1 GENERAL DESCRIPTION

Bluetooth wireless technology is a short-range communications system intended to replace the cable(s) connecting portable and/or fixed electronic devices. The key features of Bluetooth wireless technology are robustness, low power consumption, and low cost. Many features of the specification are optional, allowing product differentiation.

There are two forms of Bluetooth wireless technology systems: Basic Rate (BR) and Low Energy (LE). Both systems include device discovery, connection establishment and connection mechanisms. The Basic Rate system includes an optional Enhanced Data Rate (EDR) extension. The Basic Rate system offers synchronous and asynchronous connections with data rates of 721.2 kb/s for Basic Rate and 2.1 Mb/s for Enhanced Data Rate. The LE system includes features designed to enable products that require lower current consumption, lower complexity and lower cost than BR/EDR. The LE system is also designed for use cases and applications with lower data rates and has lower duty cycles. The LE system includes an optional 2 Mb/s physical layer data rate and also offers isochronous data transfer in a connection-oriented and connectionless mechanism that uses the isochronous transports. Depending on the use case or application, one system including any optional parts may be more optimal than the other.

Devices implementing both systems can communicate with other devices implementing both systems as well as devices implementing either system. Some profiles and use cases will be supported by only one of the systems. Therefore, devices implementing both systems have the ability to support the most use cases.

The Bluetooth core system consists of a Host and one or more Controllers. A Host is a logical entity defined as all of the layers below the non-core profiles and above the Host Controller interface (HCI). A Controller is a logical entity defined as all of the layers below HCI. An implementation of the Host and Controller may contain the respective parts of the HCI.

An implementation of the Bluetooth Core has only one Controller which may be one of the following configurations:

- a BR/EDR Controller including the Radio, Baseband, Link Manager and optionally HCI.
- an LE Controller including the LE PHY, Link Layer and optionally HCI.
- a combined BR/EDR Controller portion and LE Controller portion (as identified in the previous two bullets) into a single Controller.

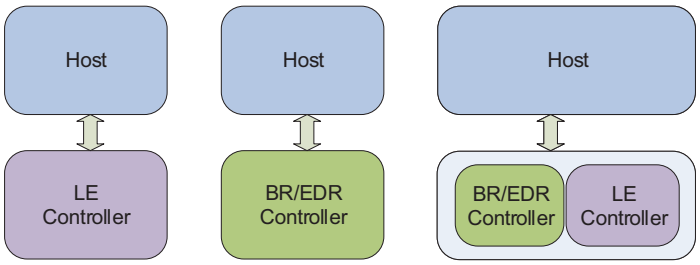

Figure 1.1: Bluetooth Host and Controller combinations: (from left to right): LE Only Controller, BR/EDR only Controller, and BR/EDR/LE Controller

This Part of the specification provides an overview of the Bluetooth system architecture, communication topologies, and data transport features. The text in this Part of the specification should be treated as informational and used as a background and for context-setting.

1.1 OVERVIEW OF BR/EDR OPERATION

The Basic Rate / Enhanced Data Rate (BR/EDR) radio (physical layer or PHY) operates in the unlicensed ISM band at 2.4 GHz. The system employs a frequency hopping transceiver to combat interference and fading and provides many FHSS carriers. Basic Rate radio operation uses a shaped, binary frequency modulation to minimize transceiver complexity. The symbol rate is 1 megasymbol per second (Msym/s) supporting the bit rate of 1 megabit per second (Mb/s) or, with Enhanced Data Rate, a gross air bit rate of 2 Mb/s or 3 Mb/s. These modes are known as Basic Rate and Enhanced Data Rate respectively.

During typical operation a physical radio channel is shared by a group of devices that are synchronized to a common clock and frequency hopping pattern. One device provides the synchronization reference and is known as the Central. All other devices synchronized to a Central's clock and frequency hopping pattern are known as Peripherals. A group of devices synchronized in this fashion form a piconet. This is the fundamental form of communication in the Bluetooth BR/EDR wireless technology.

Devices in a piconet use a specific frequency hopping pattern, which is algorithmically determined by certain fields in the Bluetooth address and clock of the Central. The basic hopping pattern is a pseudo-random ordering of the 79 frequencies, separated by 1 MHz, in the ISM band. The hopping pattern can be adapted – on a per-Peripheral basis – to exclude a portion of the frequencies that are used by interfering devices. The adaptive hopping technique improves Bluetooth co-existence with static (non-hopping) ISM systems when they are co-located.

The physical channel is sub-divided into time units known as slots. Data is transmitted between Bluetooth devices in packets that are positioned in these slots. When circumstances permit, a number of consecutive slots may be

allocated to a single packet. Frequency hopping may take place between the transmission or reception of packets. Bluetooth technology provides the effect of full duplex transmission through the use of a Time-Division Duplex (TDD) scheme.

Above the physical channel there is a layering of links and channels and associated control protocols. The hierarchy of channels and links from the physical channel upwards is physical channel, physical link, logical transport, logical link and L2CAP channel. These are discussed in more detail in Section 3.3 to Section 3.6 but are introduced here to aid the understanding of the remainder of this section.

Typically within a physical channel, a physical link is formed between a Central and one or more Peripherals. Exceptions to this include Inquiry scan and Page scan physical channels, which have no associated physical link. The physical link provides bidirectional packet transport between the Central and Peripherals, except in the case of a Connectionless Peripheral Broadcast physical link. In that case, the physical link provides a unidirectional packet transport from the Central to a potentially unlimited number of Peripherals. Since a physical channel could include multiple Peripherals, there are restrictions on which devices may form a physical link. There is a physical link between each Peripheral and the Central. Physical links are not formed directly between the Peripherals in a piconet.

The physical link is used as a transport for one or more logical links that support unicast synchronous, asynchronous and isochronous traffic, and broadcast traffic. Traffic on logical links is multiplexed onto the physical link by occupying slots assigned by a scheduling function in the resource manager.

A control protocol for the baseband and physical layers is carried over logical links in addition to user data. This is the Link Manager protocol (LMP). Devices that are active in a piconet have a default asynchronous connection-oriented logical transport that is used to transport the LMP protocol signaling. For historical reasons this is known as the ACL logical transport. With the exception of Connectionless Peripheral Broadcast devices, the primary ACL logical transport is the one that is created whenever a device joins a piconet. Connectionless Peripheral Broadcast devices may join the piconet purely to listen to Connectionless Peripheral Broadcast packets. In that case, a Connectionless Peripheral Broadcast logical transport is created (also called a CPB logical transport) and no ACL logical transport is required. For all devices, additional logical transports may be created to transport synchronous data streams when required.

The Link Manager function uses LMP to control the operation of devices in the piconet and provide services to manage the lower architectural layers (radio and baseband). The LMP protocol is carried on the primary ACL and Active Peripheral Broadcast logical transports.

Above the baseband the L2CAP layer provides a channel-based abstraction to applications and services. It carries out segmentation and reassembly of application data and multiplexing and de-multiplexing of multiple channels over a shared logical link. L2CAP has a protocol control channel that is carried over the default ACL logical transport. Application data submitted to the L2CAP protocol may be carried on any logical link that supports the L2CAP protocol.

1.2 OVERVIEW OF BLUETOOTH LOW ENERGY OPERATION

Like the BR/EDR radio, the LE radio operates in the unlicensed 2.4 GHz ISM band. The LE system employs a frequency hopping transceiver to combat interference and fading and provides many FHSS carriers. LE radio operation uses a shaped, binary frequency modulation to minimize transceiver complexity. LE uses terminology that differs from BR/EDR to describe supported PHYs with regards to differences in modulation, coding that may be applied, and the resulting data rates. The mandatory symbol rate is 1 megasymbol per second (Msym/s), where 1 symbol represents 1 bit therefore supporting a bit rate of 1 megabit per second (Mb/s), which is referred to as the LE 1M PHY. The 1 Msym/s symbol rate may optionally support error correction coding, which is referred to as the LE Coded PHY. This may use either of two coding schemes: S=2, where 2 symbols represent 1 bit therefore supporting a bit rate of 500 kb/s, and S=8, where 8 symbols represent 1 bit therefore supporting a bit rate of 125 kb/s. An optional symbol rate of 2 Msym/s may be supported, with a bit rate of 2 Mb/s, which is referred to as the LE 2M PHY. The 2 Msym/s symbol rate supports uncoded data only. LE 1M and LE 2M are collectively referred to as the LE Uncoded PHYs. Section 3.2.2 describes this terminology in more detail.

LE employs two multiple access schemes: Frequency division multiple access (FDMA) and time division multiple access (TDMA). Forty (40) physical channels, separated by 2 MHz, are used in the FDMA scheme. Three (3) are used as primary advertising channels and 37 are used as general purpose channels (including as secondary advertising channels). A TDMA based polling scheme is used in which one device transmits a packet at a predetermined time and a corresponding device responds with a packet after a predetermined interval.

The physical channel is sub-divided into time units known as events. Data is transmitted between LE devices in packets that are positioned in these events. The following types of events exist: Advertising, Extended Advertising, Periodic Advertising, Connection, and Isochronous events (which are partitioned into BIS, BIG, CIS, and CIG events).

Devices that transmit advertising packets on the advertising PHY channels are referred to as advertisers. Devices that receive advertising packets on the advertising physical channels without the intention to connect to the advertising device are referred to as scanners. Transmissions on the advertising PHY channels occur in advertising events. At the start of each advertising event, the advertiser sends an advertising packet corresponding to the advertising event

type. Depending on the type of advertising packet, the scanner may make a request to the advertiser on the same advertising PHY channel which may be followed by a response from the advertiser on the same advertising PHY channel. The advertising PHY channel changes on the next advertising packet sent by the advertiser in the same advertising event. The advertiser may end the advertising event at any time during the event. Each advertising packet in an advertising event uses a different advertising PHY channel. Each advertising event may use a different order for the advertising PHY channels.

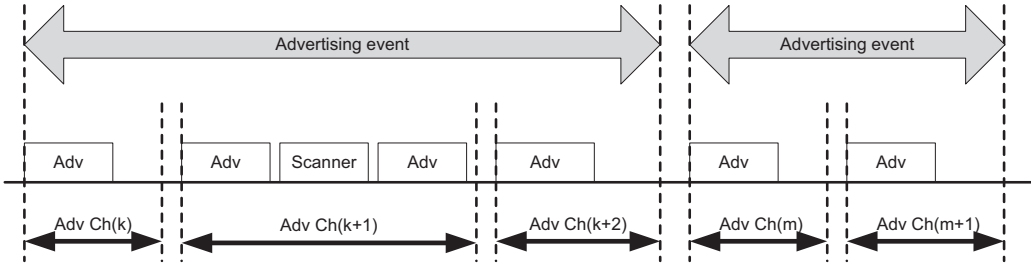

Figure 1.2: Advertising events

LE devices may fulfill the entire communication in the case of unidirectional or broadcast communication between two or more devices using advertising events. LE devices may also use advertising events to establish bi-directional connections with another device and to establish asynchronous or isochronous periodic broadcasts. Asynchronous periodic broadcasts may allow the advertiser to receive responses from one or more devices. These additional activities make use of the general purpose channels in various ways.

Devices that need to form an ACL connection to another device listen for connectable advertising packets. Such devices are referred to as initiators. If the advertiser is using a connectable advertising event, an initiator may make a connection request using the same advertising PHY channel on which it received the connectable advertising packet. The advertising event is ended and connection events begin if the advertiser receives and accepts the request for a connection be initiated. Once a connection is established, the initiator becomes the Central in what is referred to as a piconet and the advertising device becomes the Peripheral. Connection events are used to send data packets between the Central and Peripherals. In connection events, channel hopping occurs at the start of each connection event. Within a connection event, the Central and Peripheral alternate sending data packets using the same data PHY channel. The Central initiates the beginning of each connection event and can end each connection event at any time.

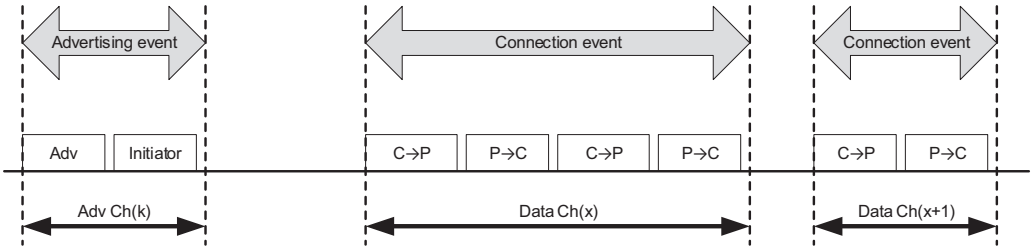

Figure 1.3: Connection events

Devices in a piconet use a specific frequency hopping pattern, which is algorithmically determined by a field contained in the connection request sent by an initiating device. The hopping pattern used in LE is a pseudo-random ordering of the 37 frequencies in the ISM band. The hopping pattern can be adapted to exclude a portion of the frequencies that are used by interfering devices. The adaptive hopping technique improves Bluetooth co-existence with static (non-hopping) ISM systems when these are co-located and have access to information about the local radio environment, or detected by other means. A Peripheral can classify frequencies as good and bad and provide that information to the Central. The Central can take this information into consideration while adapting the hopping pattern.

Using an ACL connection, a Central can establish one or more isochronous connections that use the isochronous physical channel. An isochronous connection is used to transfer isochronous data between the Central and a Peripheral by using a logical transport, which is referred to as a Connected Isochronous Stream (CIS). A CIS consists of CIS events that occur at regular intervals (designated ISO_Interval). Every CIS event consists of one or more subevents. In each subevent, the Central transmits once and the Peripheral responds. If the Central and Peripheral have completed transferring the scheduled isochronous data in a CIS event, all remaining subevents in that event will have no radio transmissions and the event is closed. Each subevent uses a PHY channel which is determined by using the channel selection algorithm. The PHY channel that is used for a subevent is marked as ISO Ch(eventcount, subeventcount), as shown in Figure 1.4.

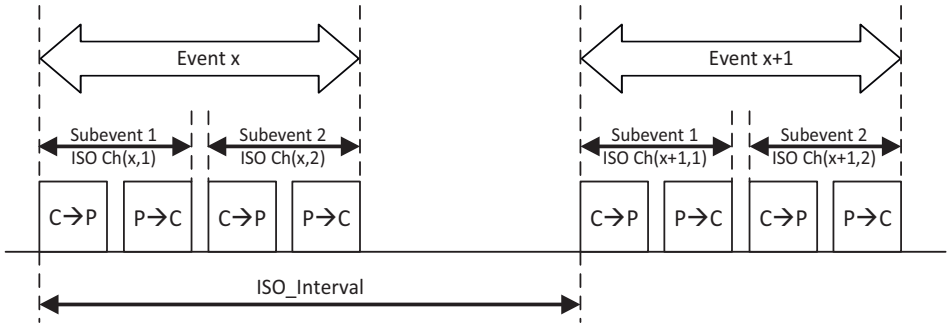

Figure 1.4: CIS events and subevents

A device can use an isochronous physical channel to broadcast isochronous data by using isochronous connectionless logical transports. An isochronous connectionless logical transport is referred to as a Broadcast Isochronous Stream (BIS). A BIS consists of BIS events that occur at regular intervals (designated ISO_Interval). Every BIS event consists of one or more subevents. In every subevent, a broadcasting device transmits an isochronous data packet. Each subevent uses a PHY channel that is determined using the channel selection algorithm.

A device can transmit several BISes with synchronized timing; this is referred to as a Broadcast Isochronous Group (BIG). The various BIS events together form a BIG event. The device can also use the isochronous physical channel to broadcast control information in a Control subevent, which is transmitted at the end of all subevents for a BIG, as shown in Figure 1.5.

A device that transmits BIG events also transmits periodic advertisement events that contain synchronization information of the BIG. A device that is scanning can synchronize to those periodic advertising events and receive the synchronization information. Using this synchronization information, the device can synchronize to one or more BISes in the BIG and receive the isochronous data. Figure 1.5 shows two BIG events: one with and one without a Control subevent. Each subevent uses a PHY channel marked as ISO Ch(eventcount, subeventcount), as shown in Figure 1.5.

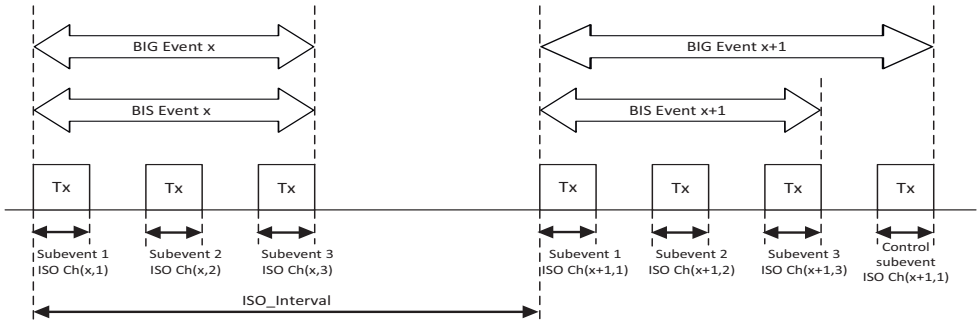

Figure 1.5: BIG and BIS events, BIS subevents, and Control subevent

Above the physical channel there are concepts of links, channels and associated control protocols. The hierarchy is physical channel, physical link, logical transport, logical link, and L2CAP channel. These are discussed in more detail in Section 3.3 to Section 3.6 but are introduced here to aid the understanding of the remainder of this section.

Within a physical channel, a physical link is formed between devices. The active physical link provides bidirectional packet transport between the Central and Peripherals. Centrals may have physical links to more than one Peripheral at a time and Peripherals may have physical links to more than one Central at a time. A device may be Central and Peripheral in different piconets at the same time. Role changes between a Central and Peripheral are not supported. The advertising and periodic physical links provide a unidirectional packet transport from the advertiser to a potentially unlimited number of scanners or initiators.

The physical link is used as a transport for one or more logical links that support asynchronous traffic. Traffic on logical links is multiplexed onto the physical link assigned by a scheduling function in the resource manager.

A control protocol for the link and physical layers is carried over logical links in addition to user data. This is the Link Layer protocol (LL). Devices that are active in a piconet have a default LE asynchronous connection logical transport (LE ACL) that is used to transport the LL protocol signaling. The default LE ACL is the one that is created whenever a piconet is created.

The Link Layer function uses the LL protocol to control the operation of devices in the piconet and provide services to manage the lower architectural layers (PHY and LL).

Overall, a piconet consists of one ACL logical transport over the active physical link plus zero or more CIS logical transports over the isochronous physical link(s).

Just as in BR/EDR, above the Link Layer the L2CAP layer provides a channel-based abstraction to applications and services. It carries out fragmentation and de-fragmentation of application data and multiplexing and de-multiplexing of multiple channels over a shared logical link. L2CAP has a protocol control channel that is carried over the primary ACL logical transport.

In addition to L2CAP, LE provides two additional protocol layers that reside on top of L2CAP. The Security Manager protocol (SMP) uses a fixed L2CAP channel to implement the security functions between devices. The other is the Attribute Protocol (ATT) that provides a method to communicate small amounts of data over a fixed L2CAP channel. The Attribute Protocol is also used by devices to determine the services and capabilities of other devices. The Attribute Protocol may also be used over BR/EDR.

The LE radio provides a means for detecting the relative direction of another LE radio by using the Angle of Arrival (AoA) or Angle of Departure (AoD) method.

1.3 [THIS SECTION IS NO LONGER USED]

1.4 NOMENCLATURE

Where the following terms appear in the specification they have the meaning given in Table 1.1.

Active Peripheral Broadcast (APB)	The logical transport that is used to transport L2CAP user traffic and some kinds of LMP traffic to all active devices in the piconet over the BR/EDR Controller. See Section 3.5.4.4
Ad Hoc Network	A network typically created in a spontaneous manner. An ad hoc network requires no formal infrastructure and is limited in temporal and spatial extent.
Advertiser	A Bluetooth Low Energy device that broadcasts advertising packets during advertising events on advertising channels
Advertising event	A series of between one and three advertising packets on different advertising physical channels sent by an advertiser.
Advertising Packet	A packet containing an advertising PDU. See [Vol 6] Part B, Section 2.3.1
Angle of Arrival (AoA)	Angle of Arrival is the relative direction at which a propagating RF wave that was transmitted by a single antenna is incident on an antenna array.
Angle of Departure (AoD)	Angle of Departure is the relative direction from which a propagating RF wave that was transmitted using an antenna array is incident on another antenna.

Table 1.1: Nomenclature (Sheet 1 of 7)

BD_ADDR	The Bluetooth Device Address, BD_ADDR, is used to identify a Bluetooth device.
Bluetooth	Bluetooth is a wireless communication link, operating in the unlicensed ISM band at 2.4 GHz using a frequency hopping transceiver. It allows real-time AV and data communications between Bluetooth Hosts. The link protocol is based on time slots.
Bluetooth Baseband	The part of the Bluetooth system that specifies or implements the medium access and physical layer procedures to support the exchange of real-time voice, data information streams, and ad hoc networking between Bluetooth Devices.
Bluetooth Clock	A 28 bit clock internal to a BR/EDR Controller sub-system that ticks every 312.5 µs. The value of this clock defines the slot numbering and timing in the various physical channels.
Bluetooth Controller	A generic term referring to a Controller.
Bluetooth Device	A device that is capable of short-range wireless communications using the Bluetooth system.
Bluetooth Device Address	A 48 bit address used to identify each Bluetooth device.
BR/EDR	Bluetooth basic rate (BR) and enhanced data rate (EDR).
BR/EDR Controller	A term referring to the Bluetooth Radio, Baseband, Link Manager, and HCI layers.
BR/EDR Piconet Physical Channel	A Channel that is divided into time slots in which each slot is related to an RF hop frequency. Consecutive hops normally correspond to different RF hop frequencies and occur at a standard hop rate of 1600 hops per second. These consecutive hops follow a pseudo-random hopping sequence, hopping through a 79 RF channel set, or optionally fewer channels when Adaptive Frequency Hopping (AFH) is in use.
BR/EDR/LE	Bluetooth basic rate (BR), enhanced data rate (EDR) and low energy (LE).
C-plane	Control plane
Channel	Either a physical channel or an L2CAP channel, depending on the context.
Connect (to service)	The establishment of a connection to a service. If not already done, this also includes establishment of a physical link, logical transport, logical link and L2CAP channel.

Table 1.1: Nomenclature (Sheet 2 of 7)

Connectable device	A BR/EDR device in range that periodically listens on its page scan physical channel and will respond to a page on that channel. An LE device that is advertising using a connectable advertising event.
Connected devices	Two BR/EDR devices and with a physical link between them.
Connecting	A phase in the communication between devices when a connection between the devices is being established. (Connecting phase follows after the link establishment phase is completed.)
Connection	A connection between two peer applications or higher layer protocols mapped onto an L2CAP channel.
Connection establishment	A procedure for creating a connection mapped onto a channel.
Connection event	A series of one or more pairs of interleaving data packets sent between a Central and a Peripheral on the same physical channel.
Connectionless Peripheral Broadcast (CPB)	A feature that enables a Central to broadcast information to an unlimited number of Peripherals.
Connectionless Peripheral Broadcast Receiver	A Bluetooth device that receives broadcast information from a Connectionless Peripheral Broadcast Transmitter. The device is a Peripheral of the piconet.
Connectionless Peripheral Broadcast Transmitter	A Bluetooth device that sends Connectionless Peripheral Broadcast messages for reception by one or more Connectionless Peripheral Broadcast receivers. The device is the Central of the piconet.
Controller	A collective term referring to all of the layers below HCI.
Coverage area	The area where two Bluetooth devices can exchange messages with acceptable quality and performance.
Creation of a secure connection	A procedure of establishing a connection, including authentication and encryption.
Creation of a trusted relationship	A procedure where the remote device is marked as a trusted device. This includes storing a common link key for future authentication, or pairing, when a link key is not available.
Device discovery	A procedure for retrieving the Bluetooth Device Address, clock, and Class of Device from discoverable devices.
Discoverable device	A BR/EDR device in range that periodically listens on an inquiry scan physical channel and will respond to an inquiry on that channel. An LE device in range that is advertising with a connectable or scannable advertising event with a discoverable flag set in the advertising data. This device is in the discoverable mode.

Table 1.1: Nomenclature (Sheet 3 of 7)

Discoverable Mode	A Bluetooth device that is performing inquiry scans in BR/EDR or advertising with a discoverable or connectable advertising event with a discoverable flag set in LE.
Discovery procedure	A Bluetooth device that is carrying out the inquiry procedure in BR/EDR or scanning for advertisers using a discoverable or connectable advertising event with a discoverable flag set in LE.
HCI	The Host Controller interface (HCI) provides a command interface to the baseband Controller and link manager and access to hardware status and control registers. This interface provides a uniform method of accessing the Bluetooth baseband capabilities.
Host	A logical entity defined as all of the layers below the non-core profiles and above the Host Controller interface (HCI); i.e., the layers specified in Volume 3. A Bluetooth Host attached to a Bluetooth Controller may communicate with other Bluetooth Hosts attached to their Controllers as well.
Initiator	A Bluetooth Low Energy device that listens on advertising physical channels for connectable advertising events to form connections.
Inquiring device	A BR/EDR device that is carrying out the inquiry procedure. This device is performing the discovery procedure.
Inquiry	A procedure where a Bluetooth device transmits inquiry messages and listens for responses in order to discover the other Bluetooth devices that are within the coverage area.
Inquiry scan	A procedure where a Bluetooth device listens for inquiry messages received on its inquiry scan physical channel.
Interoperability	The ability of two or more devices to exchange information and to use the information that has been exchanged.
Isochronous data	Information in a stream where each information entity in the stream is bound by a time relationship to previous and successive entities.
Known device	A Bluetooth device for which at least the BD_ADDR is stored.
L2CAP	Logical Link Control and Adaptation Protocol
L2CAP Channel	A logical connection on L2CAP level between two devices serving a single application or higher layer protocol.
L2CAP Channel establishment	A procedure for establishing a logical connection on L2CAP level.
LE	Bluetooth Low Energy

Table 1.1: Nomenclature (Sheet 4 of 7)

Link	Shorthand for a logical link.
Link establishment	A procedure for establishing the default ACL link and hierarchy of links and channels between devices.
Link key	A secret key that is known by two devices and is used to authenticate the link.
LMP authentication	An LMP level procedure for verifying the identity of a remote device.
LMP pairing	A procedure that authenticates two devices and creates a common link key that can be used as a basis for a trusted relationship or a (single) secure connection.
Logical link	The lowest architectural level used to offer independent data transport services to clients of the Bluetooth system.
Logical transport	Shared acknowledgment protocol and link identifiers between different logical links.
Name discovery	A procedure for retrieving the user-friendly name (the Bluetooth Device Name) of a connectable device.
Packet	Format of aggregated bits that are transmitted on a physical channel.
Page	The initial phase of the connection procedure where a device transmits a train of page messages until a response is received from the target device or a time-out occurs.
Page scan	A procedure where a device listens for page messages received on its page scan physical channel.
Paging device	A Bluetooth device that is carrying out the page procedure.
Paired device	A Bluetooth device for which a link key has been created (either before connection establishment was requested or during connecting phase).
Passkey	A 6-digit number used to authenticate connections when Secure Simple Pairing is used.
Periodic advertising synchronization information	The control information describing a periodic advertisement that a Bluetooth Low Energy device uses to synchronize to the advertisement it describes.
Physical Channel	Characterized by synchronized occupancy of a sequence of RF carriers by one or more devices. A number of physical channel types exist with characteristics defined for their different purposes.
Physical link	A Baseband or Link Layer level connection between two devices.
Physical Transport	PHY packet transmission and/or reception on an RF channel using one or more modulation schemes.

Table 1.1: Nomenclature (Sheet 5 of 7)

Piconet	A collection of devices (up to eight devices in BR/EDR, exactly two devices in LE) occupying a shared physical channel where one of the devices is the Piconet Central and the remaining devices are connected to it.
Piconet Central	The BR/EDR device in a piconet whose Bluetooth Clock and Bluetooth Device Address are used to define the piconet physical channel characteristics. The LE device in a piconet which initiates the creation of the piconet, chooses the Access Address that identifies the piconet, and transmits first in each connection event.
Piconet Peripheral	Any BR/EDR device in a piconet that is not the Piconet Central, but is connected to the Piconet Central. The LE device in a piconet which is not the Central but communicates with it.
PIN	A user-friendly number that can be used to authenticate connections to a device before pairing has taken place.
Profile Broadcast Data (PBD)	A logical link that carries data from a Connectionless Peripheral Broadcast Transmitter to one or more Connectionless Peripheral Broadcast Receivers.
Resolving List	A list of records used to generate and resolve Resolvable Private Addresses. Each record contains a local Identity Resolving Key, a peer Identity Resolving Key, and a peer Identity Address.
Scanner	A Bluetooth Low Energy device that listens for advertising events on the advertising physical channels.
Scatternet	Two or more piconets that have one or more devices in common.
Service discovery	Procedures for querying and browsing for services offered by or through another Bluetooth device.
Service Layer Protocol	A protocol that uses an L2CAP channel for transporting PDUs.
Silent device	A Bluetooth enabled device appears as silent to a remote device if it does not respond to inquiries made by the remote device.
Synchronization Scan Physical Channel	A physical channel that enables a Peripheral to receive synchronization train packets from a Central.
Synchronization Train	A series of packets transmitted on a set of fixed frequencies that deliver sufficient information for a receiving device to start receiving corresponding Connectionless Peripheral Broadcast packets or to recover the current piconet clock after missing a Coarse Clock Adjust.

Table 1.1: Nomenclature (Sheet 6 of 7)

Tick	(BR/EDR) the time between changes of the value of the Bluetooth Clock: 312.5 µs.
U-plane	User plane
Unknown device	A Bluetooth device for which no information (Bluetooth Device Address, link key or other) is stored.

Table 1.1: Nomenclature (Sheet 7 of 7)

2 CORE SYSTEM ARCHITECTURE

The Bluetooth Core system consists of a Host and a Controller. A minimal implementation of the Bluetooth BR/EDR core system covers the four lowest layers and associated protocols defined by the Bluetooth specification as well as one common service layer protocol; the Service Discovery Protocol (SDP) and the overall profile requirements are specified in the Generic Access Profile (GAP). A minimal implementation of a Bluetooth LE only core system covers the four lowest layers and associated protocols defined by the Bluetooth specification as well as two common service layer protocols; the Security Manager (SM) and Attribute Protocol (ATT) and the overall profile requirements are specified in the Generic Attribute Profile (GATT) and Generic Access Profile (GAP). Implementations combining Bluetooth BR/EDR and LE include both of the minimal implementations described above.

A complete Bluetooth application requires a number of additional service and higher layer protocols that are defined in the Bluetooth specification, but are not described here. The core system architecture is shown in Figure 2.1.

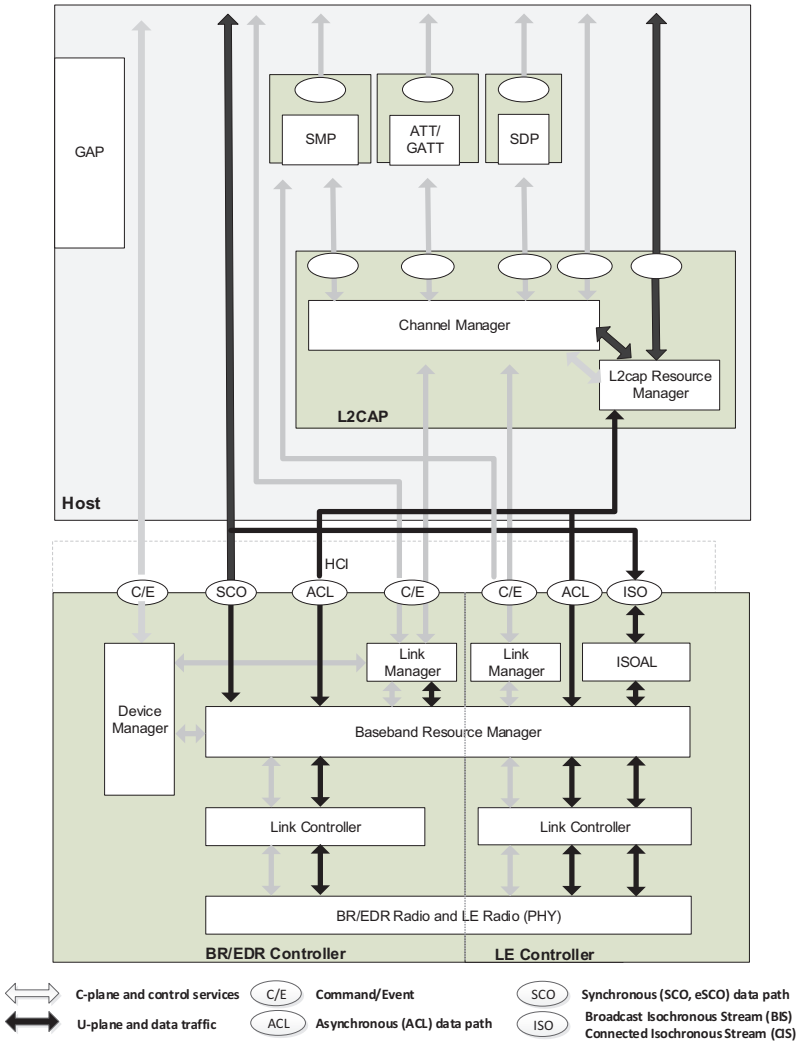

Figure 2.1: Bluetooth core system architecture

Figure 2.1 shows the Core blocks, each with its associated communication protocol. Link Manager, Link Controller and BR/EDR Radio blocks comprise a BR/EDR Controller. Link Manager, Link Controller and LE Radio blocks comprise an LE Controller. L2CAP, SDP and GAP blocks comprise a BR/EDR Host. L2CAP, SMP, Attribute Protocol, GAP and Generic Attribute Profile (GATT) blocks comprise an LE Host. A BR/EDR/LE Host combines the set of blocks from each respective Host. This is a common implementation involving a standard physical communication interface between the Controller and the Host. Although this interface is optional the architecture is designed to allow for its existence and characteristics. The Bluetooth specification enables interoperability between independent Bluetooth systems by defining the protocol messages exchanged between equivalent layers, and also interoperability between independent Bluetooth Controllers and Bluetooth

Hosts by defining a common interface between Bluetooth Controllers and Bluetooth Hosts.

A number of functional blocks and the path of services and data between them are shown. The functional blocks shown in the diagram provide a set of conceptual entities that are used when describing the requirements of the specification; in general the Bluetooth specification does not define the details of implementations except where this is required for interoperability. Thus the functional blocks in Figure 2.1 are shown in order to aid description of the system behavior. An implementation may be different from the system shown in Figure 2.1.

Standard interactions are defined for all inter-device operation, where Bluetooth devices exchange protocol signaling according to the Bluetooth specification. The Bluetooth core system protocols are the Radio (PHY) protocol, Link Control (LC) and Link Manager (LM) protocol or Link Layer (LL) protocol, and Logical Link Control and Adaptation protocol (L2CAP), all of which are fully defined in subsequent parts of the Bluetooth specification. In addition, the Service Discovery protocol (SDP) and the Attribute Protocol (ATT) are service layer protocols that may be required by some Bluetooth applications.

The Bluetooth core system offers services through a number of service access points that are shown in the diagram as ellipses. These services consist of the basic primitives that control the Bluetooth core system. The services can be split into three types. There are device control services that modify the behavior and modes of a Bluetooth device, transport control services that create, modify and release traffic bearers (channels and links), and data services that are used to submit data for transmission over traffic bearers. It is common to consider the first two as belonging to the C-plane and the last as belonging to the U-plane.

A service interface to the Bluetooth Controller is defined such that the Controller may be considered a standard part. In this configuration the Bluetooth Controller operates the lowest four layers. The Bluetooth Host operates the L2CAP layer and other higher layers. The standard interface is called the Host Controller interface (HCI) and its service access points are represented by the ellipses on the upper edge of the Bluetooth Controller in Figure 2.1. Implementation of this standard service interface is optional.

As the Bluetooth architecture is defined with the possibility of separate Host and Controller(s) communicating through one or more HCI transports, a number of general assumptions are made. Bluetooth Controllers are assumed to have limited data buffering capabilities in comparison with the Host. Therefore the L2CAP layer is expected to carry out some simple resource management when submitting L2CAP PDUs to the Controller for transport to a peer device. This includes segmentation of L2CAP SDUs into more manageable PDUs and then the fragmentation of PDUs into start and continuation packets of a size suitable for the Controller buffers, and

management of the use of Controller buffers to ensure availability for channels with Quality of Service (QoS) commitments.

The BR/EDR Baseband and LE Link Layer provide the basic acknowledgment/repeat request (ARQ) protocol in Bluetooth. The L2CAP layer can optionally provide a further error detection and retransmission to the L2CAP PDUs. This feature is recommended for applications with requirements for a low probability of undetected errors in the user data. A further optional feature of L2CAP is a window-based flow control that can be used to manage buffer allocation in the receiving device. Both of these optional features augment the QoS performance in certain scenarios. Not all of the L2CAP capabilities are available when using the LE system.

Although these assumptions are not always required for embedded Bluetooth implementations that combine all layers in a single system, the general architectural and QoS models are defined with these assumptions in mind, in effect a lowest common denominator.

Automated conformance testing of implementations of the Bluetooth core system is required. This is achieved by allowing the tester to control the implementation through the PHY interface, test interfaces such as Direct Test Mode (DTM), and test commands and events over HCI which are only required for conformance testing.

The tester exchanges messages with the Implementation Under Test (IUT) through the PHY interface to ensure the correct responses to requests from remote devices. The tester controls the IUT through HCI, DTM, or test commands to cause the IUT to originate exchanges through the PHY interface so that these can also be verified as conformant.

2.1 CORE ARCHITECTURAL BLOCKS

This section describes the function and responsibility of each of the blocks shown in Figure 2.1. An implementation is not required to follow the architecture described above, though every implementation is still required to conform to the protocol specifications, behaviors, and other requirements specified in subsequent parts of the Bluetooth specification.

2.1.1 Host architectural blocks

2.1.1.1 Channel manager

The channel manager is responsible for creating, managing and closing L2CAP channels for the transport of service protocols and application data streams. The channel manager uses the L2CAP protocol to interact with a channel manager on a remote (peer) device to create these L2CAP channels and connect their endpoints to the appropriate entities. The channel manager interacts with its local link manager to create new logical links (if necessary)

and to configure these links to provide the required quality of service for the type of data being transported.

2.1.1.2 L2CAP resource manager

The L2CAP resource manager block is responsible for managing the ordering of submission of PDU fragments to the baseband and some relative scheduling between channels to ensure that L2CAP channels with QoS commitments are not denied access to the physical channel due to Controller resource exhaustion. This is required because the architectural model does not assume that a Controller has limitless buffering, or that the HCI is a pipe of infinite bandwidth.

L2CAP Resource Managers may also carry out traffic conformance policing to check that applications are submitting L2CAP SDUs within the bounds of their negotiated QoS settings. The general Bluetooth data transport model assumes well-behaved applications, and does not define how an implementation is expected to deal with this problem.

2.1.1.3 Security Manager Protocol

The Security Manager Protocol (SMP) is the peer-to-peer protocol used to generate encryption keys and identity keys. The protocol operates over a dedicated fixed L2CAP channel. The SMP block also manages storage of the encryption keys and identity keys and is responsible for generating random addresses and resolving random addresses to known device identities. The SMP block interfaces directly with the Controller to provide stored keys used for encryption and authentication during the encryption or pairing procedures.

This block is only used in LE systems. Similar functionality in the BR/EDR system is contained in the Link Manager block in the Controller. SMP functionality is in the Host on LE systems to reduce the implementation cost of the LE only Controllers.

2.1.1.4 Attribute Protocol

The Attribute Protocol (ATT) block implements the peer-to-peer protocol between an ATT Server and an ATT Client. The ATT Client communicates with an ATT Server on a remote device over a dedicated fixed L2CAP channel. The ATT Client sends commands, requests, and confirmations to the ATT Server. The ATT Server sends responses, notifications and indications to the client. These ATT Client commands and requests provide a means to read and write values of attributes on a peer device with an ATT Server.

2.1.1.5 [This section is no longer used]

2.1.1.6 Generic Attribute Profile

The Generic Attribute Profile (GATT) block represents the functionality of the ATT Server and, optionally, the ATT Client. The profile describes the hierarchy

of services, characteristics and attributes used in the ATT Server. The block provides interfaces for discovering, reading, writing and indicating of service characteristics and attributes. GATT is used on LE devices for LE profile service discovery.

2.1.1.7 Generic Access Profile

The Generic Access Profile (GAP) block represents the base functionality common to all Bluetooth devices such as modes and access procedures used by the transports, protocols and application profiles. GAP services include device discovery, connection modes, security, authentication, association models and service discovery.

2.1.2 BR/EDR/LE Controller architectural blocks

In implementations where the BR/EDR and LE systems are combined, the architectural blocks may be shared between systems or each system may have their own instantiation of the block.

2.1.2.1 Device manager

The device manager is the functional block in the baseband that controls the general behavior of the Bluetooth device. It is responsible for all operations of the Bluetooth system that are not directly related to data transport, such as inquiring for the presence of nearby Bluetooth devices, connecting to Bluetooth devices, or making the local Bluetooth device discoverable or connectable by other devices.

The device manager requests access to the transport medium from the baseband resource Controller in order to carry out its functions.

The device manager also controls local device behavior implied by a number of the HCI commands, such as managing the device local name, any stored link keys, and other functionality.

2.1.2.2 Link manager

The link manager is responsible for the creation, modification and release of logical links (and, if required, their associated logical transports), as well as the update of parameters related to physical links between devices. The link manager achieves this by communicating with the link manager in remote Bluetooth devices using the Link Manager Protocol (LMP) in BR/EDR and the Link Layer Protocol (LL) in LE.

The LM or LL protocol allows the creation of new logical links and logical transports between devices when required, as well as the general control of link and transport attributes such as the enabling of encryption on the logical transport, the adapting of transmit power on the physical link, or the adjustment of QoS settings in BR/EDR for a logical link.

2.1.2.3 Baseband resource manager

The baseband resource manager is responsible for all access to the radio medium. It has two main functions. At its heart is a scheduler that grants time on the physical channels to all of the entities that have negotiated an access contract. The other main function is to negotiate access contracts with these entities. An access contract is effectively a commitment to deliver a certain QoS that is required in order to provide a user application with an expected performance.

The access contract and scheduling function must take account of any behavior that requires use of the Controller. This includes (for example) the normal exchange of data between connected devices over logical links, and logical transports, as well as the use of the radio medium to carry out inquiries, make connections, be discoverable or connectable, or to take readings from unused carriers during the use of adaptive frequency hopping mode.

In some cases in BR/EDR systems the scheduling of a logical link results in changing a logical link to a different physical channel from the one that was previously used. This may be (for example) due to involvement in scatternet, a periodic inquiry function, or page scanning. When the physical channels are not time slot aligned, then the resource manager also accounts for the realignment time between slots on the original physical channel and slots on the new physical channel. In some cases the slots will be naturally aligned due to the same device clock being used as a reference for both physical channels.

2.1.2.4 Link Controller

The Link Controller is responsible for the encoding and decoding of Bluetooth packets from the data payload and parameters related to the physical channel, logical transport and logical link.

The Link Controller carries out the link control protocol signaling in BR/EDR and Link Layer protocol in LE (in close conjunction with the scheduling function of the resource manager), which is used to communicate flow control and acknowledgment and retransmission request signals. The interpretation of these signals is a characteristic of the logical transport associated with the baseband packet. Interpretation and control of the link control signaling is normally associated with the resource manager’s scheduler.

2.1.2.5 PHY

The PHY block is responsible for transmitting and receiving packets of information on the physical channel. A control path between the baseband and the PHY block allows the baseband block to control the timing and frequency carrier of the PHY block. The PHY block transforms a stream of data to and from the physical channel and the baseband into required formats.

2.1.2.6 Isochronous Adaptation Layer

The Isochronous Adaptation Layer (ISOAL) enables the upper layer to send or receive isochronous data to or from the Link Layer in a flexible way such that the size and interval of data packets in the upper layer can be different from the size and interval of data packets in the Link Layer. The ISOAL uses fragmentation/recombination or segmentation/reassembly operations to convert upper layer data units into lower layer data units (or the other way around).

2.1.3 [This section is no longer used]

3 DATA TRANSPORT ARCHITECTURE

The Bluetooth data transport system follows a layered architecture. This description of the Bluetooth system describes the Bluetooth core transport layers up to and including L2CAP channels. All Bluetooth operational modes follow the same generic transport architecture, which is shown in Figure 3.1.

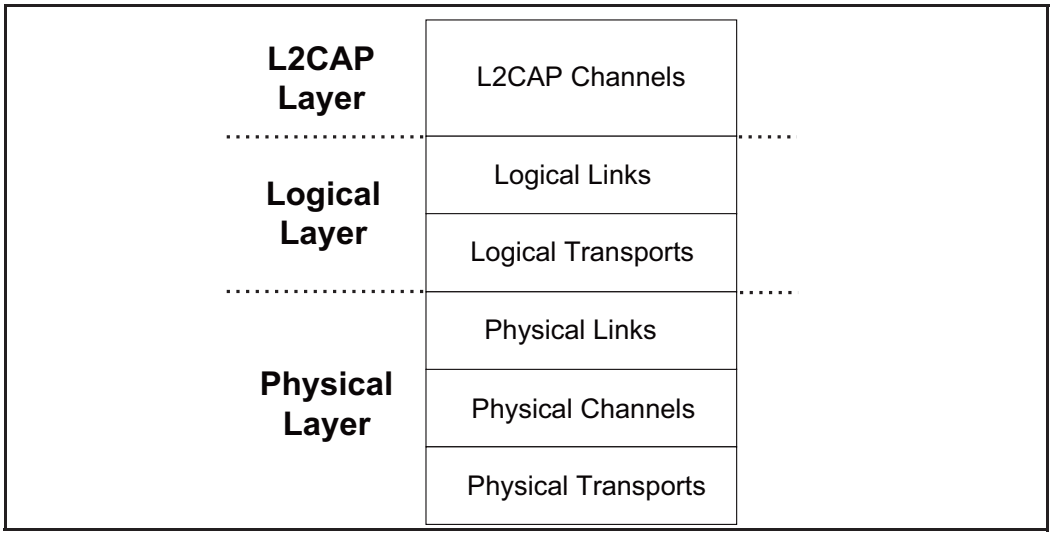

Figure 3.1: Bluetooth generic data transport architecture

For efficiency and legacy reasons, the Bluetooth transport architecture includes a sub-division of the logical layer, distinguishing between logical links and logical transports. This sub-division provides a general (and commonly understood) concept of a logical link that provides an independent transport between two or more devices. The logical transport sub-layer is required to describe the inter-dependence between some of the logical link types (mainly for reasons of legacy behavior).

The ACL, SCO, and eSCO connections are considered as logical transports but often behave as separate physical links. However, they are not as independent as might be desired, due to their shared use of resources such as the LT_ADDR and acknowledgment/repeat request (ARQ) scheme. Hence the architecture is incapable of representing these logical transports with a single transport layer. The additional logical transport layer goes some way towards describing this behavior.