Understanding Bluetooth Fundamentals

Table of contents

If you are able to see this document, it is because your eyes are susceptible to the frequency range of 430 THz to 770 THz **Electro-magnetic waves*** (Human Visible Range). If you can hear to what the other person says, it's because your ears are susceptible to the frequency range of 20Hz to 20KHz (Human Audible Range) **pressure waves** in the air medium*.

In the same way, if you want to communicate over Bluetooth, you should be able to generate voice at 2.4 Ghz of Electro-magnetic waves (and not pressure waves), to which Bluetooth device's antenna is tuned.

"Human Visible frequency range is 1 Lakh 75 thousand times more than Bluetooth frequency range and the same BT frequency range is 1 Lakh 20 thousand times more than Human Audible frequency range".

If by chance, your ear starts to listen to 2.4 Ghz band of EM waves and at the same time your mind is able to interpret these messages, *may be* you would be a Bluetooth Receiver!!!

1. Bluetooth Fundamentals:

Bluetooth wireless technology is mainly used for the transfer of voice / audio / data over a short distance, but how does this happen from the moment Bluetooth is turned ON in a mobile phone until the message is successfully transmitted, is described in this document.

So much is being told about frequency and frequency band, let us understand what they physically mean. Water waves are made-up of variations in the height of the water level, sound waves are made-up of variation in the intensity of air pressure. In the same way, electro-magnetic waves are caused by variations in electric and magnetic fields and propagate without a need of physical medium. These variations are not random in nature, but are periodic. The number of times these variations happen per unit-time is called **frequency** of a wave. Frequency of waves is measured in units called as Hertz (Hz). I.e. *Number of Variations / second.*

The frequency of electrical signals sent to speakers are in the range of 20Hz to 20KHz and speakers convert these electrical signals to pressure waves, but how can the same voice / audio signals of 20Hz to 20KHz range be sent over Bluetooth which operates in the range of 2.4 Ghz ?. The solution to this problem is **modulation.** The signals at their original frequency are called as **baseband signals**. Here voice signals at 20Hz to 20 KHz range are at their Baseband. The intelligence carried by the Baseband signals either in the form of amplitude/ frequency/phase is imparted onto carrier wave in the range recognized by 2.4 GHz frequency and this process is known as *modulation*. At the receiver side, the message signal is appropriately de-modulated to get back

the original baseband signal.

As said, Bluetooth uses **2.4GHz** Industrial, Scientific, and Medical **(ISM) band** for transmitting information. Do you remember the last time you listened to music over Bluetooth headset, or when you transferred a file over Bluetooth, you did all of that for no cost!! , because it is one of the license-free frequency bands. We call this as **band** of frequencies because, it's not one frequency, it's a set of frequencies from 2.4000 GHz to 2.4835 GHz (i.e. there are 2.4000 Giga – 2.4835 Giga = 83.5 million unique frequencies in the band). This 2.4GHz band, which is useable anywhere in the world upon restrictions on range of transmission and transmit power. Having a **bandwidth** of (2.4835 GHz - 2.4000 GHz) about 83.5MHz (of which 79MHz is used in Bluetooth for communication).

Bluetooth (BR/EDR) uses Gaussian **frequency hopping** spread spectrum (G-FHSS) as modulation scheme where the bandwidth of 79MHz is divided into narrow channels of 1MHz each so we get 79 equi-distant frequency channels. To send a zero, a negative frequency deviation is used. To send a one, a positive frequency deviation is used.

Successful communication between any 2 wireless devices can happen only when both devices' transceivers are tuned to the same frequency at any point in time. Unlike other wireless communication techniques, Bluetooth uses hopping through **79 channels** in a pseudo-random order. The order of hopping through frequencies has to be known prior to communication by both the communicating devices. Hence the hopping cannot be random but '**pseudo random**' which means that hopping sequence appears to be random for other devices which are not actively taking part in communication but is well deterministic for those who are active in a specific communication.

What does Gaussian frequency hopping modulation means?
We already know, if receiver has to receive messages transmitted by the transmitter, both the devices have to be tuned to same frequency channel. The unique characteristics of frequency hopping spread spectrum modulation is, the devices participating in communication will not stay in one frequency but for every fixed time interval 't' time units, jumps to the next frequency in the given set of frequencies and stay there for 't' time units and this mechanism repeats. For example, for every 1 minute, transmitter and receivers will be tuning to frequency in the following order of channels - 0, 3, 78, 55, 62, 43, 38, 66, 1, 22, 15.....

Device which provides this synchronization reference to calculate next hopping frequency, and the phase (time to hop to that frequency) is called as **master** and other devices which are synchronized to the frequency and timing reference provided by the master is known as **slave**. This kind of synchronized network is called as **piconet**. Slaves in the piconet are to be synchronized to the master if communication has to happen between master and slaves.

Hopping sequence and phase of hopping is algorithmically determined by BD_ADDR (Bluetooth Device Address) which is unique to each controller and clock of the master. The basic hopping pattern determined is a pseudo-random ordering of the 79 frequencies (each of 1MHz BW) in the ISM band.

If communication has to happen in a piconet, it has to happen between master and slaves in the **physical channel**, and physical channel is sub-divided into time units known as **slots**. Communication messages which are in the form of packets are transmitted over a physical channel in master-slave fashion where master polls a slave in even numbered time slots (which is dynamically determined by baseband manager sub-system of the master device) to which slave responds in the next odd time slot . When circumstances permit, a number of consecutive slots may be allocated to a single packet hence this communication is happening in **Time Division Duplex** (TDD) mannerism.

Communication in a piconet happens after connection is established between master and a slave with the time slot of 625 microseconds each. Frequency hopping of all the devices connected to the piconet happens 1600 times a second i.e. for every slot, a new frequency is hopped to by all the devices in the piconet determined by pseudo-random hopping sequence.

1.1 Why 2.4GHz band is licence free band?

If 2.4GHz frequency band is used for long range communication, humidity present in the atmosphere (water content in the atmosphere) absorbs this frequency and gets heated up and signals fail to reach far away distances. Hence this frequency range is unsuitable for long-range communication.

In the same frequency range, 2.45GHz is used in microwave ovens for di-electric heating. Water, oils and fats gets heated up while the wave’s passes through plastic and glass which are least exited to the applied frequency and power.

Federal Communications Commission (FCC) of the USA and International Telecommunication Union (ITU) got around to establish which frequencies unlicensed gadgets could use. There were already some frequencies used by Tv, Radio (for commercial purposes – which were to be licensed for usage) and even microwave ovens which were gaining popularity in household, and the frequency band used by microwave ovens was the same frequency industries, scientific community and medicine fields were also using for di-electric heating. So this frequency range with enough space around it from 2400 to 2483.5 MHz was declared license-free. Microwaves and industrial heating saw further improvements and stated perforated shields which would restrict microwave emissions from these heating devices getting out.

So, this band of frequency was allowed to be used for short range wireless communication with temporal restrictions on spatial and power ranges.

** We have compared Electro-magnetic waves (ISM band, microwaves, visible spectrum) with sound waves for better understanding purpose only. They are completely different kind of waves, EM waves are transverse waves while pressure waves such as sound waves are longitudinal waves. On having same frequency, they never can be used vice-versa i.e. we can't hear to 20Khz EM waves (transverse waves) when the same is false with longitudinal waves and we can't see 500 THz longitudinal waves when the same is false with EM waves (transverse waves).*

2. The Anatomy of Bluetooth:

Bluetooth Host – Controller Architecture

"Anatomy in general is the art of studying different parts of any organized body".
Anatomy can be related here, in understanding functional blocks of BT architecture.

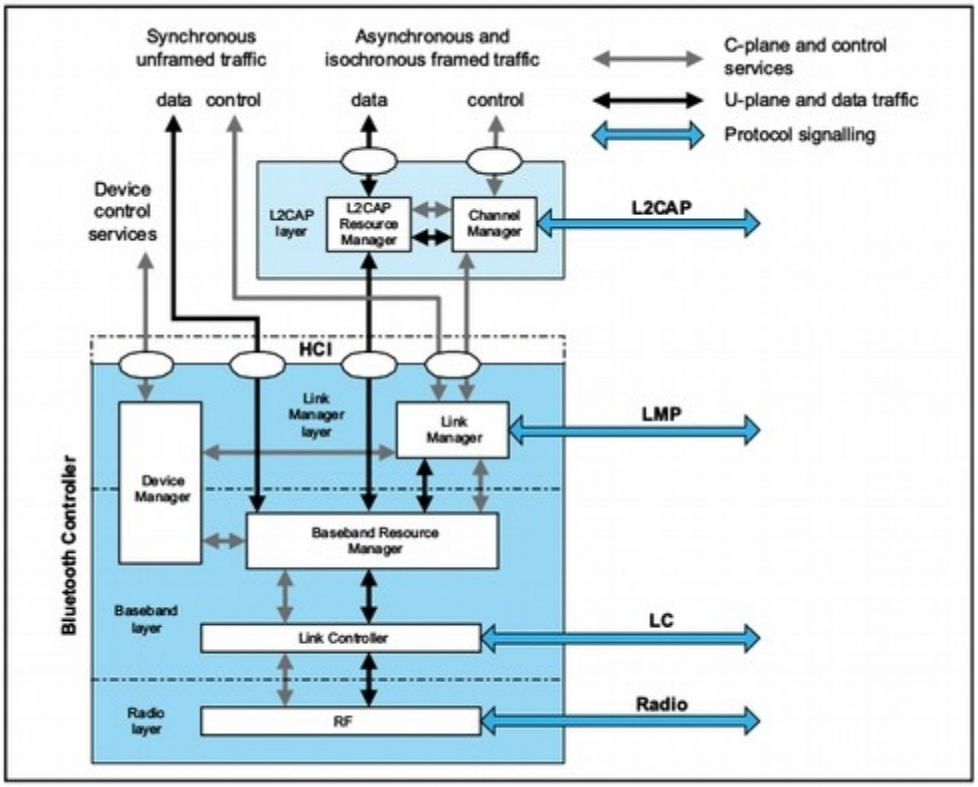


Figure 2.1: Bluetooth core system architecture

Bluetooth system comprises of the following components,

Bluetooth Host	Includes implementations of higher layer of BT architecture which includes core Bluetooth protocols such as L2CAP, SDP, AVDTP and BT profiles such as A2DP, HFP...
Host Controller Interface (HCI)	Delivers data between the Bluetooth host and the Bluetooth controller.
Bluetooth Controller	A Bluetooth device that implements the lowest levels of the Bluetooth architecture.
Bluetooth Application	Application which takes inputs from the user and appropriately uses BT profiles to provide the services of BT
Bluetooth Stack	Comprises of Bluetooth Host, HCI and Bluetooth Controller

Bluetooth Controller part implements Radio, Baseband and Link Management layers as a combination of hardware and software.

An interface, namely HCI is defined by the BT specification to provide a clean standard mechanism for the interaction between BT Host and BT controller. In this configuration the Bluetooth controller operates the lowest three layers.

The host system comprises of L2CAP layer, protocols such as Service Discovery and profiles such as Hands Free and also applications which use these profiles to offer services to the user.

2.1 Bluetooth Controller:

2.1.1 Device Manager:

Device manager is the functional block that controls the general behaviour of Bluetooth controller.

Communication between 2 BT devices will happen after device discovery and connection establishment procedures. Device manager is also responsible for all these activities other than data communication like inquiring for nearby devices, connecting with devices, making the very own device discoverable and connectable by other BT devices.

It is generally implemented as a microcontroller aided with SRAM and Flash. It runs the HCI, link manager and part of baseband resource manager (scheduler part) as the controller part of software stack.

2.1.2 Link Manager:

After Device Discovery and Connection Establishment, communication can happen between the devices which are part of a piconet. This communication happens through links (physical and logical). Physical links are needed for communication between master and multiple slaves, logical links are needed to support multiple applications to talk with each other over a single physical link.

The link manager functional unit is responsible for the creation, modification and release of logical links (and, if required, their associated logical transports), as well as for the updating 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 Management Protocol (LMP).

It is generally implemented as software on microcontroller which performs link management tasks, translating commands and data into operations at the baseband resource manager level.

2.1.3 Baseband Resource Manager:

Though there are one or more logical transports between master and each slave, there is only one physical channel which is unique to the piconet. The same physical channel is utilized by multiple logical transports between master and slaves in the piconet. So there is a need for allocating physical channel to each transport for a specific time. Scheduler in Baseband resource manager takes care of this.

The scheduling part of Baseband Resource Manager is generally implemented as software stack which is run by the microcontroller in the Controller part of Bluetooth system. Baseband Resource Manager is responsible for granting time on the physical channel according to the policy of access contract.

Baseband Resource Manager’s function is also to negotiate access contract with entities demanding for the time on physical channel in order to provide with the demanded 'performance delivery requirements’ by the user applications running on the host.

Scheduling function of Baseband Resource Manager is generally implemented as software running on the microcontroller. It also handles I/O and interrupt related operations concerned with the movement of data to and from link controller.

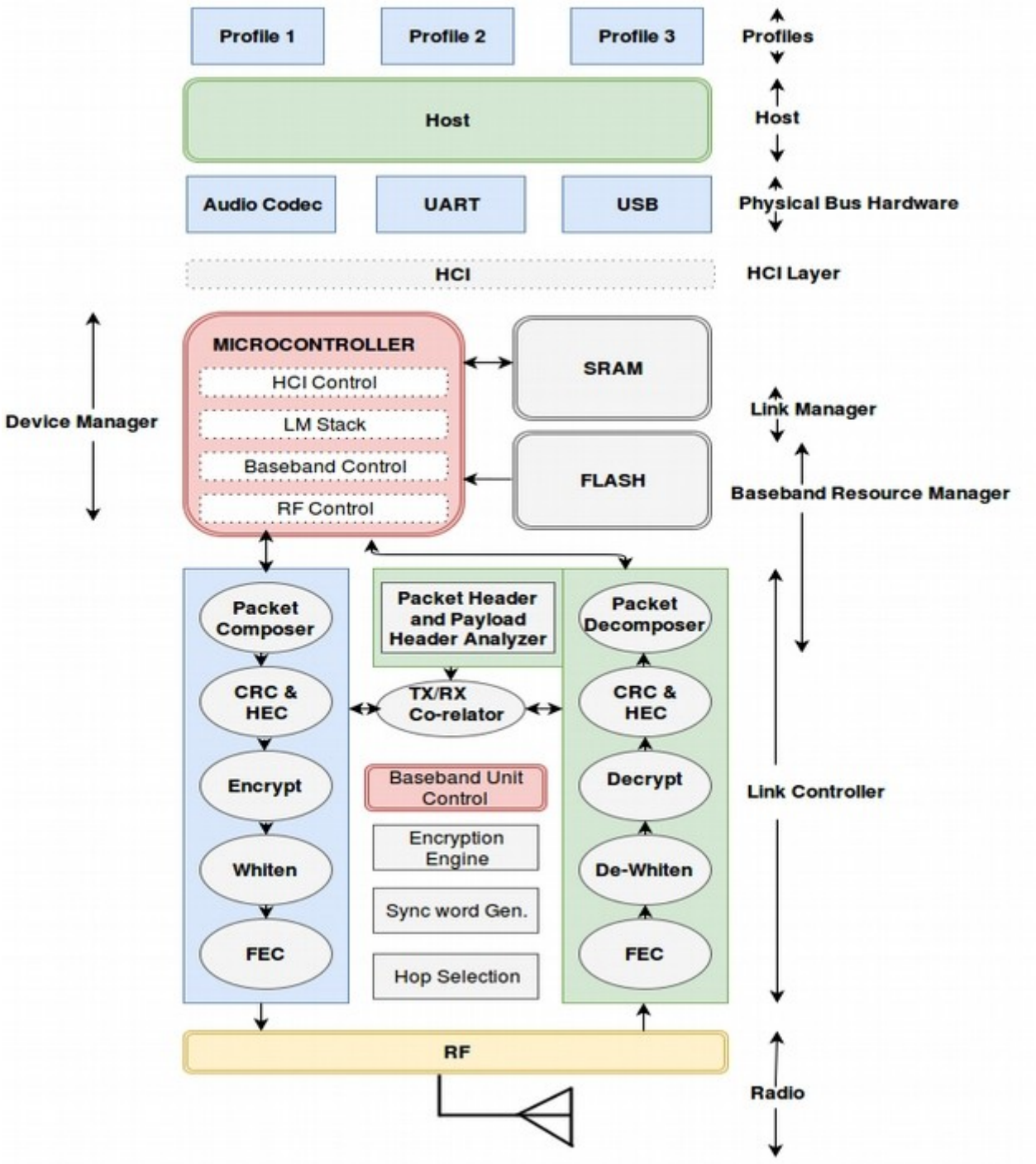
2.1.4 Link Controller:

Link Controller is hardware unit responsible for composition of packets, inclusion of packet header, and access code. Link controller also does encoding of Bluetooth packets, takes care of CRC (Cyclic Redundancy Check) for frame synchronization and error- detection, FEC (Forward Error Correction) for possible Error correction mechanism. Whitening for DC offset reduction so that decoding ONEs and ZEROs with the reference is easier.

Link Controller from the other end also is responsible for Packet De-composition from the received bit-stream with the reference to packet and payload header analyser. It's reverse engineering of Packet composition done in Bit-stream processing unit of Sender's link controller.

Link Controller which does bit-intensive operations is generally implemented as a separate hardware in the controller part of BT device.

3.



The Physiology of Bluetooth:
Bluetooth Communication Architecture

"*Physiology in general deals with functions and activities of an organized body".*

It can be related here, in knowing the interaction between the functional blocks – physical and logical.

Bluetooth communication architecture can be divided into:

1) Physical Transports
2) Physical Channels
3) Physical Link
4) Logical Transports
5) Logical Links
6) L2CAP channels

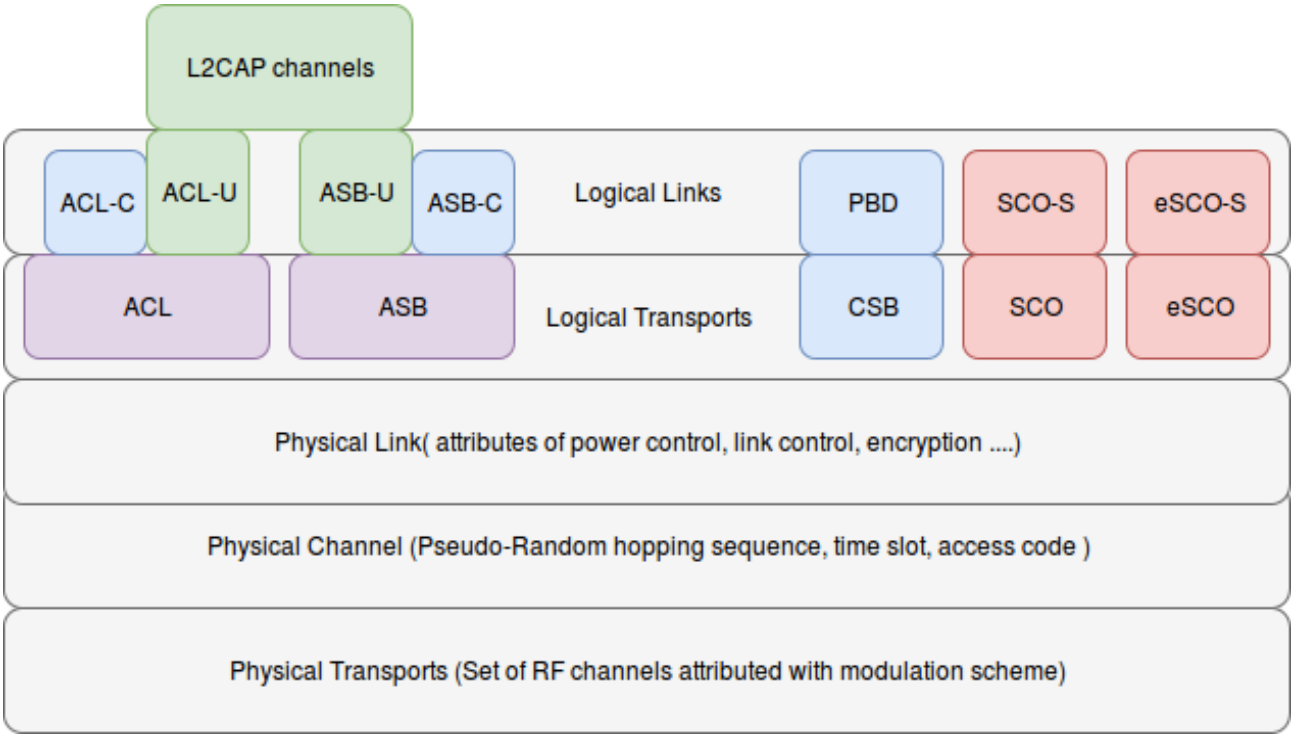


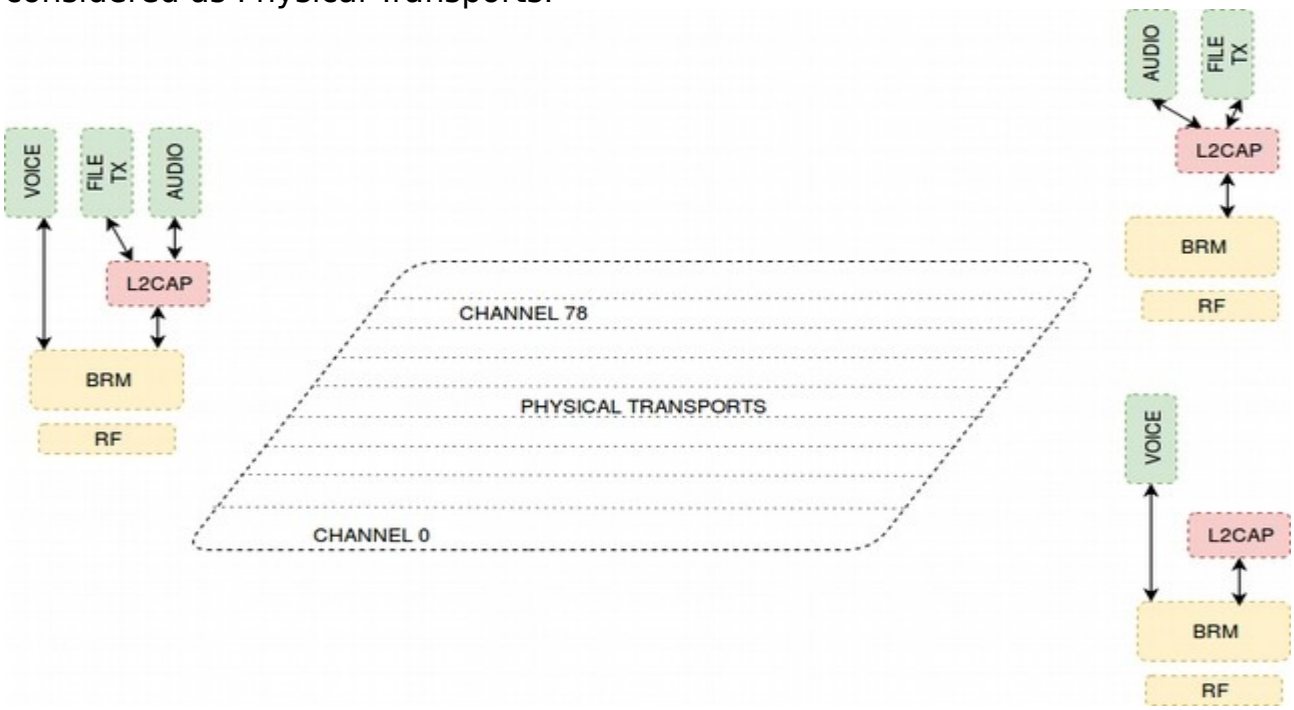
Fig: Core Traffic Bearers

3.1 Physical Transport:

The set of Radio frequency bands that are used for communication between the Master and Slave devices within a piconet is called ***Physical Transport****.*

Since ISM band with central frequency of 2.4 GHz (BW = 79 MHz) is

divided into 79 Channels of 1 MHz each, the set of 79 RF carriers can be considered as Physical Transports.



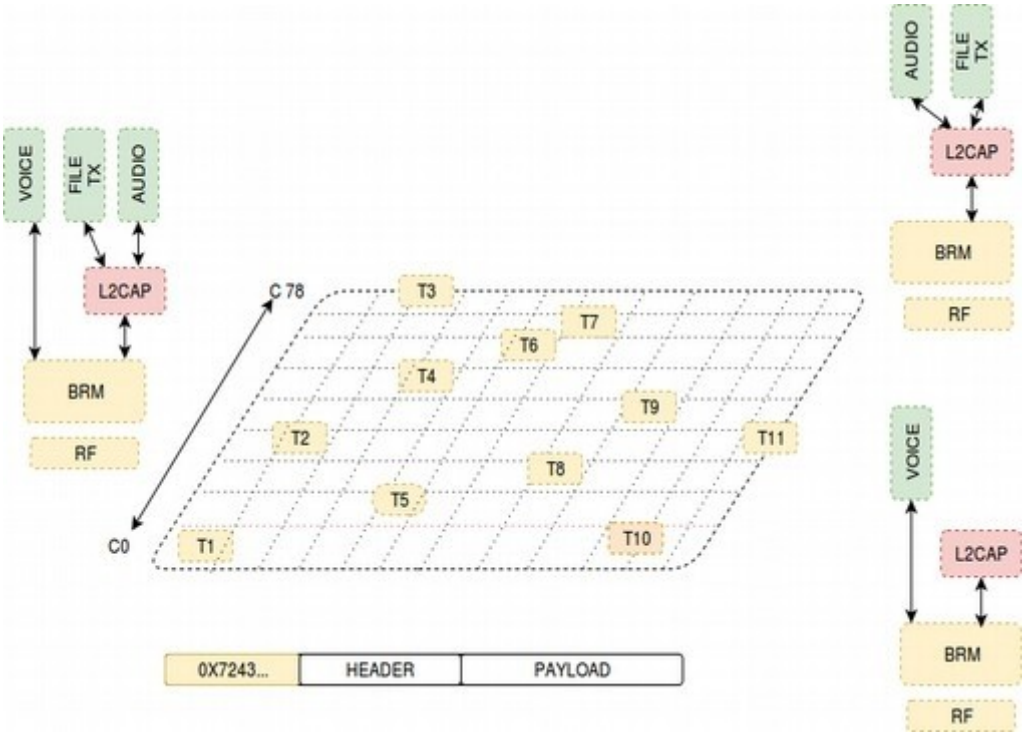
3.2 Physical Channel:

Physical Channel *is characterized by pseudo-random RF channel hopping sequence, time slot for packet transmission and access code.*

Two devices wishing to communicate must be present in the same physical channel and their transceivers must be tuned to the same radio frequency matching the phase.

All packets transmitted between the master and slaves include the **channel access code**. This is used to identify communications on a particular physical channel, and to exclude or ignore packets on a different physical channel that happens to be using the same RF carrier in physical proximity. Channel access code is always present in the packets transmitted in a piconet and is a property of the physical channel.

A device is said to be part of a piconet when it is connected to the physical channel of the piconet. When the device is synchronized to the timing, frequency and the access code, it is said to be **connected** to the physical channel which is unique to the piconet.



There are 5 types of Physical channels defined,

3.2.1 Basic Piconet Physical Channel:

Basic Piconet Physical Channel is used during communication between Bluetooth devices in a piconet. Master and its slave devices will be hopping through 79 RF channels, phase of hopping is according to the master's clock and the access code is derived from the BD_ADDR of the master. All the devices participating in the piconet are time and hop synchronized to the physical channel.

3.2.2 Adapted Piconet Physical Channel:

Adapted Piconet Physical Channel can also be used during communication but differs from basic piconet channel in 2 ways a.) Slave transmits in the same frequency in which the master addressed it, in the preceding even slot. b.) Adapted piconet may be based on less than 79 RF channels, where at least 20 RF channels are to be present according to the specification.

Adapted Piconet Physical Channel was developed with an objective of providing reliable communication during co-existence of non-hopping SRW technologies occupying the same 2.4 GHz ISM band.

3.2.3 Page Scan Physical Channel:

Page Scan Physical Channel is used during connection establishment using subset 32 Wakeup frequencies or RF channels. Here aspiring master and aspiring slave do not hop at the same rate.

Paging device (Aspiring master) hops to new pseudo-random frequency (of 32 wakeup frequencies with period 32) for every 312.5 microseconds but Page Scan device (Aspiring slave) will stay in the same frequency for 1.28 seconds (2048 timeslots) for increasing the chances of connection establishment.

Access code which is the property of Page Scan Physical Channel is called **Device Access Code** and is derived from the BD_ADDR of page scanning device (aspiring slave). This is so because, only particular Bluetooth device has to respond to connection establishment packets and this makes other devices to reduce overhead of analysing packet and payload headers not addressed to them.

3.2.4 Inquiry Scan Physical Channel:

Inquiry Scan Physical Channel is used during device discovery using subset 32 Wakeup frequencies or RF channels (Out of 79 RF frequencies). Here aspiring master and aspiring slave do not hop at the same rate.

Inquiring device (Aspiring master) hops to new pseudo-random frequency (of 32 wakeup frequencies with period 32) for every 312.5 microseconds but Inquiry Scanning device (Aspiring slave) will stay in the same frequency for 1.28 seconds (2048 timeslots) for increasing the chances of device discovery.

Access code which is the property of Inquiry Scan Physical Channel is called **Inquiry Access Code** and uses Generic Inquiry Access Code (GIAC) (0x9E8B33) for general inquiries. This is so because enquiry procedure is a broadcast message which is received and responded by all the devices which are in enquiry scan state (the state in discoverable mode).

3.2.5 Synchronization Scan Physical Channel:

Synchronization Scan Physical Channel is used by the devices to obtain timing and frequency information about Connection-less Slave Broadcast physical link and/or to recover piconet clock.

Physical Channel	Access Code Used	Derived From
Basic Piconet Physical Channel	Channel Access Code	Master's BD_ADDR
Adapted Piconet Physical Channel	Channel Access Code	Master's BD_ADDR
Page Scan Physical Channel	Device Access Code	Aspiring Slave's BD_ADDR
Inquiry Scan Physical Channel	Inquiry Access Code (Generic)	GIAC (0x9E8B33)

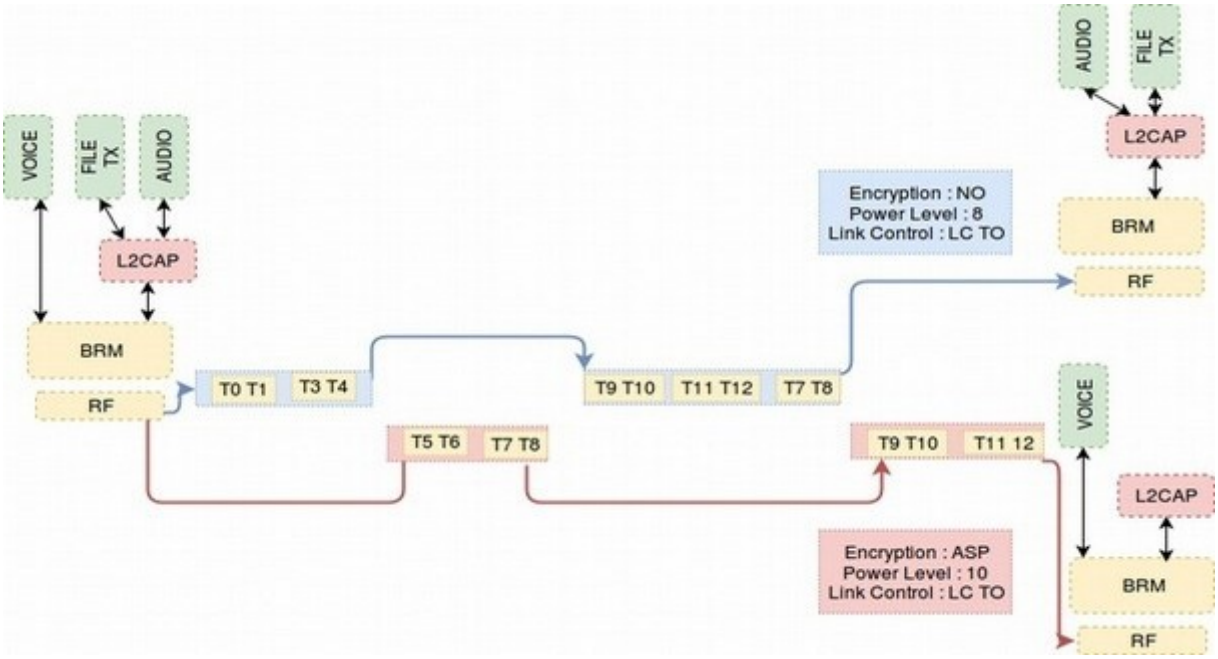
3.3 Physical Link:

Physical Link *describes the common attributes of transmission of all the logical transports at the link level on a physical channel.*

Physical Link *can also be looked as, time slots describing baseband connection between master and a particular slave in a piconet confirming to the attributes of link control, power control, encryption and many others, where time slots are dynamically allocated for ACL logical transport and statically allocated for SCO and eSCO.*

A Physical link is always associated with the single physical channel and supports the common features of all the logical transports that are multiplexed over it.

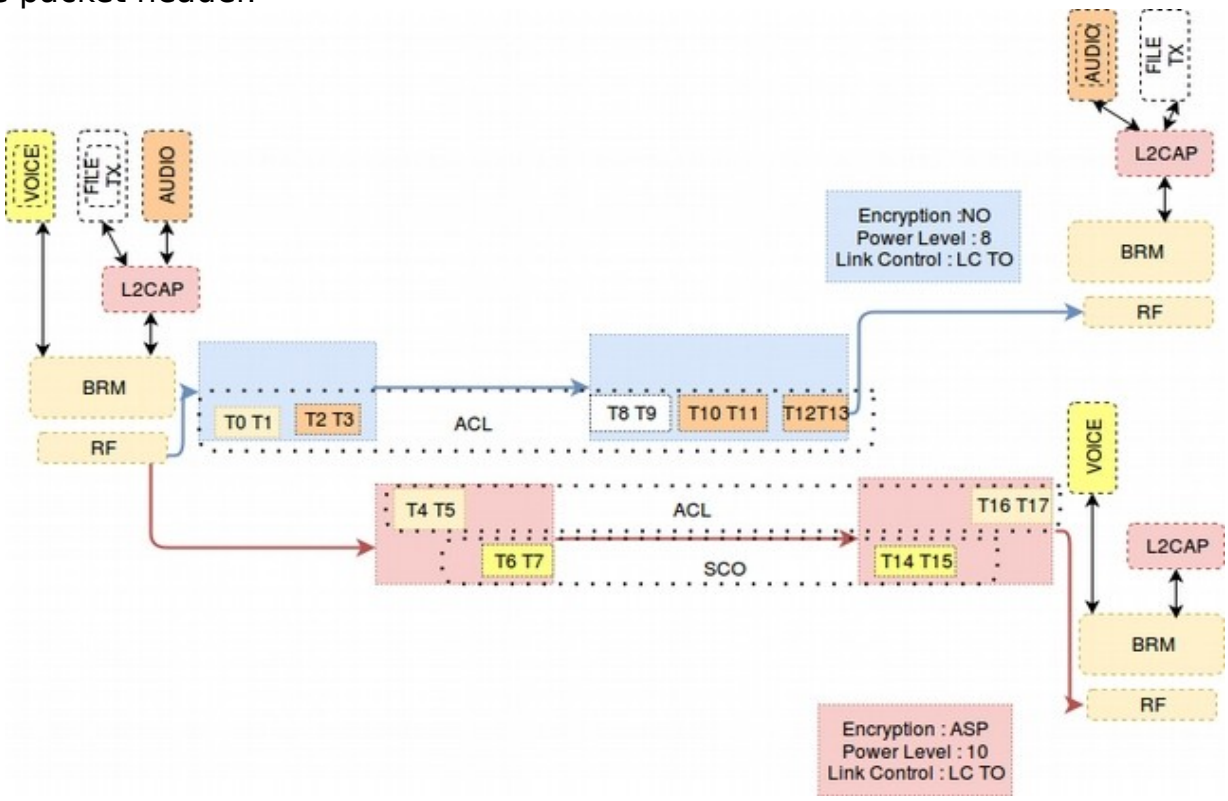
Some Physical links have modifiable properties such as transmit power for the link, while others have no modifiable properties. Link manager updates the properties of physical links.



3.4 Logical Transports:

Logical Transports *defines the communication semantics.*

Logical Transports can exist between a master and a particular slave in a piconet (connection oriented) or between master and all the slaves in the piconet (connection-less). Logical Transports are identified by **LT_ADDR** field in the packet header.



3.4.1 If Logical Transport is **Synchronous Connection Oriented (SCO)**, pre-determined time slots are to be allocated by baseband resource manager to SCO logical link, where there is no retransmission of error-prone or unreached packets.

This logical transport exist between the master and a particular slave in the piconet. SCO logical transport shares LT_ADDR of the default ACL logical transport.

3.4.2 If Logical Transport is **extended Synchronous Connection Oriented (e-SCO)**, pre-determined time slots are to be allocated by baseband resource manager to eSCO logical link, with an added benefit of retransmission of error-prone or unreached packets.

This logical transport exist between the master and a particular slave in the piconet. eSCO logical transport gets a new LT_ADDR.

3.4.3 If Logical Transport is **Asynchronous Connection Oriented (ACL)**, time slots are dynamically allocated to ACL-C and ACL-U logical links by the baseband resource manager (in which SCO and eSCO logical transports are not scheduled). Re-transmission of error-prone or unreached packets is present.

This logical transport exist between the master and a particular slave. LT_ADDR of default ACL logical transport is called as **primary LT_ADDR** and has to be shared with SCO logical transport (if exists).

3.4.4 If Logical Transport is **Active Slave Broadcast (ASB),** time slots are dynamically allocated for LMP control signalling and connectionless L2CAP user data to all the slaves in the piconet. There is no response or re-transmission of packets, to increase reliability the same data packets are transmitted multiple times.

This logical transport exist between the master and all the slaves in the piconet. Since ASB logical transport is for broadcasting, LT_ADDR for ASB is 0 (and is called **reserved LT_ADDR**).

3.4.5 If Logical Transport is **Connectionless 'Slave Broadcast' (CSB)**, time slots are fixed and periodic for profile broadcast data and the messages are received by all configured connectionless broadcast slaves. There is no response or re-transmission of packets, to increase reliability the same data packets are transmitted multiple times.

This logical transport exist between master and 'connection-less broadcast configured' slaves. There is unique LT_ADDR given by master to identify the CSB transport. This unique LT_ADDR is shared between master and

all CSB configured slaves. CSB logical transport can only exist on Adaptive Piconet physical channel.

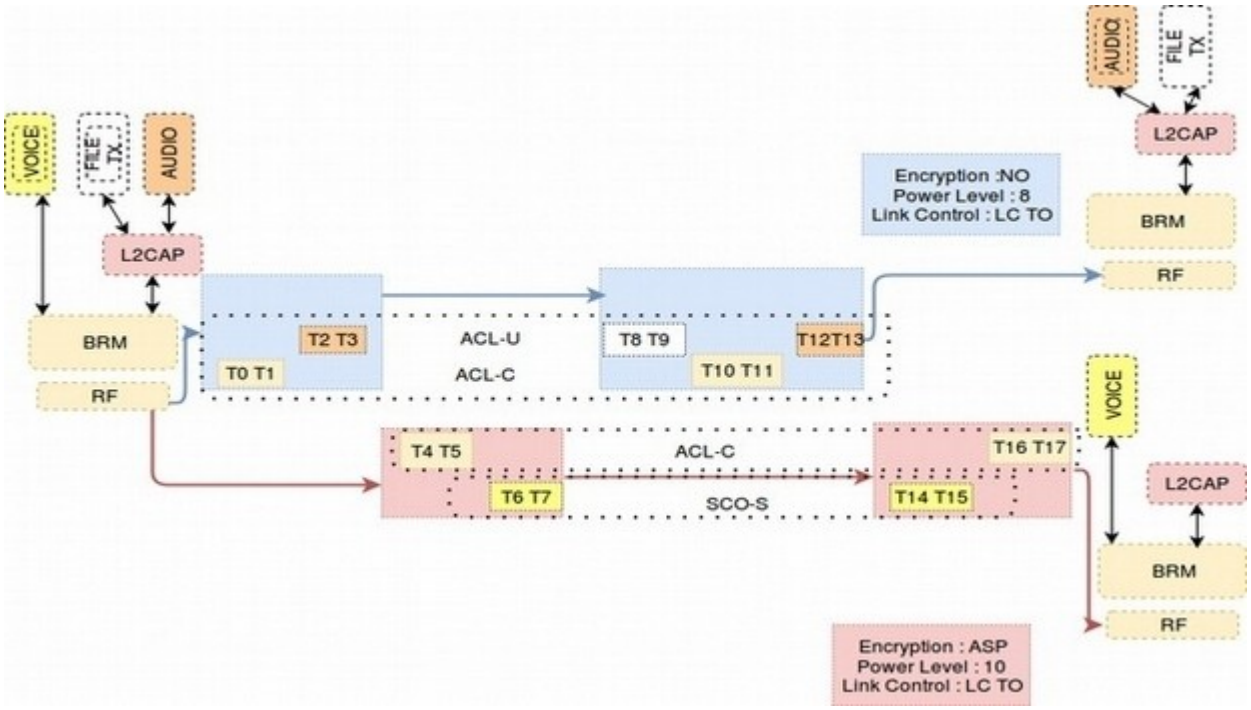
3.5 Logical Links:

Logical Links *define the type of data that is being transceived.*

SCO logical transport supports (User Synchronous Data) **SCO-S logical link**, which carries isochronous unframed user data. Data is delivered in constant sized units at a constant rate.

e-SCO logical transport supports (User Extended Synchronous Data) **e-SCO logical link,** which carries isochronous unframed user data. Data is delivered in constant sized units at a constant rate.

CSB logical transport supports (Profile Broadcast Data) **PBD logical link** which is used to broadcast isochronous unframed data to multiple receivers. Profile directly talks to HCI to transfer unframed profile data skipping L2CAP layer.



ACL logical transport supports **ACL-C and ACL-U logical links**, where ACL-C logical link carries LMP signalling messages and ACL-U logical link carries L2CAP user data and L2CAP signalling messages. Variable rate isochronous data also has to be transported using ACL logical transport.

ASB logical transport supports **ASB-C** and **ASB-U** logical links, where ASB-C logical link carries LMP signalling and ASB-U logical link carries L2CAP user data and L2CAP signalling messages. It's important to note that a subset of LMP signalling and only L2CAP connectionless user traffic can be sent over ASB logical transport.

Note: Since both SCO and ACL share the same LT_ADDR, default ACL logical transport can be identified with the combination of **LT_ADDR** field and Packet **TYPE** field in the packet header.

ACL-C and **ACL-U** logical links in ACL logical transport are identified using **LLID** (Logical Link ID) field in the payload header. Similarly, **ASB-C** and **ASB-U** logical links in ASB logical transport are identified using LLID field in the payload header. **PBD** logical link of CSB logical transport, which is only used for broadcast of profile data, will contain LLID of 10 in payload header, where CSB logical transport having own LT_ADDR.

There is no LLID field in the SCO and eSCO packets because these logical transports support single logical links.

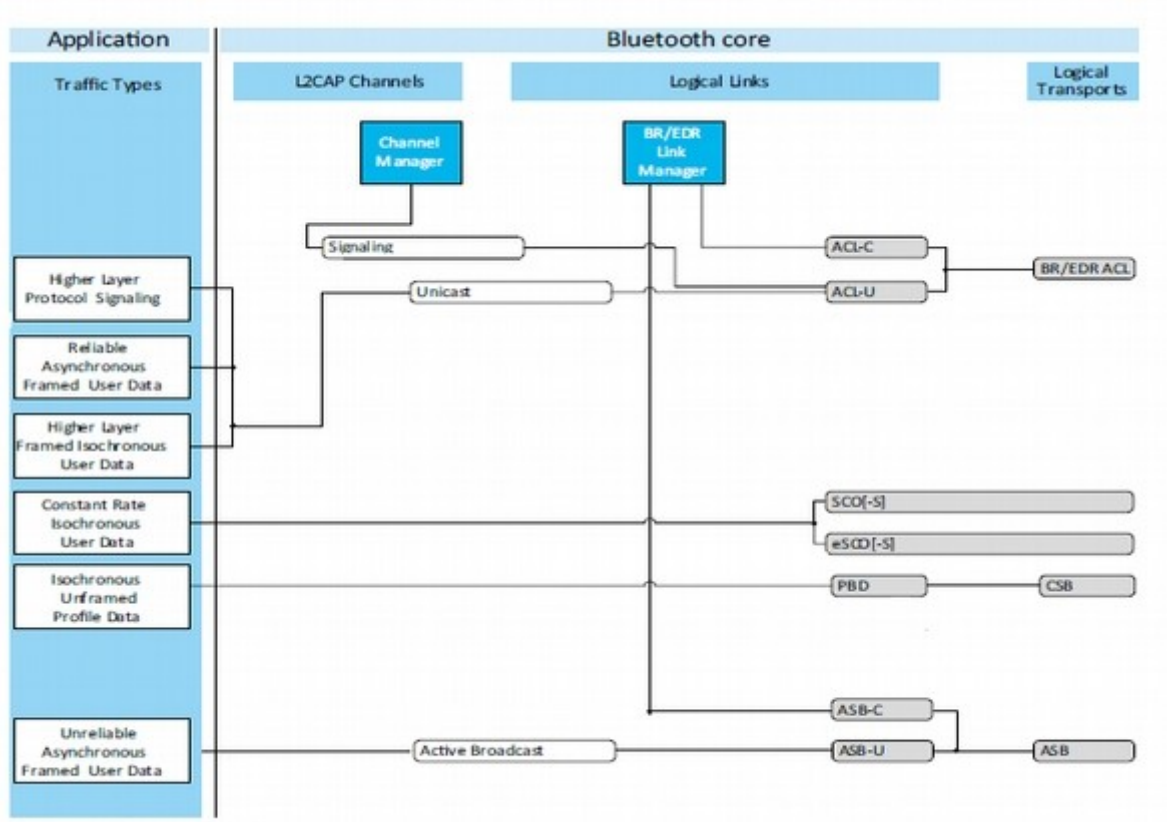


Figure 3.2: Bluetooth traffic bearers

3.6 Analogy of Traffic Bearers with Vehicular Transport on a High-Way

For a better understanding, Bluetooth Traffic bearers (Physical Transports, Physical Channels, Physical Links, Logical Transports, and Logical Links) can be compared with vehicular transport on a high-way.

Physical Transport can be thought as lanes on a highway.
If there are 6 lanes on a highway that can be mapped to 6 Physical Transports.

Physical Channel can be thought as shifting between these physical lanes, staying in each lane for a particular time period and type of vehicle permitted. Random shifting between these lanes is pseudo-random hopping through frequency channels. Time of stay in each lane is time period and permitted vehicle type is the access code.

Physical Link can be thought as attributes referring to the transport on physical channel. E.x: Speed Limit, Right hand driving, diesel/petrol engine etc.. In the same way, attributes of power control, link control, encryption defines physical link.
Logical Transport can be thought of as vehicles transporting on physical channel like Bus, Car, Bike, etc...

If it is a Bike with a rider, travelling between the house and the office every day in the morning and in the evening. This can be thought of SCO, between master and a particular slave, having fixed intervals for communication.

If it is a Bus, it at least has a Driver and a Conductor and will be travelling many times randomly according to the need. This can be thought of ACL, between master and a particular slave, and offers service at random time i.e. random time slots.

Logical Link can be thought of as passengers in a vehicle.

Generally in Bike, it’s a single rider. So SCO logical transport has just single logical link called as SCO-S.

In Bus, there at least has to be a driver who is needed for sure and the same can be attributed to ACL-C logical link. On explicit demand from the passengers, there is need for conductor who offers service to them and this can be attributed to ACL-U logical link.

L2CAP channels can be thought of as passengers other than driver and conductor in bus.

So, these passengers other than driver and conductor who demands ticket for their journey in the Bus can be mapped to L2CAP channels and tickets can be mapped to channel Ids.

4. Bluetooth peer-to-peer Interaction:

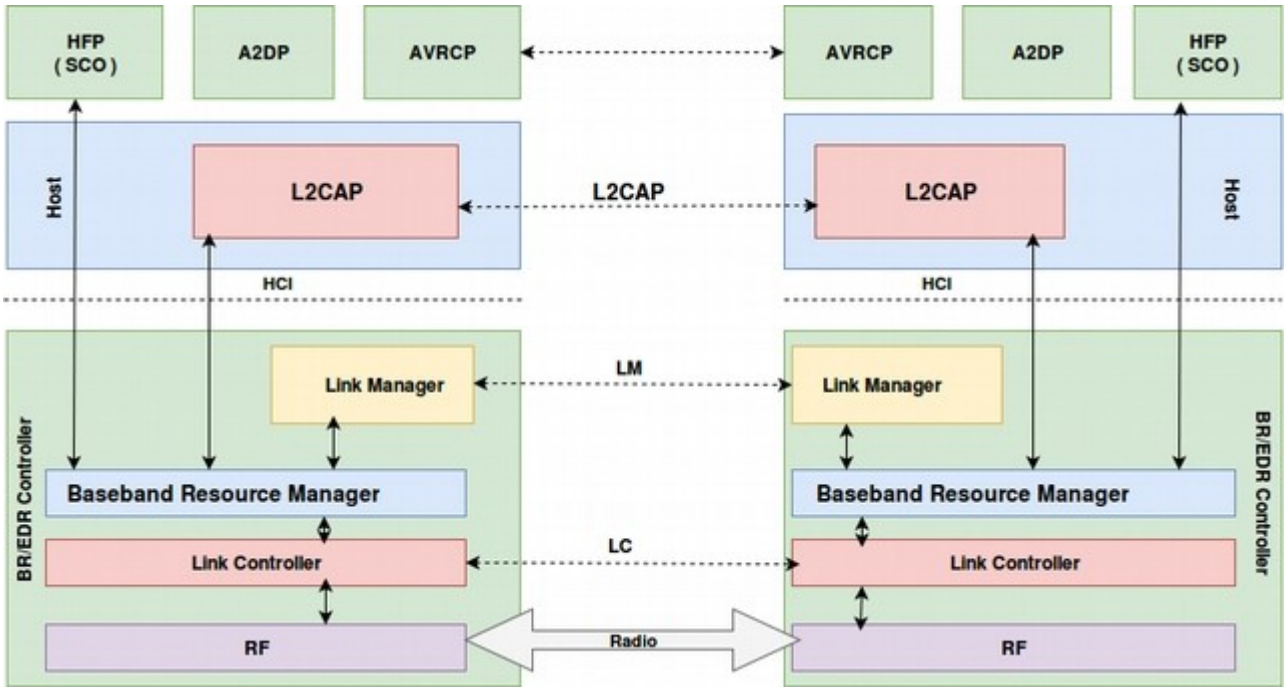


Fig : Peer to peer interaction between two Bluetooth devices

At the RF layer, communication is direct: devices use G-FHSS modulation scheme where frequency deviation (positive or negative frequency deviation) is used to represent either zero or one respectively (the form in which information is represented). There is no intermediate node between a master device and a slave device to communicate in a piconet.

At the higher layers, however, communication must move down through the layers of one device, over to the device B, and back up through the layers. In many implementations at link controller, packet composer composes the packet in the form that can be transmitted to the receiving device. Packet header analyser and payload header analyser at the link controller, unwraps the packets and signals Baseband Resource Manager to route the packet internally to appropriate higher layer (either Link Manager or L2CAP in the host or directly to application based on the packet header and payload header fields).

A packet is 'not ignored' by the Link controller only if the access code in the packet matches with the context of physical channel used .i.e. Inquiry Access Code for Inquiry procedure, Device Access Code for Connection

establishment and Channel Access Code(particular to the specific piconet) for Communication over the piconet. If anything other than the expected access code is present or on analysis, header bit fields not sinking with HEC code, the packet is rejected.

Accepted packet is analysed by Link controller's packet analyser for LT_ADDR field, the content has to be either 1.) The reserved LT_ADDR (i.e. 0) or 2.) LT_ADDRs communicated previously in the FHS packet of the master during connection establishment or 3.) LT_ADDR of e-SCO or CSB logical transports explicitly created on demand from application. Logical Transport is identified by the combination of LT_ADDR and TYPE (of packet) field of the packet header.

LT_ADDR field of Packet Header	**TYPE field of Packet Header**	**Logical Transport**
Reserved LT_ADDR (0)	-	ASB
Default LT_ADDR	Of ACL packet Type	ACL
	Of SCO packet Type	SCO
LT_ADDR assigned to e-SCO	-	e-SCO
LT_ADDR assigned to CSB	-	CSB

Payload analyser of Link Controller analyses packets of the ACL, ASB and CSB logical transports identified by packet analyser. It analyses for logical links according to the LLID field in the payload header. CSB logical transport will always have 10 (Profile Broadcast Data – PBD logical link) in LLID field. ACL and ASB logical transports carry both LMP signalling and L2CAP signalling and user data and hence for these logical transports have to be distinguished by LLID filed in payload header so that Baseband Resource Manager routes packet appropriately to either LM layer or L2CAP of the host.

Logical Transport **(determined from LT_ADDR:TYPE of packet header)**	**LLID field of payload header**	**Logical Link**	**Functional Unit**
ACL	To LM of Controller	ACL -C	LM
	To L2CAP of Host	ACL -U	L2CAP
ASB	To LM of Controller	ASB -C	LM
	To L2CAP of Host	ASB -U	L2CAP
CSB	Always to profile through L2CAP	PBD	Profile (Through L2CAP)

4.1 Session based visualization of logical transports:

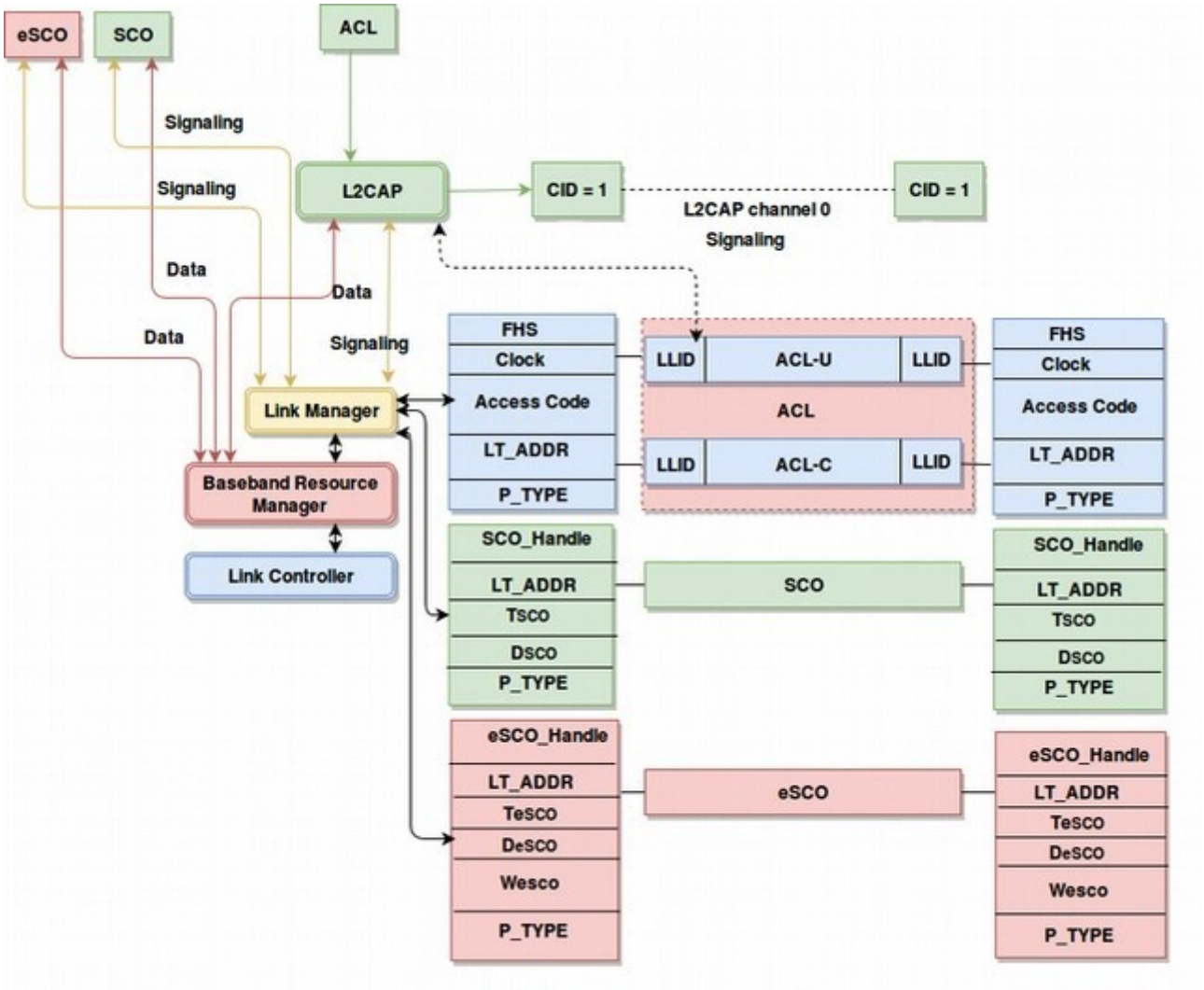


Fig: Session based visualization of Logical Transports

Communication happening between master and slaves in a piconet can be 'connection-oriented' or 'connection-less'.

The communication can be called as connection-oriented only if a dedicated session is created at both the ends for communication. Dedicated session is created only when negotiation happens between the master and the salve for its (session's) creation and the set of parameters that identify the dedicated session belongs to that of both the master and the particular slave.

The communication can be called as connection-less when there is no creation of dedicated session between master and the particular slave (as parameters that identify the session for transaction will only be that of masters own or slave's own and not of the both).

Hence ACL, SCO, e-SCO are connection oriented logical transports where dedicated session for transaction is created at both master and slave while ASB and CSB are connection-less logical transports having session for transaction but the parameters do not uniquely identify the session and hence never is 'dedicated'.

Creation of session for default ACL logical transport:

During Connection establishment procedure, when master sends FHS packet contain LT_ADDR as one of its field, an ACL logical transport session is created at both the aspiring master and paged device (aspiring slave). ACL session at both the ends is identified by Frequency Hopping Sequence (FHS), clock of the master, channel access code, primary LT_ADDR and packet type.

The same instance when default ACL logical transport is created, ACL-C logical link as a sub session within the ACL logical transport session exist. Through this ACL-C logical link sub-session LM talks with its counterpart in the other Bluetooth device to negotiate for creation of ACL-U logical link sub-session. When both LMs exchange LMP_setup_complete PDU, session for ACL-U logical link is established. LLID field identifies the sub-session of ACL-U or ACL-C in default ACL session.

Creation of session for SCO, e-SCO logical transports:

On demand from the application, link manager of either the master or the slave device sends LMP_SCO_link_req. On reception of LMP_accepted by LM of the other device, session for transaction for SCO logical transport is created at both end devices, which shares the LT_ADDR of default ACL logical transport and is uniquely identified by SCO handle, Tsco, Dsco fields and packet type.

The same is the case with creation of e-SCO logical transport session, where either the master or the slave device sends LMP_eSCO_link_req and on receiption of LMP-accepted by LM of the other device, session for transaction

for e-SCO logical transport is created at both end devices. E-SCO logical transport is uniquely identified with eSCO handle, eSCO LT_ADDR, De-sco, Te-sco, We-sco and packet type {M to S and S to M}.

Creation of session for ASB logical transport:

After the procedure of connection-establishment (i.e. creation of session for ACL logical transport with both ACL-C and ACL-U sub-sessions) a session, by default is created for ASB logical transport at master and slave side having LT_ADDR 0. Since creation of ASB logical transport session happens without LMP signalling, it cannot be considered as dedicated session (no negotiation). Any slave active in the piconet can receive the packet sent with LT_ADDR as 0, since a session for ASB is present in all Bluetooth devices participating in the piconet.

Creation of session for CSB logical transport:

Session for CSB logical transport is created by the master's (sender's) LM on demand from the host and session for CSB logical transport is created by the slave (receiver) whenever configured for reception of Profile Broadcast Data. Session for CSB logical transport is uniquely identified with CSB LT_ADDR assigned by master's LM, but there is no LMP PDU to negotiate between master and the slave in the piconet for the creation of CSB logical transport at the slave end and hence there is a different mechanism involved.

Synchronization scan physical channel is used for this purpose. Master shall enter into **synchronization train sub-state** to transmit synchronization train packets, (uses a subset of RF channels). Slave shall enter **synchronization scan sub-state** and wait in a single frequency to receive synchronization train packets. This operation happens only on synchronization scan physical channel.

The contents of synchronization train packet broadcasted by master is *CSB LT_ADDR, CSB interval, CLK of master, AFH channel map, and master BD_ADDR.* The packet type of this synchronization train packet is basic rate ACL DM3 packet with LT_ADDR as 0, as it is to be received by any slave willing to establish CSB logical transport. Access code is derived from BD_ADDR of master and the packet is transmitted on synchronization scan physical channel.

Session for CSB logical transport is created by master when host demands controller to send Profile Broadcast Data and hence CSB logical transport is created by Master's LM and enters into synchronization train sub-state. Slave has to be configured to receive Profile Broadcast Data and may periodically enter into synchronization scan sub-state to receive train packets to create session for CSB. On reception of train packet, slave creates a session for CSB and goes back to its previous state. The session created in slaves will all bare the same CSB LT_ADDR and is not dedicated for a master – particular

slave transaction.

CSB can exist in a slave even without necessarily having default ACL logical transport and hence it's an advantage to have theoretically limit-less slaves waiting for profile broadcast data which will be sent by master periodically. The period (CSB interval) is communicated in synchronization train packet so that configured CSB slaves can wakeup only during those intervals to listen for the packets from the master.

5. Bluetooth Device Discovery and Connection Establishment

Discovering Bluetooth device in special range and undergoing connection establishment procedure in Bluetooth wireless technology is equivalent to plugging Ethernet cable into NIC cards of 2 hosts while communication using TCP/IP stack.

The procedure of Device Discovery and Connection Establishment is described in the following sections,

5.1 Bluetooth Inquiry Procedure:

On demand from application, the device enters into inquiry state. The device entering into inquiry state is known as inquiring device (or also called as aspiring master). * Other possibilities of Bluetooth device entering into inquiry state are not considered *

Every device gets into inquiry scan state periodically (configurable), and will be momentarily called as inquiry scanning device (or also called as aspiring slave) for the duration of inquiry scan window.

The procedure of Inquiry happens over Inquiry Scan physical channel. * Refer to the properties of page scan physical channel *

When Bluetooth is turned ON, the device is said to be in its native state and this native state is called **STANDBY** state, the device's controller can get into **inquiry state** to inquiry for Bluetooth devices around it, on demand from application, but any device has to get into **inquiry scan state** periodically once in every 1.28 seconds and remain in that state for at least 10ms. This 10ms of duration in which the device enters to scan for the inquiry requests is called **scan window**. After completion of scan window time interval, the device gets back to its original state – either standby or connection state.

For faster inquiry, a subset of 79 frequency bands i.e. only 32 equispaced frequency bands (with a period of 32) are used and these are called as **wake-up frequencies**. These 32 wake-up frequencies are again divided into 2 trains of 16 frequencies each, **Train A** (16 frequency band subset) and **Train B** (16 frequency band subset)**.**

Packets used for Inquiry are:

ID packet	Inquiring Device to Inquiry Scanning Device (Aspiring Master to Aspiring Slave)	Contain Generic Device Access Code (0x9E8B33) for general inquiry.
FHS packet	Inquiry Scanning device to Inquiring Device (Aspiring Slave to Aspiring Master)	Contain BD_ADDR and CLK_{27-2} of inquiry scanning device.

Procedure of Inquiry:

Aspiring master will send the ID packets in two different wake-up frequencies {f (k), f (k+1)} for 312.5 µsecs each in TX slots (of 625 µsecs). ID packet contains the **Generic Inquiry Access Code** (GIAC) 0x9E8B33. Master device tunes back to the same frequency set {f (k), f (k+1)} and waits for the response in RX slot of 625 µsecs (312.5 µsecs in f1 and 312.5 µsec in f2).

Hence, aspiring master tunes to new frequency, every 312.5 µsecs but aspiring slave remains in one frequency for 1.28 sec (2048 slots).

If an aspiring slave is tuned to the same frequency as that of the aspiring master, the aspiring slave will receive the ID packet. In response to the ID packet, aspiring slave has to send FHS packet after 625 µsecs, but since ID packet was not addressed to a particular slave and is a broadcast, any Bluetooth device on reception of ID packet for inquiry, generates a random number 'b' from the closed interval [0, 1023] and suspends the inquiry process for a duration of 'b' slots. This process is introduced to avoid collision of responses in the case when more than one devices are listening on the same frequency. Once the timeout generated has expired, the device re-enters the inquiry scan mode and responds to the ID packet. The response packet is a so-called FHS packet containing the Bluetooth device address and clock values of the responding Bluetooth device.

ID packets are transmitted twice in each TX slot in two hopping frequencies (one at the beginning and one at the middle of TX slot). Aspiring master takes 8 TX slots to transmit whole Train of 16 frequencies. Because TX and RX slots are interleaved a total length of time to cover each train is 16 slots (8 TX slots, 8 RX slots).

Total time taken by the Train A to cover 16 slots = 16 * 625 µsec = 10 msec.

The inquiry happens 256 times for each train. For error free response collection, at least four Trains must be used. Hence total time taken for Inquiry = 4 Trains * 256 times * 10 music = 10.24 sec.

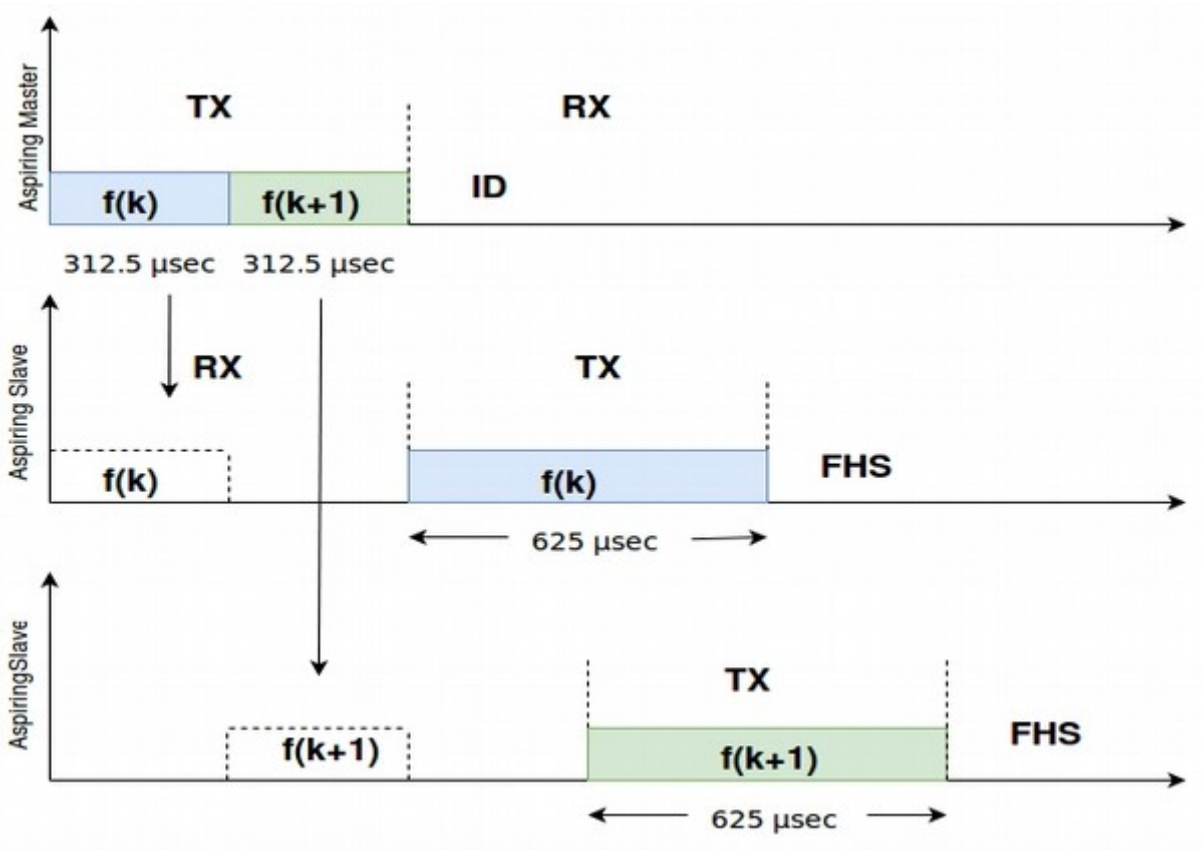


Fig: Packet transaction for inquiry procedure

5.2 Inquiry Procedure State Diagram:

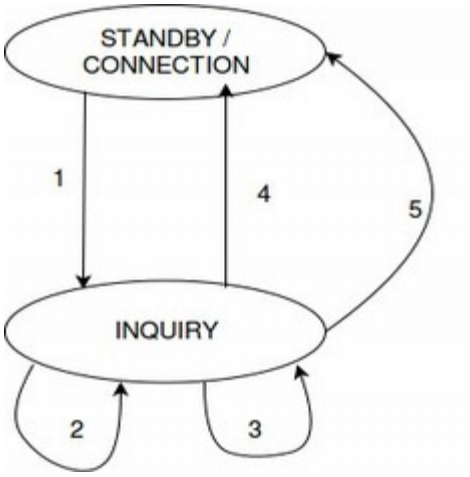


Fig a: Inquiring Device

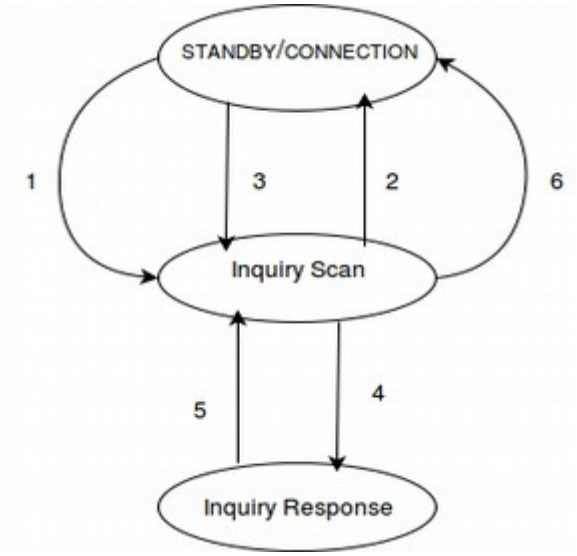


Fig b: Inquiry Scanning Device

5.2.1 Inquiring Device:

#a.1: Baseband Resource Manager enters into inquiry state when device manager asks to, on demand from application.
InquiryTO is turned ON.

#a.2: Aspiring Master sends ID packets in 2 different frequencies {f (k), f (k+1)} for 312.5 µsecs each in one TX time slot.

#a.3: Aspiring master expects for an FHS packet from the discoverable devices in the same 2 frequencies {f (k), f (k +1)} in the succeeding RX time slot. Baseband layer informs device manager on reception of FHS packet.

#a.4: Baseband Resource Manager returns to its previous state (STANDBY/ CONNECTION) when asked by device manager.

#a.5: Baseband Resource Manager returns to its previous state on timeout of InquiryTO.

5.2.2 Inquiry Scanning Device:

#b.1: Periodically Baseband Resource Manager enters into Inquiry Scan State when Device manager asks so for every 1.28sec and stays in Inquiry Scan State for 10 msec.

Device Link Controller in order to compose the packets, starts inqrespTO timer and initializes the flag BackoffTime to False.

#b.2: If ID packet is received and BackoffTime is false irRAND timer is started (Duration is 0 to 1023 slots) and moves to the original state.

#b.3: The device is allowed to spend irRAND timeslot in its STANDBY / CONNECTION state. Upon expiry of the irRAND timer the device moves to the Inquiry Scan state.

#b.4: After the Backoff period but before the expiry of inqrespTO timer if the device receives a second ID packet in the Inquiry Scan state, it starts another one slot timer we call oneslotTO. After the expiry of the oneslotTO it moves to the Inquiry Response State.

#b.5: After waiting for oneslotTO timer it transmits an FHS packet, reinitialize BackoffDone flag to false and moves to Inquiry Response State.

#b.6: After inqrespTO timer expires the device moves from Inquiry Scan state to its original STANDBY / CONNECTION state.

5.3 Connection Establishment Procedure:

On demand from application, the device enters into paging state. The device entering into paging state is known as paging device (or also called as aspiring master). *Other possibilities of Bluetooth device entering into paging state are not considered*

Every device gets into page scan state periodically (configurable), and will be momentarily called as page scanning device (or also called as aspiring slave) for the duration of page scan window.

The procedure of connection establishment happens over page scan physical channel. *Refer to the properties of page scan physical channel *

The device's controller can get into **paging state** to establish connection with a particular Bluetooth device, on demand from application. On the other hand, any device has to get into **page scan state** periodically according to the mode:

R0: the device listens continuously for a master paging it.
R1: the device listens at least every 1.28 seconds (2048 slots).
R2: the device listens at least every 2.56 seconds (4096 slots).

Ideally, we will take the case of R1 mode where for every 1.28 seconds the device enters into page scan state. This 10ms of duration in which the device enters to scan for the paging requests is called **scan window**. After completion of scan window time interval, the device gets back to its original state – either standby or connection state.

For faster inquiry, a subset of 79 frequency bands i.e. only 32 equi-spaced frequency bands (with a period of 32) are used and these are called as **wake-up frequencies**. These 32 wake-up frequencies are again divided into 2 trains of 16 frequencies each, **Train A** (16 frequency band subset) and **Train B** (16 frequency band subset)**.**

*The term paging is said to be derived from pager. **Pager** is a small radio device, which emits a series of bleeps or vibrates to inform the wearer that someone wishes to contact them or that it has received a short text message. Since the device which needs to establish connection with the other device will request the other device the name paging is given for connection establishment.*

Packets used for Paging are:

ID packet	Paging Device to Page Scanning Device (Aspiring Master to Aspiring Slave)	Contains Device Access Code (DAC) of the particular Slave
ID packet	Page Scanning device to Paging Device (Aspiring Slave to Aspiring Master)	Contains Device Access Code (DAC) of itself (as an ACK for ID packet).
FHS packet	Paging Device to Page Scanning Device (Aspiring Master to Aspiring Slave)	Contain BD_ADDR, Class of Device, and CLK_{27-2} of paging device (Master). Also contain LT_ADDR, which is taken as primary LT_ADDR by the slave for default ACL logical transport.
ID packet	Page Scanning device to Paging Device (Aspiring Slave to Aspiring Master)	Contains Device Access Code (DAC) of itself (as an ACK for FHS packet).

Connection Establishment Procedure:

Aspiring master sends ID packets in two different wake-up frequencies {f (k), f (k+1)} for 312.5 µsecs each in TX slots (of 625 µsecs). ID packet contains Device Access Code (**DAC**) of a particular slave. Master device tunes back to the same frequency set {f (k), f (k+1)} and waits for the response in RX slot of 625 µsecs (312.5 µsecs in f1 and 312.5 µsec in f2).

Note: ID packets are also sent in frequencies which are generated by calculating frequency hopping sequence and 'estimating' phase of aspiring slave from the BD_ADDR and Clock of the aspiring slave communicated in FHS packet during inquiry procedure previously performed, for faster connection establishment.

Hence, aspiring master tunes to new frequency, every 312.5 µsecs but aspiring slave remains in one frequency for 1.28 sec (2048 slots).

If an aspiring slave is tuned to the same frequency as that of the aspiring master, the aspiring slave will receive the ID packet. In response to the ID packet, aspiring slave sends ID packet containing access code derived from BD_ADDR of its own -as an acknowledgement, 625 µsecs after receiving ID packet from the aspiring master. The response ID packet acts as an ACK from the particular slave because both access codes remain the same.

While sending ID packet as an ACK, aspiring slave freezes the clock (CLKN) at the value it had at the time when the page message was received (So no hopping to next frequency) and waits for FHS packet from the aspiring master.

'Master' on receiving ID packet from the 'slave', freezes the clock(CLKN) to the value it had at the time when master received ID packet, composes FHS packet which contain master's BD_ADDR, CLK to calculate the hopping sequence and phase of hopping by the slave. FHS packet also contain LT_ADDR which is the primary LT_ADDR for default ACL logical transport.

On receiving FHS packet from the master, slave device calculates hopping sequence and updates CLKN to CLK information present in FHS packet, sends an ID packet in response to the FHS packet and de-freezes the clock.

Master device receiving ID packet, de-freezes the clock. Now both Master device and slave device are having the same hopping sequence and phase of hopping remains the same due to the updation of CLK information. The first packet transmitted by the master to the slave is the POLL packet, on default ACL logical transport for which it expects any packet packet type in response. Slave responds with NULL packet which confirms the establishment of connection between the master and the slave.

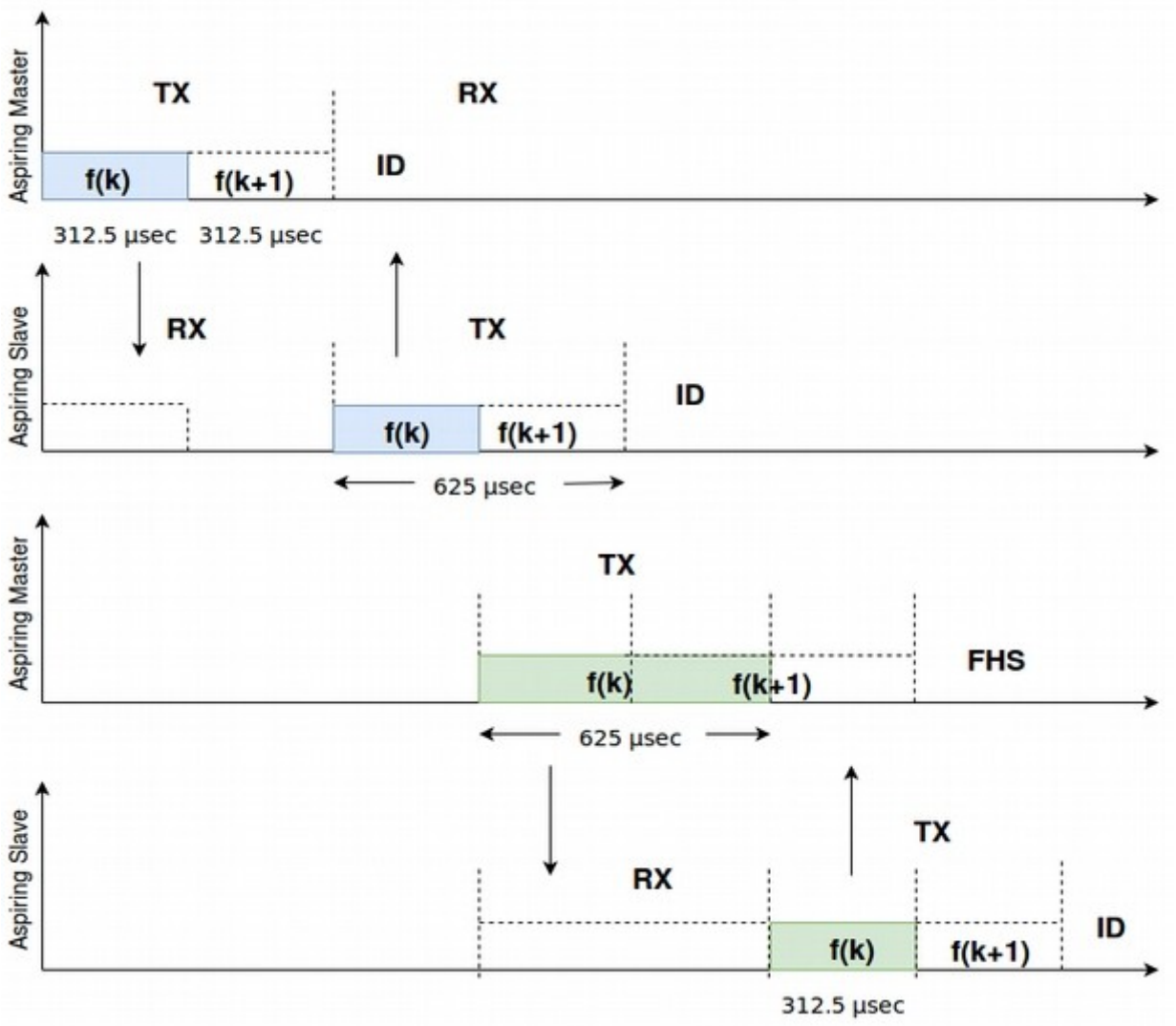


Fig: Packet transaction for paging procedure

5.4 Paging Procedure State Diagram

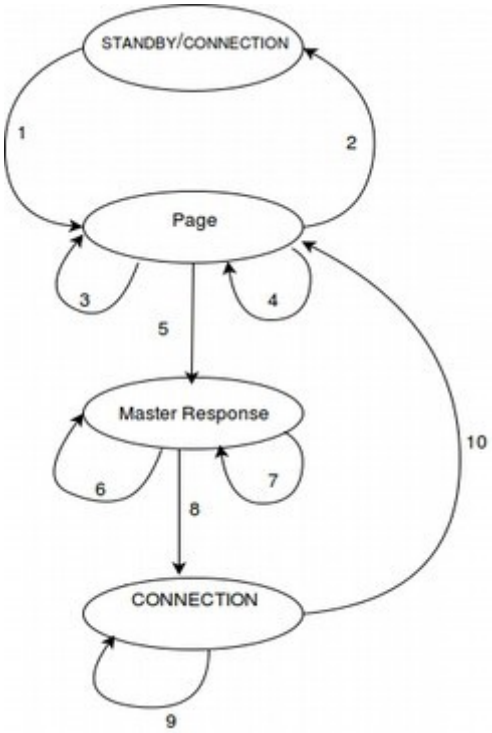


Fig c: Aspiring Master

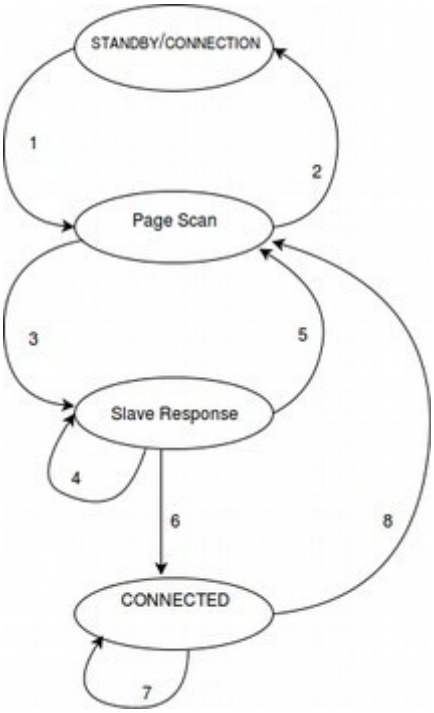


Fig d: Aspiring Slave

5.4.1 Paging Device:

#c.1: Baseband Resource Manager enters into paging state when device manager asks to, on demand from application.
PageTO is turned ON.

#c.2: In the Page state, if the aspiring master receives command from device manager or pageTO timeout occurs, the designated master moves back to it's previous to STANDBY/CONNECTION state.

#c.3: In Page state, aspiring master sends ID packets containing DAC (Device Access code) of slave in two different hop frequencies for 312.5µsec each.

#c.4: After sending ID packets, aspiring master is tuned to the same frequency and expects ID packets as an Acknowledgment from slave in same two frequencies.

#c.5: On the reception of ID packet, aspiring master enters into Master Response State and freezes the current clock input. Aspiring master sends FHS packet (After 312.5µsec of reception of ID), which contains Master's BD_ADDR, real time Bluetooth clock, BCH parity bits, class of device. FHS packet also contain primary LT_ADDR of default ACL logical transport.
PageRespTO timer is put ON.

#c.6: Aspiring master waits for ID packet containing slave's DAC as an ACK for FHS packet. If no response is received, aspiring master retransmits FHS packet with updated clock.

#c.7: If no ID packet is received for time pageregpTO , an error message is sent to Device Manager.

#c.8: If ID packet is received within pageregpTO, master shall change to using master parameters and use channel access code and master clock. Aspiring master enters into CONNECTION state and newconnectionTO is turned ON.

#c.9: Hopping sequence uses all 79 channels in pseudo random fashion and sends its first traffic packet in hop determined by new parameters. This packet is POLL packet.

#c.10: If POLL packet is not received by slave or POLL packet response is not received by designated master within newconnectionTO , the designated master and the designated slave shall return to the Page and Page Scan substates.

5.4.1 Page Scanning Device:

#d.1 : Periodically Baseband Resource Manager enters into Page Scan State when Device manager asks so for every 1.28sec (for R1 mode) and stays in Page Scan State for 10 msec.

#d.2: When the device receives command from Device manager in Page Scan state or after completion of page scan window time (in R1 and R2 modes), device moves back to STANDBY/CONNECTION state.

#d.3: On arrival of ID packet containing DAC of slave from master, slave enters into Slave Response state.

PageregpTO timer is turned ON.

Slave waits for625µsec after receiving ID packet and sends ID packet as ACK in response. Clock input CLKN shall be frozen at the value it had at the time the page message was received.

#d.4: After sending ID packet as an ACK, slave waits for arrival of FHS packet.

#d.5: Slave shall remain in #4 until the expiry of pageregpTO timer. On expiry, slave returns back to Page Scan state.

#d.6: If FHS packet is received by slave in Slave Response substate then, Slave sends ID packet in response of FHS packet.

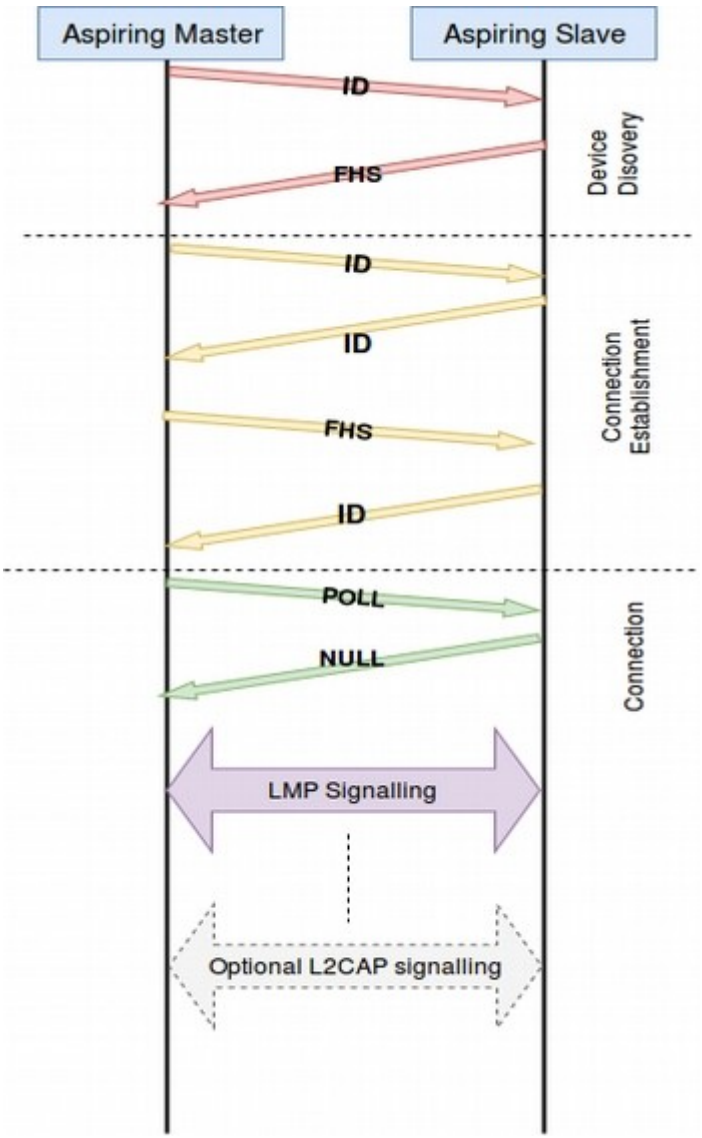
Slave changes to the master's channel access code and clock as received in

the FHS packet.

#d.7: The connection made shall start with a POLL packet transmitted by the master. Slave may respond with any type of packet within the timeout of newconnectionTO.

#d.8: If slave fails to respond with any packet in the newconnectionTO, master and slave return to Page and Page Scan substates respectively.

5.5 Sequence Chart:



6. Packet Structure:

Fig: General format of basic rate packet

The above figure represents general packet format of Basic Rate packets. Each packet consists of 3 entities: Access code, Header, and Payload.

The access code is 72 or 68 bits and the header is 54 bits. The payload ranges from zero to maximum of 2790 bits.

Any of the following packet types are valid:

The shortened access code only (Eg: ID packet)
The access code and the packet header (Eg: POLL packet)
The access code, the packet header and the payload (Eg: DM1 packet)

Access Code: It Contains *Preamble + Sync Code + (Optional) Trailer*.

Access code identifies all the packets exchanged on a physical channel i.e. all the packets sent on the same physical channel contain the same access code.

Access code is also used for frequency and phase re-synchronization of all the slaves to the master in the piconet.

Packet Header: Contains

LT_ADDR	3 bit Logical Transport Address
TYPE	4 bit packet type code
	LT_ADDR and TYPE fields in combination identify Default ACL Logical Transport, as the same LT_ADDR is shared for ACL and SCO logical transports
FLOW	1 bit flow control (Master -> Slave or Slave -> Master)
ARQN	1 bit acknowledgement indicator
SEQN	1 bit sequence number
	SEQN for ordering of received packets and ARQN for re-transmission for unreached packets
HEC	Header error check code.

Payload: Contents of Payload varies according to the logical transport used for packet transfer. In SCO and e-SCO logical transports, **payload header is absent**, but it is not the case with ACL logical transport. Since ACL logical transport contain ACL-C and ACL-U logical links, there is a need to identify LMP signalling and L2CAP PDUs which is a field of payload header.

6.1 Default ACL Logical Transport Packet Structure:

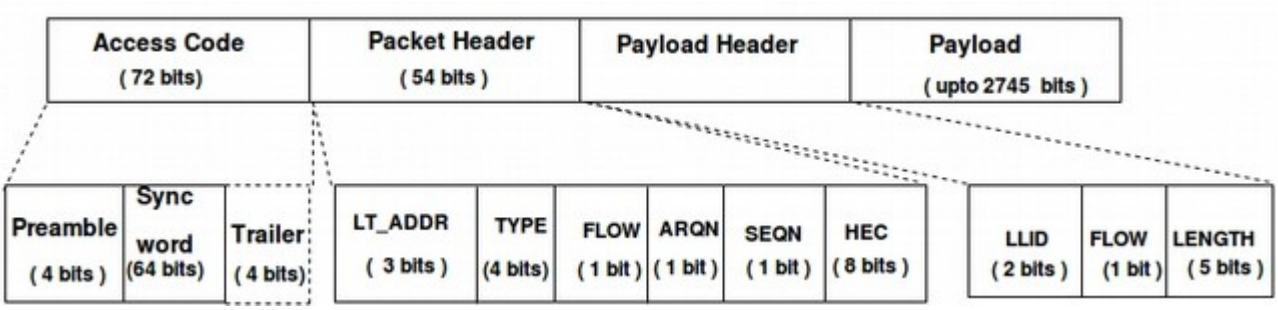


Fig: ACL logical transport packet structure (general)

The above figure represents packet structure of default ACL logical transport, which is used to carry both LMP signalling and, L2CAP signalling and user data.

ACL logical transport contain payload header in addition to packet header which is having 3 fields as described below:

LLID: 2 bit field

LLID	Logical Link	Information
00	N/A	Reserved for future use
01	ACL-U and ASB-U	Continuation fragment of an L2CAP message
10	ACL-U and ASB-U	Start of an L2CAP message / No fragmentation
	PBD	Profile Broadcast Data, No fragmentation (Will not pass through L2CAP, profile directly interacts with HCI)
11	ACL-C and ASB-U	LMP message

FLOW: L2CAP layer flow control bit to control flow of L2CAP messages.

FLOW = 0	STOP	Flow off
FLOW = 1	GO	Flow on

LENGTH: This field specifies length of payload.

6.2 Logical Transport Packet types:

6.2.1 ACL packets

ACL packets are used on the asynchronous logical transport. The information carried may be user data or control data.

6.2.1.1 ACL packets for Basic Rate Operation:

DM1 packet - Data Medium Rate (1 slot)

Header (1byte)	Payload (18 bytes)	2/3 FEC	CRC (16 bit)

DH1 packet - Data High Rate (1 slot)

Header (1byte)	Payload (28 bytes)	CRC (16 bit)

DM3 packet – Data Medium Rate (3 slots)

Header (2byte)	Payload (123 bytes)	2/3 FEC	CRC (16 bit)

DH3 packet – Data High Rate (3 slots)

Header (2byte)	Payload (185 bytes)	CRC (16 bit)

DM5 packet – Data Medium slot (5 slots)

Header (2byte)	Payload (226 bytes)	2/3 FEC	CRC (16 bit)

DH5 packet – Data High Rate (5 slots)

Header (2byte)	Payload (341 bytes)	CRC (16 bit)

AUX1 packet

Header (1byte)	Payload (30 bytes)

6.2.1.2 ACL packets for Enhanced Data Rate operation:

2-DH1 packet

Header (2byte)	Payload (54 bytes)	CRC (16 bit)

2-DH3 packet

Header (2byte)	Payload (367 bytes)	CRC (16 bit)

2-DH5 packet

Header (2byte)	Payload (679 bytes)	CRC (16 bit)

3-DH1 packet

Header (2byte)	Payload (83 bytes)	CRC (16 bit)

3-DH3 packet

Header (2byte)	Payload (552 bytes)	CRC (16 bit)

3-DH5 packet

Header (2byte)	Payload (1021bytes)	CRC (16 bit)

6.2.2 SCO Packets:

HV and DV packets are used on the SCO logical transport. HV packets do not include CRC and these packets will not be re-transmitted.

HV1 Packet

Audio (10 Bytes)	FEC (1/3)

HV2 Packet

Audio (20 Bytes)	FEC (2/3)

HV3 Packet

Audio (30Bytes)

DV Packet

Audio (10 Bytes)	Header (1 Byte)	Payload (0 – 9 Bytes)	2/3 FEC	CRC (16 bits)

6.2.3 eSCO Packet Types:

EV packets are used on the synchronous eSCO logical transport. The packets includes CRC and retransmission is applied if acknowledgment is not received.

EV3 packet

Audio (30 Bytes)	CRC (16 bits)

EV4 packet

Audio (120 Bytes)	FEC (2/3)	CRC (16 bits)

EV5 packet

Audio (180 Bytes)	CRC (16 bits)

2-EV3 packet

Audio (60 Bytes)	CRC (16 bits)

2-EV5 packet

Audio (360 Bytes)	CRC (16 bits)

3-EV3 packet

Audio (90 Bytes)	CRC (16 bits)

3-EV5 packet

Audio (540 Bytes)	CRC (16 bits)

6.2.4 Common Packet Types:

6.2.4.1 NULL Packet

The NULL packet has no payload and consists of the channel access code and Packet header only. Its total (fixed) length is 126 bits.

Channel Access Code	Packet Header

6.2.4.2 POLL Packet

POLL packet is similar to that of NULL packet. It does not have payload. POLL packets shall not be sent on Connectionless slave broadcast.

Channel Access Code	Packet Header

6.2.4.3 ID Packet

For Inquiry:

Preamble (4b)	Sync word (64b)

Preamble: Depends on the first (i.e. least significant) bit of the sync word: either 0101(0...) or 1010(1...).

Sync Word: Depends upon the type of access code.

IAC (Inquiry Access Code): It is used for inquiring. For general inquiries, the GIAC (General IAC) is used, generated from the reserved LAP of 9E8B33.

For Paging:

Preamble (4b)	Sync word (64b)

Preamble: Depends on the first (i.e. least significant) bit of the sync word: either 0101(0...) or 1010(1...).

Sync Word: Depends upon the type of access code.

DAC (Device Access Code): used for paging, generated from the LAP of the paged device.

FHS Packet

Parity bits	LAP	EIR	Reserved	SR	SP	UAP	NAP	Class of device	LT_ADDR	CLK 2 7 -2	Page Scan Mode

FHS packet for Inquiry:

Parity bits: This 34-bit field contains the parity bits that form the first part of the sync word of the access code of the device that sends the FHS packet.

LAP: (Lower Address Part) This 24-bit field shall contain the lower address part of the device that sends the FHS packet (here, aspiring slave).

EIR: (Extended Inquiry Response) this bit shall indicate that an extended inquiry response packet may follow.

Undefined: This 1-bit field is reserved for future use and shall be set to zero.

SR: NA

Reserved: This 2-bit field shall be set to 10.

UAP: (Upper Address Part) This 8-bit field shall contain the upper address part of the device that sends the FHS packet (here, aspiring slave).

NAP: (Non-Significant Address Part) This 16-bit field shall contain the non-significant address part of the device that sends the FHS packet (here, aspiring slave).
Class of device: This 24-bit field shall contain the class of device of the device that sends the FHS packet (here, aspiring slave).

LT_ADDR: Zero (Since it's an inquiry packet)

CLK 27-2: This 26-bit field shall contain the value of the native clock of the device that sends the FHS packet (here, aspiring slave). The value contained is the sampled value at the beginning of the transmission of the access code of this FHS packet.

Page scan mode: NA

FHS packet for Paging:

Parity bits : This 34-bit field contains the parity bits that form the first part of the sync word of the access code of the device that sends the FHS packet(here, aspiring master).

LAP: This 24-bit field shall contain the lower address part of the device that sends the FHS packet (here, aspiring master).

EIR: This bit shall indicate that an extended inquiry response packet may follow.

Undefined: This 1-bit field is reserved for future use and shall be set to zero.

SR: This 2-bit field is the scan repetition field and indicates the interval between two consecutive page scan windows.

Reserved: This 2-bit field shall be set to 10.

UAP: This 8-bit field shall contain the upper address part of the device that sends the FHS packet (here, aspiring master).

NAP: This 16-bit field shall contain the non-significant address part of the

device that sends the FHS packet.

Class of device: This 24-bit field shall contain the class of device of the device that sends the FHS packet (here, aspiring master).

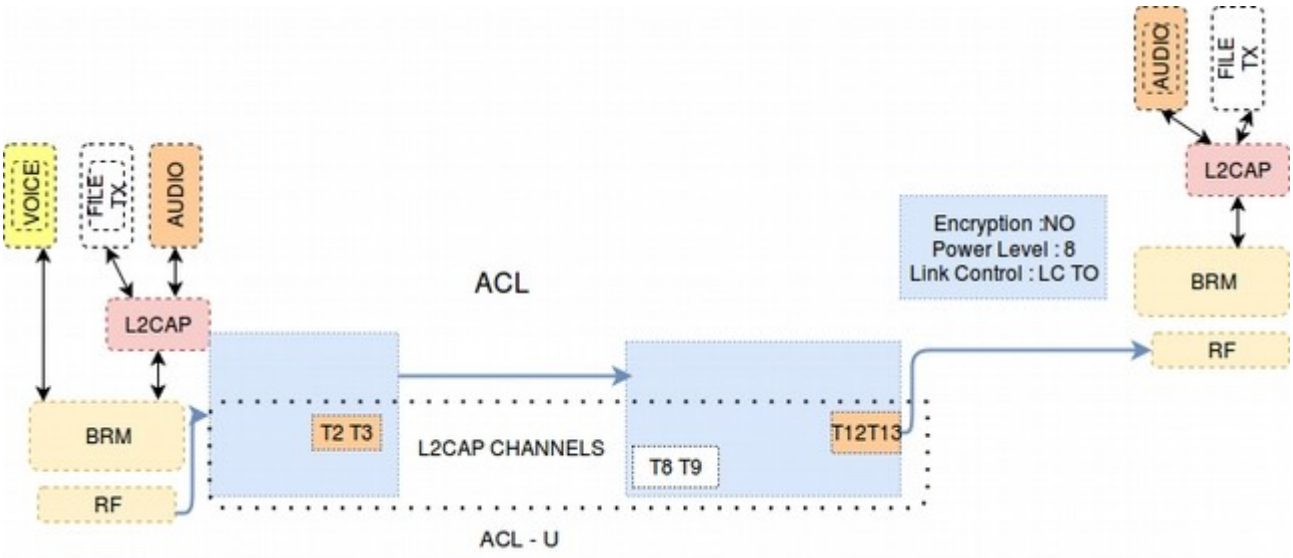
LT_ADDR: This 3-bit field shall contain the logical transport address the recipient and shall use if the FHS packet is used at connection setup or role switch. A slave responding to a master or a device responding to an inquiry request message shall include an all-zero LT_ADDR field if it sends the FHS packet.

CLK 27-2: This 26-bit field shall contain the value of the native clock of the device that sends the FHS packet (here, aspiring master). The value contained is the sampled value at the beginning of the transmission of the access code of this FHS packet.

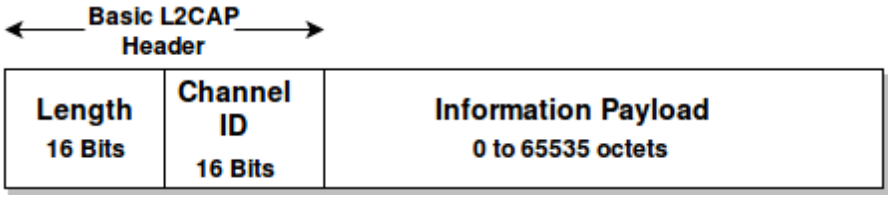
Page scan mode: This 3-bit field shall indicate which scan mode is used by default by the sender of the FHS packet.

7. L2CAP channels

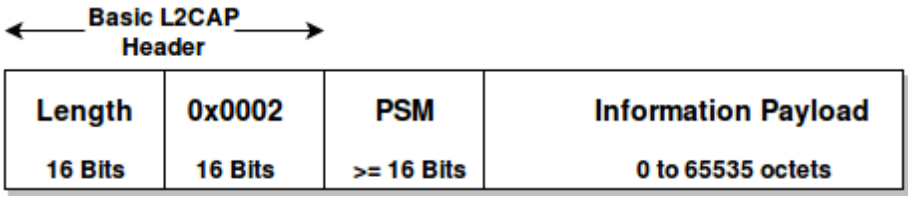
L2CAP channel endpoints are identified by their clients by Channel Identifier (CID). Channels may be Connection-oriented or Connectionless. L2CAP connectionless channels have CID 0x0002 and signalling channels have CID 0x0001 or 0x0005. All channels with dynamically allocated CID's are connection-oriented.



Connection-Oriented L2CAP channels in basic L2CAP mode



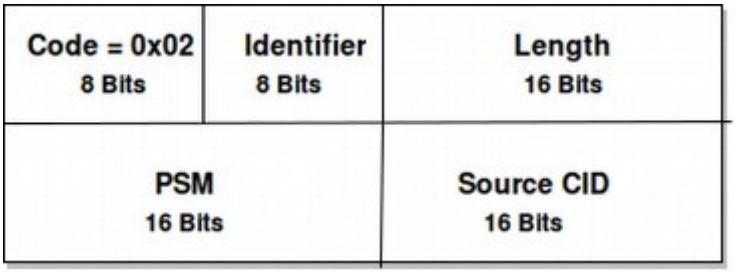
Connectionless L2CAP channels in basic L2CAP mode



Protocol/ Service Multiplex (PSM) field is present so that application can register to receive data on a particular PCM else the data received as broadcast will be discarded.

Connection Request:

Connection request packets are sent to create an L2CAP channel between two devices.



Connection Response:

When a device receives a Connection Request packet, it shall send a Connection Response packet.

Code = 0x03 8 Bits	Identifier 8 Bits	Length 16 Bits
Destination CID 16 Bits		Source CID 16 Bits
Result		Status