Bluetooth® Low Energy
# Table of Contents

Introduction to Bluetooth ........................................................................................................ 2  
Bluetooth Low Energy: Overview .......................................................................................... 3  
Market Forecast ..................................................................................................................... 6  
Specifications ......................................................................................................................... 7  
Profiles .................................................................................................................................... 9  
Applications .............................................................................................................................. 10  
Testing Bluetooth Low Energy .................................................................................................. 11  
Testing Bluetooth Low Energy with LitePoint’s IQ2010 ......................................................... 16  
Concluding Remarks ................................................................................................................ 18  
Appendix I: References .......................................................................................................... 18  
Appendix II: Curiosities ........................................................................................................... 18
Introduction to Bluetooth

Bluetooth technology is a short-range communications technology whose robustness, low power, and low cost make it ideal for a wide range of devices ranging from mobile phones and computers to medical devices and home entertainment products. The base technology is defined and maintained by the Bluetooth Special Interest Group (SIG) in the “Core Specification,” which serves a uniform structure for devices to interoperate.

Since Version 1.0 (v1.0) of the Bluetooth specification was published in 1999, the Bluetooth SIG has formally adopted several enhancements to the Bluetooth Core Specification (also shown in Figure 1):

- **Core Version 1.2** 05 November 2003
- **Core Version 2.0 + EDR** 04 November 2004
- **Core Version 2.1 + EDR** 26 July 2007
- **Core Version 3.0 + HS** 21 April 2009
- **Core Version 4.0** 30 June 2010

Bluetooth Low Energy (BLE) is the distinguishing feature (subset) of the latest Core Version, Bluetooth v4.0. With the release of BLE, the Bluetooth SIG has built upon the original key features of Bluetooth and set the stage for a variety of new markets, industries, and applications based on devices that must operate with ultra low power wireless connectivity, and be very low cost. The revolution brought forth by BLE is such that the name “Classic Bluetooth” has become popular for Bluetooth v2.1 + EDR and Bluetooth v3.0 + HS, to distinguish these technologies from Bluetooth v4.0.

About LitePoint

LitePoint provides automated, complete solutions to test all key wireless connectivity standards, including Bluetooth. As such, LitePoint is part of the Bluetooth ecosystem and takes pride in sharing its expertise with you, through its website and through its publications. If you have questions or feedback about this booklet, or simply want to connect with LitePoint, please email sales@litepoint.com.
Bluetooth Low Energy: Overview
BLE is characterized by an entirely new protocol stack, for rapid build-up of very simple links. In this chapter, we explore the motivations that led to its definition, as well as its key features and implementations.

Motivations
BLE is Bluetooth SIG’s response to the convergence of several key trends in wireless connectivity:

1. **Wireless everywhere**: connectivity is being added to an increasing number of devices, which have been traditionally connected via cables or not connected at all.

2. **Portability**: while all wireless markets have been growing steadily in the past years, those for portable wireless-enabled devices have witnessed some of the highest rates of growth. The market for smartphones is a classic example; others include watches, proximity tags, remote controls, or personal devices for entertainment and fitness. Portability usually implies that the device is powered by a small battery, such as a coin cell, or more in general that the energy available for the wireless link is limited.

3. **Low-cost**: as wireless becomes pervasive, and competition to penetrate new market opportunities becomes more fierce, pressures for minimizing the cost of adding the wireless capability to our everyday devices continue to increase.

BLE responds to the need for a simple communication link between devices that must operate with very low power consumption, and be very low cost. It is not, obviously, a one-for-all technology; instead, it is particularly suited for those devices that need to transfer very small quantity of data, and do so within relatively short ranges.

What Makes Bluetooth Low Energy Unique
BLE substantially reduces classic Bluetooth’s peak, average, and idle mode power consumption, with energy efficiencies that can be 20 times higher than Classic Bluetooth. The extremely low peak, average, and idle currents of BLE chipsets, shown in Table 1, enable BLE radios to work with very small battery power sources for a year and more.

Table 1. BLE chipsets current consumption. Values are shown as ranges. Exact values depend on the chipset and on the characteristic of the particular communication link.

<table>
<thead>
<tr>
<th>Peak Current</th>
<th>Idle Mode Current</th>
<th>Average Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>tens of mA</td>
<td>tens of nA</td>
<td>~ μA (assuming &lt;1% duty cycle)</td>
</tr>
</tbody>
</table>

BLE’s incredibly low power consumption is enabled by its very simple link layer, designed for quick connections. BLE chips spend most of their time asleep, only waking up to send data - a process that takes only few ms, compared to 100 ms with Classic Bluetooth.

In particular, BLE features:

1. **Smart Host Control.** BLE technology places a significant amount of intelligence in the controller, which allows the host to sleep for longer periods of time and be woken up by the controller only when the host needs to perform some action. This allows for the greatest current savings since the host generally consumes more power than the controller.

2. **Adjustable, ultra-low duty cycle.** While BLE still uses a synchronous protocol, its duty cycle can be adjusted down to just 0.1% (compared to Bluetooth’s 1% duty cycle).

3. **Adjustable message length.** BLE’s message length is also adjustable, to take advantage of the fact that packing large quantities of data into a long packet is more energy efficient than sending multiple packets.

In addition to all of the above, Bluetooth v4.0 also implements a number of other energy-conserving strategies pioneered by proprietary ultra-low power (ULP) technologies, such as maximized standby time, faster connections, and reduced peak transmit/receive power.

---

1 According to the Bluetooth SIG, it can be up to even 100 times higher, depending on the application
Example: Nordic nRF 8001’s power consumption

- Peak current as low as 12.5 mA
- Average current as low as 12 μA for one second connection interval

Single Mode and Dual Mode Chips

BLE chips designs allow for two types of implementation:

- In **single-mode implementation**, the low energy functionality is implemented solely (stand-alone). Single-mode chips have the lowest power consumption and are already available in the market from semiconductor companies such as Nordic Semiconductor, Texas Instruments, and CSR.

- In **dual-mode implementation**, the low energy functionality is integrated in chips that support both BLE and Classic Bluetooth. Dual-mode chips execute a protocol that mediates between the Classic Bluetooth protocol and the BLE protocol. Since they need to support both capabilities, they typically are not as power constrained as the single-mode chips.

BLE single-mode devices are not inter-operable with Classic Bluetooth devices, but only with other single-mode devices or dual-mode devices. The dual-mode devices, on the other hand, are backwards compatible and can operate with other devices supporting any version of Bluetooth technology.

It is important to note that adding BLE to devices with Classic Bluetooth already incorporated is a relatively easy task, estimated to add only a few cents to the BOM cost of the device and with no need for redesign. Unlike other similar, alternative technologies, BLE can build on the existing billions of Bluetooth devices already in the market. This is a significant advantage, which will speed the introduction of the newest BLE devices coming to market, and will be key to their success in the next few years.

Key Features of Bluetooth Low Energy

In addition to its ultra low power consumption, BLE has a number of unique features that set it apart from other available wireless technologies. We will describe in details the BLE specifications in a later section; for now, we want to focus on the following:

- Interoperability
- Robustness
- Simplicity
- Low Cost
- Bit Rates
- Latency
- Range

**Interoperability**

To be successful, any wireless technology must ensure that all devices implementing it can communicate with each other. To ensure that BLE devices can communicate with all other BLE devices, the Bluetooth SIG builds into the definition of the technology strong qualification and interoperability testing processes. Moreover, since BLE operates in the open, license free 2.4 GHz frequency band (just like previous versions of Bluetooth are), manufacturers and users of Bluetooth v4.0 devices can count on these devices to interoperate in world wide applications.

**Robustness**

Like Classic Bluetooth, BLE uses fast, frequency hopping to secure a robust transmission even in the presence of other wireless technologies. This feature makes it very suitable for the home environment, where multiple devices using different protocols, such as WiFi, use the same 2.4 GHz spectrum in a confined space. In addition, adaptive hopping and WiFi/Bluetooth coexistence schemes enable it to be used in a compact device alongside a WiFi radio.
Simplicity

The key characteristic of BLE’s new architecture, which shares much of Classic Bluetooth technology, is its simplicity, as illustrated by Figure 2. Due to this simplicity, devices with built-in single-mode BLE can be made equal to the size of the coin cells that power them, and only a few millimeters thicker.

![BLE (single-mode) Architecture](image)

**Applications**

- Generic Access Profile
- Generic Attribute Profile
- Attribute Protocol
- Security Manager
- Logical Link Control and Adaptation Protocol
- Host Controller Interface
- Link Layer
- Direct Test Mode
- Physical Layer

**Host**

**Controller**

Figure 2: BLE (single-mode) Architecture. The applications layer is built on top of the host, which includes the definition of the generic profiles. BLE technology places a significant amount of intelligence in the controller, which allows the host to sleep for longer periods of time and be woken up by the controller only when the host needs to perform some action.

Low Cost

BLE allows manufacturers to design tiny, single-mode devices with low production costs. In addition, since BLE’s architecture shares much of Classic Bluetooth technology, adding BLE to a Bluetooth chip to create a dual-mode device involves a minimal cost-add.

Figure 3: Typical size of a single-mode BLE chipset

Bit Rates

BLE is most efficient for transferring very small quantities of data. The technology supports very short data packets (8 octet minimum up to 27 octets maximum) that are transferred at 1 Mbps. All connections use advanced sniff sub-rating\(^2\) to achieve ultra low duty cycles. These and more features make BLE a great option for applications where the maximum bit rate is of just a few hundred bits-per-second, or less.

Latency

BLE is optimized for sending small pieces of information with minimal delay (latency). The total time of sending data is generally less than 6 ms, and as low as 3 ms (compared to 100 ms with Classic Bluetooth). This enables an application to form a connection and send data for a short communication burst before quickly tearing down the connection.

\(^2\) Sniff sub-rating is a Bluetooth feature that enables paired devices to negotiate, based on usage, the frequency of sending “keepalive” messages to one another. This feature was first introduced as part of the Bluetooth Core Specification Version 2.1 + EDR.
Range
Thanks to an increased modulation index, BLE technology offers a somewhat improved range with respect to Classic Bluetooth: theoretically, up to 200 feet and beyond. However, the technology is still suited for mainly small-range applications. As with previous versions of the specification, the range of the Bluetooth v4.0 radio may be optimized according to the application and the Bluetooth SIG expects most single-mode and dual-mode devices to continue using with the typical 30 foot (10 m) range of Classic Bluetooth.

Market Forecast
BLE is positioned to be a key enabling technology for several new markets, whose growth we are just starting to witness today.

The success of the Bluetooth market is well known. Forecast to grow to 1.4 billion unit shipments in 2011, the Bluetooth market enjoys remarkably high penetration rates (over 50%) in mobile phones and portable computing devices. Today, these two applications are expected to account for almost 80% of Bluetooth IC shipments during this year 2011.

The intent of the Bluetooth SIG with BLE is to diversify the use of Bluetooth into new markets. Opportunities abound in markets ranging from health and fitness monitors, to automotive devices, to solutions home entertainment and control, as will be discussed later in this booklet. In these and more markets, single mode BLE is forecast to grow to over one billion units shipped in 2015, as shown in Figure 4 (data from ABI Research).

The market drive of single mode BLE devices is not to be underestimated. By providing the ability to use BLE separately from standard Bluetooth devices, it is bound to attract new players and their innovations in the market. Dual mode BLE devices are forecast to be equally successful in the market. As Figure 5 shows, dual mode chipset will grow to over two billion shipments in 2015. Classic Bluetooth devices (standalone, without BLE) will almost disappear by this date.

![Figure 4. World market forecast of single mode BLE unit shipments](image)

![Figure 5. World market forecast of standalone Classic Bluetooth and BLE dual-mode shipments](image)
Specifications
In addition to the key features discussed before, BLE differs from Classic Bluetooth by a number of technical specifications, which are the subject of this chapter. Some important differences, along with some important similarities, are summarized in Table 1.

Not included in this section are the important differences between Classic Bluetooth and BLE with respect to the test specifications. This topic is the subject of a later chapter of this document.

Table 2. Comparison of Classic Bluetooth and BLE Technical Specifications

<table>
<thead>
<tr>
<th>Technical Specification</th>
<th>Classic Bluetooth</th>
<th>Bluetooth Low Energy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>2400 to 2483.5 MHz</td>
<td>2400 to 2483.5 MHz</td>
</tr>
<tr>
<td>Modulation Technique</td>
<td>Frequency Hopping</td>
<td>Frequency Hopping</td>
</tr>
<tr>
<td>Modulation Scheme</td>
<td>GFSK</td>
<td>GFSK</td>
</tr>
<tr>
<td>Modulation Index</td>
<td>0.35</td>
<td>0.5</td>
</tr>
<tr>
<td>Number of Channels</td>
<td>79</td>
<td>40</td>
</tr>
<tr>
<td>Channel Bandwidth</td>
<td>1 MHz</td>
<td>2 MHz</td>
</tr>
<tr>
<td>Nominal Data Rate</td>
<td>1 - 3 Mbps</td>
<td>1 Mbps</td>
</tr>
<tr>
<td>Application Throughput</td>
<td>0.7 - 2.1 Mbps</td>
<td>&lt; 0.3 Mbps</td>
</tr>
<tr>
<td>Nodes / Active Slaves</td>
<td>7</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Security</td>
<td>56 to 128 bit</td>
<td>128-bit AES</td>
</tr>
<tr>
<td>Robustness</td>
<td>FHSS</td>
<td>FHSS</td>
</tr>
<tr>
<td>Voice</td>
<td>Capable</td>
<td>Not capable</td>
</tr>
</tbody>
</table>

Frequency and Modulation Scheme
Key Similarities with Classic Bluetooth are, as we have already discussed, the frequency range (in the 2.4 GHz band) and the use of frequency hopping.

Also, the modulation scheme is the same: both technologies use a Gaussian Frequency Shift Keying (GFSK) modulation. BLE, however, uses a modulation index of 0.5 (close to a Gaussian Minimum Shift Keying (GMSK) scheme), compared to 0.35 for Classic Bluetooth technology. This change lowers power consumption and also improves the range of BLE versus Classic Bluetooth.

Channels
One important difference between BLE and Classic Bluetooth is that, to obtain simpler and cheaper radio chipsets, BLE uses only 40 channels, 2 MHz wide, while Classic Bluetooth uses 79 channels, 1 MHz wide.

The 40 BLE channels are shown in Figure 6. Three channels, which are located exactly between the Wireless LAN channels, are used for device discovery and connection setup. These channels (also known as “advertising” channels) are used by the technology to search for other devices or promote its own presence to devices that might be looking to make a connection. In comparison, Classic Bluetooth technology uses 32 channels for the same task.

This drastic reduction is one more trick that BLE uses to minimize time on air, so as to reduce power consumption. BLE has to switch “on” for just 0.6 to 1.2 ms to scan for other devices using its three advertising channels. Classic Bluetooth, instead, requires 22.5 ms to scan its 32 channels. The power savings are significant: BLE consumes 10 to 20 times less power than Classic Bluetooth technology to locate other radios.
The use of just three advertising channels is not all positive; instead, it comes at a (slight) cost in terms of robustness. With fewer advertising channels, the chance is greater that another radio, broadcasting on one of the chosen frequencies, might be corrupting the signal. This is the reason why the Bluetooth SIG has chosen the advertising channels exactly between the non-overlapping Wireless LAN channels: so that BLE devices will not collide with WiFi devices in these channels.

Protocol
Classic Bluetooth uses 9 different protocols to implement different device functionality. BLE uses only the Attribute Protocol (ATT), a derivative of the classic Service Discovery Protocol (SDP) but adapted and simplified. ATT is sequential (only one request at a time). It uses a client/server architecture, which allows a client to read/write certain attributes exposed by the server in a simple manner, thus reducing the power consumption over more traditional Bluetooth protocols.

Security
Data privacy and integrity is always a concern in wireless applications, and Bluetooth applications are no different. Bluetooth is intrinsically safer than other alternative technologies because it uses a process in which two devices need to be paired to communicate with each other. This process, called “pairing,” is typically triggered automatically the first time a device receives a connection request from a device with which it is not yet paired. Once a pairing has been established it is remembered by the devices, which can then connect to each without user intervention. When desired, the pairing relationship can later be removed by the user. To increase security even further, BLE includes security mechanisms such as authentication, authorization, encryption, and man-in-the-middle protection.

Packets
BLE only has one fixed packet structure with two types of packets: advertising and data.

The key feature of the low-energy stack is a lightweight Link Layer (LL) that provides ultra-low power idle mode operation, simple device discovery and reliable point-to-multipoint data transfer with advanced power-save and encryption functionalities. Figure 7 shows the LL packet format.

<table>
<thead>
<tr>
<th>Preamble (1 octet)</th>
<th>Access Address (4 octets)</th>
<th>PDU (2 to 39 octets)</th>
<th>CRC (3 octets)</th>
</tr>
</thead>
</table>

Figure 7. BLE link layer (LL) packet format

1 similar to 802.15.4 with command and data frame types, but 802.15.4 also uses two extra types: beacon and ACK.
The BLE packet includes:

- **preamble** for synchronization
  - contrary to Classic Bluetooth, BLE’s synchronization word is constructed differently and dynamically assigned during the link setup exchange
- 4 octet (32 bit) **access address** for physical link identification on every packet for each slave
  - the long access address allows billions of devices to be connected
- **PDU** of variable length (from two to 39 packets)
  - this implementation obtains significant power savings by omitting unnecessary information (already known by the receiving device) when possible
  - the PDU header is also different from that of Classic Bluetooth and is shown in Figure 8
- 3 octet (24 bit) **cyclic redundancy code** (CRC)
  - the CRC ensures correctness of the data in the PDU on all packets, thus increasing robustness against interference

<table>
<thead>
<tr>
<th>Header</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLID (2 bits)</td>
</tr>
<tr>
<td>NESN (1 bit)</td>
</tr>
<tr>
<td>SN (1 bit)</td>
</tr>
<tr>
<td>MD (1 bit)</td>
</tr>
<tr>
<td>RFU (3 bits)</td>
</tr>
<tr>
<td>Length (5 bits)</td>
</tr>
<tr>
<td>RFU (3 bits)</td>
</tr>
</tbody>
</table>

Figure 8. Data channel PDU header

**Profiles**

**What is a Profile?**

While the Bluetooth Core Specification (also known as Volume I) defines the base technology, the Profile Definitions (Volume II) defines specific usage of the base technology to support targeted applications, ensuring interoperability between products developed by different manufacturers.

Creating profiles in Classic Bluetooth is usually a challenging task. It requires specifying the low level protocol (L2CAP, RFCOMM, SCO), and high level protocol (AT-commands, IrOBEX, SBC codec). Not only does the definition involve very detailed and large specifications, but also implementation and testing is generally a slow process.

BLE significantly simplifies the task. BLE profiles do not include a definition of the protocol, since only one exists for the technology (ATT). The fact that profiles require very little specification to be written makes them easier to implement, interpret, and adopt.

**Bluetooth Low Energy Profiles**

Bluetooth SIG maintains the official list of Bluetooth specifications on the official Bluetooth website, at the link: https://www.bluetooth.org/Technical/Specifications/adopted.htm. In the table at this link, the BLE profiles are marked “GATT-based profiles.”

Within the latest Bluetooth v4.0 specification, four adopted BLE profiles exist at the time of writing of this document. Two profiles are applicable to proximity sensing and security; the others, to health and wellness.

1. **The BLE Find Me** profile targets smartphone applications, and will allow users to pair small, commonly misplaced everyday objects with their smartphone in order to locate them. One early product example will be BLE key rings to find a misplaced phone (by pushing a button on the ring to make the phone sound an audible alert), or a misplaced key ring (by pushing a button within a smartphone app to make the key ring sound an alert).

2. **The BLE Proximity** profile targets smartphones, computer laptops, and tablets. It extends the functionality of the Find Me profile to include more advanced capabilities such as the ability to trigger an automatic security lock-down if a smartphone or laptop/tablet is separated from its owner by more than a certain threshold distance, or wake a sleeping desktop computer as soon as the user sits down in front of it.

3. **The BLE Health Thermometer** profile was built to enable the wireless monitoring of body functions – in this case, body temperature. For instance, one potential use case for the Health Thermometer Profile involves a thermometer patch that can send temperature measurements to a smartphone every half hour to enable a family member to closely monitor the fever of a sick relative.
4. The BLE **Heart Rate** profile, similarly to the Health Thermometer profile, enables the wireless monitoring of an important body parameter - the heart rate. What's important about this and the previous profile is that they are the model for many more health-related profiles coming soon to support devices like blood pressure monitors, weight scales, and blood glucose meters.

Also expected in the third quarter of 2011 are the Time Profile and Phone Alert Status Profile. The Time Profile will enable devices to receive time, date, and time zone information from another device such as a mobile phone or positioning device with accurate time information. The Phone Alert Status Profile will enable a watch or similar device to notify the user that their mobile phone is ringing, vibrating, or displaying a message. By the end of August 2011, more profiles including the Blood Pressure Profile, Network Availability Profile, and Alert Notification Profile are expected to be finalized.

**Applications**

BLE enables new types of devices that are able to operate for months or even years on tiny batteries. The following markets, and many others, will be certainly enhanced by the availability of coin-cell battery powered wireless products and sensors that use BLE technology:

- Consumer Electronics
- Health and Fitness
- Mobile Phones
- Automotive
- Smart Energy

As of July 2011, many devices are under development and headed to market soon, including the first wave of mobile phones with BLE technology due out in late 2011. To help drive the proliferation of billions of Bluetooth enabled devices into key vertical markets, the Bluetooth SIG created five Bluetooth Ecosystem Teams (BETs) in late 2010, each with focus on one of the application areas listed above.

**Consumer Electronics**

Consumer electronics devices that will benefit from the availability of BLE are, for example, home entertainment devices such as media center remotes and RF remote controls, which will become a necessity for new generations of internet-connected televisions and which could replace the current infrared remote controls.

Portable devices such as watches are also looking at the technology to offer new functionalities to their users. Casio, for example, recently added BLE to its G-SHOCK watch that is capable of sending mobile alerts, transferring incoming call/email/SMS alerts from a BLE-enabled mobile phone to the watch, and locating the phone by transferring signal to the phone alarm.

More traditional segments include, of course, laptops and tablets. Just recently (in July 2011), Apple has announced the addition of the technology to its latest MacBook Air and Mac Mini models.

**Mobile Phones**

A mobile phone is an obvious home for a dual-mode Bluetooth device, since it can provide the ideal end-terminal to connect the user to the variety of single-mode Bluetooth devices about to come into the marketplace. A mobile phone enabled by a dual-mode Bluetooth chip can receive health and fitness information from a monitoring device; it can remotely control the opening of your car doors and receive information about any malfunctioning of the vehicle and its parts; and, it can become the hub for all the Bluetooth-enabled smart energy appliances in your home.

The powerful advantage of being able to connect any BLE device to a mobile phone is such that the Bluetooth SIG sees the future of BLE technology tied strongly to how quickly phone manufacturers will incorporate it in their phones. Currently, the Bluetooth SIG forecasts the smartphone market to reach 700 million units by 2015, and expects BLE technology ICs to be incorporated in all such phones. Early indications are that high volumes of BLE-enabled phones will be shipping as early as in 2012.
Monitoring Devices for Health and Fitness

BLE connected health and fitness devices are forecasted to reach hundreds of millions of annual device shipments in the next five years. BLE-enabled sensors, coupled with a mobile phone, will make it possible to monitor patient information and route it to physicians and other care providers, enabling new, more effective, and more affordable ways of health care delivery. The intrinsic security, high reliability, low power, and simplicity of BLE are a perfect fit for these types of devices.

The Bluetooth SIG has explicitly chosen to initially focus its efforts on the Health and Fitness markets; since September 2010, the SIG partners with industry leaders in health and fitness, phone manufacturers, IMS Research and a major mobile operator to research new BLE technology products for these applications.

Automotive

Within the area of automotive, BLE can be featured in applications relating to the security of the car, for instance by including it into key-fob and other “secure entry” contactless devices for identifying the driver, opening the car, disabling security systems and even starting the car. Key fob systems already exist, of course, but they have low efficiency and lack the ability to connect to other devices such as mobile phones. BLE will offer all of that and much more.

Furthermore, manufacturers can aim to integrate BLE-enabled pressure sensors into the car to feature applications in automotive diagnostics such as tire pressure monitoring. These sensors would communicate wirelessly to warn the driver of any malfunctioning.

Smart Grid

Currently, Bluetooth technology is already used to support a variety of smart energy applications, and enables with wireless connectivity devices that range from simple energy sensors to complex mesh networks controlling solar arrays. BLE technology can provide solutions in smart energy particularly for applications where robust operation, data transmission efficiency, and ability to coexist with other technologies are very important, and the application throughput can be small. Examples of these devices are remote control and home automation devices, including home appliances.

As already mentioned, one of the major advantages of the technology for the smart grid area is the existing Bluetooth ecosystem, which makes it seamless for consumers to start using BLE in their smart grid devices. Bluetooth is already in mobile phones and many personal computers, which can provide the necessary user interface for smart energy applications. Thanks to Bluetooth, the integration of a smart ecosystem throughout the home could be made very easy, and very fast.

Testing Bluetooth Low Energy

The Bluetooth SIG has included in the definition of BLE a number of important changes, with respect to Classic Bluetooth, for manufacturers on how to test their devices. The key changes are:

- **Introduction of a Predefined Test Mode**, which allows sending N packets from the device and counting the packets received by the device. (In addition, it also sets the frequency.)
  - Importantly, the Bluetooth SIG makes a Direct (Non Link) Test Mode mandatory, as opposed to leaving to manufacturers of Bluetooth devices the choice between Non Link test mode and Link test mode as in the past. In Non Link test mode for BLE, test procedures assume full control over the Host Control Interface or UART interface to test directly at the PHY level.
- **Simplified and Optimized Test Cases**, which include the definition of:
  - Dirty Packets for Sensitivity Testing
  - PER Testing (as opposed to Classic Bluetooth’s BER Testing) for the Receiver Test Cases
- **Predefined Test Packets**. For the first time with BLE, the test packets have been fully defined in the test specification.

This section is entirely focused on the key changes above, and on the impact that these changes have on the manufacturing practices of BLE device makers. For a complete list of the BLE test specifications, we refer to the Bluetooth Low Energy RF PHY Test Specification (document no. RF-PHY.TS/4.0.0) published by the Bluetooth SIG.
BLE Direct (Non Link) Test Mode

Traditionally, Bluetooth SIG has given manufacturers the option to test their devices with either Link or Non Link mode. The difference between the two approaches is schematically shown in Figure 10.

The Link test mode requires the test software to interface with the Bluetooth software stack to establish a link—as if the tester were a Bluetooth device. This approach has become popular because it is well known and established, it tests for software failures in addition to hardware failures, and it does not require any code development for the tester to communicate with the device.

In a production line, however, one does not need to test software. Failures are due to manufacturing differences, which only affect the hardware: for manufacturing testing, one should assume that the software is working correctly, and only look for manufacturing defects. It makes no sense in a manufacturing environment to test in every chip if the DSP code has somehow changed. Hence, the time needed in a Link-based test to setup and teardown a connection (link) between the tester and the device is essentially a wasted and expensive resource, and drives manufacturing costs up.

The Non Link based test mode, contrary to the Link based mode, interfaces directly with the lowest layer of the BLE protocol stack (the PHY). Since the software stack is bypassed, the Non Link-based test verifies the functionality of the device hardware only. The obvious advantage of this approach is that it is considerably faster than Link testing, since the tester does not need to establish a link with the device, and to do so every time the frequency changes. Despite this advantage, the Non Link approach to testing is relatively new and little-known, hence has not been widely adopted by Bluetooth device manufacturers. Also, using Non Link testing requires the development of a test program up front, a task that might have contributed to impeding adoption of this approach.

With the adoption of BLE, one of the goals of the Bluetooth SIG has been to create a very low-cost technology for applications in a variety of new market segments. Consistently with this goal, the Bluetooth SIG has decided to make testing of BLE devices with Non Link mode mandatory, by including this approach to test as part of the technology specifications.

Manufacturers of Bluetooth devices that support BLE, in either single mode or dual mode implementations, now have an even stronger incentive to adopt the newest Non Link based test mode. Not only does Non Link enable significant time (cost) savings in a manufacturing environment, but also, it enables the manufacturer to fully comply with the latest Bluetooth specifications.

LitePoint has pioneered the use of Non Link testing to verify Bluetooth chipsets functionality in a manufacturing environment with its innovative wireless test equipment and technology. In particular, Non Link testing of any Bluetooth device - including BLE devices - is supported by LitePoint’s IQ2010, a powerful multi-radio test system described in a later section of this document. Moreover, manufacturers of Bluetooth wireless devices can leverage LitePoint’s extensive software expertise to accelerate the development of a test program for their Bluetooth devices. In a high-volume manufacturing environment, the significant reduction in test time per device typically offsets the effort required to meet this requirement.
BLE RF PHY Test Cases
To ensure interoperability between all BLE devices in the marketplace, as well as to verify that a basic level of system performance is guaranteed for all BLE products, the Bluetooth SIG defines the BLE RF PHY Test Cases. These are a series of functional and parametric tests, over a specified range of parameter variation, which verifies the functionality of the BLE RF PHY.

BLE RF PHY test cases and test case implementations are derived from the Basic Rate Bluetooth RF test cases. However, the introduction of Non Link (direct) test mode and a combination of the following factors contributes to minimizing BLE RF PHY testing time substantially:

- Relaxed RF PHY spec (e.g. blocking resolution)
- Reduction of the number of RF PHY test cases (e.g. removal of regulatory tests)
- Optimized test case implementations

Tables 3 and 4 summarize the BLE RF PHY transmitter and receiver test cases, respectively. The test frequencies differ depending on the test case and on the particular device. We refer to the Test Specifications for a complete list of these frequencies and details of each test case.

Table 3. Transmitter Tests

<table>
<thead>
<tr>
<th>TRM-LE/CA/01/C</th>
<th>Output power at NOC¹</th>
<th>verifies the maximum peak and average power emitted from the BLE device at normal operating conditions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRM-LE/CA/02/C</td>
<td>Output power at EOC¹</td>
<td>verifies the maximum peak and average power emitted from the EUT at extreme operating conditions.</td>
</tr>
<tr>
<td>TRM-LE/CA/03/C</td>
<td>In-band emissions at NOC¹</td>
<td>verifies that the in-band spectral emissions are within limits at normal operating conditions.</td>
</tr>
<tr>
<td>TRM-LE/CA/04/C</td>
<td>In-band emissions at EOC¹</td>
<td>verifies that the in-band spectral emissions are within limits at extreme operating conditions.</td>
</tr>
<tr>
<td>TRM-LE/CA/05/C</td>
<td>Modulation characteristics</td>
<td>verifies that the modulation characteristics of the transmitted signal are correct (i.e. the frequency deviation is measured with different payload sequences).</td>
</tr>
<tr>
<td>TRM-LE/CA/06/C</td>
<td>Carrier frequency offset and drift at NOC¹</td>
<td>verifies that the carrier frequency offset and carrier drift of the transmitted signal is within specified limits at normal operating conditions.</td>
</tr>
<tr>
<td>TRM-LE/CA/07/C</td>
<td>Carrier frequency offset and drift at EOC¹</td>
<td>verifies that the carrier frequency offset and carrier drift of the transmitted signal is within specified limits at extreme operating conditions.</td>
</tr>
</tbody>
</table>

Note:
1. NOC and EOC tests are the same except for the operating conditions (extreme temperature, air humidity, supply voltage), which do not impact the test equipment requirements.
Table 4. Receiver Tests

<table>
<thead>
<tr>
<th>Test Case</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RCV-LE/CA/01/C</td>
<td>Receiver sensitivity at NOC&lt;sup&gt;1&lt;/sup&gt; verifies that the receiver sensitivity is within limits for non-ideal signals at normal operating conditions. The non-ideal signals (dirty packets) used in this test are within the specification limits, but deviate from the ideal case. All BLE devices must meet PER better than 30.8% for a minimum of 1500 packets transmitted by the tester at -70 dBm input power.</td>
</tr>
<tr>
<td>RCV-LE/CA/02/C</td>
<td>Receiver sensitivity at EOC&lt;sup&gt;1&lt;/sup&gt; verifies that the receiver sensitivity is within limits for non-ideal signals at extreme operating conditions. The non-ideal signals (dirty packets) used in this test are within the specification limits, but deviate from the ideal case. All BLE devices must meet PER better than 30.8% for a minimum of 1500 packets transmitted by the tester at -70 dBm input power.</td>
</tr>
<tr>
<td>RCV-LE/CA/03/C</td>
<td>C/I and receiver selectivity performance&lt;sup&gt;2&lt;/sup&gt; verifies the receiver's performance in presence of co-/adjacent channel interference. The receiver mirror image rejection performance is also verified in this test.</td>
</tr>
<tr>
<td>RCV-LE/CA/04/C</td>
<td>Blocking performance&lt;sup&gt;2&lt;/sup&gt; This test verifies that the receiver performs satisfactory in the presence of interference sources operating outside the 2400MHz - 2483.5MHz band.</td>
</tr>
<tr>
<td>RCV-LE/CA/05/C</td>
<td>Intermodulation performance&lt;sup&gt;2&lt;/sup&gt; verifies that the receiver intermodulation performance is satisfactory (PER better than 30.8% for a minimum of 1500 packets transmitted by the tester). The frequency relation between the wanted signal and the interferers.</td>
</tr>
<tr>
<td>RCV-LE/CA/06/C</td>
<td>Maximum input signal level verifies that the receiver is able to demodulate a wanted signal at high signal input levels (-10 dBm or higher).</td>
</tr>
<tr>
<td>RCV-LE/CA/07/C</td>
<td>PER Report Integrity verifies that the device report mechanism reports the correct number of received packets to the tester.</td>
</tr>
</tbody>
</table>

Note:
1. NOC and EOC tests are the same except for the operating conditions which do not impact the test equipment requirements.
2. Testing selectivity, blocking, and intermodulation performance requires 2 signal sources.

Testing with Dirty Packets
The Bluetooth Low Energy RF PHY Test Spec document specifies the use of non-ideal signals, also known as “dirty packets,” for receiver sensitivity test cases.

Every 50 packets, the carrier frequency offset, modulation index, and symbol timing error are changed to specific value combinations described in the Test Spec and reported here in Table 5.

<table>
<thead>
<tr>
<th>Test run</th>
<th>Carrier frequency offset</th>
<th>Modulation index</th>
<th>Symbol timing error</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100 kHz</td>
<td>0.45</td>
<td>- 50 ppm</td>
</tr>
<tr>
<td>2</td>
<td>19 kHz</td>
<td>0.48</td>
<td>- 50 ppm</td>
</tr>
<tr>
<td>3</td>
<td>- 3 kHz</td>
<td>0.46</td>
<td>+ 50 ppm</td>
</tr>
<tr>
<td>4</td>
<td>1 kHz</td>
<td>0.52</td>
<td>+ 50 ppm</td>
</tr>
<tr>
<td>5</td>
<td>52 kHz</td>
<td>0.53</td>
<td>+ 50 ppm</td>
</tr>
<tr>
<td>6</td>
<td>0 kHz</td>
<td>0.54</td>
<td>- 50 ppm</td>
</tr>
<tr>
<td>7</td>
<td>- 56 kHz</td>
<td>0.47</td>
<td>- 50 ppm</td>
</tr>
<tr>
<td>8</td>
<td>97 kHz</td>
<td>0.5</td>
<td>- 50 ppm</td>
</tr>
<tr>
<td>9</td>
<td>- 25 kHz</td>
<td>0.45</td>
<td>- 50 ppm</td>
</tr>
<tr>
<td>10</td>
<td>- 100 kHz</td>
<td>0.55</td>
<td>+ 50 ppm</td>
</tr>
</tbody>
</table>

Table 5. Transmitter parameters for Dirty Packets
In addition to fixed frequency offset, a defined frequency drift is added to the signal characteristics. This is implemented by adding a sinusoidal low frequency modulation to the signal, with deviation of 50 kHz and a modulation frequency of 625 Hz (90° should be equivalent to the duration of a packet). The modulating signal is synchronized with the packets so that each alternating packet starts at 0° and 180° of the modulating signal. Figure 11 illustrates the frequency drift emulation principle.

Figure 11. Frequency drift in BLE sensitivity testing.

**What Difference do Dirty Packets make?**

By comparing the results of testing receiver sensitivity in the same BLE devices with and without dirty packets, we have shown that the main difference between the two approaches is a deviation of about 1 to 2 dB in the receiver input power at which the device meets the sensitivity threshold, as shown in Figure 12.

When testing their BLE devices in a manufacturing line, this deviation can result in a difference in the number of pass/fail devices during receiver sensitivity testing. LitePoint recommends using dirty packets in sensitivity testing of BLE devices. Alternatively, manufacturers can choose to test with standard packets and tighten the pass/fail threshold (limit setting) during sensitivity testing appropriately.

Figure 12. PER measurement of BLE device, with and without dirty packets, -90 dBm to -100 dBm receiver input power. The plot shows a difference of about 1 dB in the receiver input power at which the device meets the sensitivity threshold of 30.8%.
PER Testing
PER Test is used for BLE receiver testing, as opposed to the use of BER Test for Classic Bluetooth devices. The PER requirement is expressed as: PER < 30.8% after at least 1500 packets.

This PER requirement equates to a BER of 0.1% under a series of assumptions specified in the Test Specifications document. These assumptions are used to describe a hypothetical (yet, realistic) situation in which the number of significant bits in an LE test packet is 368 bits (out of a total of 376 bits), and the probability of the sequence of containing no bit errors is $0.999368 = 0.692$, hence the resulting PER requirement is $(1 - 0.692) \cdot 100\% = 30.8\%$.

Test Packets
The packet format used in all BLE tests is fully defined in the Test Specification document. The reference packet consists of:

- preamble (8 bit)
- synchronization word (32 bit)
- PDU header (8 bit)
- PDU length (8 bit), payload (296 bit) and CRC (24 bit), totaling 376 bits.
  - depending on the test, the packet payload content may vary.

Note that test packets do not incorporate a PDU address field. Figure 13 illustrates the Reference Signal Packet Format.

Testing Bluetooth Low Energy with LitePoint’s IQ2010
Full support for all versions of Bluetooth, including BLE, is included in LitePoint’s IQ2010 Multi-Radio Test System.

LitePoint’s IQ2010 is the first and only tester with concurrent and sequence-based test capabilities for multiple wireless standards. In addition to Bluetooth, IQ2010 base system also tests WiFi and can be technology license-configured to add GPS, FM, NFC and WiMAX capabilities. ZigBee support can be also added to the system by installing the LitePoint’s ZigBee Software on any IQ2010 configuration.

LitePoint’s BLE analysis in the IQ2010 addresses all key transmitter and receiver analysis changes over Classic Bluetooth described in this document. All tests cases described in Table 3 and Table 4 are supported, including the new sensitivity measurement based on the impaired or “dirty packets” described above. The new BLE test packets, as fully defined in the Test Specification document by the Bluetooth SIG, are also included in the IQ2010 analysis software.

IQ2010 tests both Classic Bluetooth and BLE devices with Non Link test mode, enabling you to save in test time and cost per single Bluetooth device, and, to comply with the latest Bluetooth SIG specifications.

---

4 Testing selectivity (RCV-LE/CA/03/C), blocking (RCV-LE/CA/04/C), and intermodulation performance (RCV-LE/CA/05/C) requires 2 signal sources. The tester provides the “wanted signal” source only. The analysis program analyzes one packet per capture. For more details on LitePoint’s BLE Transmitter and Received Measurements, please consult the IQ2010 Test System Datasheet available on LitePoint’s website, www.litepoint.com.
To verify the performance of your BLE devices, IQ2010 offers a C / C++ API test automation method and also includes a simple, easy-to-use graphical user interface (GUI). Figure 14 shows an actual GUI BLE transmitter measurement.

![Figure 14](image)

Figure 14. Actual BLE transmitter measurement in IQ2010's graphical user interface programming environment.

In addition to offering full support to Bluetooth and all key connectivity standards, the IQ2010 offers the fastest test times thanks to the innovative LitePoint technology built onto the tester's powerful architecture.

IQ2010 makes single-insertion testing of multi-standard devices possible, thereby reducing the test time by 20% over multi-insertion techniques. Furthermore, the IQ2010 allows multi-radio concurrent testing: up to 3 standards can be tested at the same time (i.e. GPS, FM, and Bluetooth), enabling up to 50% test time reduction with respect to traditional approaches when multiple standards need testing. Finally, proprietary sequence-based testing capability dramatically reduces WiFi test time for supported devices, for example by allowing multiple transmit data rates to be tested in 1 capture, eliminating the communication between the device and tester during PER testing, and more.

In addition, the IQ2010 Extensions (a measurement-oriented library of commands) further reduce test time substantially by addressing all components of test time. They do so while working with ordinary WiFi/Bluetooth manufacturing drivers, without any special device requirements.

To learn more about LitePoint’s Bluetooth support and the advantages of testing your devices with the powerful IQ2010 Multi-Radio Test System, please visit [www.litepoint.com](http://www.litepoint.com) or email sales@litepoint.com.
Concluding Remarks
There is no doubt that BLE has opened entirely new markets for devices that require low cost components and low power wireless connectivity. LitePoint Corporation, the leader in wireless test solutions, is at the forefront of wireless technology and creates powerful solutions to help you test these devices. LitePoint’s mission is to simplify testing and to enable you to achieve the lowest test cost while shortening your time-to-market and ensuring high-quality test coverage for your devices. LitePoint is your ideal partner during the development and manufacturing of your wireless innovations for the promising and fast-growing BLE market.

Appendix I: References
  - This document describes the Bluetooth low energy physical layer.
  - This document defines test structures and procedures for qualification testing of Bluetooth implementations of the Bluetooth Low Energy RF physical layer.

Appendix II: Curiosities
Why is It Called Bluetooth?
The developers of this wireless technology first used the name “Bluetooth” as a code name, but the name stuck. The word “Bluetooth” is taken from the 10th century Danish King Harald Bluetooth. King Bluetooth had been influential in uniting Scandinavian Europe during an era when the region was torn apart by wars and feuding clans.

The founders of the Bluetooth SIG felt the name was fitting because Bluetooth technology was first developed in Scandinavia, and is able to unite very differing industries under a common, simple wireless communication radio.

Where Did the Logo Come From?
A Scandinavian firm originally designed the logo at the time the SIG was formally introduced to the public. Keeping to the same origin as the Bluetooth name, the logo unites the Runic alphabetic characters “H”, which looks similar to an asterisk, and a “B”, which are the initials for Harald Bluetooth.

About the Author
Marta Gaia Zanchi lives in Silicon Valley, California, where she graduated with a Ph.D. in electrical engineering from Stanford University. She enjoys helping innovative organizations deliver their technologies into the marketplace, through effective business planning and the development of successful product management tools and strategies. Her core technical expertise is in the areas of wireless communications and medical devices and applications.