CHAPTER 6

Bluetooth Low Energy—Fundamentals

6.1 Introduction

As described in Chapter 1, Bluetooth Low Energy is the next major evolution of the Bluetooth technology. It specifies requirements for devices to have ultra low power consumption. This is a radical change from the direction in which the technology was evolving through previous versions. While the focus of previous versions was either feature enhancements or increase in the throughput, LE focused in an entirely new direction—how to cut down the power consumption drastically? LE technology is fully optimized from the ground up to ensure that the power consumption is kept to a minimum. This meant a complete redesign of several key components to ensure that all steps are taken to reduce the power requirements.

In general Bluetooth devices are battery powered. It's expected that the LE devices may have smaller batteries like the coin cell batteries (or even smaller ones). This technology focuses on reducing both the peak current and the average current. A reduced average current ensures that the battery drains down slowly. A reduced peak current means that the devices can continue operating even when the battery has started running down and the maximum current that the battery can provide has been reduced.

Some of the uses for LE were shown in Chapter 1. These included finding devices, alerting devices, proximity detection, sensors, healthcare, sports and fitness equipment, mobile payments, etc. It may be noted that none of those use cases focused on high throughput or transferring big chunks of data. Rather the use cases focused on transferring very short pieces of information that could be transferred only when needed, which may generally not be very frequent.

Typical LE use cases would include creating a connection, transferring a few bytes or kilobytes of data and then disconnecting. The connection time is so low that it's easier to reestablish the connection every time a data transfer is needed without any impact on the user experience. This is in contrast to BR/EDR use cases like a connection that is maintained for a long time to ensure that there is least latency when there is an incoming call, or use cases like the exchange of big file in the case of FTP profile.

There are two broad classifications of Bluetooth systems.

- The first is the classic Bluetooth system that conforms to versions prior to 4.0 of the Bluetooth specification. It is also referred to as BR/EDR. BR stands for Basic Rate indicating that the device can support up to a maximum data rate of 721 kbps. EDR stands for Enhanced Data Rate indicating that the device can support up to a maximum data rate of 2.1 Mbps.
- The second is the LE system which conforms to 4.0 (or higher) version of the Bluetooth specification and supports enhancements for ultra low power. These systems have lower complexity and lower cost compared to BR/EDR systems. The throughput is significantly lower. The maximum throughout is about 305 kbps for 4.0 compliant devices and 800 Kbps for 4.2 compliant devices, though devices generally don't need or use such high rate data transfers.

A device can support only BR/EDR, only LE, or both BR/EDR and LE. A device which supports both BR/EDR and LE is also referred to as BR/EDR/LE or dual mode device. This will be explained in further detail later in this chapter.

The architecture of BR/EDR devices was covered in detail in previous chapters. This chapter and further chapters will focus on the architecture of LE devices.

6.2 Single Mode versus Dual Mode Devices

Depending on the functionality supported, the Bluetooth devices may be categorized into 3 types:

1. *BR/EDR Devices:* These are the classic Basic Rate/Enhanced Data rate devices which do not support the LE functionality.
2. *LE Only Devices or Single Mode LE Devices:* These devices support only LE functionality. Examples of these devices include watches, key fobs, heart rate monitors, thermometers, sports and fitness equipment, sensors, etc. These devices are expected to have ultra low power consumption and last for several months or years on coin cell batteries.
3. *BR/EDR/LE or Dual Mode Devices:* These devices support both BR/EDR and LE functionality. Typically these devices are smartphones, tablets, PCs, etc. These devices are expected to communicate with both the BR/EDR devices and single mode LE devices even at the same time. These devices don't have as stringent requirements on power consumption as the single mode LE devices since these have bigger batteries or are generally recharged frequently.

The use cases of LE only devices were explained in Chapter 1. Some of the possible use cases of Dual Mode devices are as follows:

1. A person is listening to music or taking a call on the Bluetooth headset and the child (or the pet) goes out of range. In this case the user would be

alerted about the child (or the pet) going out of range by the proximity detection feature of LE so that the person can take immediate action.

2. A person walks into the home while on a call. The presence detection function of LE may automatically switch on the lights or switch on the air conditioning.
3. A person is jogging on a treadmill and wants to listen to music on the Bluetooth headset and at the same time monitor his/her heart rate, number of steps he/she has run, etc.
4. A person using a GPS enabled smartphone while cycling wants to see distance covered on the track and parameters like current heart rate, maximum heart rate, average heart rate, calories burnt, etc. In addition to displaying on the smartphone, the same data could be sent to the laptop or fitness center for further analysis using the smartphone as a gateway.

Table 6.1 provides information on compatibility between different categories of devices.

Some examples of communication between the various devices types are provided below:

1. BR/EDR to BR/EDR—Classic Bluetooth communications between:
   a. Mobile phone to headset.
   b. Laptop to laptop.
   c. PC to printer.
2. Single Mode LE to Single Mode LE—Low energy ecosystem
   a. Sports sensor displaying data on a watch.
3. Single Mode LE to Dual Mode
   a. A laptop sending an alert to a key fob.
   b. A heart rate monitor sending data to the hospital's computer using smartphone as the gateway.

6.3 Bluetooth Smart Marks

The Bluetooth smart marks were created to help consumers ensure compatibility among their Bluetooth devices. There are two trademarks from the Bluetooth SIG:

Table 6.1 Compatibility Between Single Mode and Dual Mode Devices

	BR/EDR	*Single Mode LE*	*Dual Mode*
BR/EDR	Yes	No	Yes
Single Mode LE	No	Yes	Yes
Dual Mode	Yes	Yes	Yes

- Bluetooth Smart;
- Bluetooth Smart Ready.

6.3.1 Bluetooth Smart (Sensor-Type Devices)

Bluetooth Smart devices are sensor-type devices that are used to collect a specific piece of information. After collecting this information, these devices send it to the Bluetooth Smart Ready devices. Bluetooth Smart devices include only a single mode LE radio and are expected to consume ultra low power.

Some examples of Bluetooth Smart devices are heart rate monitors, thermometers, sports equipment, etc. These devices collect a specific piece of information like heart rate or temperature and then relay it to the Bluetooth Smart Ready devices.

Bluetooth Smart trademark was developed to brand qualified devices as meeting the following three requirements:

1. Conform to Bluetooth 4.0 or higher with GATT based architecture.
2. Contain Single mode LE radio.
3. Use GATT-based architecture to enable a particular functionality (GATT-based architecture will be explained in detail in subsequent sections).

6.3.2 Bluetooth Smart Ready (Hubs)

Bluetooth Smart Ready devices are the devices that receive data sent from the classic Bluetooth and Bluetooth Smart devices and give it to applications that make use of that data. The applications could be running on these devices themselves or could be running anywhere else on the internet. These devices implement the dual mode radio and can connect to the BR/EDR devices as well as the Bluetooth Smart devices. Such devices have one single Bluetooth device address which is used for both the BR/EDR and LE radios. Some examples are phones, tablets, PCs etc.

Bluetooth Smart Ready mark was developed to brand qualified devices as meeting the following three requirements:

1. Conform to Bluetooth 4.0 or higher with GATT based architecture.
2. Contain Dual mode radio.
3. Provide a means by which the end user can choose to update the functionality for a Bluetooth Smart device on a Bluetooth Smart Ready device. For example if the user buys a new Bluetooth Smart device then new software can be installed on the smart phone to communicate to that device.

Figure 6.1 shows Bluetooth, Bluetooth Smart and Bluetooth Smart Ready devices. In this scenario, the mobile phone is the Smart Ready device and it is communicating to two devices at the same time:

1. Streaming audio data to a Bluetooth headset.
2. Collecting temperature information from a Bluetooth Smart thermometer and acting as a hub to relay that information to a server located in the hospital. The server can then take the appropriate action like informing the doctor or pharmacist.

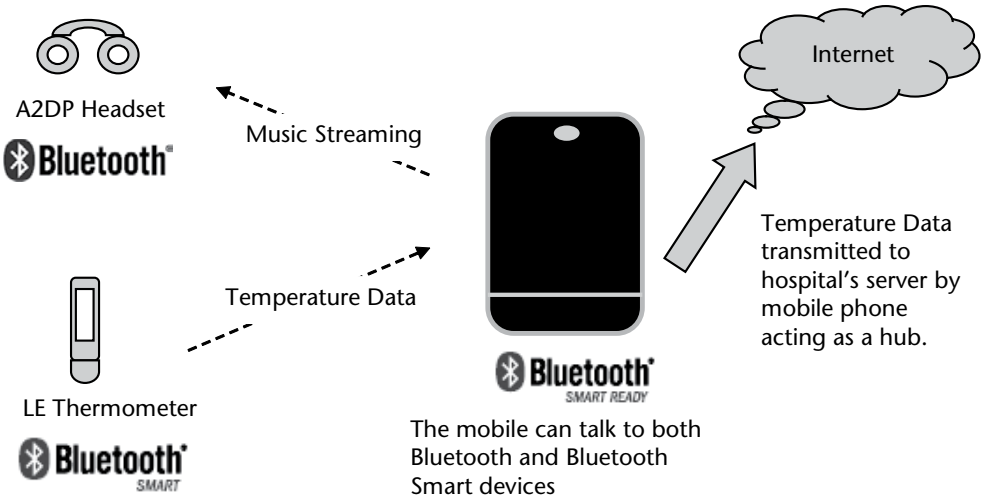

Figure 6.1 Bluetooth, Bluetooth Smart, and Bluetooth Smart ready devices.

6.4 LE Fundamentals

The devices which are based on BR/EDR require a recharge in a few days or few weeks and are generally using larger batteries than coin cell batteries. Take, for example, a Bluetooth keyboard, mouse, headset, etc. All have relatively large batteries and need a recharge every few days or weeks.

Achieving a power consumption of several months to several years with LE was not as easy as optimizing the power consumption of various layers in the Bluetooth architecture. That would not have led to drastic reduction in the power consumption. So LE has been designed almost from scratch to ensure that all possibilities to achieve ultra low power consumption have been incorporated. It is designed ground up for simplicity, low cost and ultra-low power consumption without compromising robustness, security, global usage, or ease of use. Most importantly the compatibility of dual mode devices with the existing BR/EDR devices has been preserved to ensure that nothing gets broken when manufacturers upgrade their existing devices to BT 4.0-based devices.

There are several enhancements done in BT 4.0 specification to achieve low power. Some of the fundamental concepts related to LE operation are introduced below. These will be explained at length in the following chapters.

6.4.1 Frequency Bands

Similar to the BR/EDR radio, the LE radio operates in the 2.4 GHz ISM band. This band is globally license free and is shared by several other wireless technologies. LE also uses a frequency hopping mechanism to combat interference. (Frequency hopping was explained in Chapter 3).

One important difference between BR/EDR and LE is that while BR/EDR uses 79 channels for frequency hopping, LE uses only 40 channels. Secondly there are

dedicated channels for advertising and sending data in the case of LE. This will be explained in detail later in Chapter 8.

6.4.2 Mostly Off Technology

LE can be termed as a "mostly off" technology. This means that the LE devices are expected to be sending data only occassionally and be in a switched-off state for the remaining time. For example, the heart rate monitor may collect all data and then send it across once per hour or once per day, the weighing machine may send the weight only once per day or once per week, or a temperature sensor may send the data only if the temperature crosses a certain threshold limit.

LE technology is designed in such a manner that the LE devices remain off most of the time and switch on only when they need to transmit some data. This ensures that the duty cycle (ratio of device off to device on) is almost close to zero and the device will only switch on when some specific conditions are triggered. Normally the device would just remain off.

6.4.3 Faster Connections

LE takes much less time to create connections as compared to BR/EDR. This is because LE uses only 3 dedicated advertising channels which can be used for creating connections. This is in contrast to BR/EDR where 32 channels are used for inquiry and paging (connection).

Since BR/EDR has more channels, the device takes more time in scanning across all channels before a connection can be created. A typical BR/EDR connection can take up to 20 milliseconds while in the case of LE the connection time is less than 3 milliseconds because the device has to scan on only 3 channels.

A faster connection means that whenever the device needs to send the data, it can quickly connect, transmit data, and then disconnect. The total time for this transaction may be in the range of only 3 to 4 milliseconds. This means that the LE radio needs to be switched on for a very short time. The shorter the time that the radio is switched on the lower the power consumption. The device may switch itself off until it needs to transmit data again.

This is in contrast to BR/EDR. For example, in the case of a headset that is connected to a mobile phone, the headset may remain connected to mobile phone for several days. During this time the headset would be in sniff mode. This would mean that it would be waking up periodically to see if the mobile phone has data to send. This would translate into continuous drain of battery since the headset would wake up periodically and check to see if the mobile phone has any data to send.

6.4.4 Reduced Functionality

LE incorporates some major reductions in the functionality so that it can target a specific market—the one which needs devices to be consuming ultra low power. So it cuts down heavily on the functionality to reduce the memory required to implement that functionality.

Some of the major reductions are:

1. Not mandatory to implement both transmitter and receiver—LE is designed in such a manner that a device can implement only transmitter, only receiver or both transmitter and receiver. For example an LE weighing machine may implement only the transmitter. As soon as it has measured the weight, it just transmits and does not need to receive anything. Such devices would reduce the silicon area to almost half as compared to devices which implement both transmitter and receiver.
2. No support for voice channels—LE is intended for devices that send short amount of data infrequently. It is not intended for devices like headsets which need to transfer continuous stream of voice data. So the SCO/eSCO functionality has been completely removed.
3. No support for Scatternet—LE provides support for only a piconet and the support for scatternet has been removed. This has simplified the state machine of the link layer since a device can only be in one piconet at a particular time. While BR/EDR supports only up to 7 devices in a piconet, an LE piconet can have any number of devices, limited only by the resources available on the piconet master device. So removal of scatternet functionality in LE did not put any restriction on the number of devices that could be connected together while it also simplified the link layer state machine. The support for scatternets was added in specifications 4.1 as optional, so the system designers could choose this flexibility at the cost of adding complexity.
4. No support for Master/Slave role switch—BR/EDR allowed the possibility to switch the roles of Master and Slave. In LE, once a connection is made, the role switch is not permissible. It is also clearly defined right in the beginning which device will end up being a Master and which device will end up being a Slave. This led to a lot of simplification of the link layer state machine.
5. No need for continuous polling of the link. In the case of BR/EDR, even if there is no data exchange, POLL/NULL packets are continuously exchanged to check if the remote device is still present, leading to consumption of power. In the case of LE, there is no need to continuously monitor the link. Devices can just shut down the link and recreate it whenever needed without any impact on the user experience. This is because the link setup time is far less in case of LE as compared to BR/EDR.
6. No support for sniff and park modes. The LE controllers are designed to be very simple and power efficient from ground up. The connection is created for a very short duration—only when the data is transferred, and then disconnected. So there is no need for separate power saving modes. It can be said that the default mode for LE is already power savings mode and so no additional power savings modes are defined.

6.4.5 Shorter Packets

LE uses packets of much shorter size as compared to BR/EDR which means that the time needed to transmit or receive them is lesser. So the radio will be switched on for a lesser time leading to savings in power consumption.

Besides this the buffer space needed to store the packets is much lesser. The maximum size of LE packet is 27 bytes which is much shorter than the maximum size of 1021 bytes supported by BR/EDR (As discussed in Chapter 3, the maximum size of 3DH5 packets is 1021 bytes). The maximum packet size allowed by 4.2 specification is 251 bytes, which is still much shorter than BR/EDR packets.

Besides lesser times, shorter packets also require much lesser power to transmit. This is because of radio characteristics. If a long packet has to be transmitted, the radio needs to be in a high power state for a longer period of time, resulting in the heating up of silicon. This changes the material's physical characteristics and deviation in the transmission frequency which could result in a packet loss or even link loss. To counter this, the radio needs to be constantly recalibrated in order to ensure that the transmission frequency is correct. Recalibration logic makes the radio more complex and also requires power for the recalibration. In comparison shorter packets ensure that the silicon stays cool and the characteristics don't change. Hence no recalibration logic is needed.

6.4.6 Reduced Dynamic Memory Footprint

Another design principle used in LE is to optimize the usage of dynamic memory as much as possible. This is because firstly memory requires silicon area which contributes to the costs and secondly dynamic memory requires constant supply of current to retain the contents that are stored in it. So it adds to the current consumption of the device. (Dynamic memories typically need to be refreshed continuously so that they do not lose the contents. In contrast ROM and FLASH memories do not need to be refreshed).

To reduce the dynamic requirements on memory, LE incorporates the following:

1. Shorter packets—The amount of buffer memory space needed for storing packets is much smaller in case of LE due to shorter packet sizes. This was explained in the previous section.
2. Shorter headers—LE uses only a 32-bit access code to reduce the overall size of the packet. This again leads to less time to transmit the packet and lesser buffer requirement.
3. Simple Protocol—The LE protocol has been designed to be very simple so that there is least state information to be stored. For example the Link Layer has only 5 states and a very limited number of state transitions. Similarly the L2CAP layer has also been simplified a lot to support a very limited number of CIDs (Channel Identifiers) and signaling commands. These will be explained in detail in the subsequent chapters.
4. Uniform Packet Format—LE uses only one packet format for all types of packets. This makes the logic for creating packets on the transmitter side

and parsing packets on the receiver side much simpler thereby reducing the code that has to be implemented.

6.4.7 Optimized Power Consumption of Peripherals

LE is designed in such a manner that the peripherals consume the least amount of power while the central devices could consume a bit more power to compensate. This is because generally the peripherals are resource constrained. They have smaller batteries, memory and limited processing power. In contrast, the central devices may have much higher processing power and much bigger batteries. These may even be powered from mains (For example a TV, PC, or a set-top box) or may be recharged frequently (For example a mobile phone or a tablet).

As an example, if a weighing machine gets connected to a mobile phone to send data, then it's more important to optimize the power consumption of the weighing machine as compared to optimizing the power consumption of the mobile phone. The mobile phone may be charged every day or every alternate day while the weighing machine's battery may be replaced only once in a few months or years.

The LE protocol is designed in such a manner that the peripheral needs to be powered on for as less time as possible while the central device may be continuously powered on to wait for any data coming from the peripheral. So in the case of weighing machine transmitting data to the mobile phone, the mobile phone may always be scanning for packets while the weighing machine may just transmit packets when it has some information to transmit. So the weighing machine will be powered on for far lesser time as compared to the mobile phone.

Another important point is that, in the wireless radio world, transmitting packets consumes much less power than receiving packets. So LE tries to reduce the time for which the peripherals are receiving packets. Instead of this the LE protocol is designed in such a manner that the peripherals mostly transmit packets instead of scanning and receive only for very short durations, if they really have to. So in the case of weighing machine example, the weighing machine would transmit (advertise) to consume less power while the mobile phone would receive (scan). The weighing machine, may in fact never receive anything and may not even have a receiver in it.

6.4.8 No Need for Continuous Polling

In the case of LE, for devices to remain connected, there is no need for continuous exchange of packets as long as the link layer is synchronized to the timing, frequency and access address parameters.

This is in contrast of BR/EDR where, to remain connected, continuous POLL/NULL packets are exchanged even if there is no data to send. BR/EDR does provide the possibility to put the connection into low power mode to reduce the exchange of packets but packets are still exchanged leading to power consumption.

6.4.9 Backward Compatibility with BR/EDR

There are billions of BR/EDR device already in use. Mobile phones, tablets and laptops have an attach rate of almost 100%. LE technology is designed in such a manner that dual mode devices which are based on the BT 4.0 specification are backward compatible with the existing devices. This means that the next generation of mobile phones, laptops and other devices can be upgraded to BT 4.0 devices without breaking existing compatibility. Once these devices get upgraded to BT 4.0, they will also be able to talk to LE devices in addition to BR/EDR. So LE builds on to the ecosystem that has already been established by BR/EDR and paves the way for next millions and billions of devices.

A summary of the key LE features is shown in Table 6.2.

6.5 LE Architecture

LE has a layered architecture just like BR/EDR. The architecture of LE is shown in Figure 6.2. In many ways it's similar to the architecture of classic BR/EDR stack. It also uses the concept of protocols and profiles. (This was explained in Chapter 2).

The design of profiles is quite simplified in the case of LE. LE introduced the concept of GATT based profiles. Most of the common functionality that is needed by all profiles is moved into the ATT protocol and GATT profile. The profiles on top of GATT use the services that are provided by GATT and only implement the bare minimum things that are needed to support that specific use case.

In the next chapters, each of the protocol layers will be covered in details. The mechanisms that are employed by each of the protocol layers to reduce the

Table 6.2 Summary of Key LE Features

Connection Type	*Frequency Hopping Spread Spectrum.*
Spectrum	2.4 GHz ISM Band. Regulatory range: 2400 – 2483.5 MHz.
Frequency Hopping	Across 40 RF channels. The channels are separated by 2 MHz.
Modulation	Gaussian Frequency Shift Keying (GFSK).
Maximum Data Rate	305 kbps (4.0), 800 kbps (4.2)
Maximum Data Packet size	27 bytes (4.0), 251 bytes (4.2)
Typical Range	30 m to 100 m.
Topology	Master Slave architecture. The number of slaves is limited only by the availability of resources on the master.
Connection Time	In the range of 2.5 milliseconds. LE supports a much lower connection time as compared to BR/EDR. So it's easier to just re-establish the connection and transfer data in case of LE instead of keeping the connection alive.
Data Security: Authentication Key	AES 128 bit key.
Data Security: Encryption Key	AES-128 (Stronger than BR/EDR)
Voice Channels	Not supported.
Applicability	Does not require line of sight.
	Intended to work anywhere in the world since it uses unlicensed ISM band.

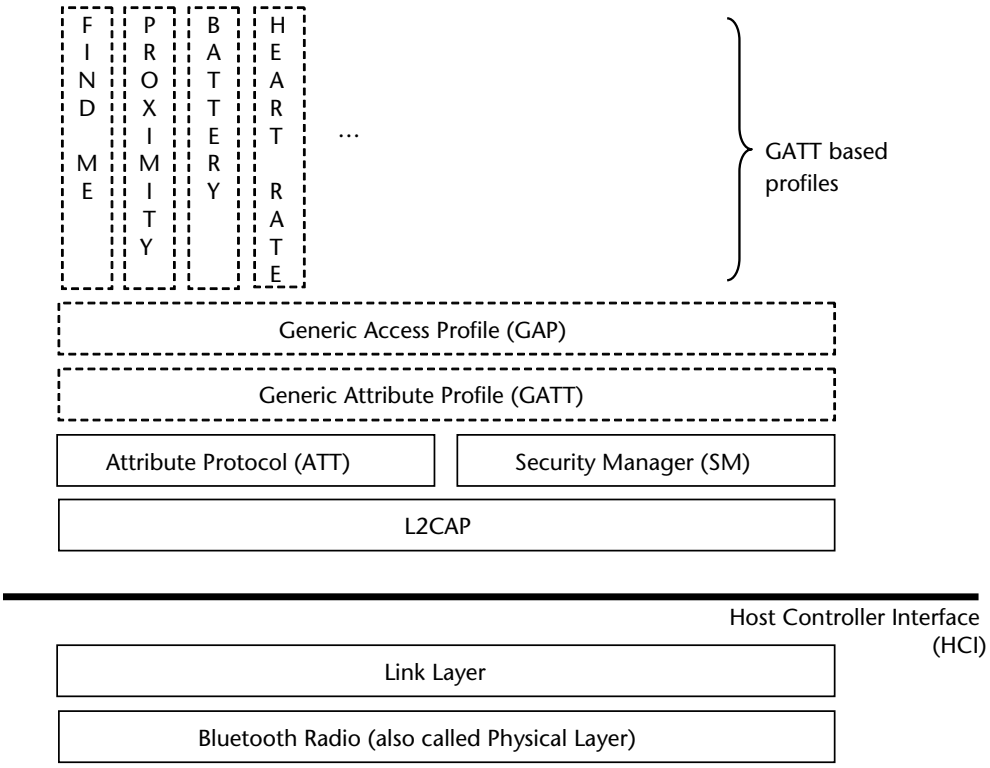

Figure 6.2 LE architecture.

power consumption will also be pointed out specifically so that the reader is able to appreciate the reasons why this technology is designed for ultra-low power operations.

6.6 Comparison between BR/EDR and LE

The architectural comparison of the BR/EDR and LE protocol stack is shown in Figure 6.3. The LE stack modifies some of the existing protocol layers and profiles like the L2CAP layer and the GAP profile. The LE radio has also been modified as explained above. LE also replaces some layers entirely to gain significant power savings. For example the link layer is defined from scratch.

In the case of dual mode devices, the implementation of some of the layers can be shared. For example a combined LE + BR/EDR radio can be used and the implementation of the L2CAP layer, HCI and GAP profile can be shared for the dual mode devices. This helps in maintaining backward compatibility as well as re-using the efforts that were spent already in developing code for these layers.

A broad level comparison between BR/EDR and LE is shown in Table 6.3. There are several other differences besides these and those differences will be highlighted in the next chapters at the appropriate places.

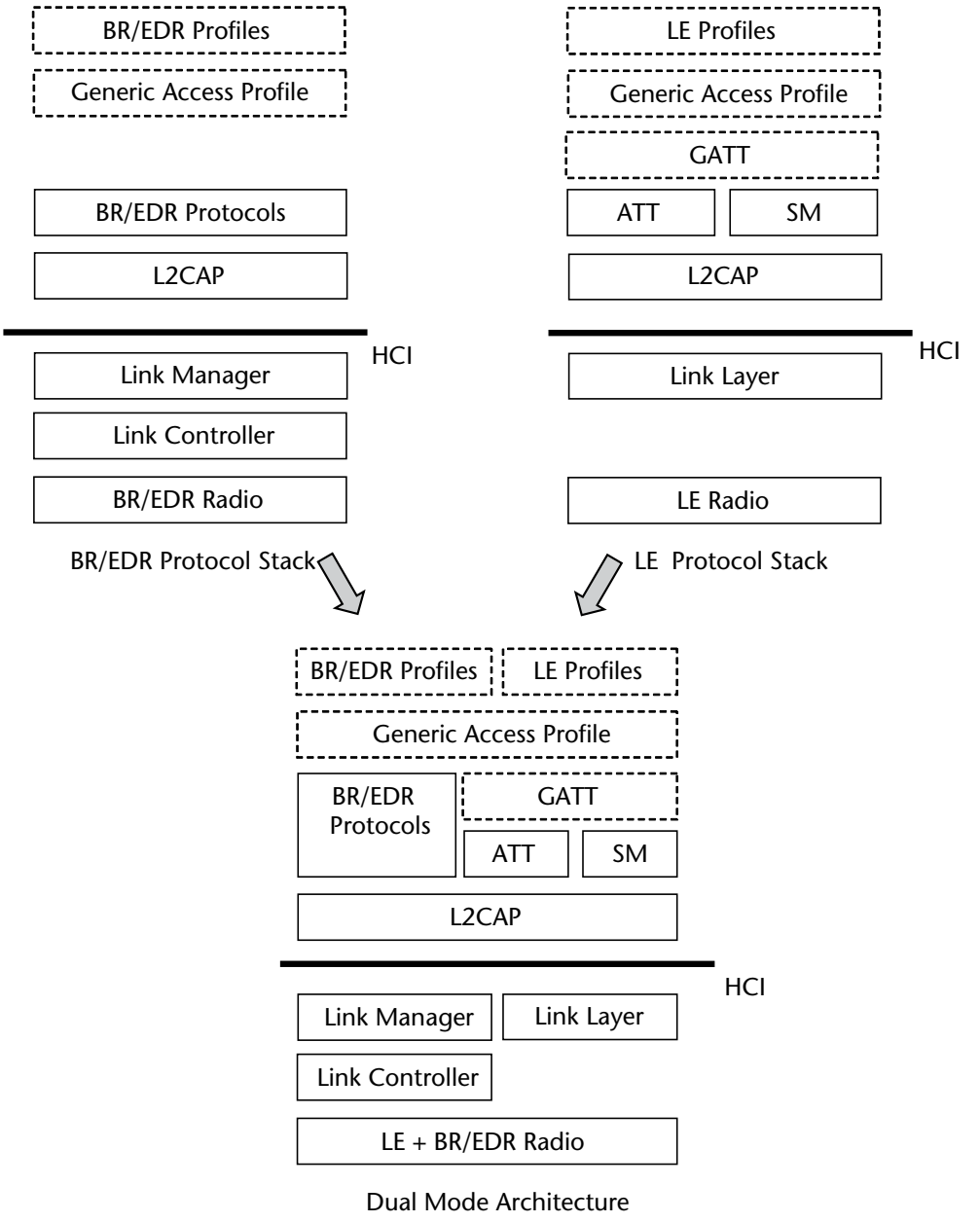

Figure 6.3 BR/EDR protocol stack, LE protocol stack, and dual mode architecture.

6.7 Summary

LE technology offers dual benefits. First, it builds on to the existing ecosystem of Bluetooth devices, and secondly, it offers a drastic reduction in the power consumption for LE only devices. This has opened up several new use cases where this technology can be effectively deployed.

Table 6.3 Comparison of BR/EDR and LE

Feature	*BR/EDR*	*LE*	*Remarks*
RF Channels and spacing	79 channels spaced by 1 MHz each	40 channels spaced by 2 MHz each	
Dedicated RF Channels	No dedicated RF channels. All are used for data.	3 channels dedicated for advertising.	
		37 channels dedicated for data.	
Range	Typically 10m to 30m. Can go to max of 100 m	Typically 30m to 50m. Can go to a max of 100m.	Typically LE based devices have a longer range
Connection time	In the range of 20 ms	Less than 3 ms	Much less time required to make a connection.
Maximum Packet Size	1021 bytes	27 bytes	LE uses much smaller packets.
Maximum Data Rate	BR: 721 kbps EDR: 2.1 Mbps	305 kb/s	LE supports much lower data rates. Even these data rates are seldom used.
Scatternet Support	Yes	No	LE simplifies implementation complexity by disallowing scatternets.
Master/Slave Role Switch	Supported	Not Supported	Simpler state machine.
Transmitter/Receiver	Both transmitter and receiver are mandatory	Device can have only transmitter, only receiver or both	LE saves a lot of silicon area if the device has to only transmit or only receive.
PDU Format	Several	One	LE has only one PDU format. This makes it simpler to create and parse packets
CRC Strength	16-bit	24-bit	Much more robust, especially in noise environments.
Voice Channels	Yes	No	No support for voice channels in LE.

The architecture of LE was introduced in this chapter. Besides this some of the enhancements done by LE to reduce power consumption were briefly introduced. These will be explained in depth in next chapters.

Bibliography

Bluetooth Core Specification 4.0 http://www.bluetooth.org.

Bluetooth SIG, Specifications of the Bluetooth System, Profiles http://www.bluetooth.org.

SIG Low Energy Training, http://www.bluetooth.org.

Bluetooth Assigned Numbers, https://www.bluetooth.org/assigned-numbers.