TechnologyOverview/Pages/Profiles.aspx

Services may contain a collection of Characteristics. Characteristics contain a single (or multi-byte) value and any number of descriptors describing the Characteristic value.

More on advertising: Undirected advertising and beacons

Bluetooth Low Energy advertising is quite different from BR/EDR. Advertisements come with a payload of data. This data can be used to describe the device, its name, available services, or simply sent as data. Advertisements can optionally be marked as directed towards a particular Scanner so that a Scanner can filter responses and further speed up the connection process.

Normal advertisements are undirected and may even be made by devices that do not even accept a connection. Think of this as a broadcast or as it is often called, a "beacon." A beacon can transmit 31 bytes of data, and a Scanner can request an extended scan of another 31 bytes from devices that support it. Apple has used this to form the iBeacon specification that works with their OS, and others have proposed and implemented alternative formats[10].

Beacons have great potential for use in retail, factory, and home settings. They can be used along with the Proximity service to locate people, places, and things. Standards and use models are still evolving, but this may well be another killer application for Bluetooth (Low Energy).

Bluetooth low energy future

The future of Bluetooth is very bright. The SIG has announced its roadmap for the next year[11] and it is clearly working towards filling gaps and pushing the technology forward to meet the needs of the IoT and keep it competitive with other available technologies. The highlights of the near term are:

- Improving IoT support with extensions supporting IP connectivity including 6LoWPAN.
- Support of Mesh networking. This is the one feature that other technologies like ZigBee support and is one of the biggest requests. Mesh networking enables several new application areas and can be used to extend range and allow cooperative devices. Several companies have introduced proprietary Mesh solutions based on Bluetooth Low Energy, and the SIG committees are working to publish one standard that will allow for interoperability.
- Higher data rates with little/no power increase, and longer range with some increase in power. Both respond to new and expanded use models and will enable new markets and applications.

---

[10] One good beacon article for further information: https://developer.mbed.org/blog/entry/BLE-Beacons-URIBeacon-AltBeacons-iBeacon/

[11] https://www.bluetooth.com/news/pressreleases/2015/11/11/bluetooth-technology-to-gain-longer-rangefaster-speedand-mesh-networking-in-2016

Conclusion

Bluetooth is a key technology for mobile devices and the IoT. It is ubiquitous, useful and cool. Throughout its development it has continued to expand in its ability to enable new and sometimes unique applications in mobile and low power connectivity.

At Plugable, we want to provide you with cool and useful products to connect you wirelessly and support your mobile needs!

Final notes

- All trademarks are property of their respective owners.
- For more information on Bluetooth technology, please visit www.bluetooth.com
- For more information on WiFi technology, please visit www.wi-fi.org
- For information about Plugable and our products, please visit www.plugable.com