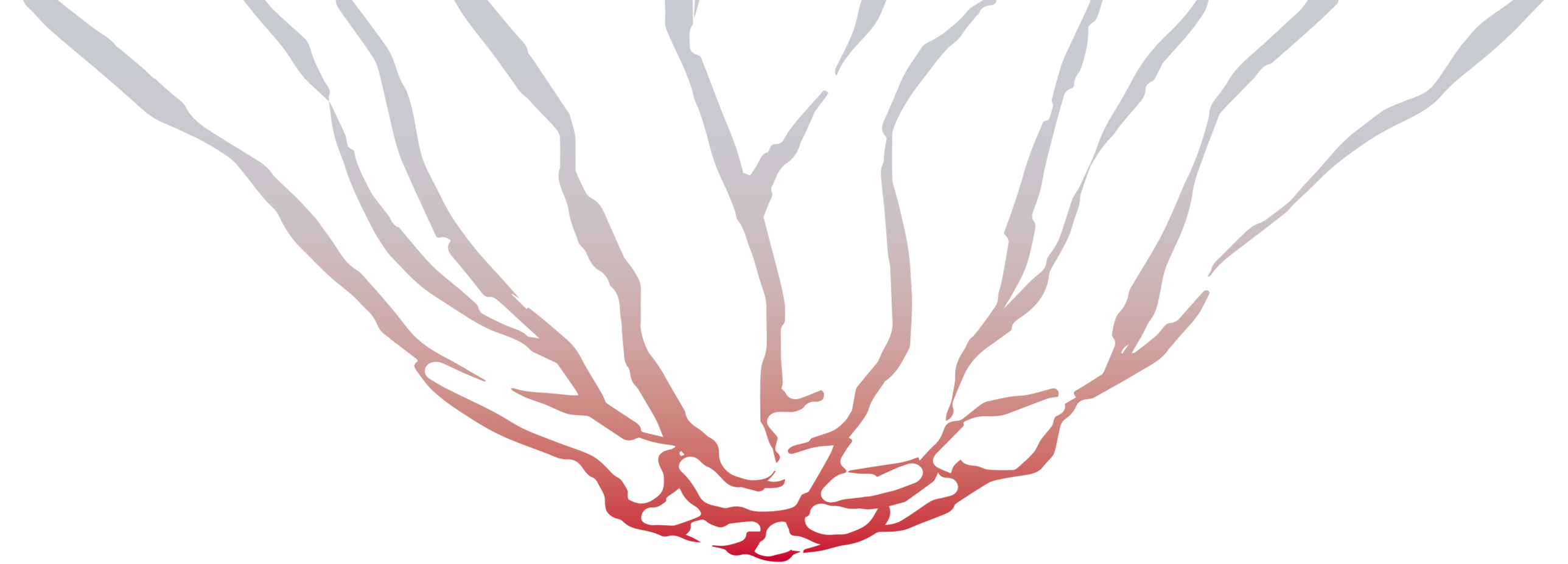


ESPRESSIF

Classic Bluetooth Basics

Karl Wang 王孟阳

August 2018

Agenda

- Introduction: Bluetooth is around us
- Bluetooth Protocol Stack
  - Stack Overview
  - Upper Layer
  - SDP and L2CAP
  - Lower Layer: PHY/RF, BB, LC and LM
  - HCI: High-Level Language to Access Bluetooth Radio
- Use a Packet Sniffer
- Summary
- References and Resources

Introduction: Bluetooth is Around Us

What is Bluetooth?

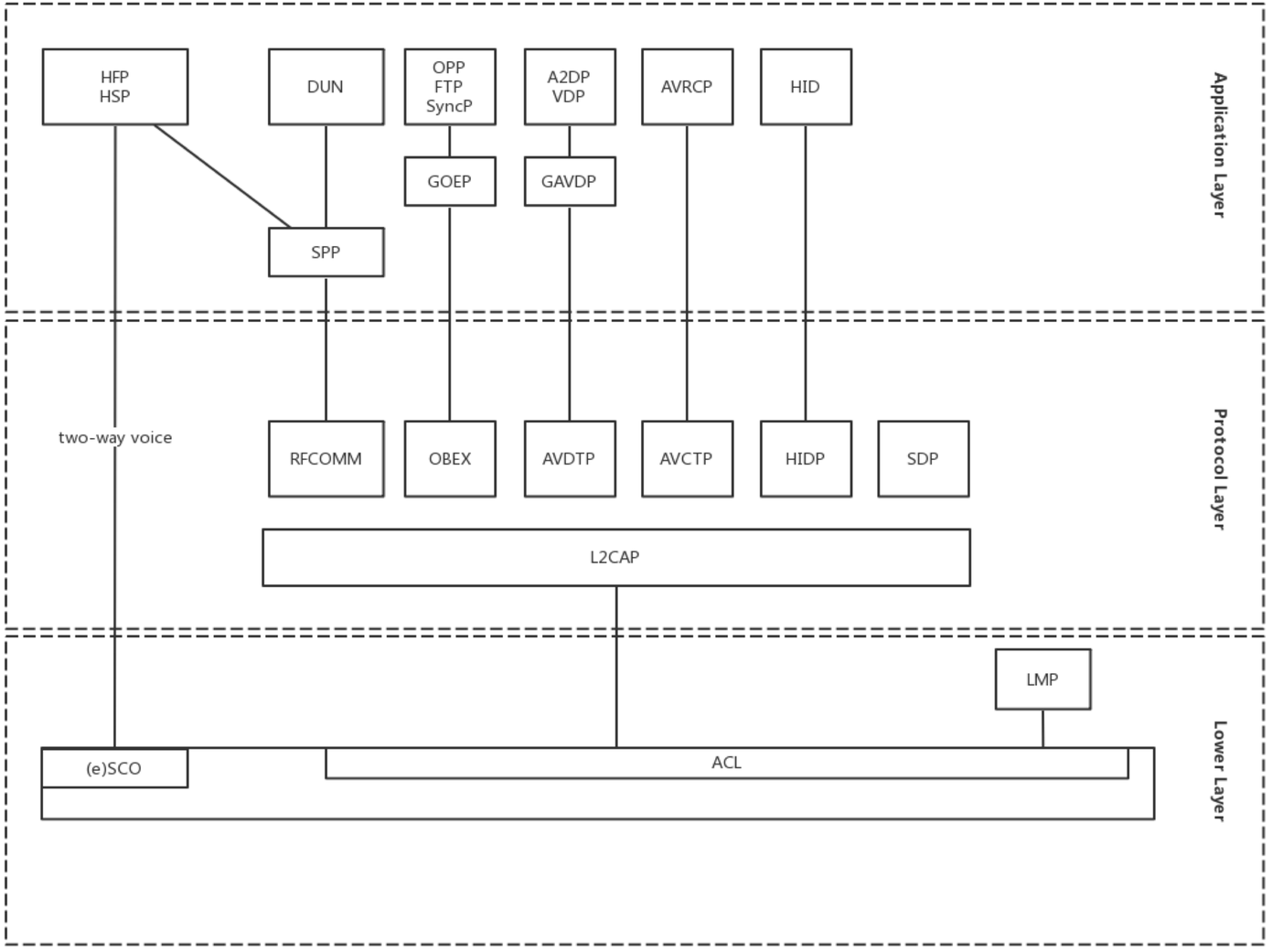
- A short-range wireless communication system intended to replace cables

User scenarios:

- Keyboards, mouses, joysticks: data input & remote control
- Headphones, speakers: audio and voice transmission
- Handhelds, PCs & Automobiles: file sharing
- Others: printers, sensors, etc.

Bluetooth makes personal area free of USB cables, headphone cables, serial ports and various other types of cables/IO ports.

Bluetooth Protocol Stack Overview



Bluetooth Protocol Stack: Concepts and Sources

- Profiles vs. Protocols
  - A Protocol defines the message set exchanged between Bluetooth devices
  - A Profile defines how protocols are used for a specific usage model

- Upper Layer Stack
  - Many protocols to support a wide range of applications
  - Some borrowed from other organizations or standards
  - Some Bluetooth invented
  - Some hybrid

Bluetooth Protocol Stack--Upper Layer

- Adopted Protocols -- “Stolen with pride”
  - HIDP: originates from USB HID Specification
  - RFCOMM: uses a subset of ETSI standard GSM 07.10, provides a transport for serial port emulation
  - OBEX: Adaptation of Ir DA Object Exchange Protocol from Infrared Data Association
  - AVDTP: based on RTP Data Transfer Protocol and RTP Control Protocol from IETF RFC3550
  - AVCTP Control: based on AV/C Digital Interface Command Set with some Bluetooth Vendor Dependent extension

Bluetooth Protocol Stack--SDP

SDP: Service Discovery Protocol

- Used for applications to discover available services and determine the features and characteristics of those services from remote device
- Client-Server Architecture

Bluetooth Protocol Stack--SDP

- SDP server database
- Example of a Hands-free service record

Item	Definition	Type	Value
Service Record Handle		Uint32	0x10002
ServiceClass ID List			
ServiceClass0		UUID	Hands-Free(0x111e)
ServiceClass1		UUID	Generic Audio(0x1203)
ProtocolDescriptorList			
Protocol0		UUID	L2CAP(0x0100)
Protocol1		UUID	RFCOMM(0x0003)
ProtocolSpecificParam0	Server Channel	Uint8	2
ProfileDescriptorList			
Profile0	Supported Profiles	UUID	Hands-Free(0x111e)
Param0	Profile Version	Uint16	0x0106
ServiceName	Display-able Text Name	String	“Handsfree”
Supported Features		Uint16	0x003f

Bluetooth Protocol Stack--L2CAP

- Logical Link Control and Adaptation Protocol
  - OSI Layer 2: Data Link Layer
  - Provides Connection-oriented and connection-less channels
  - Carries User Asynchronous(UA) and User Isochronous(UI) data
- Functionality
  - Protocol/Channel Multiplexing
  - Packet segmentation and reassembly
  - QoS admission control: bandwidth, latency, etc.
- Assumptions
  - Lower Layer provides orderly delivery of data packets
  - Lower Layer provides full-duplex communication link
  - Lower Layer provides a channel with a degree of reliability
- Different operation modes are provided that fit LE, BR/EDR and/or AMP controllers. For BR/EDR controller
  - L2CAP basic mode provides basic functionality for a default “best effort” service
  - Enhanced L2CAP operation modes can provide additional flow control, flushing or retransmission mechanism to fit different user scenarios

Bluetooth Lower Layer Stack--BR/EDR radio

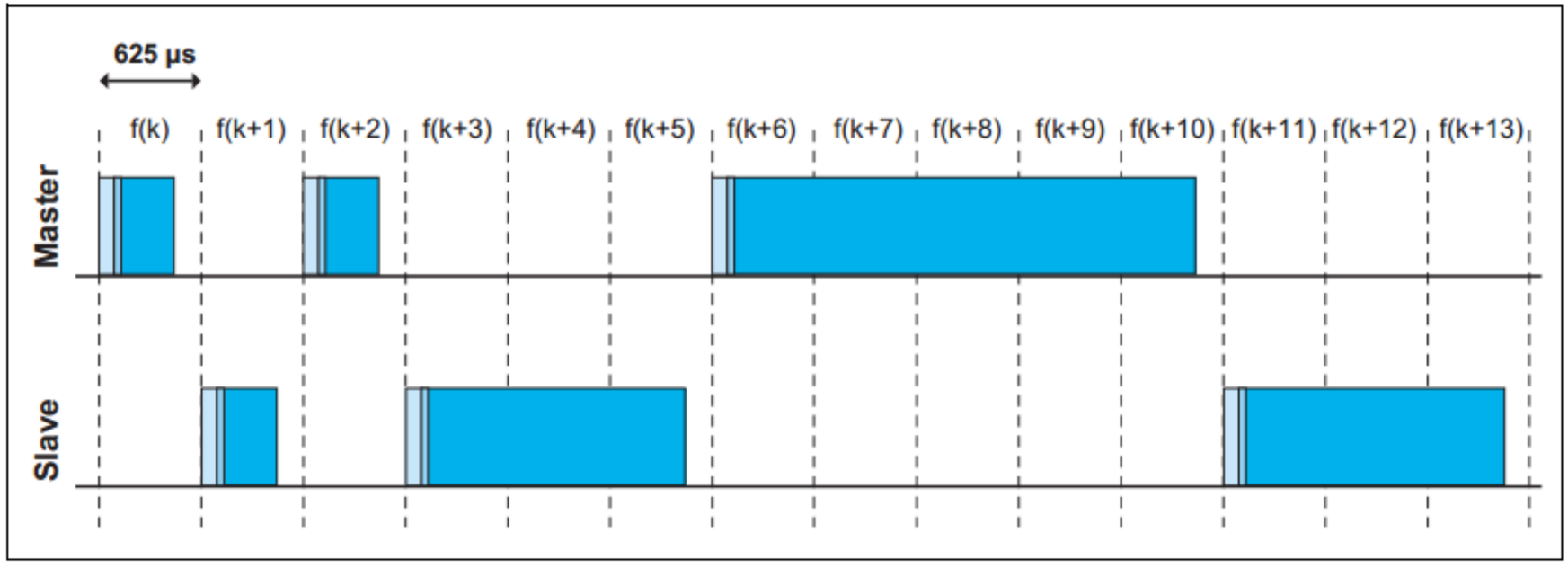
Bluetooth BR/EDR PHY and Baseband

- 2.4GHz ISM band.
- 79 hopping channels, $f_k = (2402 + k)MHz,\ k = 0,1,2...,78$
- modulation and bit rate
  - Basic Rate(BR): GFSK with BT = 0.5, 1Mbit/s
  - Extended Data Rate(EDR): π/4-DQPSK for 2Mbit/s, 8DPSK for 3Mbit/s
  - Symbol rate is 1MHz for both BR and EDR
- Frequency Hopping Spread Spectrum(FHSS)
  - Frequency hops in a pseudo-random pattern with 1600Hz hopping rate in connection state
- Time-Division Duplex(TDD)
  - divides time in 625us slots

Bluetooth Lower Layer Stack--Piconet Operation

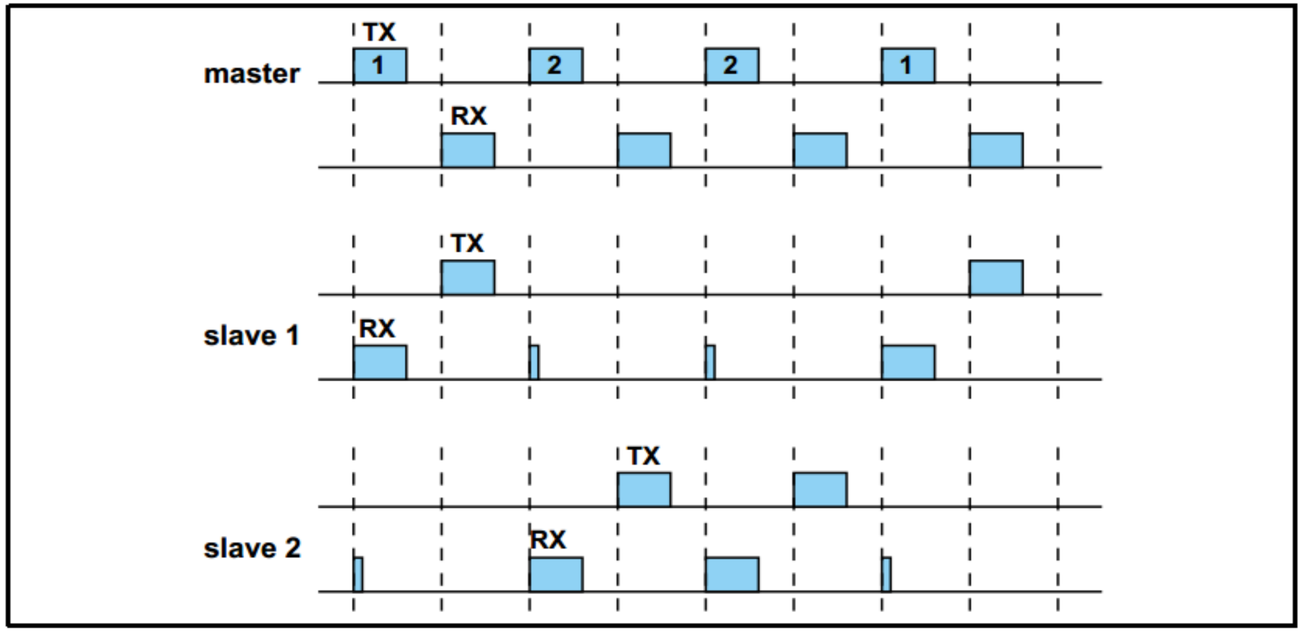
- Piconet: Master and 1 to 7 slaves in connection state
- To stay synchronized in a frequency hopping system, devices connected need to:
  - use the same set of hopping frequencies
  - use the same hopping sequence within the frequency set
  - be time synchronized within the hopping sequence
- In a piconet,
  - Hopping frequency set is all 79 channels for normal operation mode or a subset of it when Adaptive Frequency Hopping(AFH) is in use
  - Hopping sequence is determined by master MAC address, hopping phase is determined by master clock
  - Communication begins on new hopping frequency at the start of time slots according to master clock

Piconet Operation: Single-slave case



- Master and Slave alternatively transmit in each slot pairs. Master Tx is at first
- Packet transmission start is aligned with slot start
- Each transmission takes place at a new hopping frequency. Packet duration can fall into 1, 3, or 5 slots
- A polling interval T_{poll} and a link supervision timer is applied to the connection
- There can be only 1 ACL logical transport and 0 or more SCO or eSCO logical transports between a master and a slave

Piconet Operation: Multi-slave Case



- Different slaves are addressed by their LT_ADDR in the packet header. eSCO transport is assigned a different LT_ADDR
- Total throughput(all the time slots) are shared between piconet members
- Slaves in a piconet cannot exchange packets directly

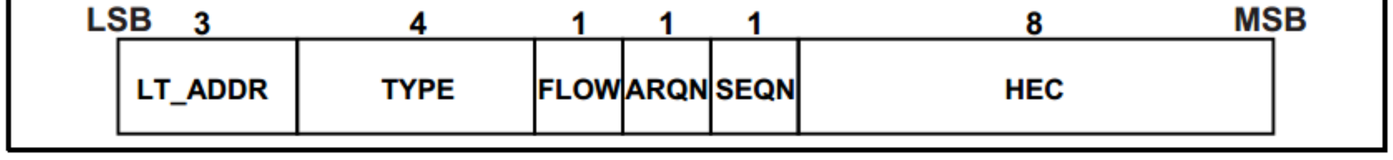
Comparison of ACL, SCO and eSCO

“packet switching” vs. “circuit switching”

ACL	SCO	eSCO
“packet switching”	“circuit switching”	
User Isochronous data(UI) User Asynchronous data(UA) with variable bit rate	User Synchronous data(US) with constant bit rate	
error check and retransmissions used to provide data integrity	no CRC, no retransmission	limited retransmission
focus on data integrity	focus on low latency	
throughput is influenced by BER	throughput is unaffected by channel integrity	

BR/EDR Connection Packet Types

- Packets differ in:
  - time slot occupation
  - payload bit rate(BR, 2Mbit/s or 3Mbit/s EDR)
  - Forward Error Correction(FEC) coding method
  - use of CRC and MIC, etc.
- Packet type can be decided according to:
  - The Logical Transport(ACL, SCO or eSCO), and
  - The “TYPE” field in the packet header
- Packet header format

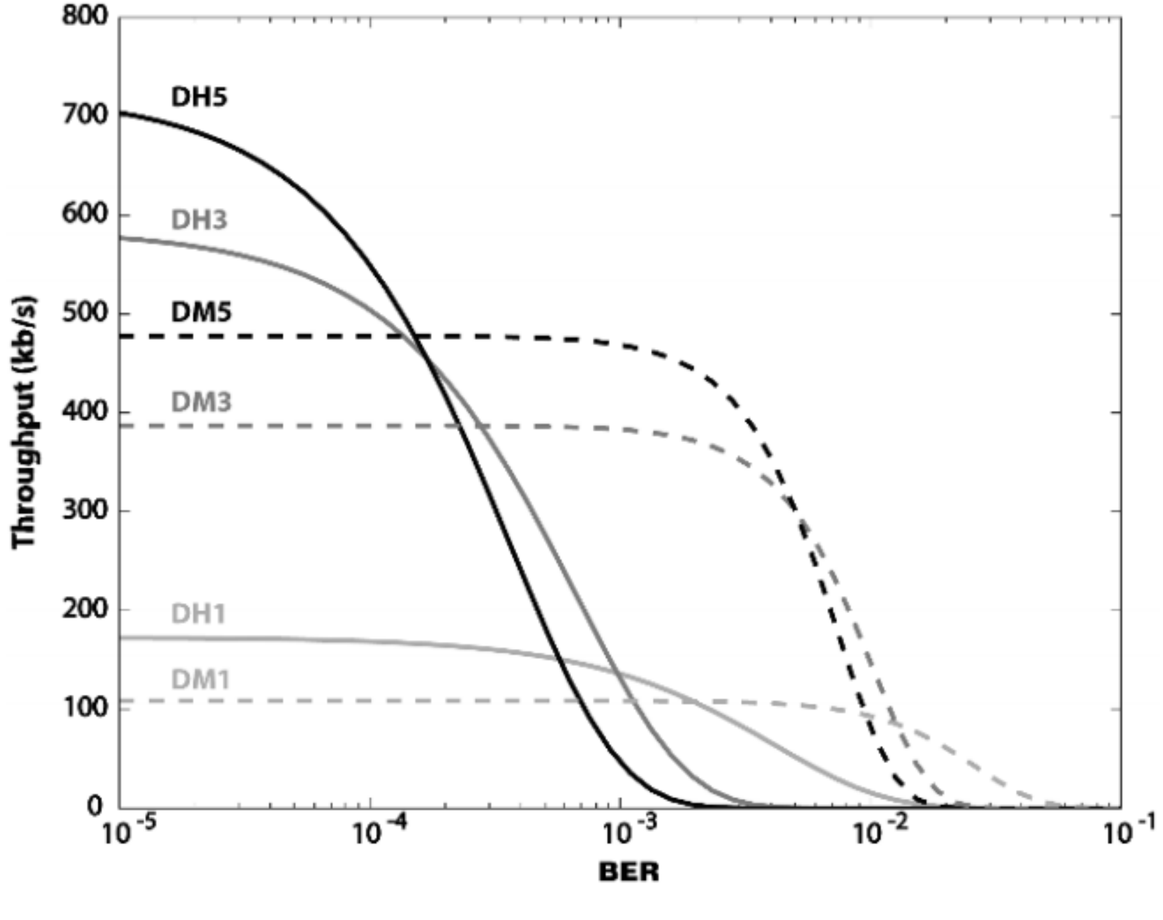


BR/EDR Connection Packets: ACL Packets

Type	time slot occupation	User Payload (bytes)	BR, 2M-EDR or 3M-EDR	FEC	MIC	CRC	Symmetric Max Rate(kb/s)	Asymmetric Max Rate(kb/s)	
								Forward	Reverse
DM1	1	0-17	BR	2/3	C.1	Yes	108.8	108.8	108.8
DH1	1	0-27	BR	No	C.1	Yes	172.8	172.8	172.8
DM3	3	0-121	BR	2/3	C.1	Yes	258.1	387.2	54.4
DH3	3	0-183	BR	No	C.1	Yes	390.4	585.6	86.4
DM5	5	0-224	BR	2/3	C.1	Yes	286.7	477.8	36.3
DH5	5	0-339	BR	No	C.1	Yes	433.9	723.2	57.6
2-DH1	1	0-54	2M-EDR	No	C.1	yes	345.6	345.6	345.6
2-DH3	3	0-367	2M-EDR	No	C.1	Yes	782.9	1174.4	172.8
2-DH5	5	0-679	2M-EDR	No	C.1	Yes	869.1	1448.5	115.2
3-DH1	1	0-83	3M-EDR	No	C.1	Yes	531.2	531.2	531.2
3-DH3	3	0-552	3M-EDR	No	C.1	Yes	1177.6	1766.4	235.6
3-DH5	5	0-1021	3M-EDR	No	C.1	Yes	1306.9	2178.1	177.1
C.1: Mandatory when encryption with AES-CCM enabled, else excluded									

- DM: Data Medium speed, 2/3 FEC code
- DH: Data High speed, no FEC
- Prefix “2-” or “3-” indicates the EDR rate: 2Mbit/s or 3Mbit/s
- Suffix “1”, “3” or “5” indicates the time slot occupation

Basic Rate ACL link Throughput under Different BER



General Rules to achieve high-throughput:

- Use DH5 for BER less than 10^{-4}
- Use DM5 for BER is between 10^{-4} and 10^{-2}
- Use DM1 when BER exceeds 10^{-2}

DM5 is used for measuring receiver sensitivity for Bluetooth certification

DM1 packet type is the major packet type for ACL-C(LMP) logical link, to ensure the data integrity of signaling messages

- Mathematical analysis of maximum asymmetric throughput with different basic rate packet types under different Bit Error Rate

BR/EDR Connection Packets: POLL and NULL

POLL and NULL are two types of control packets which:

- Consists of access code and packet header only, without any payload.
- Convey ARQ, or FLOW information on the LC level.

Differences between POLL packet and NULL packet:

- POLL is only used by master, NULL can be used by both.
- POLL packet shall have a response packet, NULL may not have to be acknowledged

BR/EDR Connection Packets: SCO Packets

Type	time slot occupation	User Payload(bytes)	BR, 2M-EDR or 3M-EDR	FEC	MIC	CRC	Symmetric Max Rate(kb/s)
HV1	1	10	BR	1/3	No	No	64.0
HV2	1	20	BR	2/3	No	No	64.0
HV3	1	30	BR	No	No	No	64.0
DV1	1	10+(0-9)D	BR	2/3 D	No	Yes D	64.0+57.6D

- HV: High-quality Voice
- DV1: Data + Voice contained in the packet
- suffix “1”, “2”, “3” indicates the FEC coding rate: 1/3, 2/3 or 3/3(No FEC)
- SCO link has fixed symmetric rate of 64kbit/s carrying two-way voice, a-law, μ-law or CVSD encoded
- **SCO link has no CRC for error detection and no retransmission**
- For an SCO connection through HV3 packet, 2 slots within every 6 slots are reserved
- For an SCO connection through HV2 packet, 2 slots within every 4 slots are reserved
- For an SCO connection through HV1 packet, all the time slots are occupied

BR/EDR Connection Packets: eSCO Packets

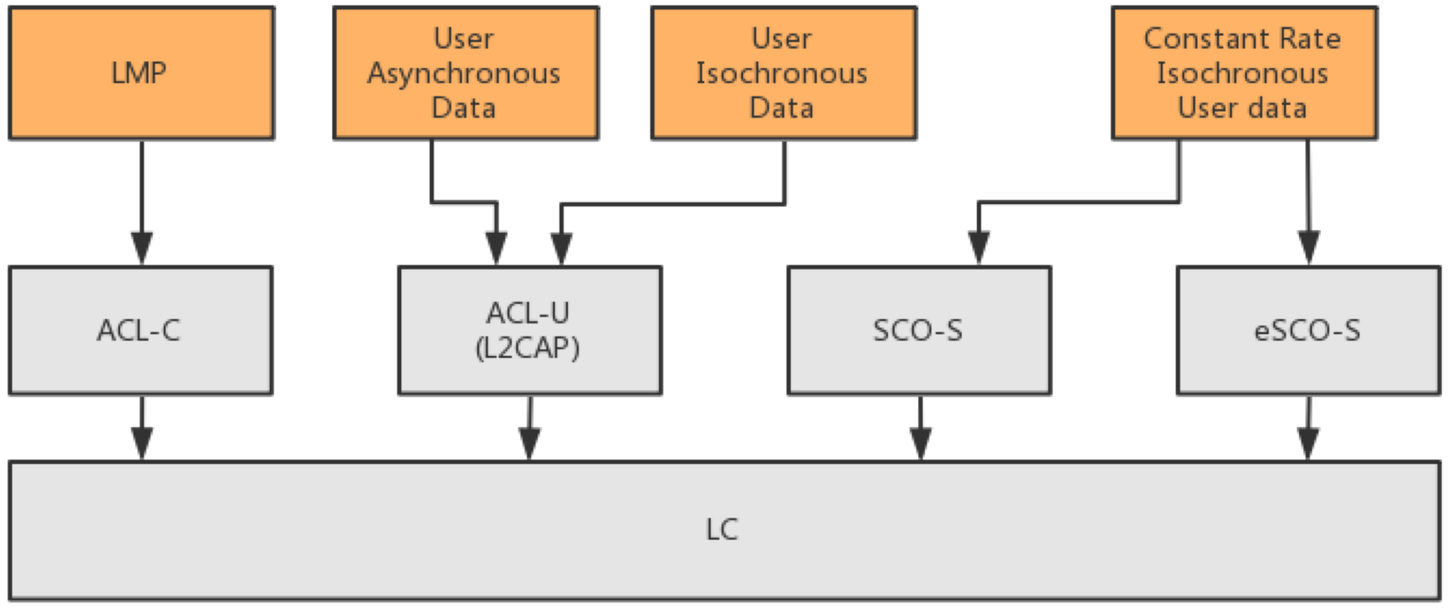
Type	time slot occupation	User Payload(bytes)	BR, 2M-EDR or 3M-EDR	FEC	MIC	CRC	Symmetric Max Rate(kb/s)
EV3	1	1-30	BR	No	No	Yes	96
EV4	3	1-120	BR	2/3	No	Yes	192
EV5	3	1-180	BR	No	No	Yes	288
2-EV3	1	1-60	2M-EDR	No	No	Yes	192
2-EV5	3	1-360	2M-EDR	No	No	Yes	576
3-EV3	1	1-90	3M-EDR	No	No	Yes	288
3-EV5	3	1-540	3M-EDR	No	No	Yes	864

- eSCO link may be used for 64kbit/s two-way voice transmission, as well as transparent data at 64kb/s and other rates; Asymmetric data rate can be configured
- CRC is used for error detection, and limited retransmission can be applied inside retransmission window
- parameter negotiation can be performed for either power or latency considerations targeted on a certain bandwidth

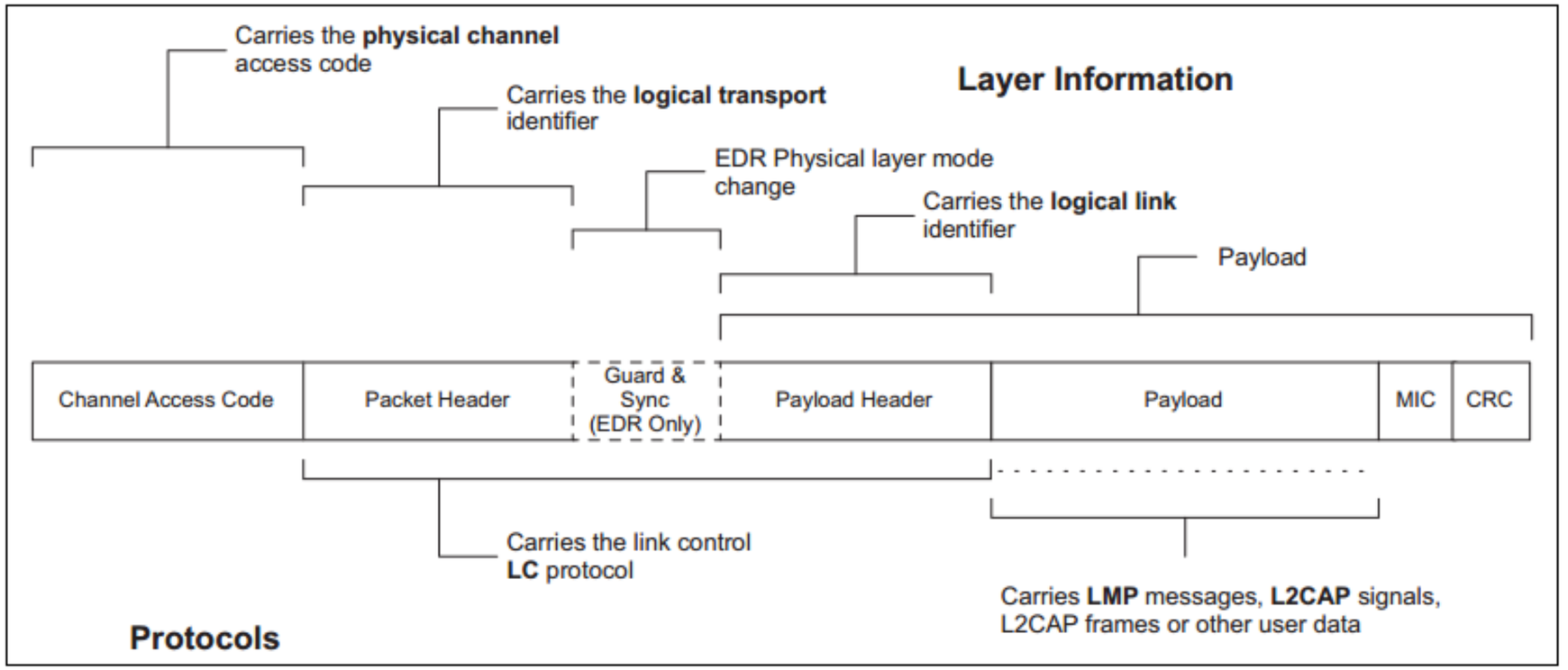
eSCO Mandatory Parameter Ranges

	Single-slot packets	3-slot packets
T_{eSCO}	EV3: 6 2-EV3: 6-12(Even) 3-EV3: 6-18(Even)	EV4: 16 EV5: 16 2-EV5: 16 3-EV5: 16
W_{eSCO}	0, 2, 4	0, 6
packet length M->S	10 * T_{eSCO}/2	10 * T_{eSCO}/2
packet length S->M	10 * T_{eSCO}/2	10 * T_{eSCO}/2
air mode	At least one of A-law, μ-law, CVSD, transparent	transparent

Piconet Operation: BR/EDR Logical Links



BR/EDR Packet Structure



Piconet Operation: Link Manager

Link Manager(LM)

- Responsible for:
  - information exchange: version, supported features, name request
  - link control: link set-up/tear-down, power control, AFH
  - packet type negotiation
  - security: authentication, pairing, encryption
  - link policy: role switch, low power mode, QoS
- Link Manager Protocol(LMP)
  - Counterpart in BLE is Link Layer Protocol(LL)
  - Used between LMs on two connected devices
  - Transferred over ACL-C logical link, which is distinguished from ACL-U that is managed by L2CAP
  - Has a higher priority over ACL-U logical link data

Piconet Operation: Link Controller

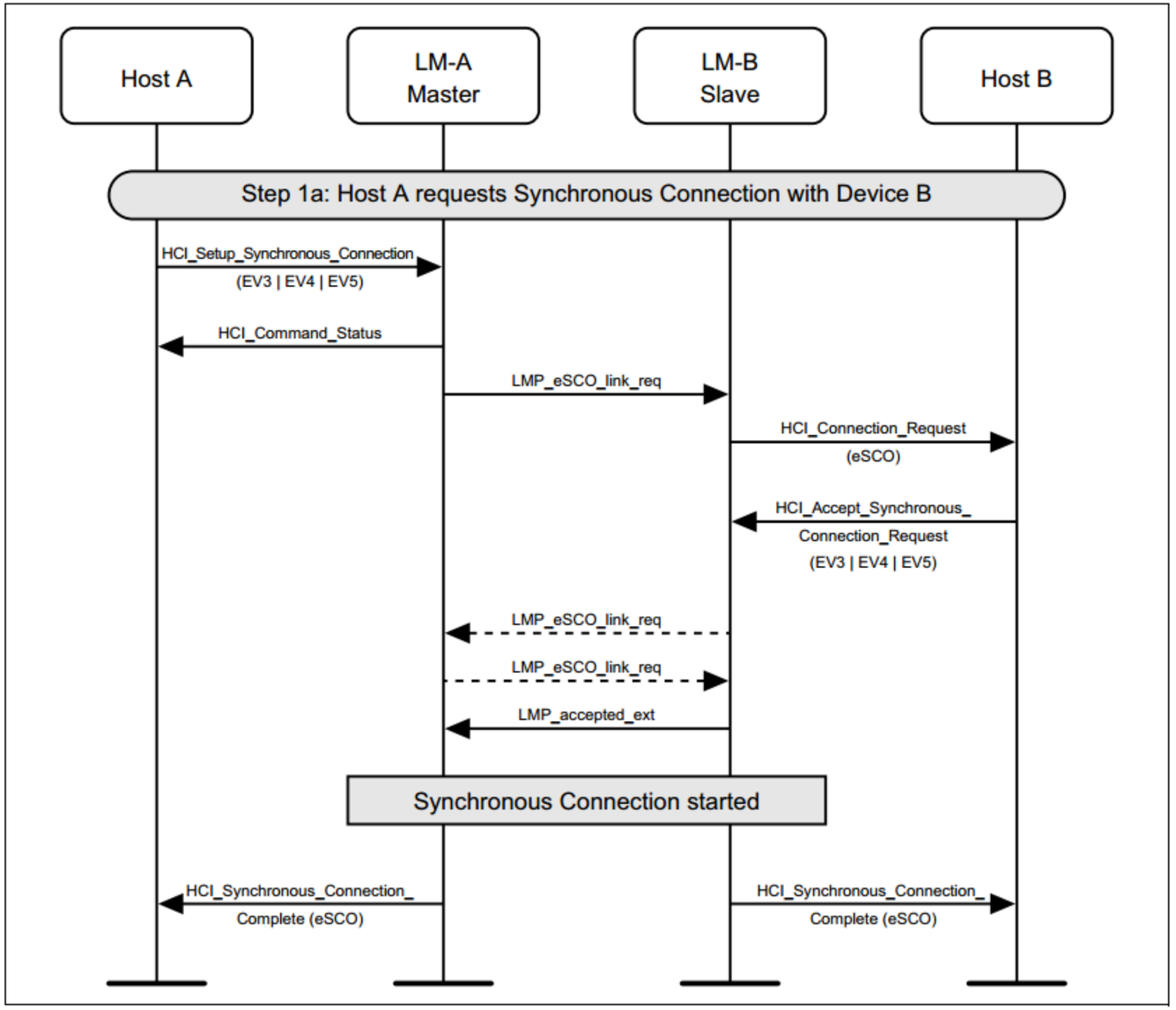
Functionality:

- baseband packet processing, packet assembly, piconet timing, frequency hopping, error control, data whitening basic security operations
- carrying out low-level link control protocol signaling such as ARQ, flow control, sequencing and payload type, mapped to the packet header
- operating in different states to support: device discovery, connection establishment, low power mode, etc

Host Controller Interface

- A uniform interface (physical and logical) to handle bluetooth radio and access controller capabilities, allowing vendor-specific extension
- A variety of physical transport can be used: USB, UART, SDIO, etc. The main goal is to achieve transparency in data delivery
- Located below L2CAP and above Link manager
  - allows adopted protocols like TCP/IP run on “Host” such as PC, and multiplexes the upper layer streams into one stream
  - provides a high-level control over the lower layer: an *abstraction* of LC or LM operations
- The logical interface provide four types of HCI packets
  - Command: Host --> Controller, used to direct the controller to perform a task
  - Event: Controller --> Host, used to respond to commands or report notifications to host
  - ACL data: Host <--> Controller, carrying packets on ACL-U, LE-U or AMP-U logical link
  - Synchronous data: Host <-->Controller, carrying packets on SCO-S or eSCO-S logical link
- HCI provides:
  - flow control mechanism for commands, ACL and synchronous data exchange between host and controller
  - segmentation of higher layer message(L2CAP) enabled by Packet_Boundary_Flag
  - erroneous data reporting ability for synchronous data packets through Packet_Status_Flag

HCI as a “High-Level Language”



God said, Let there be light: and there was light.

--The Holy Bible

Host said, Let there be a connection: and there was a connection.

Use a Packet Sniffer

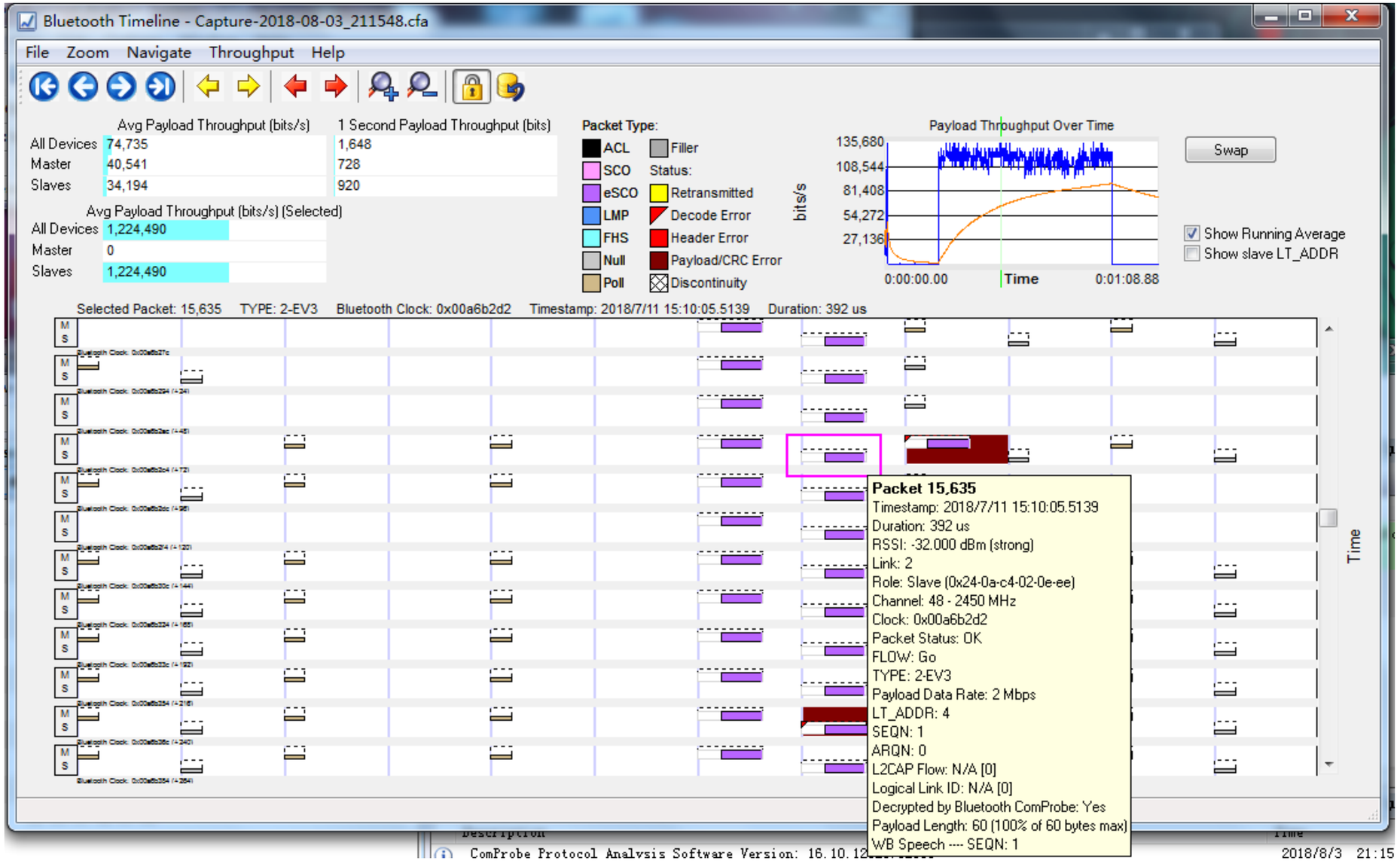
BR/EDR air packets are difficult to sniffer

- Operations like encryption, AFH, role switch brings extra challenge to the sniffer packets
- Usually a full-band sniffer is needed to track the bluetooth packets

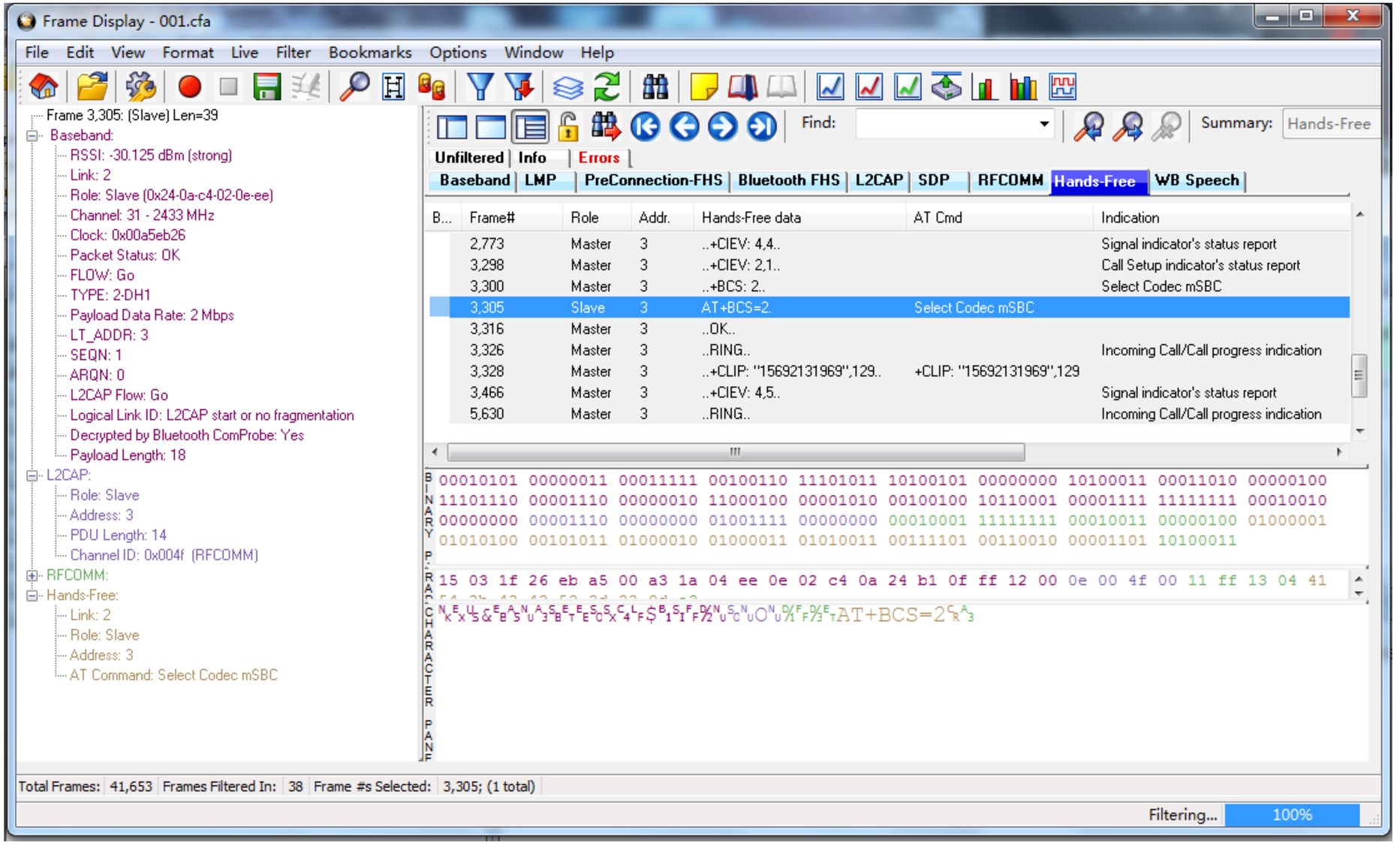
A bluetooth air sniffer and packet analyzer is expensive, but is also essential for lower-layer debugging

With your PC and a bluetooth dongle, you can use wireshark to analyze the bluetooth HCI traffic.

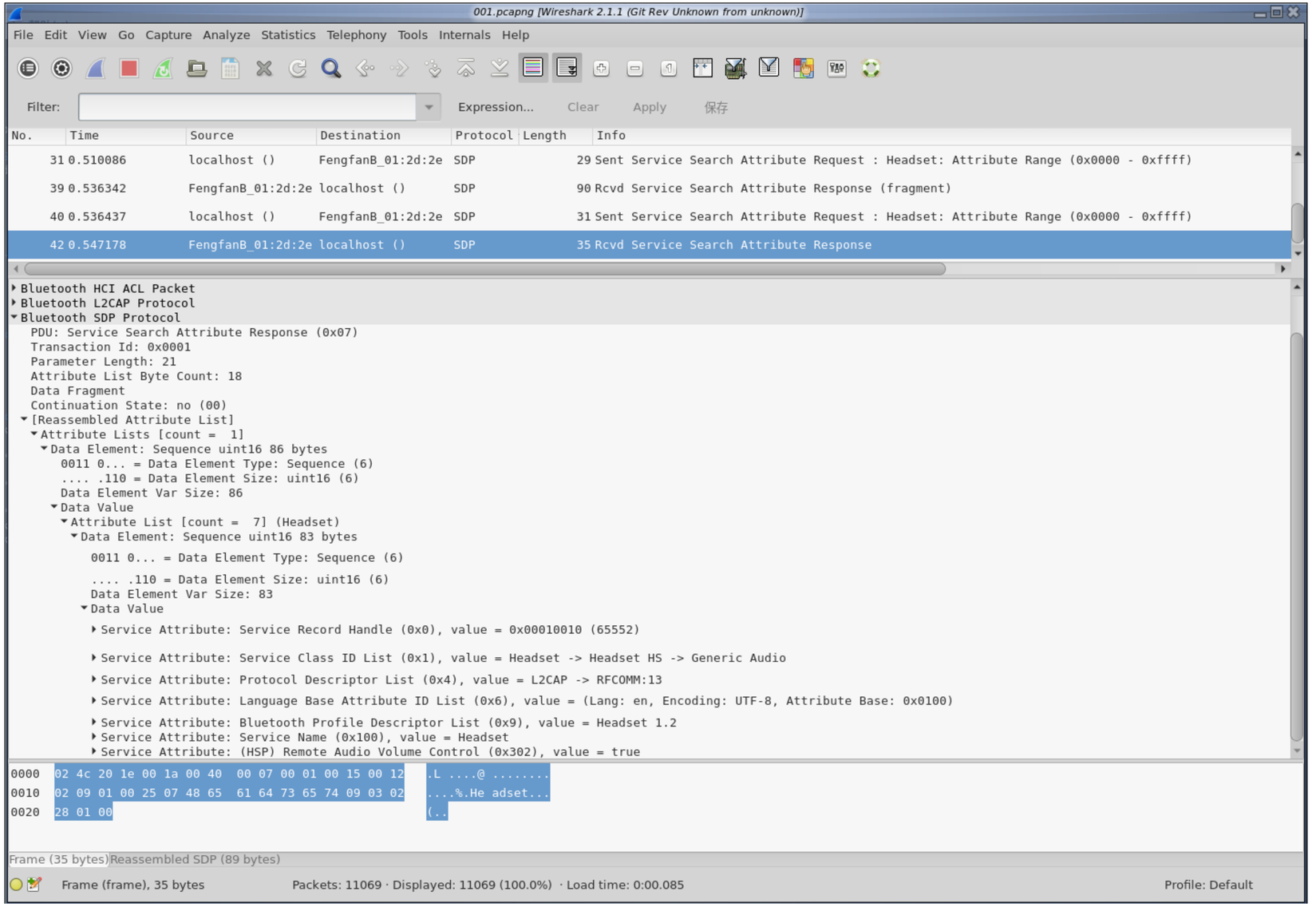
Packet Capture Example 1: eSCO transmission



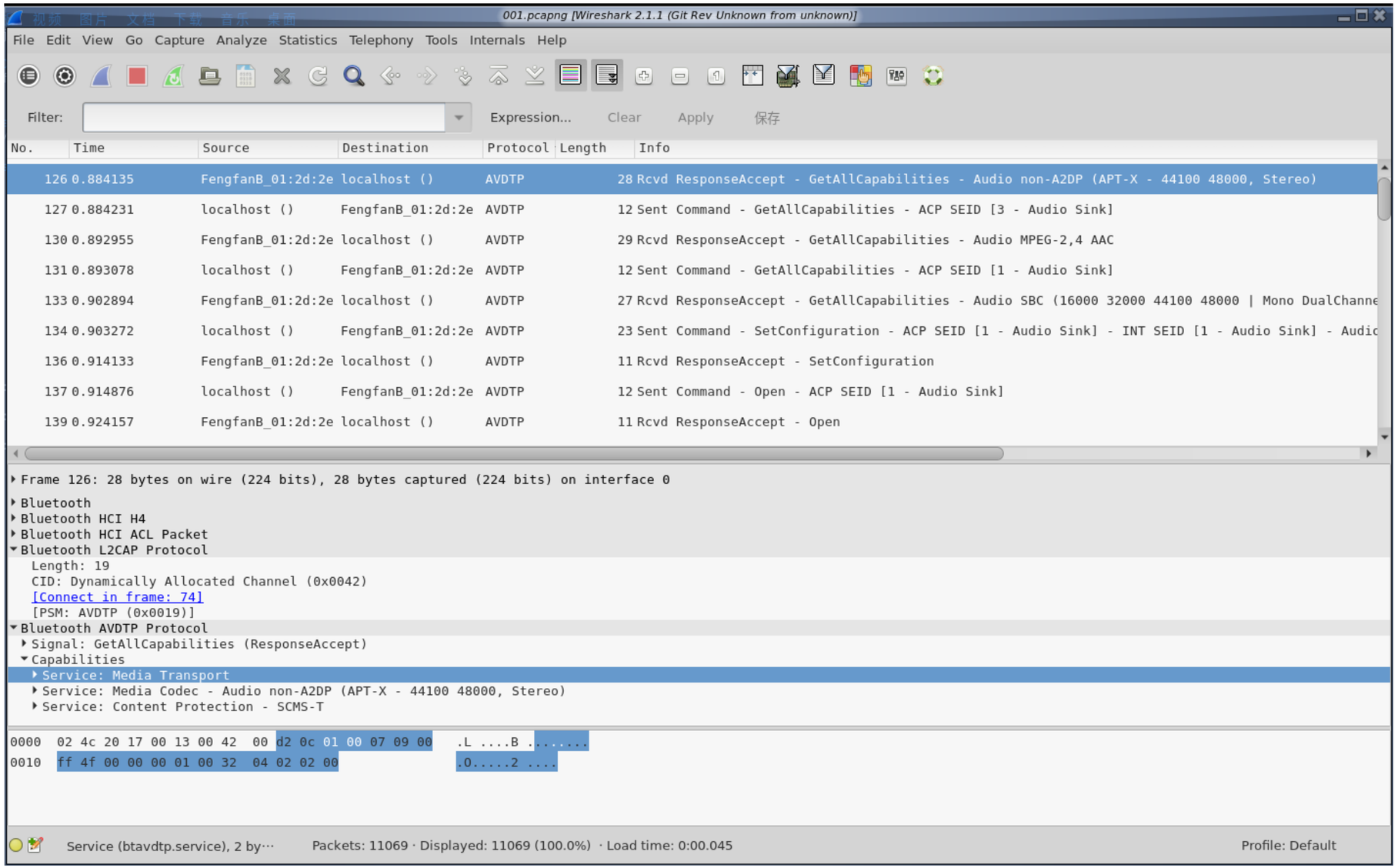
Packet Capture Example 2: HFP Codec Negotiation



Packet Capture Example 3(Wireshark): HSP SDP record



Packet Capture Example 4(Wireshark): A2DP Codec



Summary

- PHY: FHSS & TDD, 1MHz Symbol Rate, master controls the piconet with a polling scheme
- Bluetooth has a bunch of packet types differed in packet length, modulations, type of data conveyed as well as FEC coding
- Five Logical Links: LC, ACL-C(LMP), ACL-U(L2CAP), SCO-S and eSCO-S
  - LC information is conveyed over packet header, it deals with lower-layer flow control, and retransmission
  - LMP carries packets exchanged between LMs. LM is responsible for link management: packet type, power control, security, baseband parameter negotiation
  - SCO-S and eSCO-S carries two-way voice in reserved slots at a regular interval. SCO packets are never retransmitted, and eSCO packets can be retransmitted in a limited retransmission window
  - L2CAP multiplexes the upper-layer protocols into one stream and provides segmentation and reassembly for upper service packets. L2CAP different modes and optional ability like QoS, FCS can be enabled according to fit different user scenarios.
- Bluetooth higher layer adopts and adapts a variety of protocols from other domain
- Packet sniffer is a powerful tool in learning and problem analyzing

Untouched Topics

- Device Discovery Procedure (Inquiry & Inquiry Scan)
- Connection Establishment Procedure (Page & Page Scan)
- Adapted Frequency Hopping (AFH)
- Low power modes: sniff and hold
- Security aspects: pairing, authentication, encryption
- Active Slave Broadcast and L2CAP group traffic
- Scatternet
- AMP controller
- Test and Qualification

References

- Bluetooth: Operation and Use, Robert Morrow
- Bluetooth Essentials For Programmers, Albert S Huang, Larry Rudolph
- Bluetooth Low Energy: The Developer's Handbook
- Bluetooth Master/Slave Communications and Sniff/Sniff Subrating Modes White Paper
- Discovery Whitepaper Serivce Discovery Applications
- Bluetooth Core Specification, Version 4.2
- Generic Audio/Video Distribution Profile, Version 1.3
- Advanced Audio Distribution Profile, Version 1.3.1
- Audio/Video Remote Control Profile, Version 1.6.1
- Audio/Video Distribution Transport Protocol Specification, Version 1.3
- Audio/Video Control Transport Protocol Specification, Version 1.4
- Hands-Free Profile, Version 1.7.1
- Human Interface Device Profile, Version 1.1
- Generic Object Exchange Profile, Version 1.1.1
- RFCOMM with TS 07.10, Specification of the Bluetooth System, Version 1.2
- Serial Port Profile, Version 1.2

Useful Readings and Resources

Books

- 《Wireshark网络分析就这么简单》-- 林沛满
- 《Wireshark网络分析的艺术》-- 林沛满

Internet Resources

- www.bluetooth.org
- www.wikipedia.org

Free Bluetooth Stack Resources:

- www.bluez.org
- source.android.com/devices/bluetooth/
- bluekitchen-gmbh.com
- www.zephyrproject.org

Thanks for your attention!