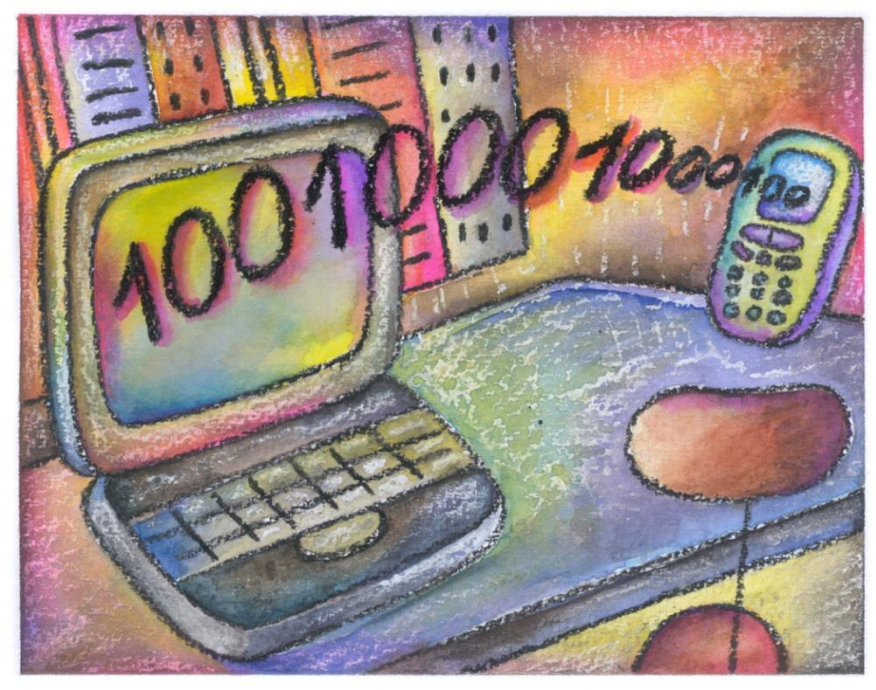
Wireless Technology Applications

Bluetooth Technology Part I

Melvyn U Myint Oo
T16620
68790688
eumoo@sp.edu.sg



At the end of this lecture, you should be able to:

Explain Bluetooth technology

1. WPAN
2. Bluetooth Network
3. Bluetooth Protocol Stack
4. Bluetooth RF Layer
5. Bluetooth Baseband Layer
6. Structure of Bluetooth Packets/Frames

WPAN

- IEEE 802.15 Working Group for Wireless Personal Area Networks (PANs) was formed to develop standards for short range wireless PANs (WPANS).
- PAN is a communications network within a small area in which all the devices on the network are typically owned by one person or perhaps a family.

WPAN

- Devices on the PAN may include portable or mobile devices.
- Such as:
  - Personal Computers
  - Personal Digital Assistants (PDAs),
  - Peripherals,
  - Cell phones
  - Consumer Electronic Devices

WPAN

- Two types of WPAN technology will be discussed in this chapter
  1. Bluetooth
  2. Ultra Wideband (not to be covered)
  3. ZigBee low power wireless sensor network (Independent learning)

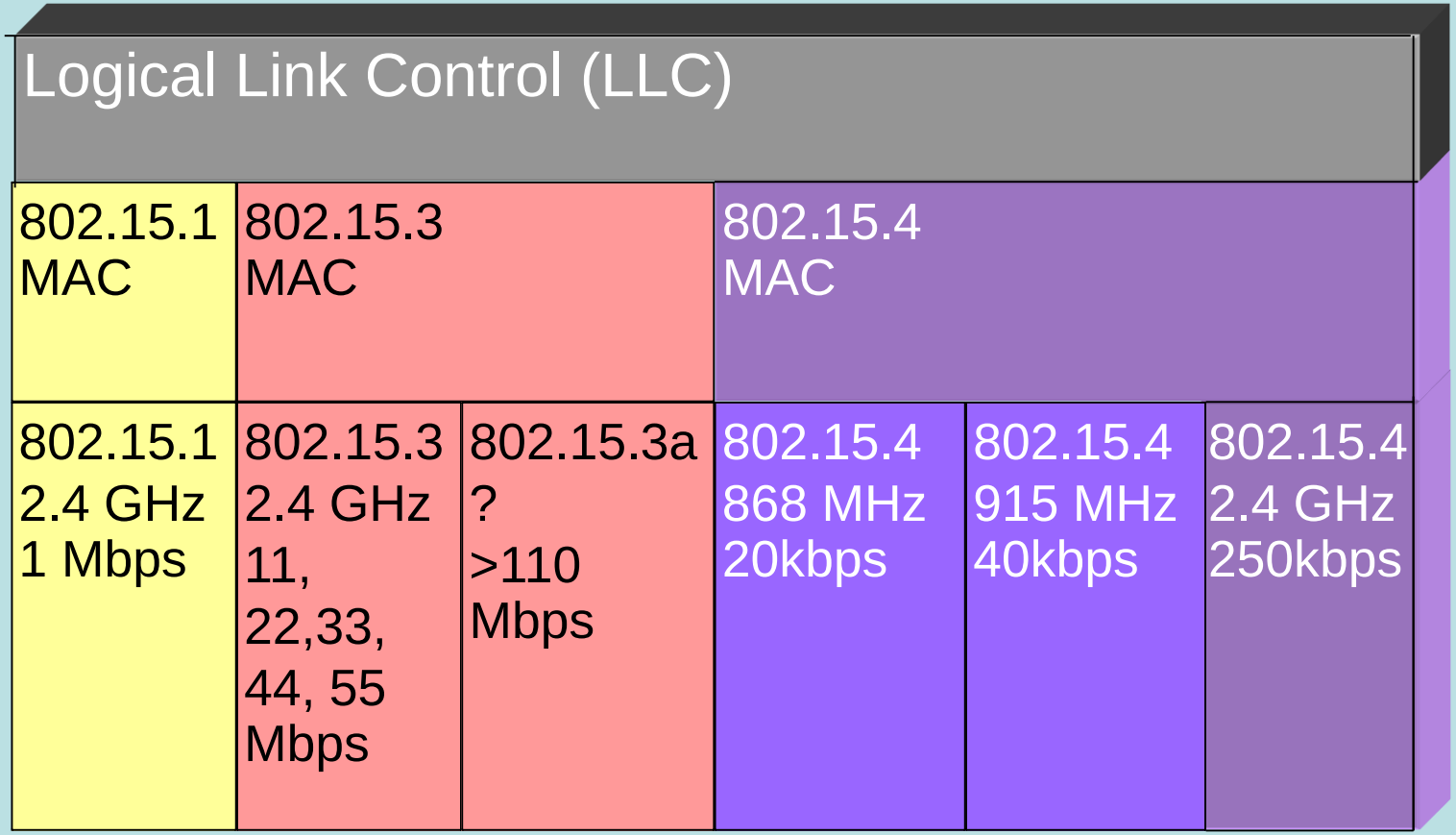


Figure 4.1 IEEE 802.15 Protocol Architecture

Extract from Wireless Communications & Networks / William Stallings/ 2nd Edition

Introduction

- Bluetooth Technology
  - Bluetooth SIG (Special Interest Group) is formed in May 1998
  - Bluetooth Specification based on IEEE 802.15.1 was release in July 1999.
  - Final approval on March 2, 2002

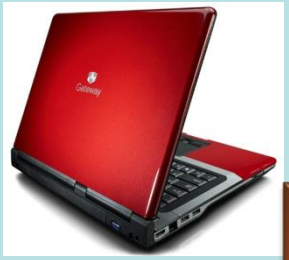
Main Function

- To replace the communication cables connecting devices

Bluetooth Devices

Two ways to enable Bluetooth in a device

Built-in,
e.g. mobile phone, laptop



Plug-in,
e.g. usb bluetooth dongle

Devices with Bluetooth connectivity are called **Bluetooth-enabled** devices

Master/Slave

- How are two Bluetooth-enabled devices connected?
- When one initiates and the other accepts the connection
- Initiator – Master
- Receptor – Slave

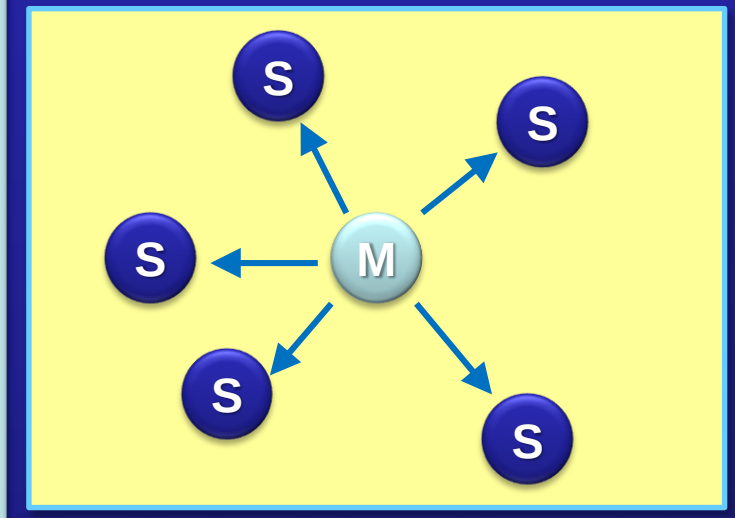
Master/Slave

- One master & one slave – point-to-point connection
- One master to more than one slave – point-to-multipoint connection
- Up to seven active slaves
- Up to 255 parked (inactive) slaves

Piconet/Scatternet

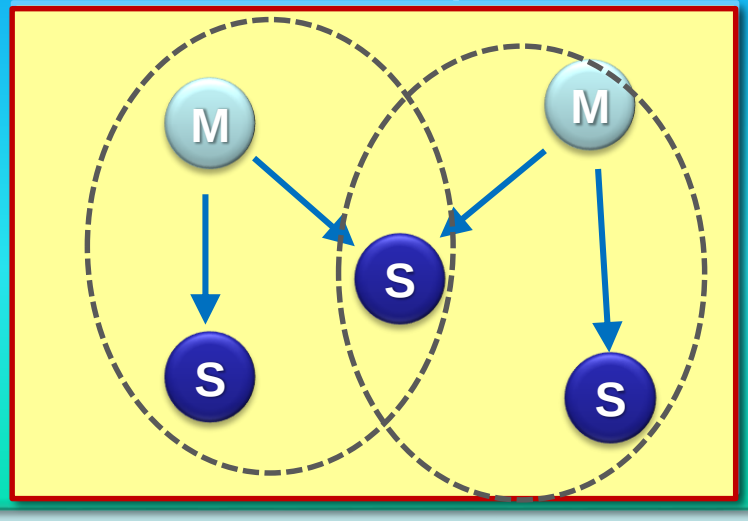
Piconet

- Network with 1 master and 1 to 7 slaves



Scatternet

- Two or more piconets
  - Master in one and slave in another
  - Slave in both piconets



Piconet/Scatternet

Example 4.1

- Is it possible to form a scatternet using a Bluetooth-enabled device that acts as a master on both piconets?
  - No, this is because the two piconets are actually one piconet since there must be one and only one master in each piconet.

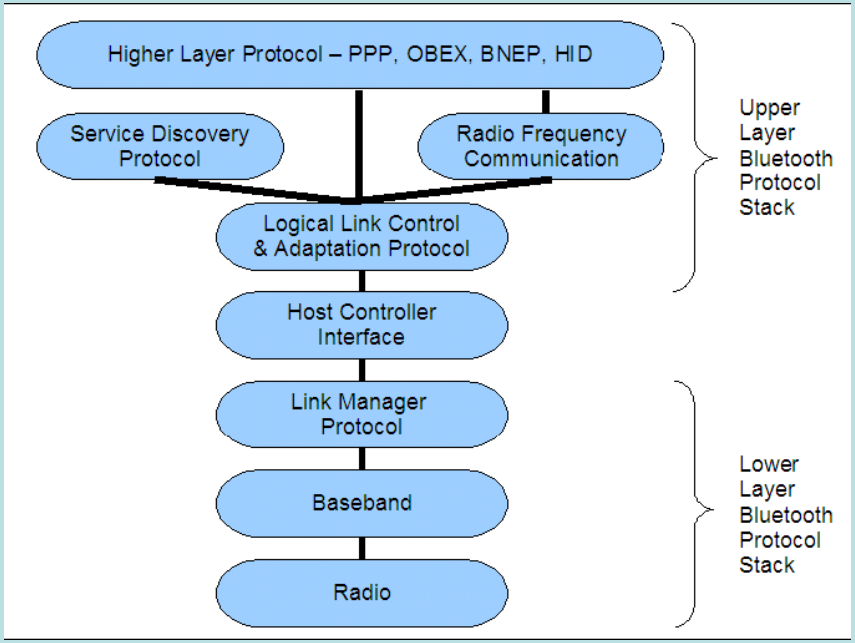
Piconet/Scatternet

Example 4.2

- Can an initiator become a slave in a piconet?
  - Yes, this happens when there is a request for master-slave switch.

Bluetooth Protocol Stack

- Lower layer is implemented in the Bluetooth chipset.
- Upper layer is implemented either in the operating system or in the Bluetooth chipset.
- Higher layer protocols are implemented in software.



Bluetooth RF Layer

Bluetooth Radio

- Three different Bluetooth class based on the maximum transmit power.

Power class	Maximum output power	Minimum output power	Power control
I	100mW (20dBm)	1mW (0dBm)	Mandatory: 4dBm to 20dBm Optional: -30dBm to 4dBm
II	2.5mW (4dBm)	0.25mW (-6dBm)	Optional: -30dBm to 4dBm
III	1mW (0dBm)	-	Optional: -30dBm to 4dBm

- Power in dBm=10×log (Power in mW)

Transmit Power

Example 4.3

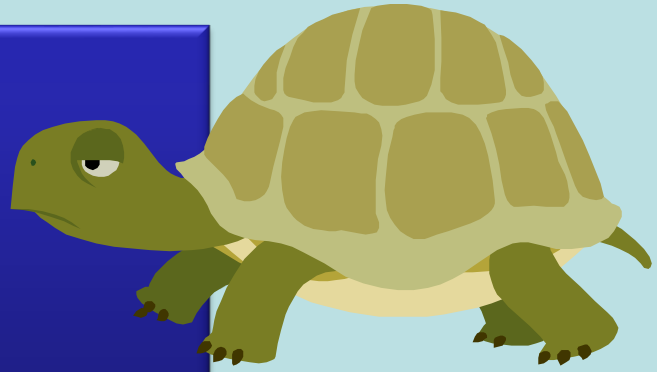
- What is the recommended power class for Bluetooth headset?
  - Bluetooth headset is used to connect a Bluetooth-enabled mobilephone to the hearer's ear, which is typically not more than 2 meters. Also, to conserve battery power, a Class III device is recommended.

Bit rate

Symbol period, T_S = 1 µs
Bit rate = symbol rate × $1/T_S$

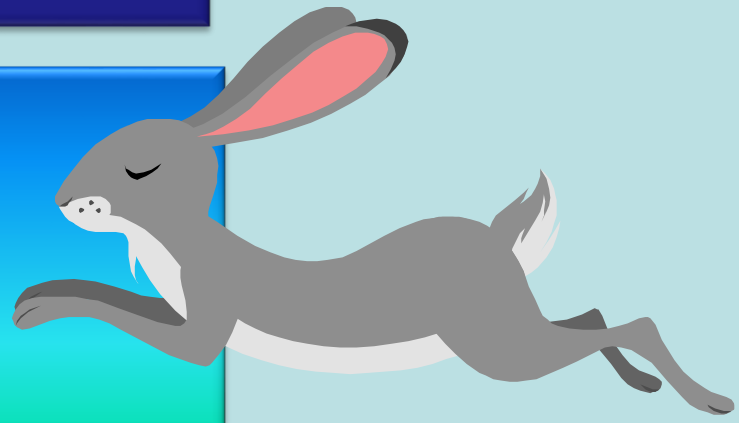
Before Bluetooth 2.0

- Modulation: GFSK
  - Symbol rate = 1 bit/symbol
- Bit Rate = 1 x 1 = 1 Mbps



Bluetooth 2.0
[Enhanced Data Rate (EDR)]

- Modulation: 8-PSK
  - Symbol rate = 3 bit/symbol
- Bit Rate = 3 x 1 = 3 Mbps



Bit Rate

- Example
- How many bits/symbol is being used in 8-PSK modulation?
  - The symbol rate for GFSK modulation and 8-PSK modulation is the same at 1 Mbaud. Therefore, to increase the bit rate from 1 Mbps to 3 Mbps, the number of bits/symbol for 8-PSK modulation has to be 3.

Modulation Technique

Version 1.1, 1.2

- modulation type: G2FSK
- symbol rate: 1 MHz
- modulation index: 0.28 – 0.35
- max. frequency deviation: 140 – 175 kHz
- baseband filter: Gauss, B*T = 0.5

Frequency

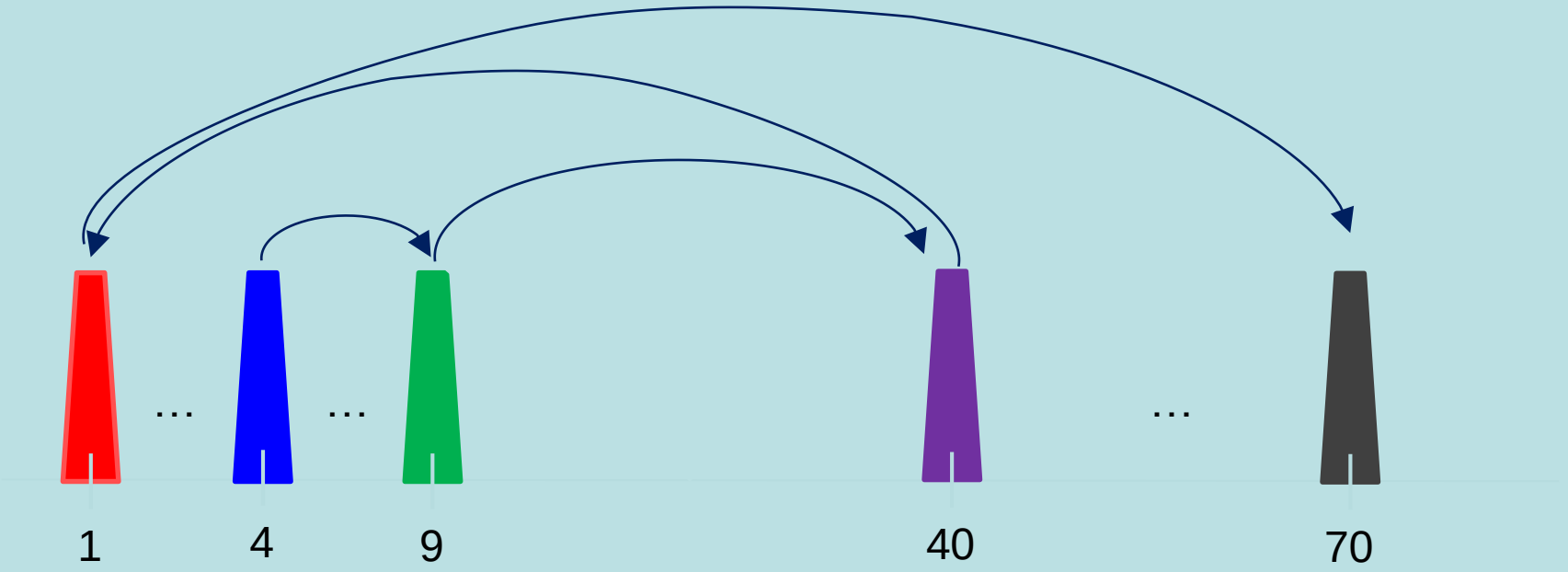
- Bluetooth uses **Frequency Hopping Spread Spectrum, 1600 hops/sec**
- Carrier frequency changed for every packet transmit
- 79 channels from 2.402 GHz to 2.480 GHz
- Each channel has bandwidth of 1 MHz
  - Channel 0 = 2.402 GHz, Channel 1 = 2.403 GHz, Channel 2 = 2.404 GHz, and so on…
- 2.4 GHz ISM band is licensed-free band

Frequency

- Adaptive Frequency Hopping (AFH) is introduced in Version 1.2 to mark out noisy channels and allocate clean channels
- Improved inter-operability with IEEE 802.11b/g
- FCC requires at least 20 channels for FHSS.

FHSS Example

- Hopping Pattern: Channels 4, 9, 40, 1, 70, …



Channel Number

- Question
  - What is the frequency for frequency channel 42?

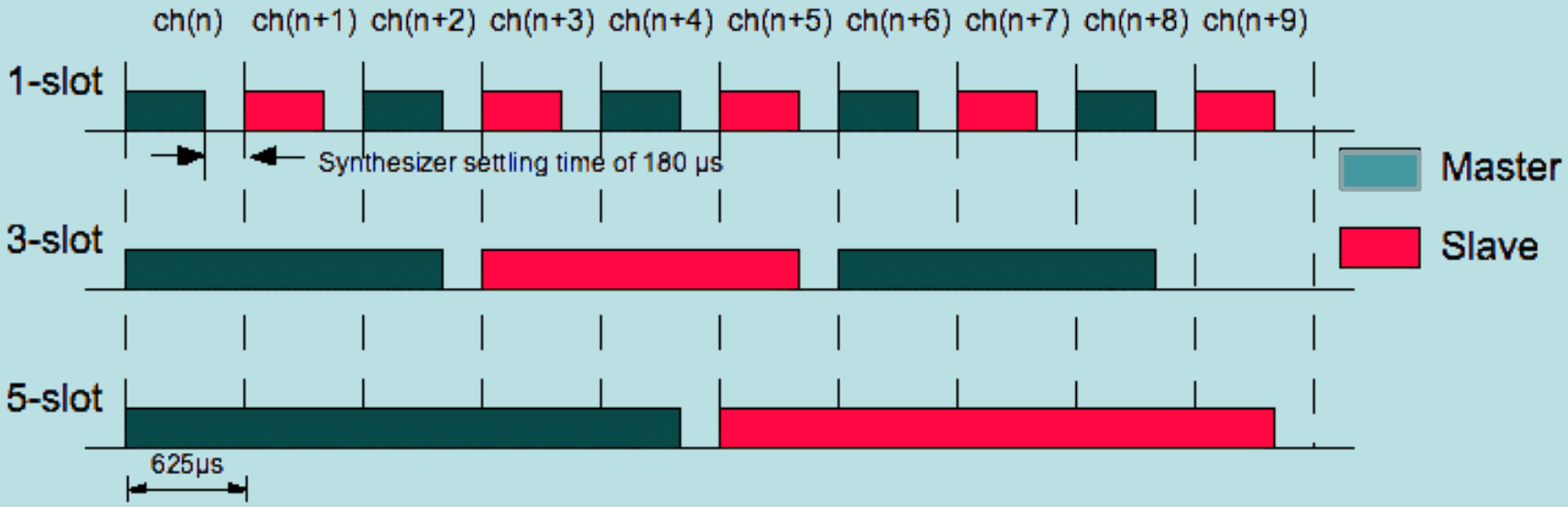
Equation 4.2

$$f_c = (2402 + n)\ \text{MHz},\ n = 0, 1, \ldots, 78$$

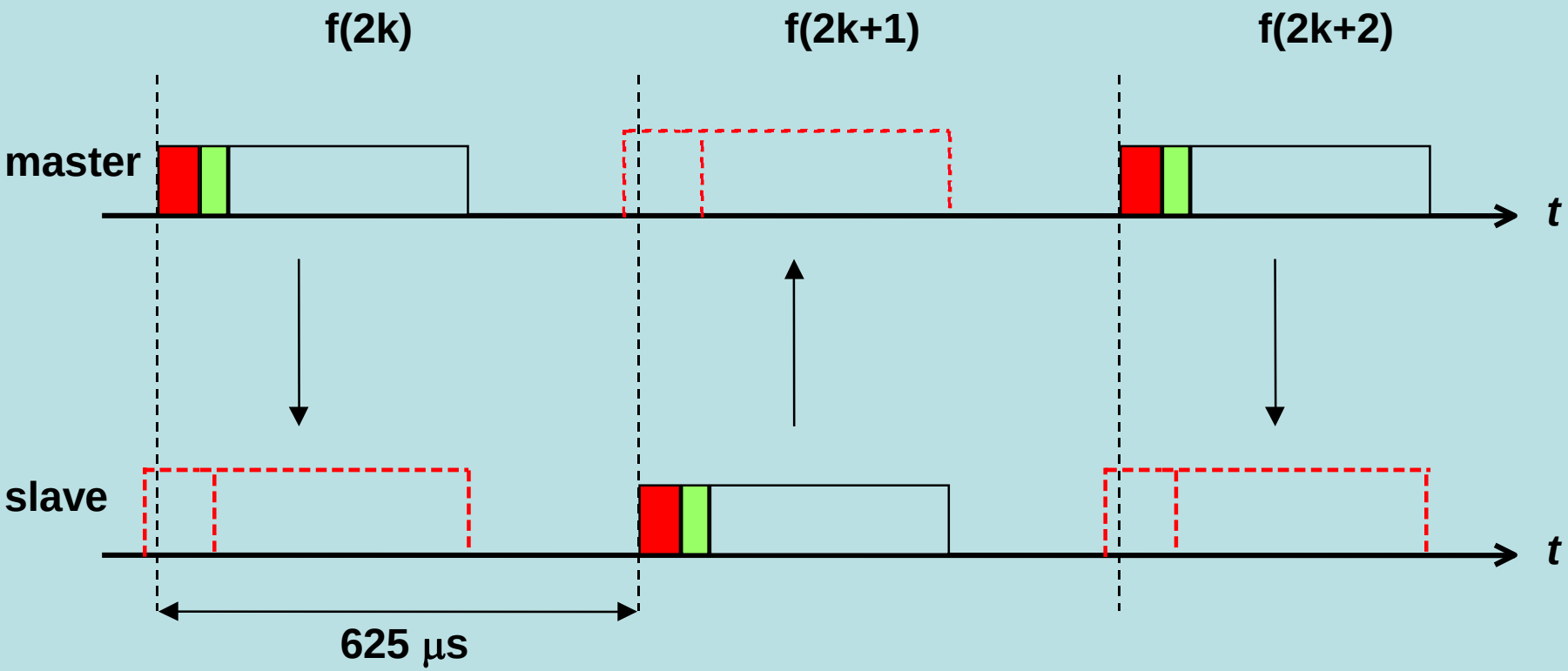
- Answer
  - The frequency is $f_c = (2402 + 42)$ MHz
    $= 2444$ MHz
    $= 2.444$ GHz

Time Division Duplexing

- Time is divided into time slots
- One time slot lasts for **625µs**

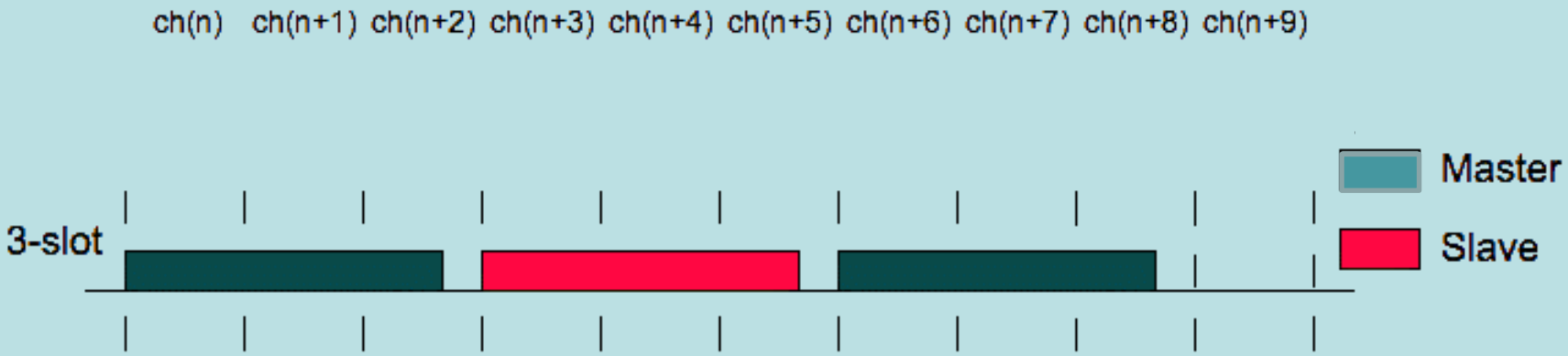


FH/TDD Channel



Time Division Duplexing

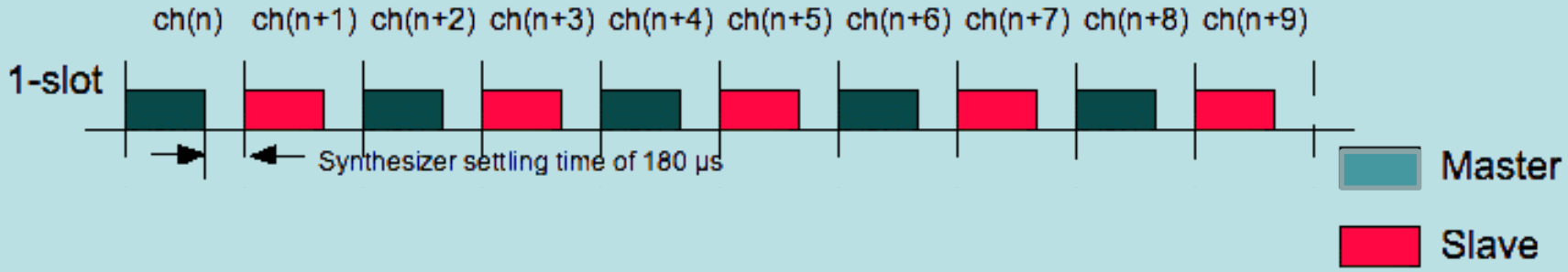
- Time is divided into time slots
- One time slot is **625µs**



- Three different packet length – **1**-slot, **3**-slot

Time Division Duplexing

- Time is divided into time slots
- One time slot is **625µs**

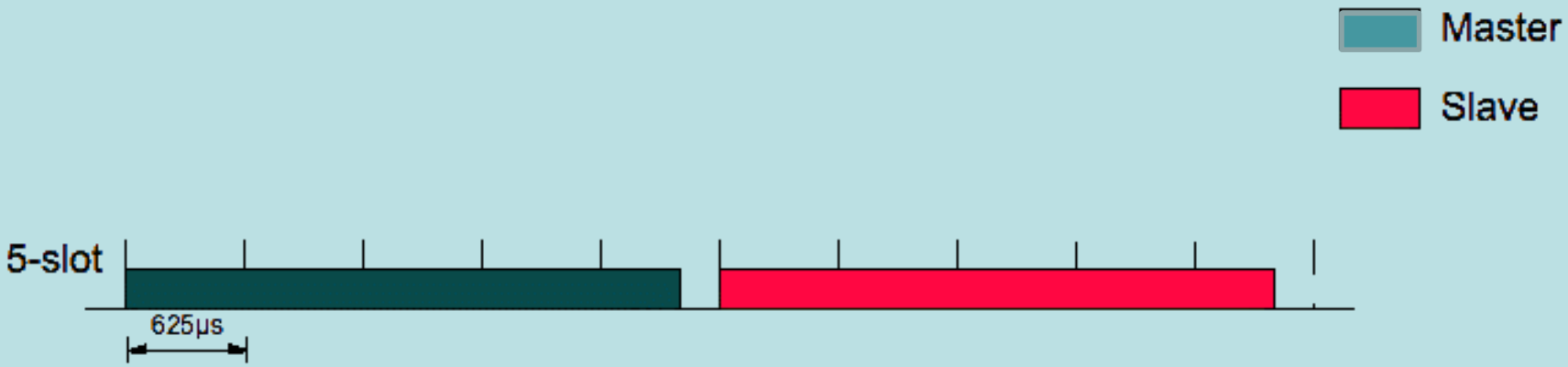


- Three different packet length – **1**-slot

Time Division Duplexing

- Time is divided into time slots
- One time slot is **625µs**

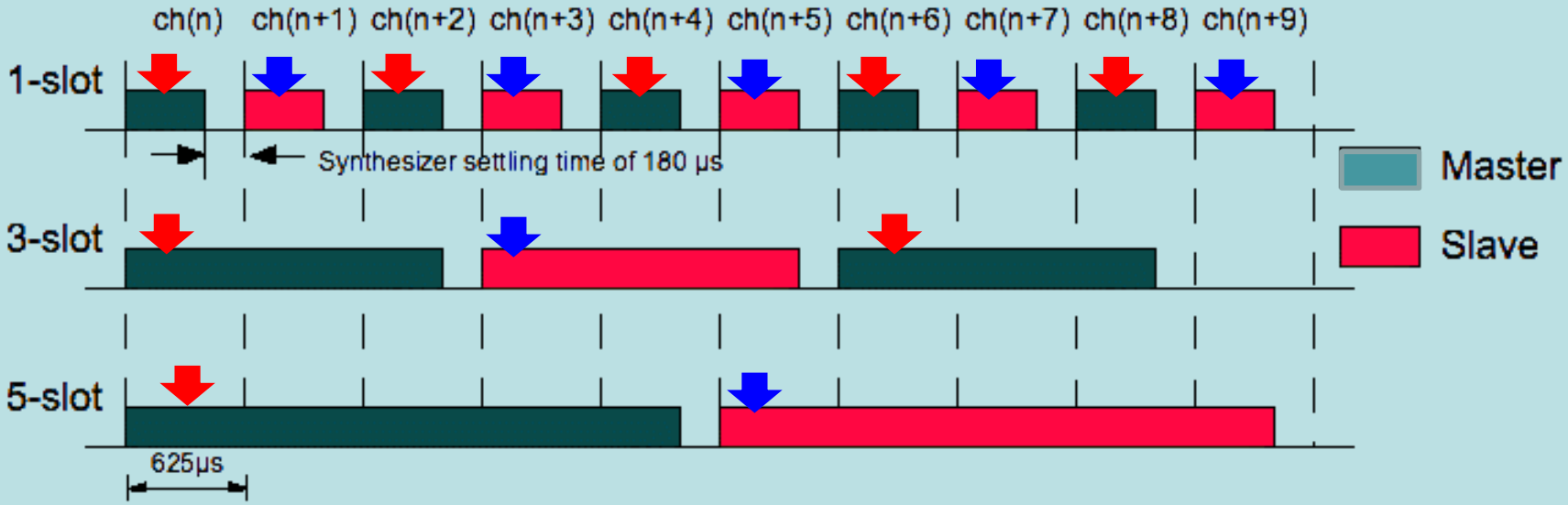
ch(n) ch(n+1) ch(n+2) ch(n+3) ch(n+4) ch(n+5) ch(n+6) ch(n+7) ch(n+8) ch(n+9)



- Three different packet length – **1**-slot, **3**-slot and **5**-slot

Time Division Duplexing

- Time is divided into time slots
- One time slot is **625µs**



- Three different packet length – **1**-slot, **3**-slot and **5**-slot
  - Master starts its transmission in **even** slots
  - Slave starts its transmission in **odd** slots

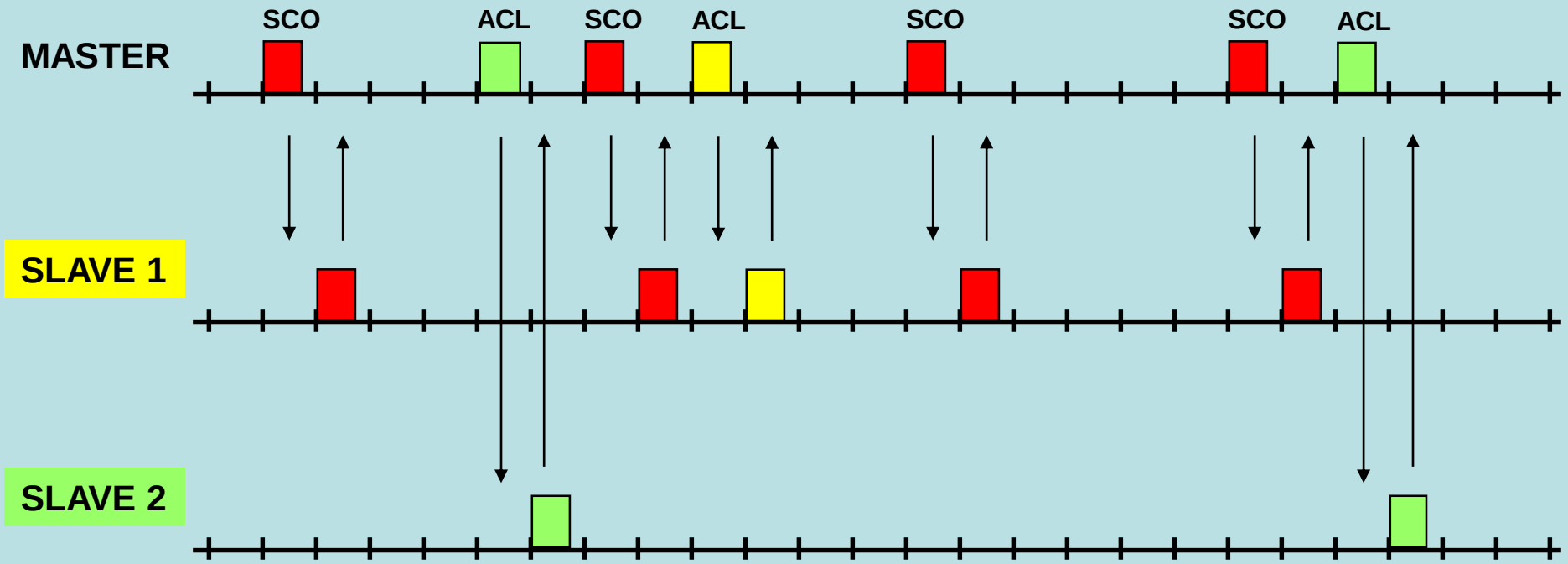
Base Band Layer

- Manages physical channels and links,
- handles packets
- does paging and inquiry to locate other Bluetooth devices in the area

Links between Bluetooth Devices

- A synchronous connection-oriented (SCO) link
  - a symmetric point-to-point link between a master and a single slave in the piconet
  - like a circuit switched link by using reserved time slots at fixed intervals
  - support up to **three** simultaneous SCO links
  - voice transmissions at a speed of 64 kbps.
- An asynchronous connectionless (ACL) link
  - a packet-switched link that is used for data transmissions
  - a point-to-multipoint link
  - single ACL link between one master and up to seven slaves
  - The time slots not reserved for the ACL links

Mixed Link Example



- SCO: Synchronous Connection-Oriented link
  - point to point between master and a single slave
    - **uses reserved time slots**
    - **can be considered as a circuit switched connection**
    - **mainly used for voice**

- ACL: Asynchronous Connection-Less link
  - point-to-multipoint between master and all slaves
    - **uses remaining time slots**
    - **packet switched connection**
    - **used for data**

Links between Bluetooth Devices

- Extended synchronous connection-oriented (eSCO) link
  - Introduced in Bluetooth version 1.2
  - to provide audio transmission with a high degree of QoS
  - to perform error detection for speech transmission work
  - the timely provision of voice data retransmissions

Bluetooth Address

- Unique 48 bit
- Divided into three sections
  - Non-significant Address Part (NAP): 16 bits
  - Upper Address Part (UAP): 8 bits
  - Lower Address Part (LAP): 24 bits

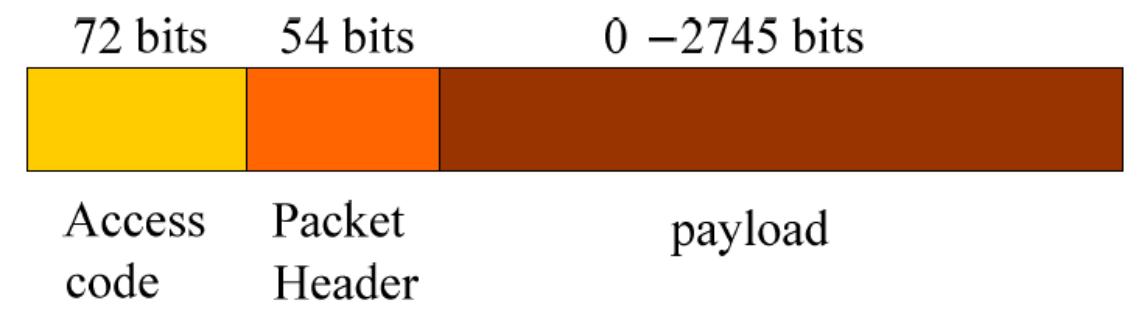
NAP UAP LAP

Bluetooth Device Address: ACDE 48 000080 (12 Digit Address, Hex. notation)

Bluetooth Frames

Each frame contains three parts:

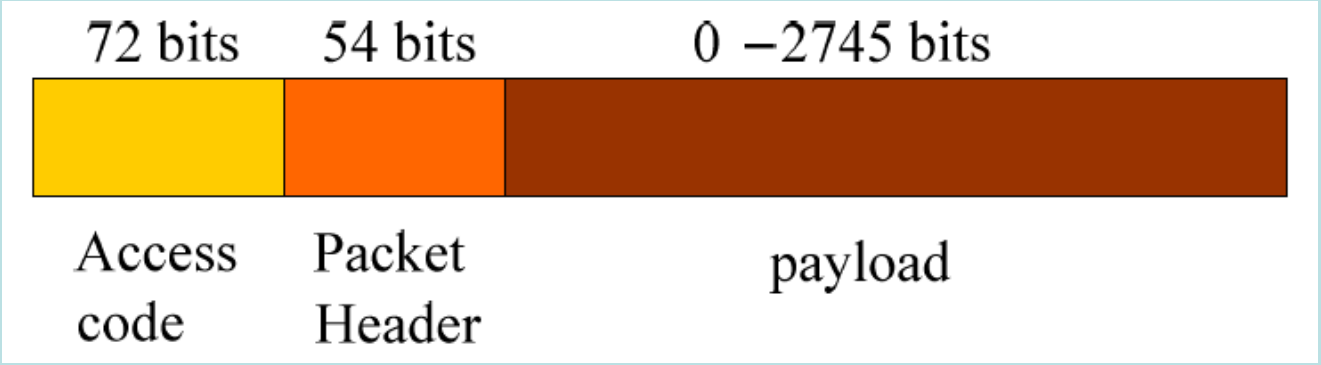
- Access code (72 bits)
  - Contains data used for timing synchronization, paging and inquiry
- Header (54 bits)
  - Contains information for packet acknowledgment, packet numbering, the slave address, the type of payload, and error checking



Bluetooth Frames

Each frame contains three parts:

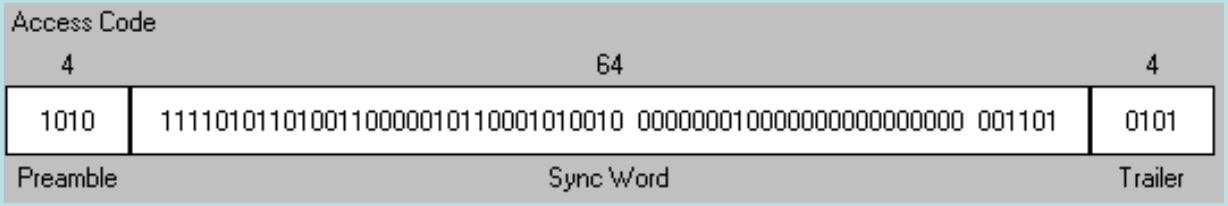
- Payload (0-2745 bits)
  - Can contain data, voice, or both

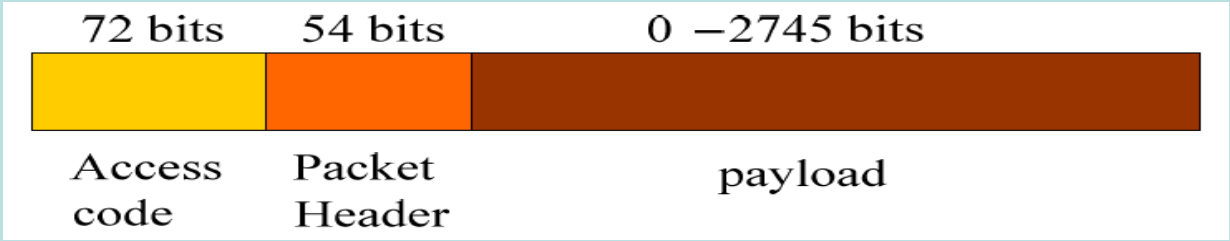


Bluetooth Frames

Access code:

- calculated from the LAP of the Bluetooth Device Address
- The Preamble and Trailer depend on the leftmost and rightmost bit of the Sync Word
- Sync Word is displayed in such a manner that the original LAP can still be seen in the middle of the word

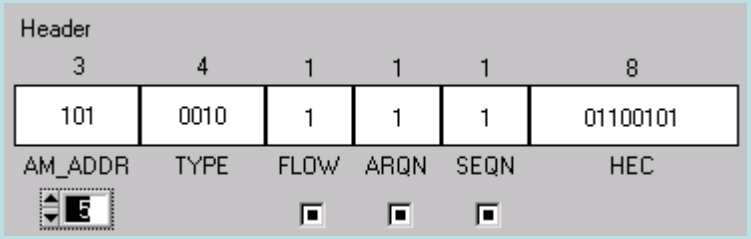


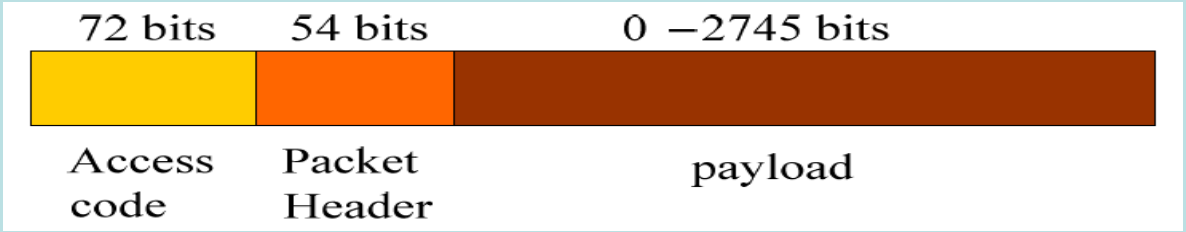


Bluetooth Frames

Packet header:

- consists of 6 parts
  - the AM address field
  - the packet type information field
  - bits for flow control
  - acknowledge
  - packet sequence number
  - the HEC (Header Error Correction) and
  - a Cyclic Redundancy (CRC) Check for checking the header for errors at the receiver

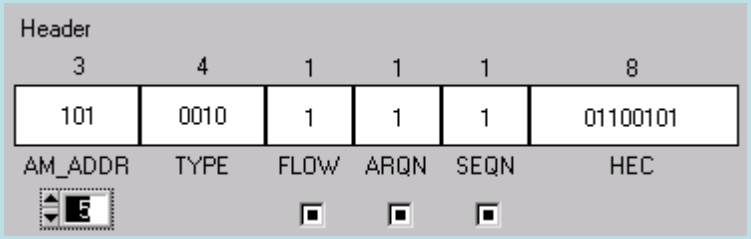




Bluetooth Frames

Packet header:

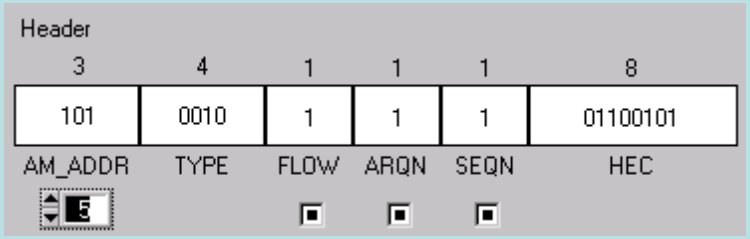
- AM_ADDR: The Active Member Address specifies the addressed slave in a piconet.
- TYPE: The packet's type code. Page 54 of the Bluetooth 1.1 specification shows a table with the defined type code numbers.
- FLOW: The flow control bit for the master's receiver queue. Shall be set to 1 when the slave is intended to keep on sending packets.
- AQRN: Acknowledge bit for received packets. Shall be set to 1 if the last packet has been received without detected errors.



Bluetooth Frames

Packet header:

- SEQN: Sequence number of the packet. In a real life scenario this bit is being alternated between sent packets, as long as no packet needs to be retransmitted. If it is necessary to retransmit a packet, the new copy gets the same number as the originally sent one.
- HEC: The Header Error Correction.
- the HEC code is calculated from the other 5 field settings
- The complete 18 header bits get a simple 1/3 Forward Error Correction (FEC), every bit is transmitted three times.
- Whitening is applied before the FEC.



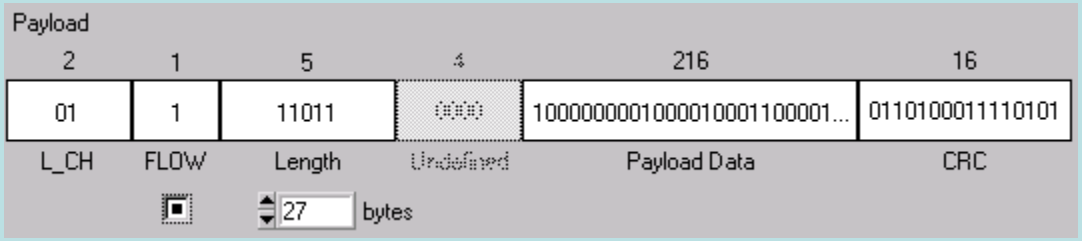
Bluetooth Frames

Payload:

- consists of a payload header, the payload data and a CRC part

payload header:

- the L_CH information field, an additional flow control bit and a 5 respectively 9 bit long length field
- Data High (DH3) and DH5 packets also include an undefined field.
- For DH1 and AUX1 packets instead this field is greyed out.



Bluetooth Frames

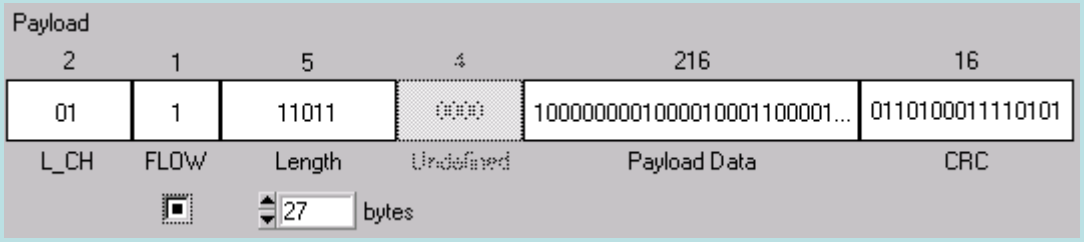
Payload:

L_CH:

- The L_CH code is used for identifying the logical channels.
- Code 01 (LSB left) identifies a starting L2CAP message
- Code 10 (LSB left) identifies a continued message part

FLOW:

- The flow control bit is used at the L2CAP level to control the information flow independently for every logical channel

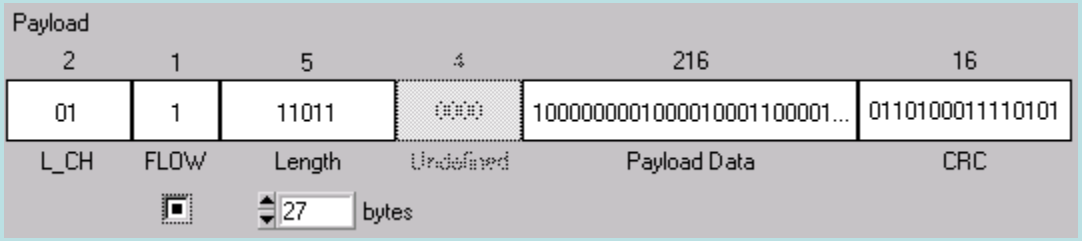


Bluetooth Frames

Payload:

Length:

- The Length information field describes the number of transmitted information octets (8 bit) in the Payload Data field (payload header and CRC are excluded).
- The length information can either take up 5 bits of header space for DH1 and AUX1 packets or 9 bits for DH3 and DH5 packets
- Undefined:
- This field is only present in DH3 or DH5 packets. All 4 bits are set to 0



Bluetooth Frames

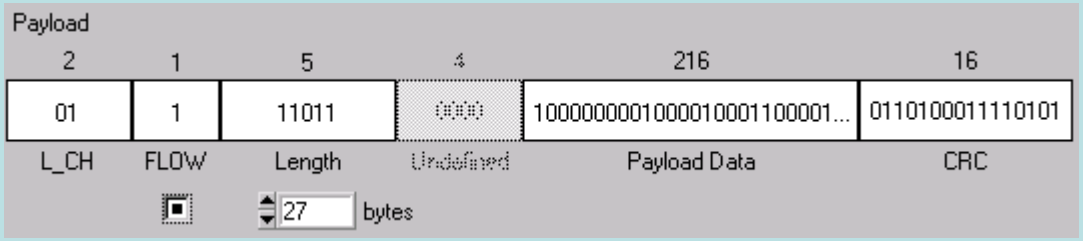
Payload:

Payload Data:

- The content of the actual data field can be filled either by a PRBS of different type, an entered pattern, all 0 or all 1 or the payload data field can be filled with a user defined file.

CRC:

- A 16 bit CRC protecting the whole payload field and making error detection possible. This CRC is not used in the AUX1 packets.



Abbreviation

- DUN – Dial Up Networking
- OBEX – Object Exchange
- HID – Human Interface Device
- NAP – Non-significant Address Part
- UAP – Upper Address Part
- LAP – Lower Address Part
- TDD – Time Division Duplexing
- CLKN – Native Clock
- GFSK – Gaussian Frequency Shift Keying
- PSK – Phase Shift Keying
- EDR – Enhance Data Rate
- AFH – Adaptive Frequency Hopping
- FHS – Frequency Hopping Synchronisation
- ACL – Asynchronous Connectionless
- SCO – Synchronous Connection Oriented
- e-SCO – Extended Synchronous Connection Oriented

Abbreviation

- CAC – Channel Access Code
- DAC – Device Access Code
- GIAC – Generic Inquiry Access Code
- DIAC – Dedicated Inquiry Access Code
- LIAC – Limited Inquiry Access Code
- LT-ADDR – Logical Transport Address
- ARQN – Automatic Request Number
- SEQN – Sequence Number
- HEC – Header Error Check
- FEC – Forward Error Correction
- DM – Data Medium
- DH – Data High
- CRC – Cyclic Redundancy Check
- PCM – Pulse Code Modulation
- ACK – Acknowledge
- NAK – Negative Acknowledge
- LLID – Logical Link Indication
- L2CAP – Logical Link and Control Adaptation Protocol

Abbreviation

- LMP – Link Manager Protocol
- SD – Secure Digital
- UART – Universal Asynchronous Receiver and Transmitter
- PSM – Protocol Service Multiplexer
- SCID – Source Channel Identifier
- SDP – Service Discovery Protocol
- RFCOMM – Radio Frequency Communication
- DCID – Destination Channel Identifier
- MTU – Maximum Transmission Unit
- MSC – Modem Status Command
- RPN – Remote Port Negotiation
- RLS – Remote Line Status
- GAP – Generic Access Profile
- HFP – Hands-Free Profile
- SAP – SIM Access Profile
- GOEP - Generic Object Exchange Profile
- FTP – File Transfer Profile
- OPP – Object Push Profile
- SYNCH – Synchronization profile
- BPP – Basic Printing Profile
- A2DP – Advanced Audio Distribution Profile
- AVRCP – Audio/Video Remote Control Profile