CHAPTER 2

Background of Bluetooth

2.1 Introduction

This chapter provides a brief background of the Bluetooth technology and explains some of the commonly used concepts and terminology. It may be skipped if the reader is well versed with the Bluetooth technology.

2.2 Ad Hoc Networks—Why?

In today's world, with the advent of the "always connected" devices and "on the move" users, users expect devices to seamlessly connect to each other and exchange information without the need to install drivers, upgrade software, figure out cable connections, lookup configurations on centralized servers or even read user manuals. Information is the key in this connected world and the ability to quickly exchange that information across various kinds of devices has become more of a necessity than a luxury.

There are many applications where the user wants to bring devices close to each other and expects them to exchange data conveniently without going through lengthy setup procedures. The faster the setup→data exchange→tear down cycle, the better is the user experience.

A wireless ad hoc network may be defined as follows:

> A wireless ad hoc network is a decentralized type of wireless network. The network is termed as ad hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in wireless networks like WiFi.

Some of the real world scenarios of an ad hoc network are described below.

2.2.1 Printing Documents, Photos

Consider the scenario where a user took some photos using a camera and wants to get them printed. The most convenient scenario would be to just select the printer and send the document or photo to it without the need of connecting any cables or installing any printer drivers. This is shown in Figure 2.1.

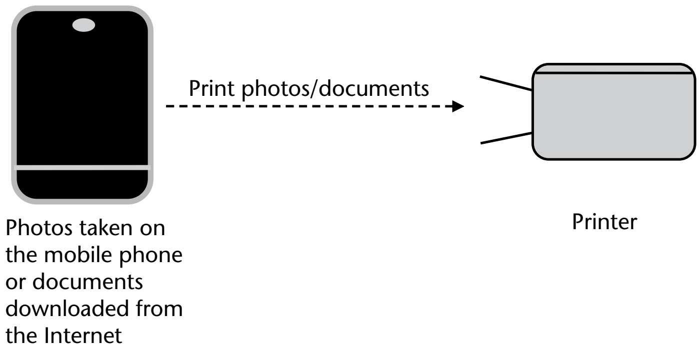


Figure 2.1 Printing documents, photos.

2.2.2 Exchanging Business Cards, Photos, Music, Files

Suppose a person meets a friend at a train station and they need to exchange phone numbers, e-mail addresses and other contact information. They may also decide to exchange some other things like photos, music, or some other files before their trains arrive and they go their respective ways. In such a scenario, an ad hoc technology is needed to quickly establish a connection and send information at a high data rate. Besides high data rate, the ad hoc technology also needs to be secure since they are using it in a public place and they want to ensure that their sensitive information is not received by others.This is shown in Figure 2.2.

2.3 What is Bluetooth?

Bluetooth is a global standard for short range, low power, low cost, small form factor wireless technology that allows devices to communicate with each other over radio links. It originated as a cable replacement technology mainly to replace the serial data cables that connect various devices. Over the years its uses have grown to exchanging files between PCs, mobile devices, listening to music, printing documents, browsing, taking mobile calls on Bluetooth headsets and car kits, and several more.

Today the attach rate of Bluetooth is almost 100% for mobile phones, tablet and laptops. Bluetooth is also widely used in wireless headsets, speakers, cam-

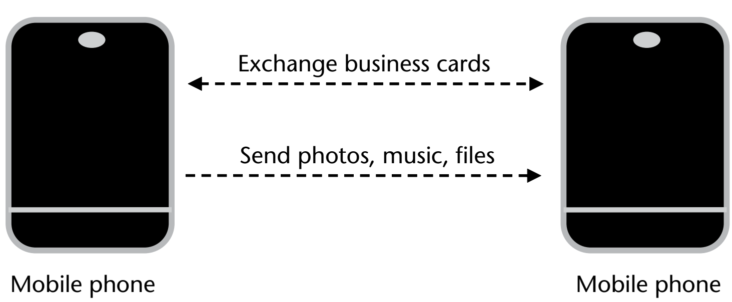


Figure 2.2 Exchanging business cards, photos, music, files.

eras, car kits, gaming consoles, and peripherals like keyboard, mouse, printer and scanner

Some of the key features of Bluetooth are:

- Ad hoc;
- Small Size;
- Low Cost;
- Low Power;
- Short Range;
- Secure;
- Interoperable;
- Global Standard;
- Ease-of-use;
- Does not require line of sight;
- Does not suffer from interference from obstacles like walls;
- Can co-exist with other wireless technologies;
- Big set of profiles already available to address real world scenarios.

Bluetooth is also termed as a Wireless Personal Area Network (WPAN) technology. As explained in Chapter 1, a Personal Area Network (PAN) is used for communication among personal devices like laptops, PCs and mobile phones. The communication may be done over wired buses like USB, Firewire, or plain old serial cables. A WPAN uses a wireless media to connect the personal devices such as mobile phones, PDAs, tablets and accessories. There are several wireless technologies like IrDA, Bluetooth, Wireless USB, NFC, and ZigBee which are used for WPANs.

2.4 Bluetooth SIG

The Bluetooth Special Interest Group (SIG) is a privately held, not-for-profit association. Bluetooth SIG does not make, manufacture, or sell Bluetooth products. The main tasks of the Bluetooth SIG are:

- Publish Bluetooth specifications.
- Administer the qualification program.
- Evangelize Bluetooth wireless technology.

The Bluetooth technology originated at Ericsson labs in Sweden in 1994. At that time Ericsson began a study to examine alternatives to cables that linked mobile phones with accessories.

The Bluetooth SIG was formally established by the following five founding members in February 1998:

- Ericsson;
- Intel;
- IBM;
- Nokia;
- Toshiba.

Over the years, several companies have signed up for the Bluetooth SIG membership. Currently the Bluetooth SIG membership surpasses 16,000 companies. The membership is open to all companies that wish to develop, market, and promote Bluetooth products.

The Bluetooth SIG offers two levels of membership to new member companies, plus promoter membership for companies represented on the Board of Directors.

- Adopter membership (Free): This provides access to Bluetooth resources and specifications to build Bluetooth products and license to use the Bluetooth word mark and logos.
- Associate membership (Annual fee): This provides early access to Bluetooth specifications which are still under development along with the opportunity to contribute to the specifications by joining working groups and committees. This membership also provides discounts on qualification fees, tools, trainings and more.

The Bluetooth SIG currently has seven promoter-level companies:

- Apple;
- Ericsson;
- Intel;
- Lenovo;
- Microsoft;
- Nokia;
- Toshiba.

The Bluetooth SIG holds regular round tables and hosts mailing lists, working groups, discussion forums, and UnPlugFests where the members can contribute to the specifications, submit errata, and test their devices for any interoperability issues.

The UnPlugFests (UPFs) are events organized by the Bluetooth SIG three times a year where the members can register, bring their products, and test them against products from other vendors.

Besides Bluetooth specifications, the SIG also provides Test Specifications which include test cases to test the Bluetooth stack and profiles. It also provides a tool called PTS (Profile Tuning Suite) which can be used to test the Bluetooth implementation in an automatic fashion. The test results of this tool can be used as direct evidence of compliance when the product is to be qualified.

The Bluetooth SIG also has a full-fledged qualification program which can be used to qualify a product before going to the market.

The Bluetooth Testing and Qualification will be covered in detail in Chapter 17.

2.5 History of the Bluetooth Specification

The word Bluetooth came from a Danish Viking and King, Harald Blåtand (Bluetooth in English). He united and controlled large parts of Norway and Denmark into one single kingdom during the 10th century. This probably provided the inspiration of the name Bluetooth—uniting a wide variety of devices from computing and communications domains.

The Bluetooth specification has evolved significantly in the last several years. Some of the major enhancements that each version added are mentioned in Table 2.1.

2.6 IEEE 802.15 Family of Specifications

IEEE 802.15 is a working group of the IEEE 802 standards committee that specifies WPAN standards. It includes seven Task Groups (TGs):

1. TG 1: Bluetooth.
2. TG 2: Coexistence for WPANs.
3. TG 3: High Rate WPAN: 11 Mbps to 55 Mbps.
4. TG 4: Low Rate WPAN: 20 kbps to 250 kbps.
5. TG 5: Mesh Networking.
6. TG 6: BAN (Body Area Networks).
7. TG 7: Visible Light Communication.

Versions 1.1 and 1.2 of Bluetooth were ratified as IEEE802.15.1-2002 and IEEE802.15.2-2005 specifications. Since then, the Bluetooth standard has evolved independently.

2.7 Bluetooth Basics

One of the first uses of Bluetooth was to replace cables between devices such as mobile phones, laptops, headphones, printers, fax machines, keyboard, mouse, and a host of other devices. Besides providing data channels, Bluetooth also provides voice channels allowing wireless connections between the mobile phones and headsets and car kits.

Bluetooth supports ad hoc networks. This means that it does not rely on any pre-existing infrastructure such as routers in wired networks or access points in wireless networks. The devices can dynamically come close to each other and exchange data and go out of range.

Bluetooth supports a maximum distance of 100 meters though typically it is used for much shorter distances. The specification provides support for different

Table 2.1 Evolution of Bluetooth Specification

Specification Version	*Release Date*	*Key features of the version*
1.0 and 1.0a	Jul 1999	These were the very first versions of the Bluetooth specification. The primary objective was to replace the serial cables with a wireless link.
1.0b	Dec 1999	This version added minor updates to fix some of issues.
1.1	Feb 2001	Bluetooth was ratified as IEEE 802.15.1-2002 standard.
1.2	Nov 2003	This release of the Bluetooth standard added new facilities including the following: • Adaptive Frequency Hopping (AFH) was introduced to provide better resistance to interference in noisy environments. • Extended Synchronous Connection Oriented (eSCO) links were added to provide better voice quality. This was also ratified as IEEE 802.15.1-2005. This was the last version issued by IEEE and after that Bluetooth technology evolved independently.
2.0 + EDR	Nov 2004	This release of the Bluetooth standard introduced enhancements to the throughput using Enhanced Data Rates (EDR). The previous versions of the standard supported a throughput up to 721 kbps. This version increased it to 2.1 Mbps. This made it more suitable for applications that required fast data transfers like file transfer, browsing, printing, etc.
2.1 + EDR	Jul 2007	This version brought in several enhancements and added SSP (Secure Simple Pairing) to both simplify the pairing mechanism and to improve security.
3.0 + HS	Apr 2009	This version provided a significant increase in throughput by introducing the support for multiple radios. This was referred to as Alternate MAC/PHY (AMP). The supported maximum throughput went up to 24 Mbps. The rationale, very briefly, was that several devices like Laptops, Mobile phones and Tablets have both Bluetooth and 802.11 chips on them. This version of the specification allowed connection using Bluetooth and then moving on to the 802.11 chip to achieve high speed data transfers.
4.0	Jun 2010	This version went into a completely different direction compared to the previous versions. While in the previous versions the main focus was to introduce new features and enhance the throughput, this version addressed the markets where the need was not of high throughput but of ultra-low power. This was referred to as Bluetooth Low Energy (LE).
4.1	Dec 2013	This version enhanced the Bluetooth Low Energy feature by allowing an LE device to act as both a hub and an end point. This was useful in Internet of Things, where devices could exchange data with each other. It also provided support for coexistence with LTE (4G) since LTE may occupy frequencies that are close to or have harmonics near those of Bluetooth. It also provided support for additional topologies in order to make the technology applicable for newer use case scenarios. The main notable changes done in this version were to put in the "Reliable BLE Packet Support by introducing the LE L2CAP Connection Oriented channels" to carry the short LE packets and add more reliability. Another notable feature is called Privacy 4.1, wherein the private addresses are scrambled during connection so that any eavesdropper has a lesser chances of capturing the information.
4.2	Dec 2014	This version further enhanced the Bluetooth Low Energy feature by allowing sensors to access the Internet, further lowering energy requirements and boosting security and privacy. One of the shortcomings of the previous version was that the packet size was smaller, and therefore the maximum throughput was lower, which made it unsuitable for applications that required high throughput, even if for a short duration of time. This version increased the packet capacity by ten times leading to a data throughput increase of 2.5 times. Comparing the specifications of 4.2 to 4.1, there are also an increased security procedure and power preserving security procedure. This power-preserving security procedure offloads most of the key management to the controller. On 4.2 dual-mode devices, there is also a provision of pairing only once with the remote device, irrespective of the authentication mode used by the device.

power levels for Bluetooth radios so that the appropriate combination of power consumption and distance can be selected based on the application that the device is intended for.

Originally Bluetooth supported a maximum data rate of 721 kbps. This is referred to as Basic Rate (BR). The Bluetooth 2.0+EDR specification added support for data rates up to 2.1 Mbps. This is referred to as Enhanced Data Rate (EDR). The Bluetooth 3.0+HS (High Speed) specification enhanced it even further to 24 Mbps.

The Bluetooth technology uses the license free 2.4 GHz ISM band for its radio signals. ISM stands for Industrial, Scientific, and Medical radio band. This band is globally unlicensed and can be used in any country without asking for prior permissions.

Since the ISM radio band is an unlicensed band, it is used by other devices including WiFi devices, and remote control toys. There is also a possibility of interference from devices like microwaves in this band. To combat interference, Bluetooth uses a Frequency Hopping Spread Spectrum (FHSS) mechanism. Instead of using a constant frequency to send and receive data, the communicating devices use a set of frequencies and hop rapidly from one frequency to another using a pseudo random pattern.

Bluetooth SIG mandates the devices to undergo qualification before being launched in the market. The purpose of the Bluetooth qualification program is to promote interoperability and enforce compliance to the specification. It is a necessary prerequisite to obtain the Bluetooth intellectual property license and use the Bluetooth logos. This program is one of the key reasons behind the success of the Bluetooth technology. When a user buys a device from one vendor, he or she is assured that the device will work well with devices from other vendors.

A summary of the key features of Bluetooth are provided in Table 2.2.

Table 2.2 Summary of Key Features

Connection Type	*Frequency Hopping Spread Spectrum*
Spectrum	2.4 GHz ISM Band. Regulatory range: 2400–2483.5 MHz.
Frequency Hopping	1600 hops per second across 79 RF channels. The channels are separated by 1 MHz.
Modulation	Gaussian Frequency Shift Keying (GFSK).
Maximum Output Power	1 mW to 100 mW.
Transmit Power	Nominal = 0dBm. Goes up to 20 dBm with power control.
Receiver Sensitivity	–70 dBm at 0.1% Bit Error Rate
Maximum Data Rate	721.2 kbps for Basic Rate.
	2.1 Mbps with Enhanced Data Rate (BT Spec 2.0+EDR).
	24 Mbps with High Speed (BT Spec 3.0+HS).
Typical Range	10 m to 100 m.
Topology	Up to 8 devices in a piconet including 1 Master and up to 7 Slaves.
Voice Channels	3
Data Security: Authentication Key	128 bit key.
Data Security: Encryption Key	8-128 bits (configurable).
Applicability	Does not require line of sight.
	Intended to work anywhere in the world since it uses unlicensed band.

2.8 Bluetooth Architecture Overview

Bluetooth has a layered architecture. The high-level architecture of Bluetooth is show in Figure 2.3. At a very broad level, the Bluetooth architecture comprises the following components going from bottom to top:

- *Lower Layers or Controller:* These are the layers responsible for performing low level operations like discovering devices in the vicinity, making connections, exchanging data packets, security, low power modes, etc. This functionality is generally implemented in a Bluetooth chip and it is also referred to as a Bluetooth Controller.
- *Upper Layers:* These layers make use of the functionality provided by the lower layers to provide more complex functionality like serial port emulation, transferring big chunks of data by splitting them into smaller pieces and reassembling them, streaming music, etc.
- *Profiles:* The profiles can be considered to be vertical slices through the protocol stack. They provide information on how each of the protocol layers come together to implement a specific usage model. Profiles help to guarantee that an implementation from one vendor works properly with implementation from another vendor. So they form the basis for interoperability and logo requirements. The profiles need to be tested and certified before a device can be sold in the market. A device can support one or more profiles at the same time.
- *Bluetooth Application*: This is the entity that generally performs the tasks of an MMI (Man Machine Interface) so that the user can make use of the Bluetooth functionality. Some examples of this are:
  - Selecting a file and then transferring it on Bluetooth;
  - Searching for Bluetooth devices in the vicinity and displaying the results;
  - Pressing a button on the headset to make a connection;
  - Browsing the files and folders of a remote device on Bluetooth.

One of the strong points of the Bluetooth technology is that it tries to reuse things are already available instead of specifying everything from scratch. It picks

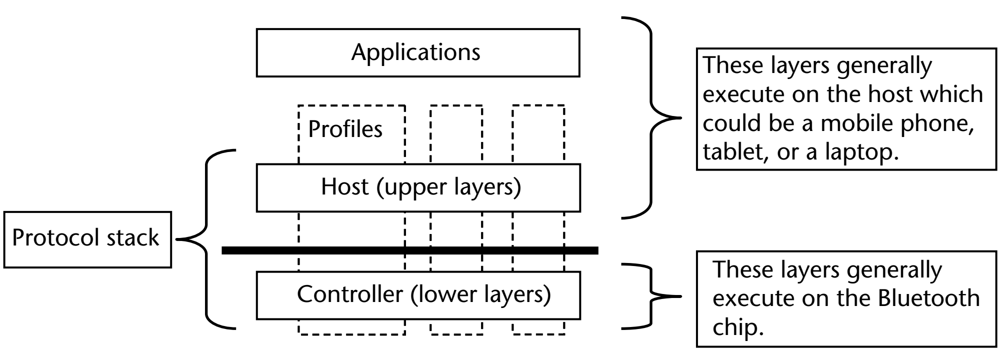


Figure 2.3 High-level Bluetooth architecture.

up some components from existing standards, adapts them as needed, and then defines only the core components that are needed for Bluetooth operations. The protocols can be broadly grouped into two categories: Core Protocols and Adopted Protocols.

The protocols that are defined from scratch by the Bluetooth SIG are referred to as core protocols. Some examples are L2CAP, Link Manager and SDP (these will be explained in detail later).

The protocols that are adopted from other standard bodies are referred to as adopted protocols. Some examples are:

- *RFCOMM:* This protocol is adopted from European Telecommunications Standards Institute (ETSI) standard 07.10.
- *OBEX:* This protocol is adopted from the IrOBEX protocol which is defined by the Infrared Data Association (IrDA).
- *TCS-BIN:* Used for the Telephony protocols.
- *IEEE 11073-20601:* Used for the MCAP protocol for health applications.
- *IrMC:* Used for SYNC profile.
- *HID profile*: This is adopted from USB HID (used in wired keyboard, mice and gaming devices).

The adopted protocols help to re-use existing specifications instead of reinventing the wheel. The existing specifications are established and are proven to work well. In many cases, even the existing software can be re-used to a large extent instead of writing the software from scratch. This helps in speedier implementations.

The detailed Bluetooth architecture is shown in Figure 2.4. The adopted protocols are shown with shaded rectangles and core protocols are shown with plain rectangles. The profiles are shown by rectangles with dashed boundaries. The protocol stacks and profiles will be covered in further details in the next two chapters.

2.9 Basic Terminology

This section introduces some of the basic terminology used in Bluetooth. Familiarity with these terms will help in a better understanding of the further chapters.

2.9.1 Host, Host Controller, and Host Controller Interface (HCI)

Based on the device on which the Bluetooth functionality is implemented, the Bluetooth architecture can be considered to be split into two broad logical parts as shown in Figure 2.5.

The Host is a logical entity that executes the upper layers of the Bluetooth protocol stack along with the profiles and applications. It includes the following:

1. The Protocol stack layers above the Host Controller Interface—L2CAP, RFCOMM, SDP, AVDTP, AVCTP, and BNEP layers.
2. The profiles like GAP, SDAP, GOEP, OPP, FTP, A2DP, AVRCP, and HF.
3. The MMI applications which interact with the user.

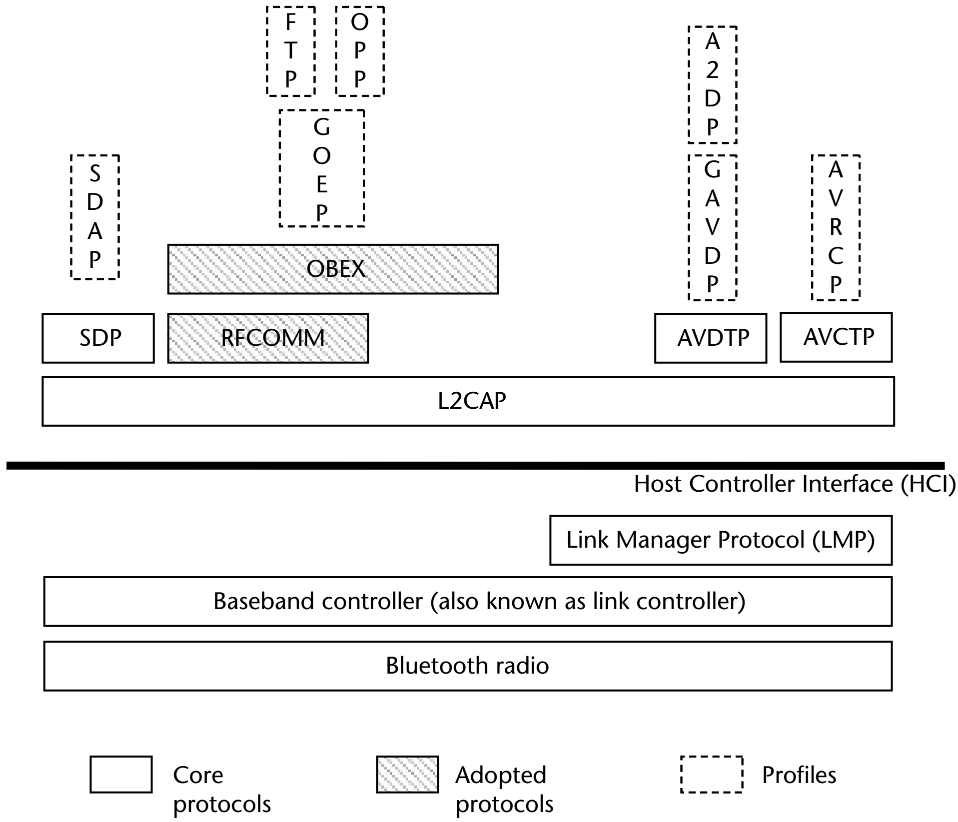


Figure 2.4 Detailed Bluetooth architecture.

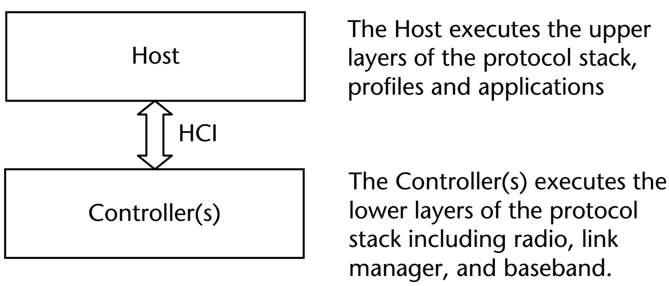


Figure 2.5 Host, Host Controller, and Host Controller Interface.

Typically the Host software executes on an application processor or microcontroller.

The Controller is a logical entity that that executes the lower layers of the protocol stack. It includes all layers below the Host Controller Interface—Radio, Link Manager, and Baseband. Typically the Controller functionality is embedded in a Bluetooth chip that is attached to the Host.

The Host Controller Interface (HCI) provides a communication interface between the Host and the Controller. Physically this may run on top of an interface like UART, RS-232, USB or SD. The set of packets that can be exchanged on this interface is defined by the Bluetooth specification. One of the strong points of the Bluetooth specification as compared to few other standards is a well-defined interface layer between the host and the wireless controller. It allows independent and parallel development of the host and controller and ensures compatibility of a host from one vendor with a controller from a different vendor.

The HCI interface is optional and may be omitted in implementations where the host and the controller are tightly coupled with each other and run on the same processor. If this interface is omitted, then the upper layers interact directly with the lower layers.

Let us consider a few scenarios to understand this well. These scenarios are shown in Figure 2.6.

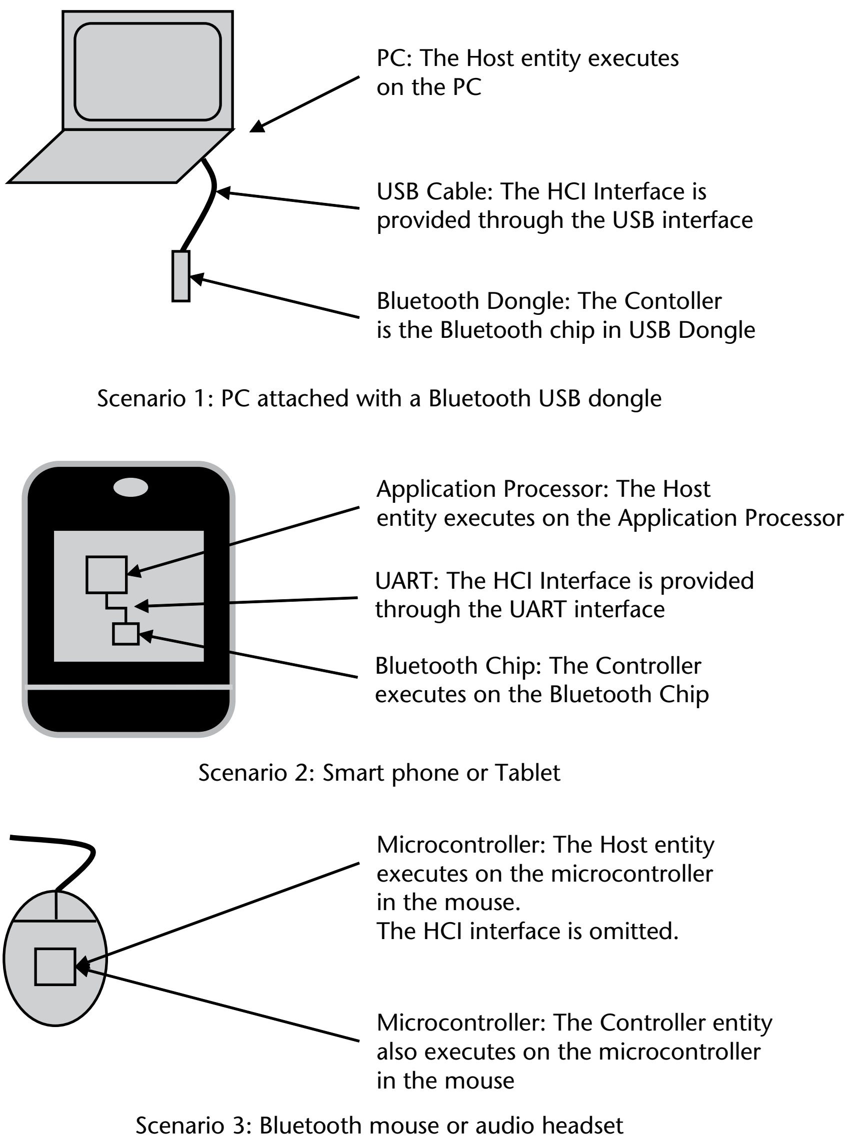


Figure 2.6 Scenarios depicting Host, Controller, and HCI.

Scenario 1: PC attached with a Bluetooth USB dongle
In this scenario:

- The Host entity executes on the PC (The Bluetooth software running on the PC Operating System).
- The Controller entity executes on the Bluetooth chip that resides inside the Bluetooth USB Dongle.
- The Host Controller interface is provided through the USB interface.

Scenario 2: Smart phone or Tablet
In this scenario:

- The Host entity executes on the Phone's application processor.
- The Controller entity executes on the Bluetooth chip that is mounted on the Phone's PCB.
- The Host Controller interface is provided through the UART (or some other) connection on the PCB between the application processor and Bluetooth chip.

Scenario 3: Bluetooth mouse or audio headset
In this scenario:

- Both the Host and the Controller entities run on a single microcontroller.
- The Host Controller interface is omitted and the upper layers of the stack interact directly with lower layers of the stack.

Prior to the Bluetooth 3.0 + HS specification, a Bluetooth system could have only one Host and one Controller. From the Bluetooth 3.0 + HS specification onwards, a system can have one host and multiple controllers. Two types of controllers are defined by Bluetooth 3.0 + HS specification: Primary controller and Secondary controller. A system can have only one Primary controller and may have zero or more Secondary controllers.

The Primary controller may support BR/EDR only, LE only or a combination of BR/EDR + LE functionality.

The Secondary controllers support one or more Alternate MAC/PHY (AMP) controllers. These AMP controllers help in increasing the throughput up to 24 Mbps by using the 802.11 transport layer instead of the classic Bluetooth transport layer for high speed data transfers.

2.9.2 Device Address (BD_ADDR) and Device Name

Each BR/EDR controller has a globally unique 48-bit Bluetooth Device Address, also referred to as BD_ADDR. This address is used to identify the device. It is similar to an Ethernet MAC address, and is in fact, administered by the same organization, IEEE.

BD_ADDR consists of two fields:

1. 24-bit company id assigned by IEEE Registration authority. This is called Organizationally Unique Identifier (OUI) [24 most significant bits].
2. 24-bit unique number assigned by the company to each controller. [24 least significant bits].

The Bluetooth device name is a friendly name that can be assigned to a device. Unlike the BD_ADDR, this can be changed by the user or application and provides an easy mechanism to identify and remember a device. It is possible (though not desirable) for several devices to have the same name. This device name is generally fetched from the remote device to identify it.

2.9.3 Class of Device (CoD)

The Class of Device is a 24-bit value used to indicate the capabilities of the local device to remote devices. This is returned as one of the parameters when searching for Bluetooth devices in the vicinity.

The CoD field has a variable format. The format is indicated using the *Format Type field* within the CoD. The length of the Format Type field is variable and it ends with two bits different from ‘11’.

In format #1 of the CoD, the bits are assigned as follows:

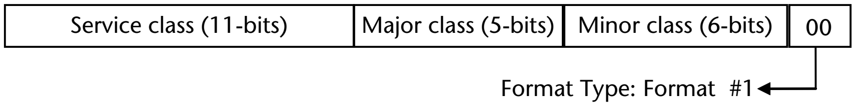
- Format Type field: Two bits: 00.
- 11-bits to indicate a high level generic category of service class. These bits are assigned as a bit mask so that more than one service class category bit can be enabled at the same time. Currently 7 categories are defined.
- 11 bits to define the device type category and other device specific characteristics. This is further divided into:
  - 5 bits to denote the Major class.
  - 6 bits to denote the Minor class.

The details on the Class of Device can be looked up in the Assigned Numbers document on the Bluetooth SIG website in the baseband section.Some of the commonly used values of Class of Device are shown in Figure 2.7.

2.9.4 Bluetooth Clock

The Bluetooth clock refers to the native clock of the Bluetooth device that is derived from the free running system clock. Each Bluetooth controller has its own clock that is started when the device is powered on.

The Bluetooth clock is used to synchronize with other devices. Since each device may have a different absolute value of the clock, the *clock offset* values are used for synchronization instead of the absolute value of the clock. When these offsets are added to the native clock on each of the Bluetooth devices, mutually synchronized clocks are obtained.



Laptop

Service Classes: Networking, capturing, telephony, object transfer
Major Class: Computer
Minor Class: Laptop (This could also be desktop or server)

Smartphone

Service Classes: Telephony
Major Class: Phone
Minor Class: Smartphone (This could also be cellular or cordless)

Headset

Service Classes: Audio
Major Class: Audio/Video
Minor Class: Wearable headset (This could also be Hands-Free device or headphones)

Figure 2.7 Class of device.

Clock offsets are very important in a Bluetooth network since all timings are based on these clocks. The worst case accuracy required for the reference crystal oscillator that drives the Bluetooth clock is +/– 20 ppm (Parts Per Million). This means that in a million ticks, the clock cannot drift by more than 20 ticks compared with a fully accurate reference clock.

The Bluetooth clock is different from a Real Time Clock (RTC) which is used to maintain the time of the day. The RTC generally runs even when the system is switched off. For example the RTC is used to provide the current time in laptops, PCs, and mobile phones.

2.9.5 Protocol Data Unit (PDU)

The term PDU is used to refer to information that is exchanged between two entities in a network. This information is in the form of data packets. Some examples of PDUs are:

1. The packets that are sent by the lower layers of one Bluetooth device to the lower layers of the peer Bluetooth device.
2. The packets that are sent by the upper layers (For example L2CAP) of the protocol stack to the corresponding layers of protocol stack on the peer Bluetooth device.

2.10 Data Rates

The data rates supported by Bluetooth have been enhanced in a major way along with evolutions of the specification.Prior to version 2.0, data rates of up to 721.2 kbps were supported. This is referred to as Basic Rate (BR).

The Bluetooth 2.0+EDR specification added support for enhanced data rates which enhanced the throughput to 2.1 Mbps. This is referred to as Enhanced Data Rate (EDR).

Several different packet types are defined by the specification with each packet type providing support for different data rates. These will be discussed in detail in the next chapter.

The term BR/EDR is often used together to refer to a system supporting Basic and Enhanced Data Rates and to distinguish it from a system that supports LE (Bluetooth Low Energy). This term is used extensively in the specification and will also be used in this book.

The Bluetooth 3.0+HS specification added support for using Alternate MAC/PHY (AMP) with which the maximum throughput was increased to 24 Mbps.

The Bluetooth 4.0 (LE) specification did not add any further data rates. Rather the focus of this specification was on reducing the current consumption to enable Low Energy devices. In fact the LE system is designed for uses and applications for lower data rates and smaller packet sizes. The maximum throughput in LE as per specifications 4.0 is 305 Kbps though in practice the applications send data at a much lower rate to conserve battery power.

While specifications 4.0 provided support for a majority of use-case scenarios for devices, there were certain scenarios in which these devices needed a higher throughput, even if it was for a shorter duration of time. For example, if the firmware of the device were to be upgraded, it would take a huge amount of time (and thus energy) to upgrade the firmware. The specifications 4.2 addressed this by increasing the packet size from 27 bytes to 251 bytes. This led to an increase in the maximum data rate from 305 Kbps to 800 Kbps.

2.11 Connection Setup and Topology

This section briefly introduces the connection setup procedure and Bluetooth topologies. These will be explained in detail in subsequent chapters.

If two devices need to communicate, then they may take the following steps:

1. One of the devices, say device B, needs to be in a mode where it can be "seen" or discovered by other devices. It is said to become *discoverable*.
2. The second device, say device A can search for devices in the vicinity. This is called *inquiry*. During the inquiry process, it will locate device B.
3. In order to make a connection, the device B needs to allow other devices to connect to it. So it needs to become *connectable*.
4. Device A, can now create a *connection* to device B. This process is called *paging*.
5. Once the connection is created, device A is said to become the *Master* and device B is said to become the *Slave* and the devices are said to be *connected*.

a. *Connection* means that device A is able to receive the packets sent by device B and vice versa. This means that they are synchronized on the frequencies that they will use for transmission and reception.

6. When the devices don't need the connection any more, they *disconnect*. Either the Master or the Slave can initiate the *disconnection*.

These steps are shown in Figure 2.8.

Bluetooth communication is based on the following two network topologies

1. Piconet;
2. Scatternet (Combination or two or more piconets).

A piconet is the smallest unit of Bluetooth communication. It consists of one Master and up to seven Slaves. So in Figure 2.8, device A and device B are said to form a piconet at step 4. Another example of piconet is shown in Figure 2.9.

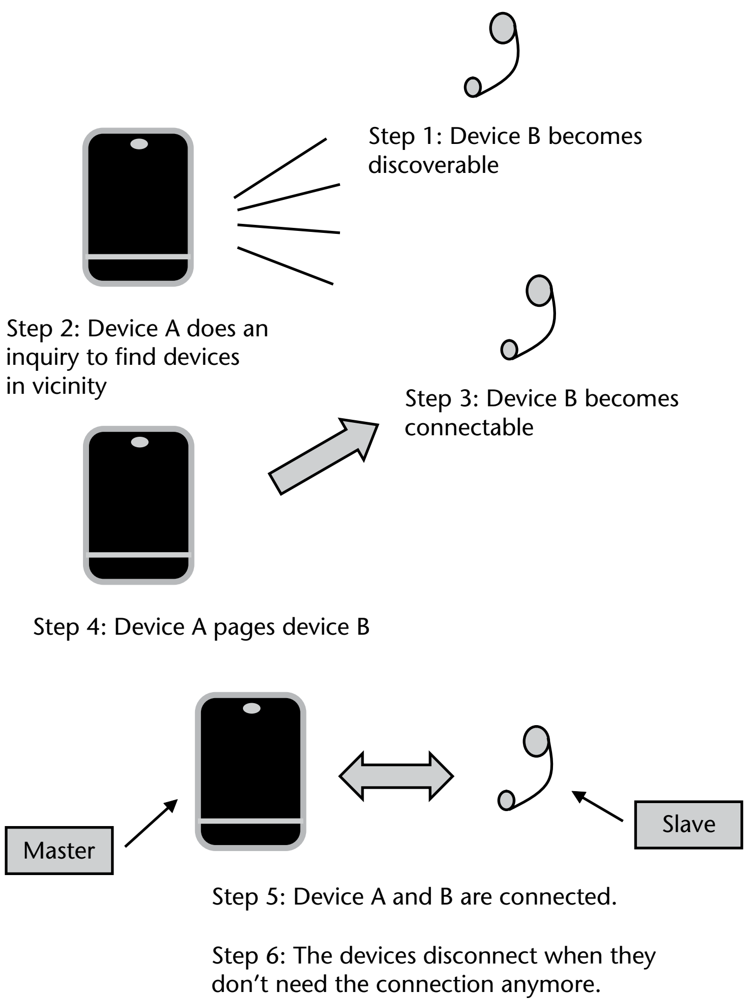


Figure 2.8 Steps during making a connection.

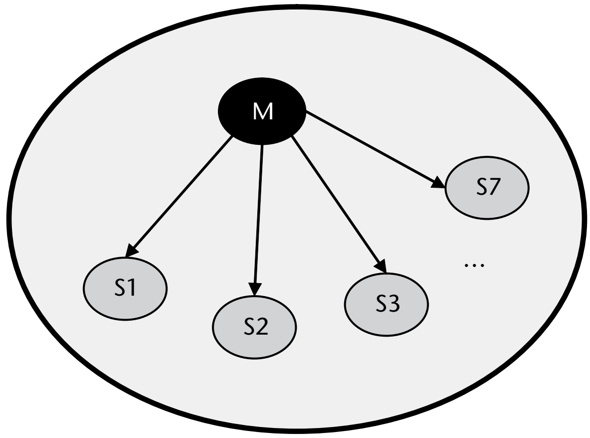


Figure 2.9 Piconet.

A scatternet is formed when two or more piconets come together by sharing a device. Scatternets help to extend the number of Bluetooth devices that can communicate with each other. They allow more than seven devices to communicate with each other. A scatternet is shown in Figure 2.10 where S7 is shared between the two piconets.

2.12 IEEE Language

The Bluetooth SIG has adopted section 13.1 of the IEEE Standard Style Manual (Ref [3]). This dictates the use of words like "shall", "should", "may", and "can" in the documentation. Understanding of this usage is very important when reading the specifications documents. A brief overview of the IEEE word usage is shown in Table 2.3

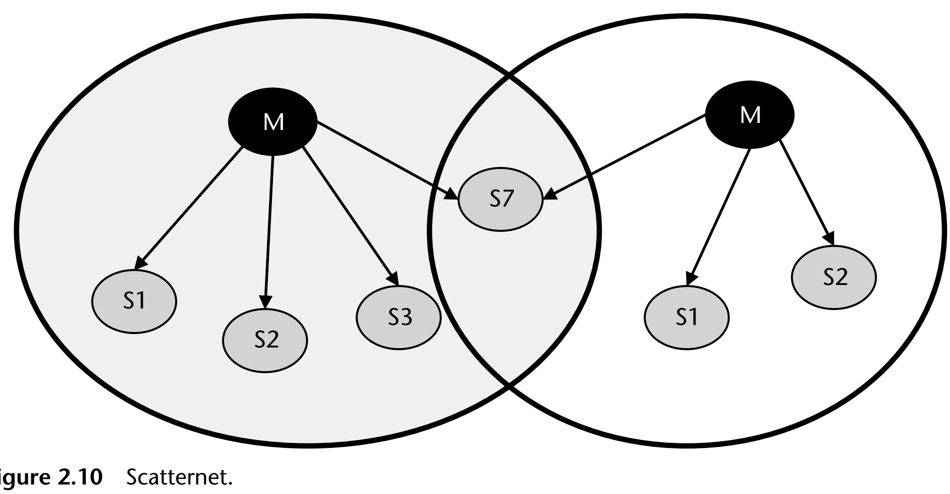


Figure 2.10 Scatternet.

Table 2.3 IEEE Word Usage (Adopted from Bluetooth Core Specification)

Shall	*is required to* – used to define requirements. The word *shall* is used to indicate mandatory requirements that shall be followed in order to conform to the specification and from which no deviation is permitted.
Must	*is a natural consequence of* – used only to describe unavoidable situations The word *must* shall not be used when stating mandatory requirements. *Must* is used only to describe unavoidable situations and is seldom appropriate for the text of a specification.
Will	*it is true that* – only used in statements of fact The word *will* shall not be used when stating mandatory requirements. The term *will* is only used in statements of fact.
Should	*is recommended that* – used to indicate that among several possibilities one is recommended as particularly suitable, but not required. The word *should* is used to indicate that among several possibilities one is recommended as particularly suitable without mentioning or excluding others.
May	*is permitted to* – used to allow options The word *may* is used to indicate a course of action that is permissible within the limitations of the specification. This is generally used when there is a single, optional attribute described, but multiple alternatives may be cited.
Can	*is able to* – used to relate statements in a causal fashion The term *can* is used for statements of possibility and capability, whether material, physical, or casual. The term *can* equals is able to.
Is	*is defined as* – used to further explain elements that are previously required or allowed
Note	<informational text ONLY>

2.13 Summary

Bluetooth technology has come a long way since it originated in the Ericsson labs as a cable replacement technology. While previous evolutions of this technology focused more on feature and throughput enhancements, the latest version, LE, focuses on drastic reductions in the power consumption.

The Bluetooth protocol stack follows a layered architecture. It borrows some of the protocols that are already available and only defines the protocols related to core Bluetooth functionality.

Bluetooth supports ad hoc networking where up to seven devices can simultaneously talk to each other. These devices are said to form a piconet. Bluetooth also provides flexibility to increase this number by forming a scatternet which combines two piconets.

This chapter introduced some of the basic concepts of Bluetooth. The next two chapters will cover the Bluetooth lower layers and Bluetooth upper layers.

References

[1] Bluetooth Core Specification 4.0 http://www.bluetooth.org.

[2] Assigned Numbers Specification: https://www.bluetooth.org/Technical/AssignedNumbers/home.htm

[3] IEEE Standards Style Manual (http://standards.ieee.org/guides/style/)