Bluetooth Networks Architecture and Protocols

Saleh Al-Harthi

California Institute for Telecommunications
and Information Technology, Cal-(IT)^2

OUTLINE

- The Bluetooth Usage Models
- The General Bluetooth Architecture:
  - Range and Power
  - Network Topology: Piconets and Scatternets
  - The Bluetooth Protocol Stack: Core & Profile Protocols
- Bluetooth Basics and Core Protocols
  - High-level Architecture of a Bluetooth Module

Hardware/ firmware

  - Radio System (RS)
  - Link Controller and Baseband (BB)
  - Link Manager (LM) and Link Manager Protocol (LMP)

Software

  - Logical Link Control and Adaptation Protocol (L2CAP)

OUTLINE—(contin.)

- Host Controller Interface (HCI): when Bluetooth is added as a separate module (a card...)
- Service Discovery Protocol (SDP) (will not be covered in this presentation)

Credits and References

- This presentation is based mainly on:
  - The Core specification Book (v1.1): Bluetooth SIG web site (www.bluetooth.com)
  - Jaap Haartsen’s articles (originator): http://utep.el.utwente.nl/~haartsen/
  - The Book: “Bluetooth Revealed: The insider’s guide to an open specification for global wireless communications” by Brent A. Miller and Chatschik Bisdikian, 2001, Prentice-Hall

Some PANs Research Issues

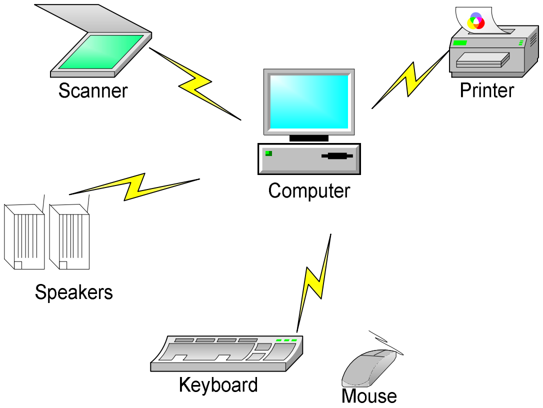
- Scheduling Internal and External traffic
- Energy efficiency and topology optimization (short range, battery powered devices)
- Special scenarios applications: e.g. “always best connected”
- Coexistence mechanisms (with other networks in unlicensed bands)

Bluetooth Usage Models

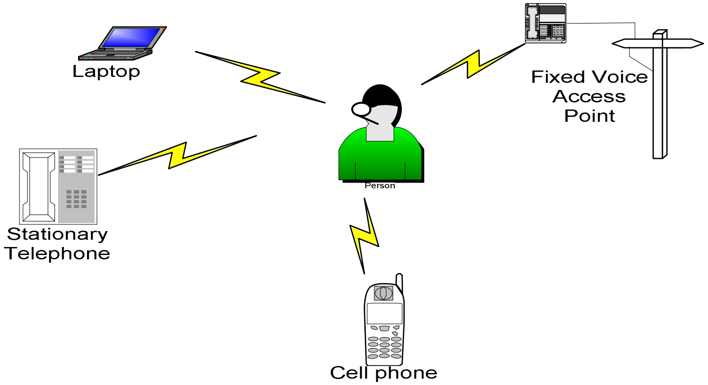
- The cordless computer
- The ultimate headset
- The Internet bridge
- The automatic synchronizer
- File transfer
- Three-in-one phone
- Others...

Bluetooth Usage Models

- The cordless computer

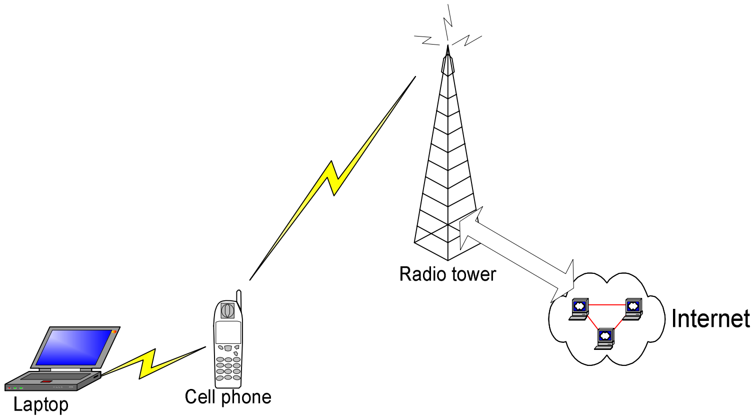


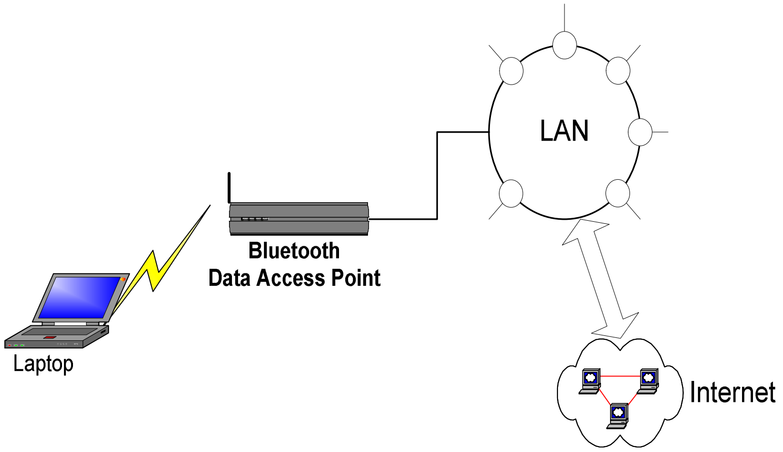
- The ultimate headset



Bluetooth Usage Models

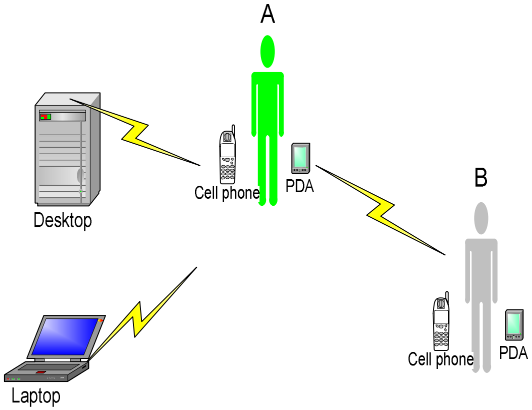
- The Internet bridge
  - Dial-up networking
  - Direct network access



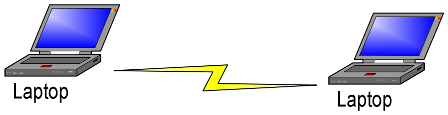


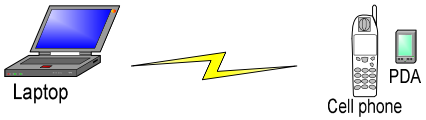
Bluetooth Usage Models

- The automatic synchronizer



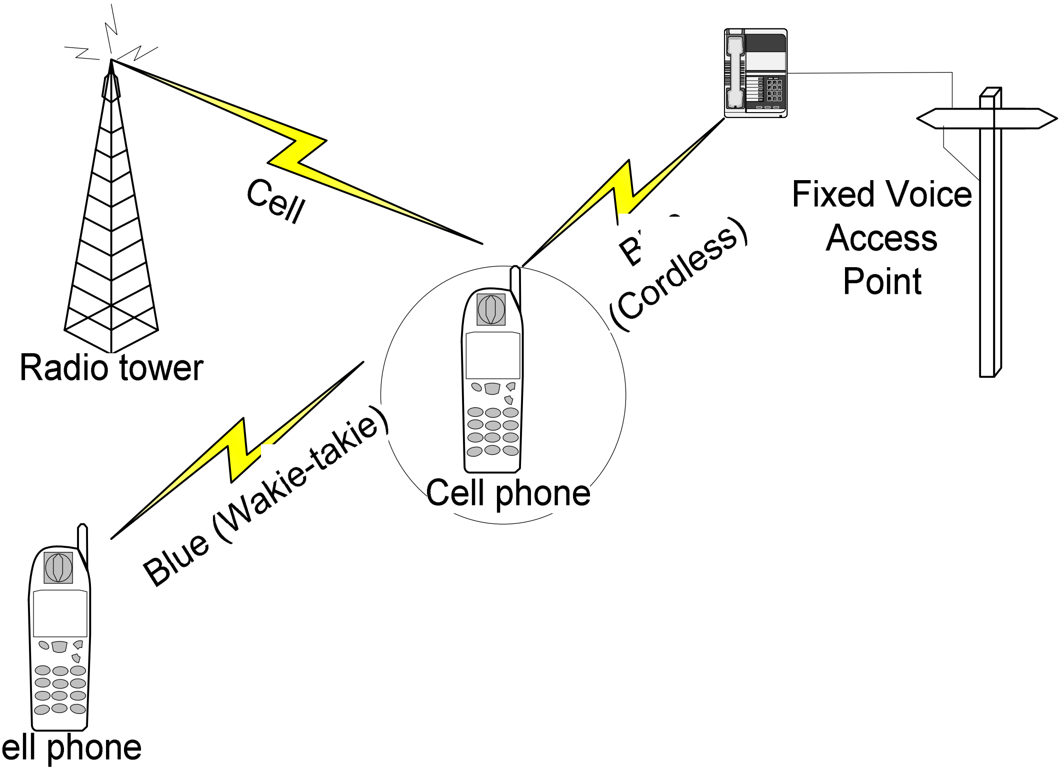
- File transfer





Bluetooth Usage Models

- Three-in-one phone



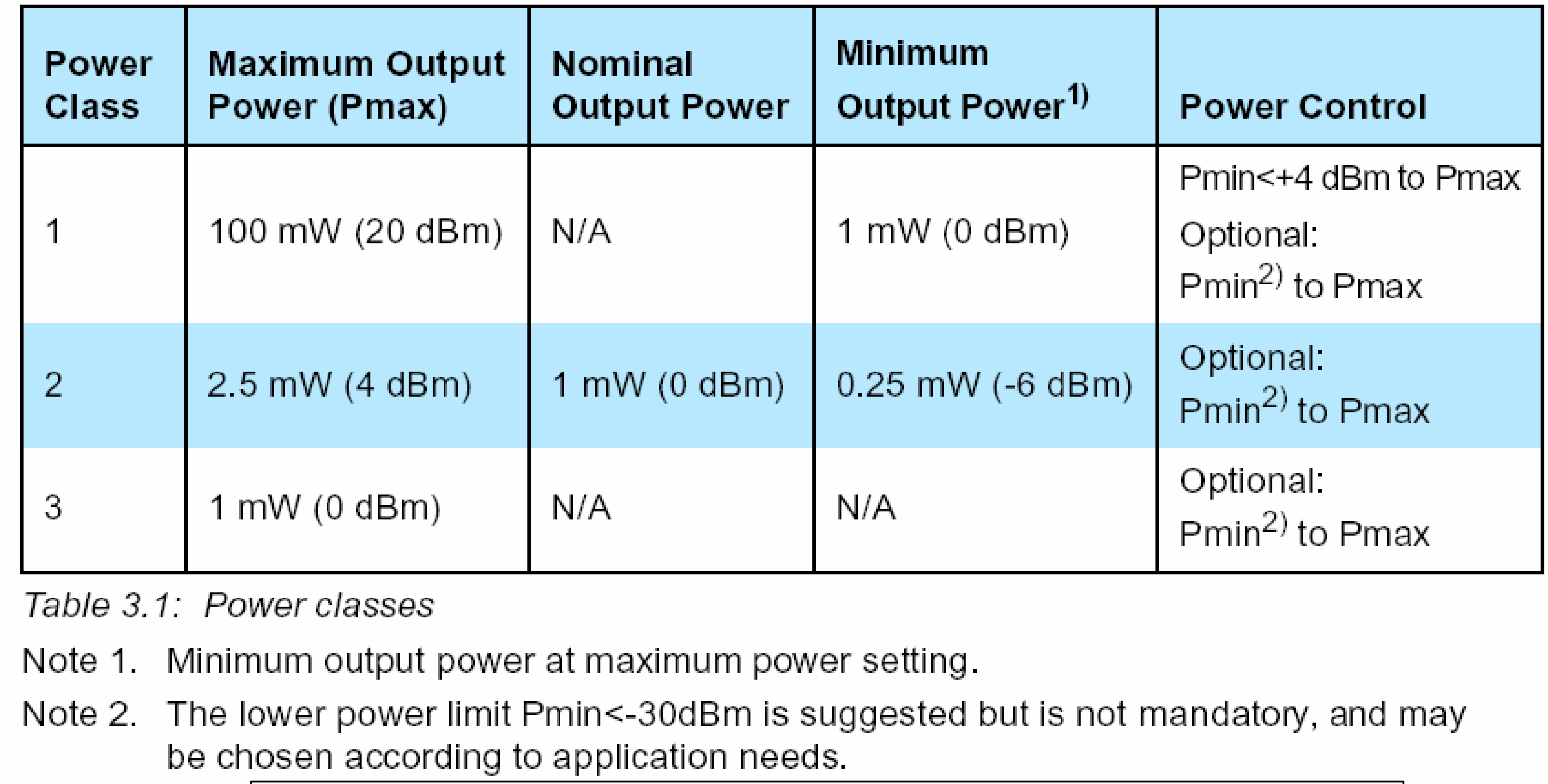
Architecture: Range and Power

Range:

~100m

~10m

~1m



Power Class	Maximum Output Power (Pmax)	Nominal Output Power	Minimum Output Power[1)]	Power Control
1	100 mW (20 dBm)	N/A	1 mW (0 dBm)	Pmin<+4 dBm to Pmax Optional: Pmin[2)] to Pmax
2	2.5 mW (4 dBm)	1 mW (0 dBm)	0.25 mW (-6 dBm)	Optional: Pmin[2)] to Pmax
3	1 mW (0 dBm)	N/A	N/A	Optional: Pmin[2)] to Pmax

Table 3.1: Power classes

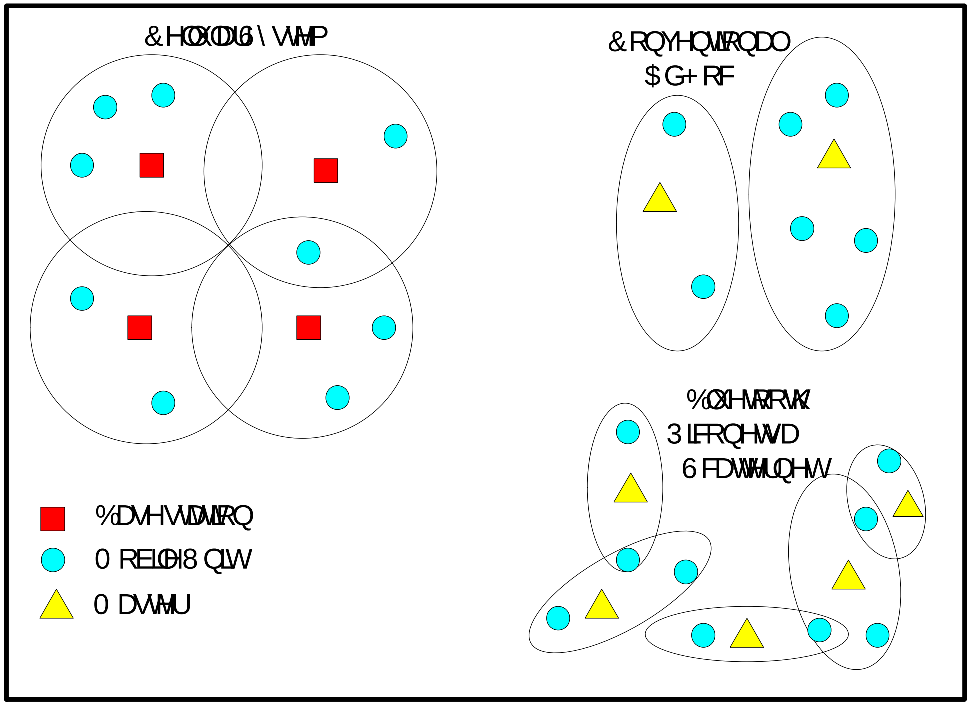
Note 1. Minimum output power at maximum power setting.

Note 2. The lower power limit Pmin<-30dBm is suggested but is not mandatory, and may be chosen according to application needs.

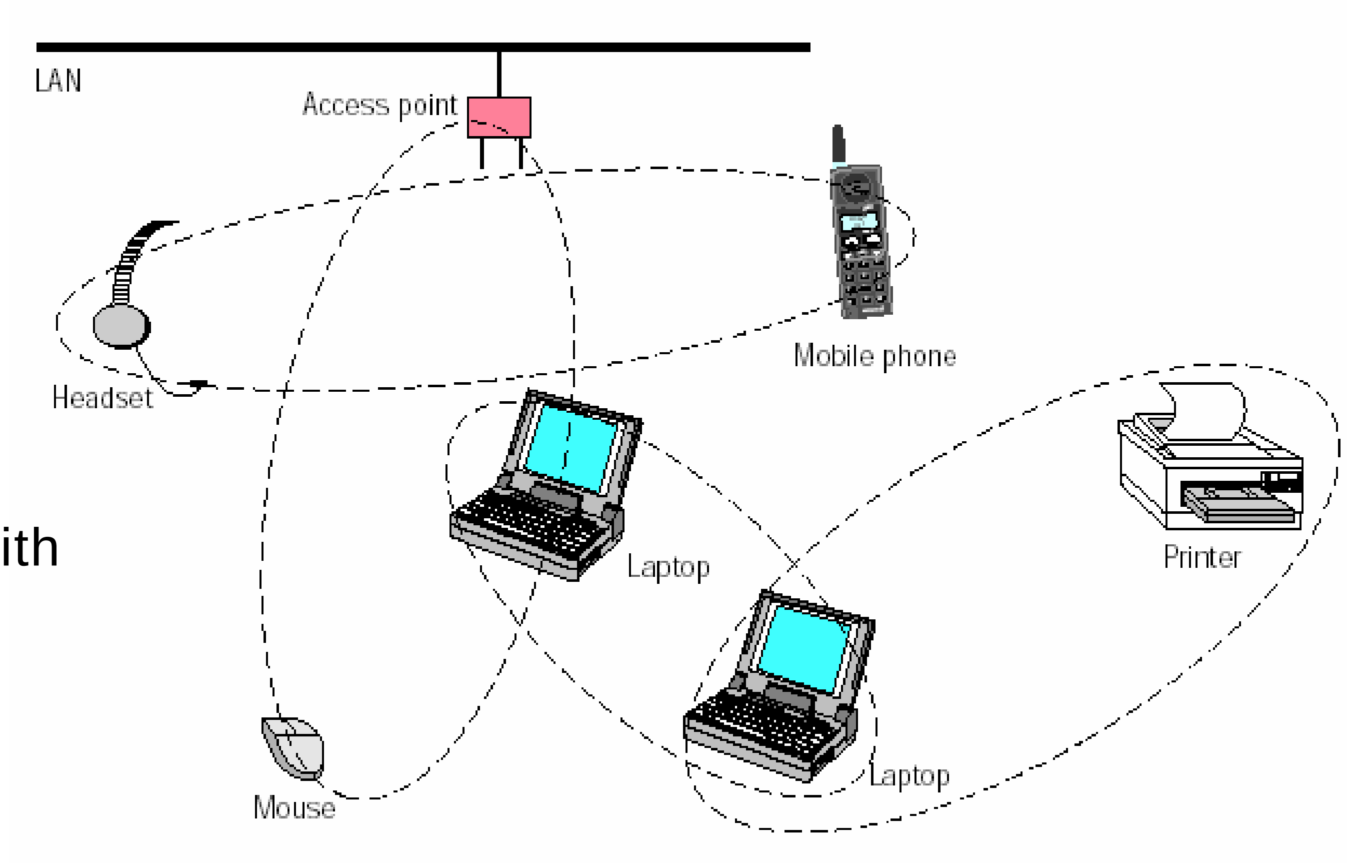
"Power control" is required for class 1 equipments, Class 1 must be able to control its transmit power down to 4dBm or less

Architecture: Topology: Piconets & Scatternets

- A Piconet: A master-slave Ad Hoc network: Must have exactly one “master” and could have up to max of 7 (active) “slaves”
- A Scatternet: Consists of two or more Piconets that are at least partially overlapped in time and space (interconnected)



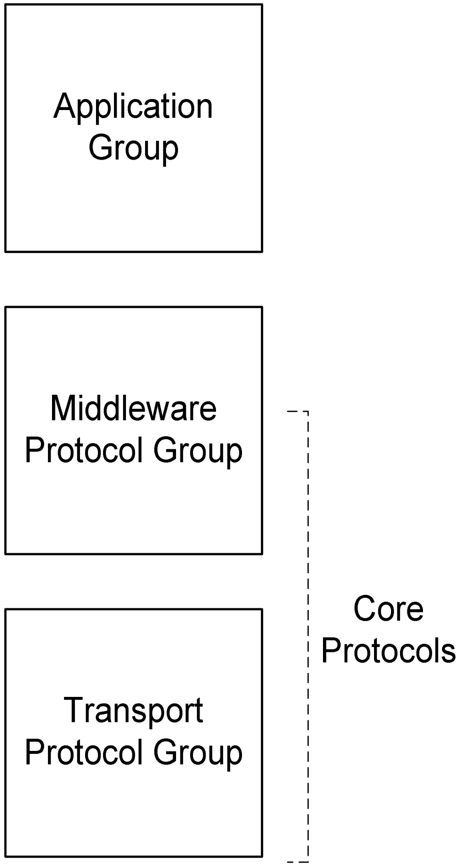
Architecture: Topology: Piconets & Scatternets



Example of
A scatternet with
four piconets

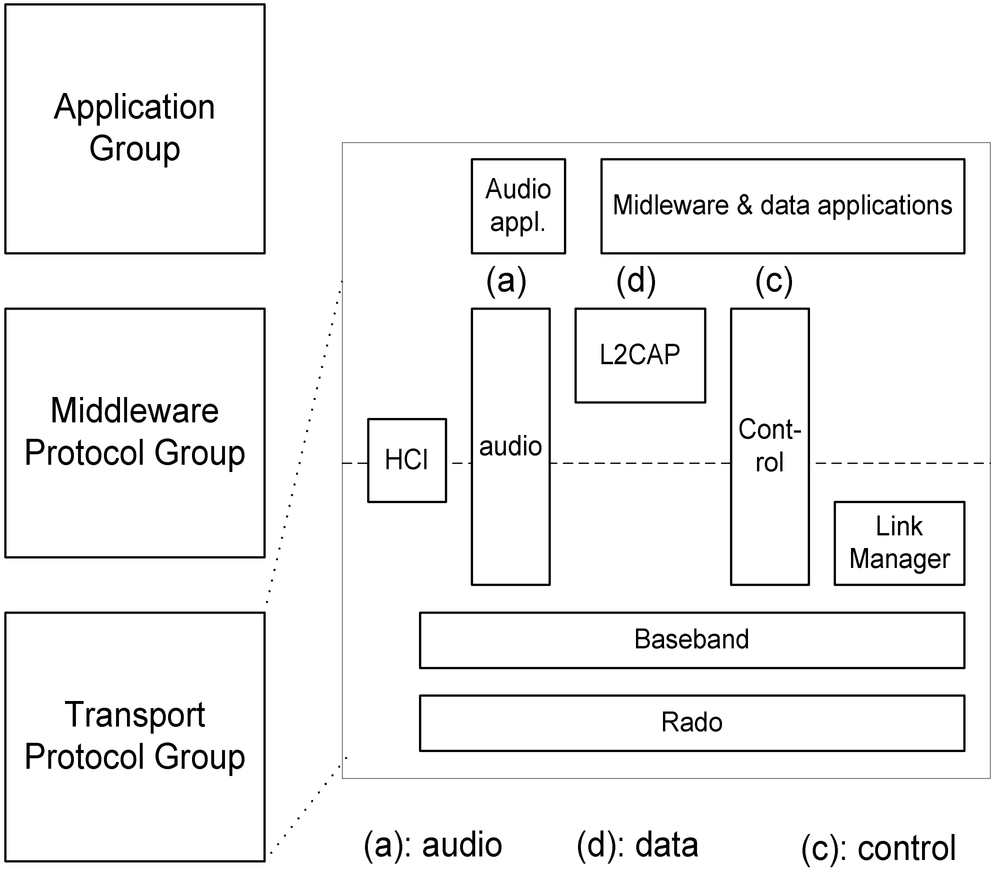
Architecture: Protocol Stack

- “Protocol stack” aimed to be general, flexible, as possible compatible with legacy protocols and applications (maxim re-use...)
- Most “Profiles” spring from usage models, however, some profiles are general
- “Profiles” can be considered “transport profiles” upon which “application profiles” can be built. They specify which protocol elements are mandatory in certain applications
- “Profiles” concept prevents devices with limited memory and processing power from implementing the entire Bluetooth stack



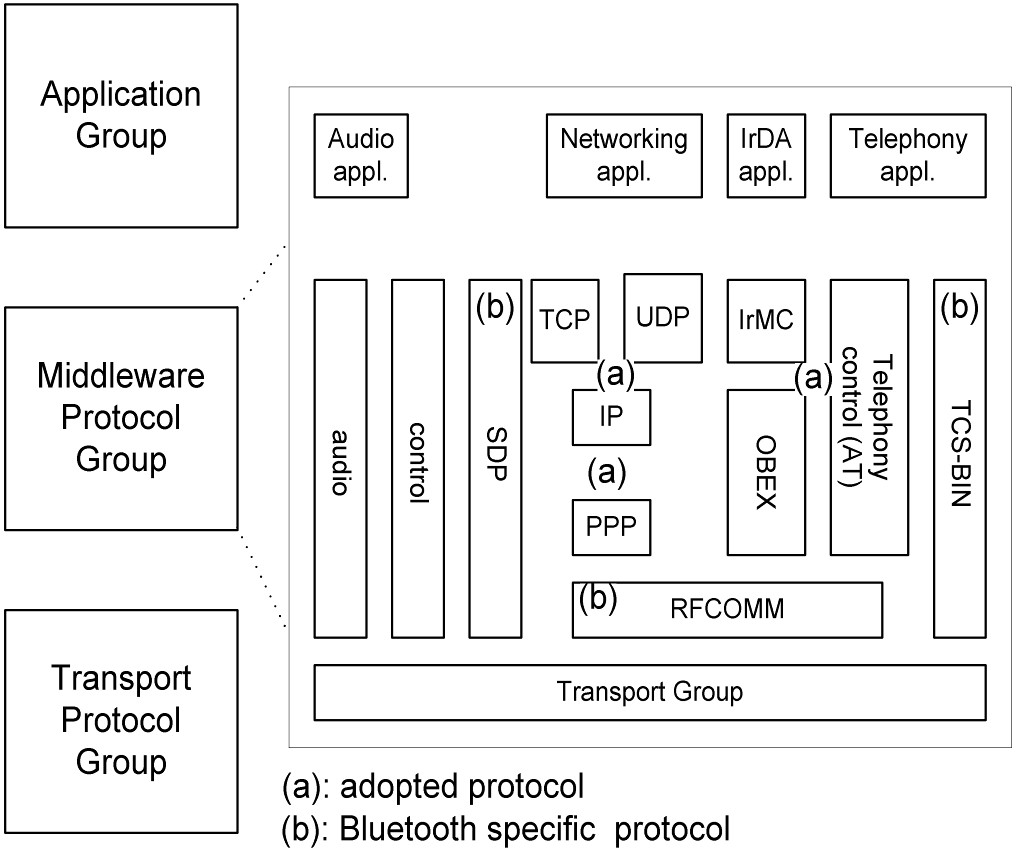
Architecture: Protocol Stack

- Transport protocols group:
  - Actually these protocols fit best within the "data link layer" and the "physical layer" of the OSI model
  - Think of them as to establish a raw bit-pipes between devices...



Architecture: Protocol Stack

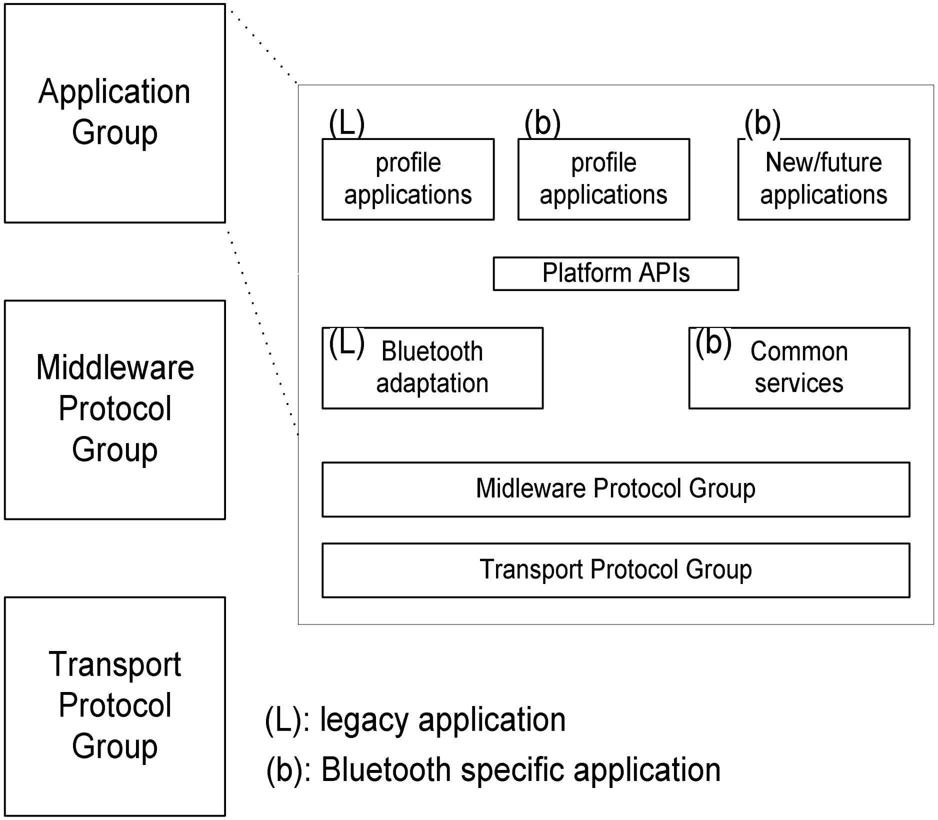
- Midleware protocols group:
  - Present to the application layers a standard interfaces that allow applications to use a higher level of abstraction than would direct communications with the lower-layer transport protocols
  - RFCOMM, SDP



(a): adopted protocol
(b): Bluetooth specific protocol

Architecture: Protocol Stack

- Application protocols group:
  - Those protocols that reside above the protocol stack as defined by the SIG
  - Note that some of the protocols in the (previous) “middleware group” could be considered application-level protocols

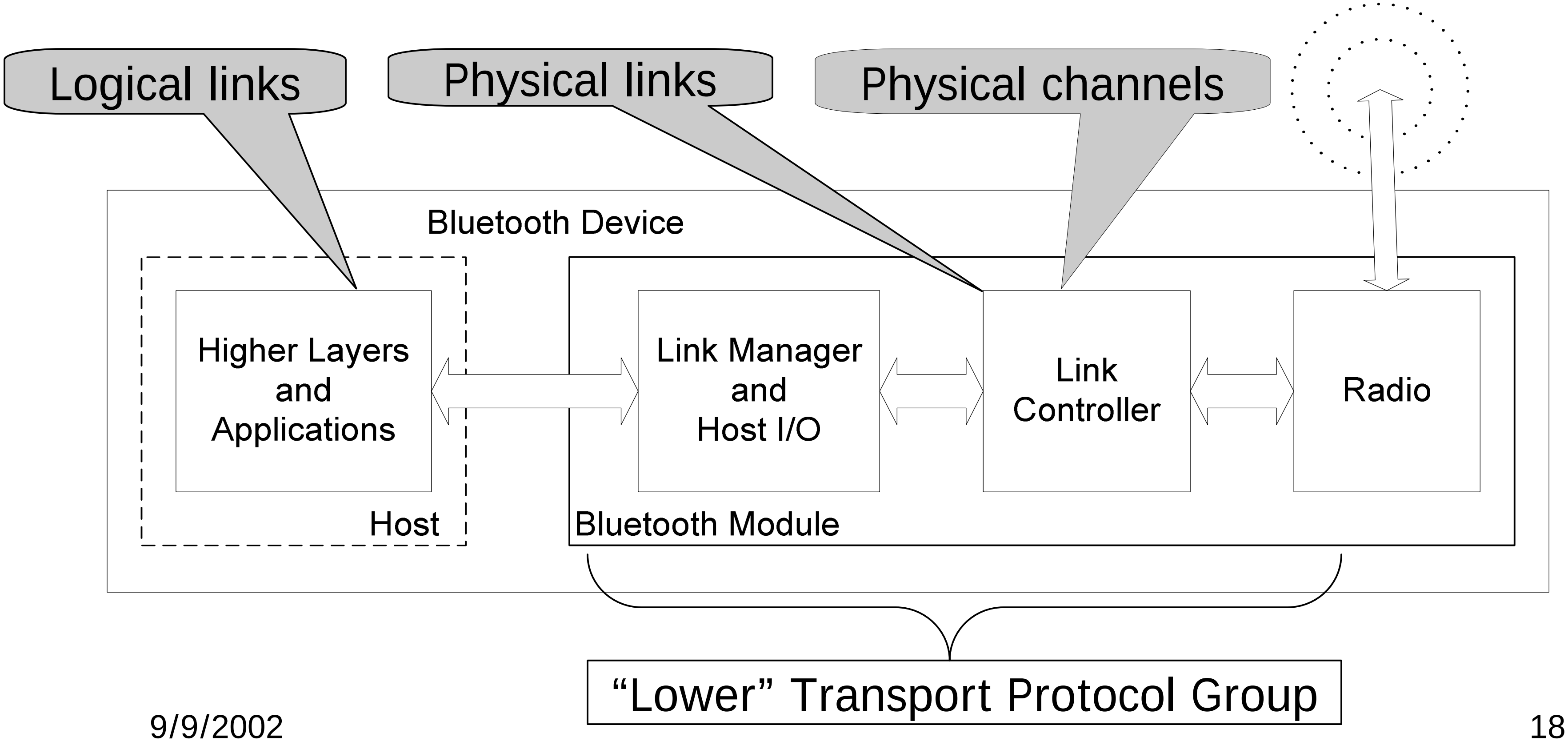


(L): legacy application

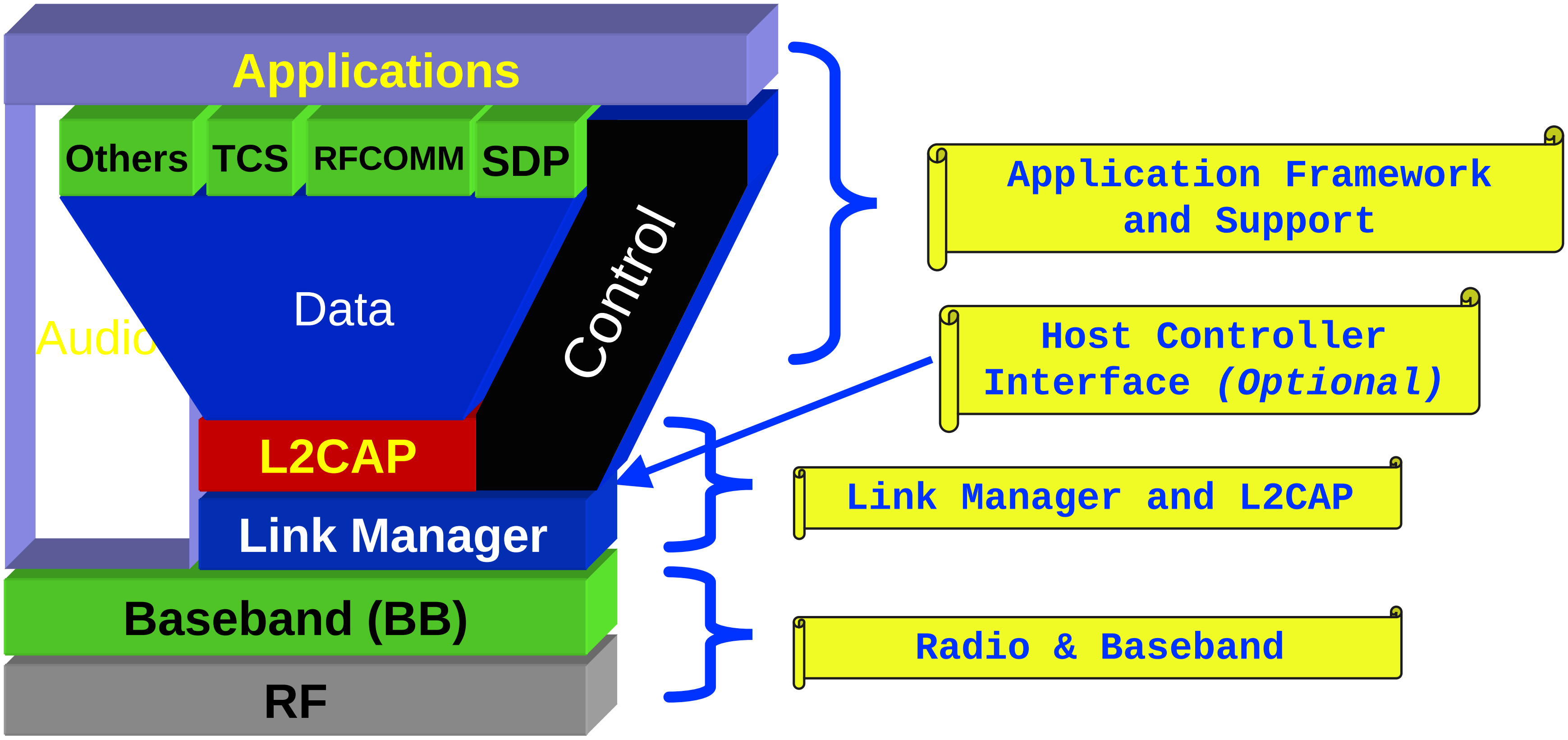
(b): Bluetooth specific application

Architecture: Unit Components

High-level functional components of a Bluetooth device



Architecture:
Summary of Protocol Stack



Application Framework and Support

Host Controller Interface *(Optional)*

Link Manager and L2CAP

Radio & Baseband

Next

- RF: Radio System
- BB
- LMP
- L2CAP
- HCI

May not have time to cover it!

Radio System

- The Spectrum, frequency bands and channel arrangements

- Key Operational Parameters of The Transceiver

Radio System

- The Spectrum
  - The actual bandwidth (BW) used = 79 MHz
  - To comply with out-of-band regulations in each country, guard bands are used
  - The Bluetooth transceiver is a frequency-hopping spread spectrum (FHSS) radio system

Geography	Regulatory Range (GHz)	RF Channels (MHz)	Lower Guard Band	Upper Guard Band

US and most other countries	2.400-2.4835	f=2402 + k,
		k=0,1,2,…, 78
			2 MHz	3.5 MHz

Radio System

- Key operational parameters of the Bluetooth radio

Modulation	GFSK	BT = 0.5 Modul. index: 0.28-0.35
Symbol rate	1 Msps	Using binary GFSK = 1Mbps
FH-rate	1,600 hps (typical)	625 µs per hop
	32,00 hps (inquiries & pages)	312.5 µs per hop
Transmit power	Class1: 20 dBm (100mW)	Required power control (PC) to at leas 4dBm; optional PC to below -30dBm
	Class2: 4 dBm (2.5mW)	Optional PC as above
	Class3: 0 dBm (1mW)	Optional PC as above
Receiver sensitivity	Must attain a raw BER of 0.1% with -70 dBm or lower	The -70dBm sensitivity is for any signal by any compliant Bluetooth transmitter

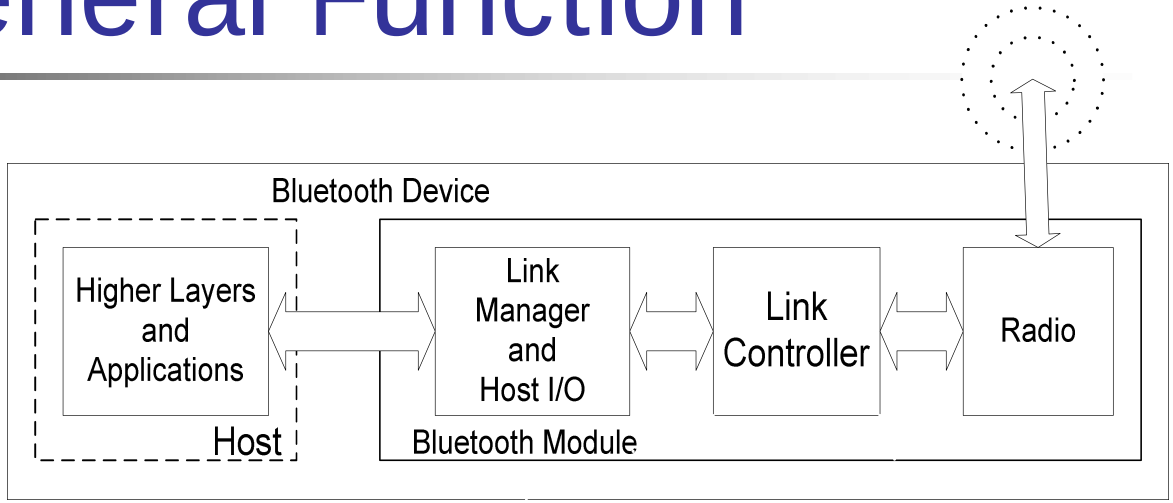
Compares to -80dBm, for a frame ER of 8% for a 1024-byte MAC DU in 802.11b

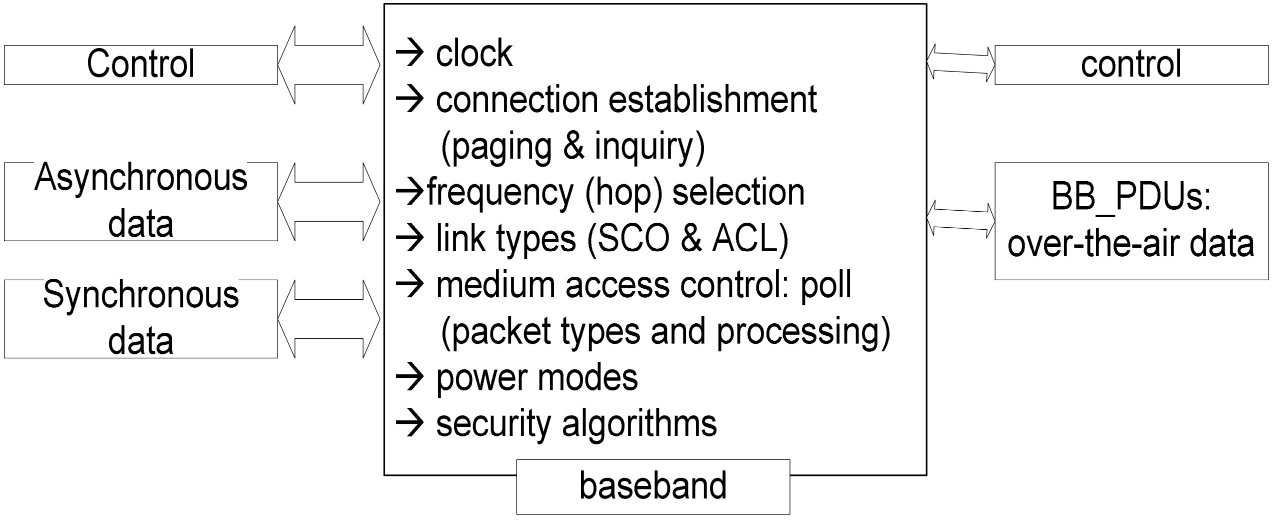
Core: Base-Band Protocols (BB)

- General functions
- Physical channel definition
- Physical link definition
  - SCO & ACL
- Packet types
- Channel Control: Bluetooth Basics

BB: General Function

- Enables physical RF links between units to form a "piconet"
- BB protocols define the timing, framing, (physical link) packets, and flow control



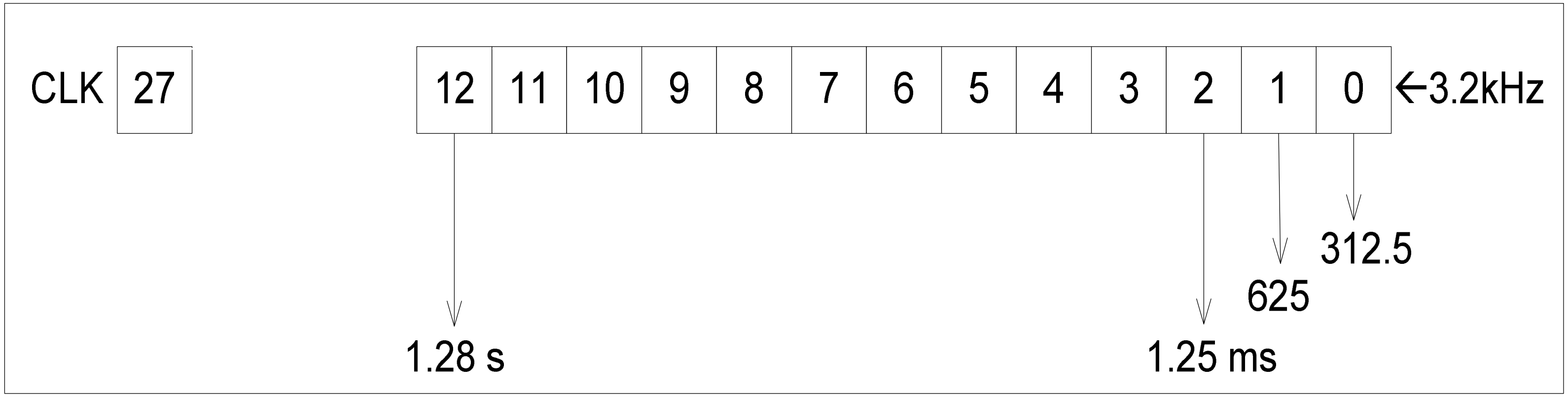


→ clock
→ connection establishment (paging & inquiry)
→frequency (hop) selection
→ link types (SCO & ACL)
→ medium access control: poll (packet types and processing)
→ power modes
→ security algorithms

BB: Physical channel definition

Two other clocks are defined: Native clock (CLKN), and estimated clock of another device (CLKE)

- A slotted channel with nominal slot length = 625 µs
- Time slots are numbered using the master's "Bluetooth clock" (CLK) from 0 to $2^{27}-1$ and is cyclic with a cycle length of 2^{27}
- "Bluetooth clock" (CLK) if implemented with a counter, a 28-bit counter is required that wraps around at $2^{28}-1$
- The LSB ticks in units of 312.5 µs, or a clock rate of 3.2 kHz
- This gives a repetition interval of about 23 hours



BB: Physical channel definition

- Master can start transmission in “even-numbered” slots only and slaves can start transmission in “odd-numbered” slots only
- Only the slave addressed by the master transmits in the immediate following slot: → Time Division Duplex (TDD)
  - In case of a broadcast, no slave is allowed to return a packet
  - If no valid Active Member address (AM_ADDR) is received, the slave may only respond if it concerns its “reserved” slave-to-master slot
- Consecutive slots must correspond to different hop-frequencies (with one exception of mutli-slot packets discussed later). Thus “nominal” dwell time is exactly 625 µs

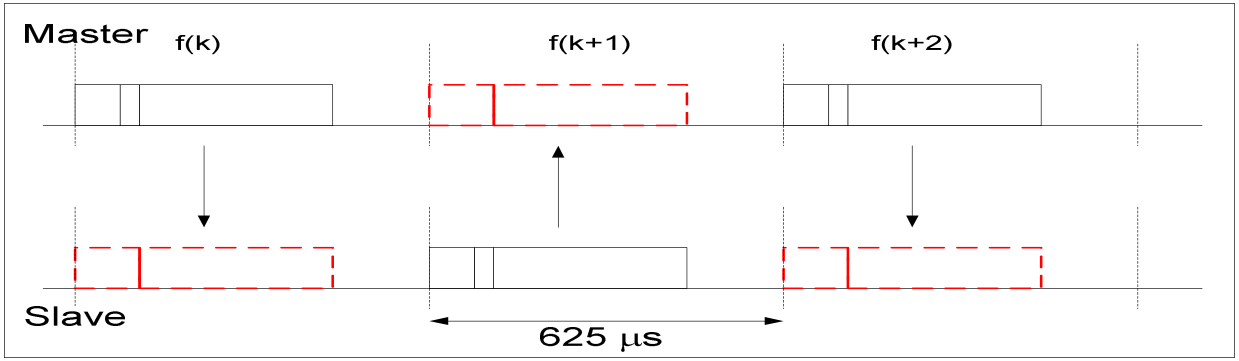
This will be explained later →

Nominal hop-rate = 1600 hops/s (= 1/625 µs)

BB: Physical channel definition

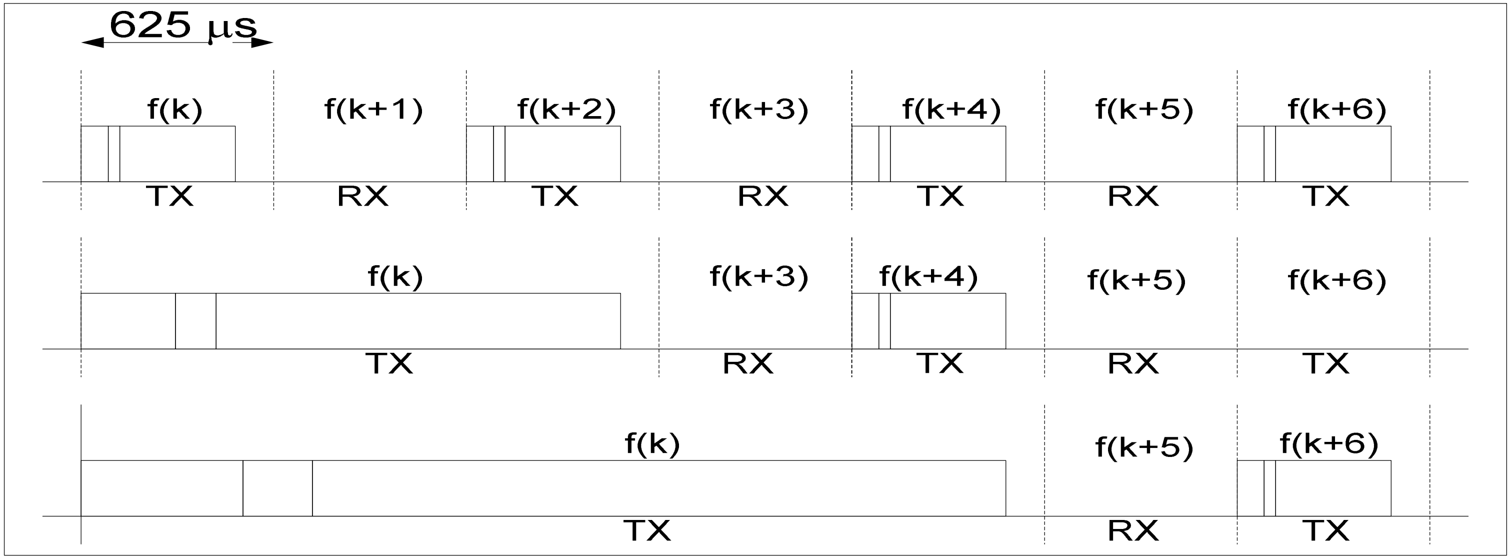
Note: FH/TDD channel

- Examples of physical channel timing: 1-, 3- & 5-slot packets are defined only



Note the TX/RX "timing" is maintained ...

Nominal hop-rate = 1600 hops/s (= 1/625 µs)



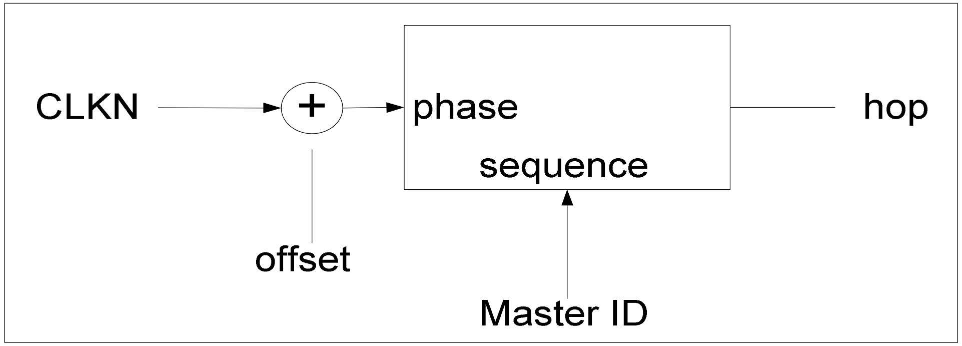
BB: Physical channel definition

- By definition, the “master” is the device that initiates the connection (will see later how)
- Each Bluetooth device has an Ethernet-like 48-bit physical address, called the “Bluetooth device address” (BD_ADDR) assigned by a central authority (to manufacturers)
- A channel is determined by a hopping-sequence derived from the BD_ADDR of the master of each piconet
- Each participant in a piconet uses the master’s ID and phase to select the channel hopping-sequence via a general “hop selection scheme”:

Not all sequences are orthogonal

Note: There is a specific selection kernel

On average, all frequencies are visited with equal probability



BB: Physical link definition

- Between a master and slave(s), two link types have been defined:
  - Synchronous Connection-Oriented (SCO) link: point-to-point (master-slave)
    - Supports time-bounded information like voice
  - Asynchronous Connection-Less (ACL) link: point-to-multipoint (master-slaves)
    - Packet-switched service: Both asynchronous and isochronous services are supported
    - Broadcast packet is defined (not addressed to any slave)

When connection is first established between two devices, it is an ACL. Any device can subsequently request a SCO link

BB: Physical link definition

- SCO
  - Master (i.e., a piconet) can support up to 3 SCO links to the same slave or to different slaves
  - A slave can support up to 3 SCO links from the same master, or 2 SCO links from different masters
  - SCO packets are sent at regular interval and NEVER retransmitted
  - SCO is established by the master sending an SCO setup message via the LM protocol (a slave can request)
    - Setup message contains timing parameters such as SCO interval T_{SCO} and the offset D_{SCO} to specify the reserved slots

BB: Physical link definition

- ACL
  - Only a single ACL link may exist between a master and a slave
  - For most ACL packets, retransmission is applied to assure data integrity (actually one is the exception, the “AUX1”)
  - Packets not addressed to a specific Active Member slave (AM_ADDR = “000”) are broadcast read by every slave
  - ACL slaves can only transmit when requested by master
  - A polling-interval is defined, T_{poll}, where a master “polls” a slave either explicitly (“POLL” packet) or implicitly by simply transmitting any payload carrying BB_PDU (this is the basis for QoS for ACL links as will be explained later)

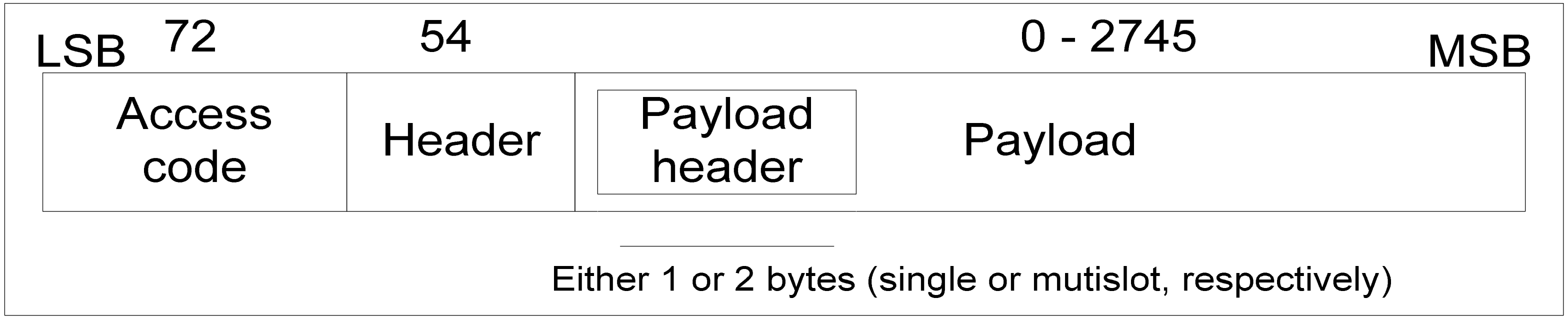
Addressing a member of a piconet will be explained under “packet header”

BB: Packet types

Little Endian format:
→LSB is the first bit sent over the air

- All packets have the same format, an access code, a header, then the user payload such that:
  - Packets may consist of (1) access code only, (2) access code & header only, or (3) access code, header, and a payload

A packet that contains ONLY the access code is called an "ID packet" and is used for signaling. In this case, it is only a 68-bit long packet



LSB 72 54 0 - 2745 MSB

Access code | Header | Payload header | Payload

Either 1 or 2 bytes (single or mutislot, respectively)

BB: Packet types

Access Code

The 72-bit channel access code (CAC) must precede all packets exchanged on the piconet channel

- Three Access codes are defined:
  - Channel access code (CAC): Identifies a piconet based on the master’s ID
  - Device access code (DAC): Used for special signaling, e.g., paging and response to paging
  - Inquiry access code (IAC)→ General (GIAC) used to inquire about any Bluetooth device and Dedicated (DIAC): Used to discover any Bluetooth device (GIAC) or a dedicated group of devices that share a common characteristics

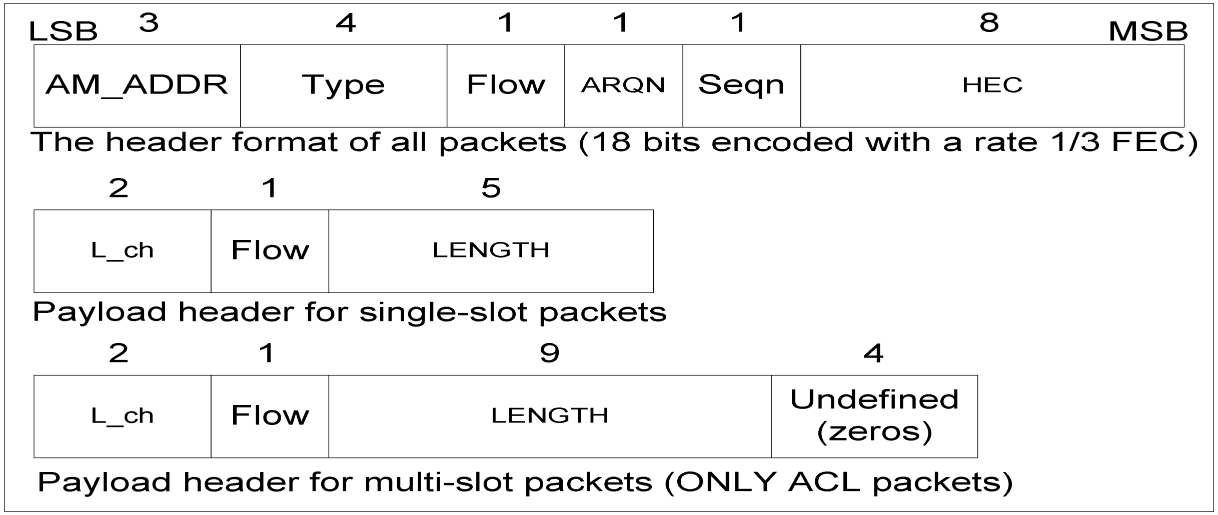
BB: Packet types

Packet Headers

Notes:

1. No AM_ADDR for the master
2. "000" is a broadcast
3. Max of 7 active slaves
4. "Flow" only over ACL link: 0=STOP, 1=GO
5. "ARQN": 0=NACK, 1=ACK

- Packet header contains link control (LC) information and has 6 fields
  - "Seqn": To discard correctly received consecutive retransmission, bit is inverted for each newly transmitted packet and stays the same for retransmitted packets (only non-broadcast packets)
  - "Type" and "LENGTH" (Next slide)



LSB ... MSB

3	4	1	1	1	8
AM_ADDR	Type	Flow	ARQN	Seqn	HEC

The header format of all packets (18 bits encoded with a rate 1/3 FEC)

2	1	5
L_ch	Flow	LENGTH

Payload header for single-slot packets

2	1	9	4
L_ch	Flow	LENGTH	Undefined (zeros)

Payload header for multi-slot packets (ONLY ACL packets)

"The header" of all packets is protected by a 1/3 rate FEC, making an 18-bits actual header a 54-bits header

Since no ACKs for broadcast packets, each is repeated N_{BC} times

BB: Packet types

Packet
Headers

- The “Type” field allows for 16 different packets:
  - 4 Link control packets (NULL, POLL, FHS, DM1)
  - 4 SCO packets (HV1, HV2, HV3, DV)
  - 6 ACL packets (DH1, AUX1, DM3, DH3, DM5, DH5)
  - 2 Undefined (for future)
- The “LENGTH” field in the “Payload” header indicates the number of bytes in the payload excluding the payload header and the CRC, i.e., the payload-body only

The 4-bit “Type” code also indicates the “physical link” associated with the packet

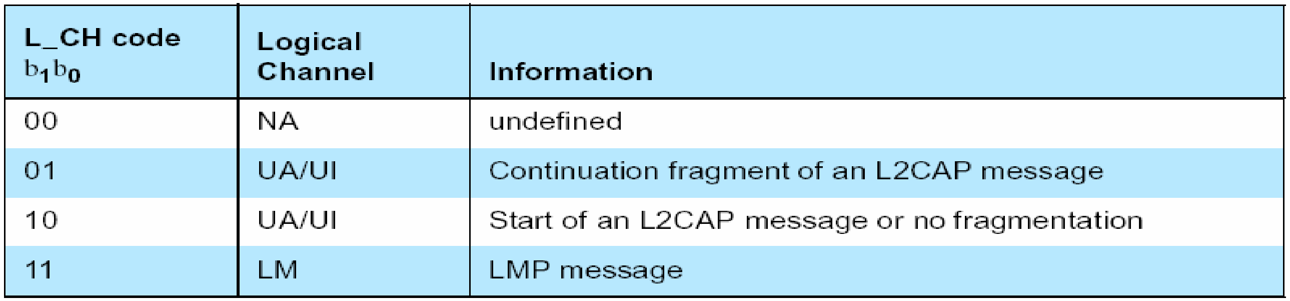
The number following the 6 ACL packets refers to the number of occupied slots (not true for the 4 SCO packets, refers to the type of FEC)

DH = Data High-rate
DM = Data Medium-rate
DV = Data-&-Voice
FHS = Frequency Hopping synchronization
HV = High-quality Voice

BB: Logical Channels

- Five logical channels are defined: LC, LM, UA, UI, US
- The control channels, LC & LM, are used at the link control level and link manager level, respectively
- The LC channel is carried in the packet header, all others are carried in the packet payload
- The first two bits, “L_CH” field, of the “payload header” defines three logical channels: LM, UA, UI, (the fourth is reserved), mainly to indicate the “start/no-fragment” or “continuation” of a L2CAP message
- The US channel is carried by the SCO link only

We will come back to this table under the L2CAP



L_CH code $b_1 b_0$	Logical Channel	Information
00	NA	undefined
01	UA/UI	Continuation fragment of an L2CAP message
10	UA/UI	Start of an L2CAP message or no fragmentation
11	LM	LMP message

Table 4.7: Logical channel L_CH field contents

BB: Packet types Summary

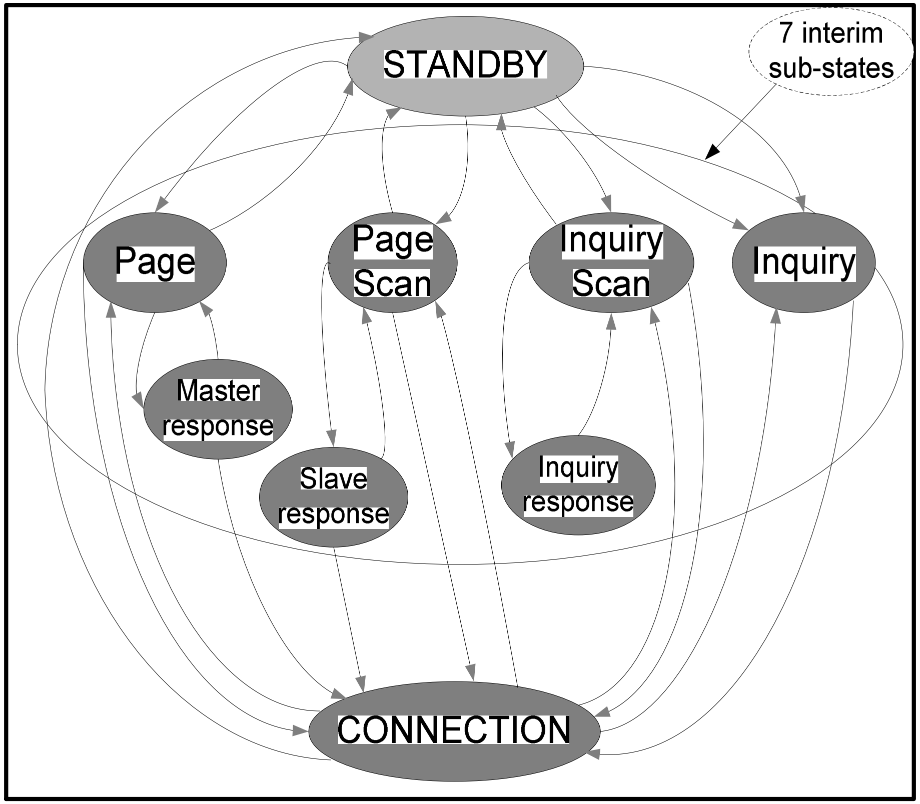
- The 4 Link control packets are:
  - POLL: sent only by a master and requires ACK
  - NULL: sent by either and does not require ACK, used if link control carried by the header is needed; e.g., flow control
  - FHS: contains all information to get two units to hop synchronized (CLK and the 48-bit identity)
  - DM1: for control data
- The other 12 packets are ACL and SCO packets

For a summary of the 16 packets, see the “Summary Table” attached.

BB: Channel Control: BT Basics

How the piconet channel is established and how units are added to, and released from the piconet?

- Overview of “States” of Bluetooth link controller:
  - Standby: Low power mode
  - Connection: Four sub-states: Active, Sniff, Hold, and Park (these modes will be considered under “Power Management” by LMs)
  - Seven interim sub-states four of which can be entered either from the Standby or the Connection states



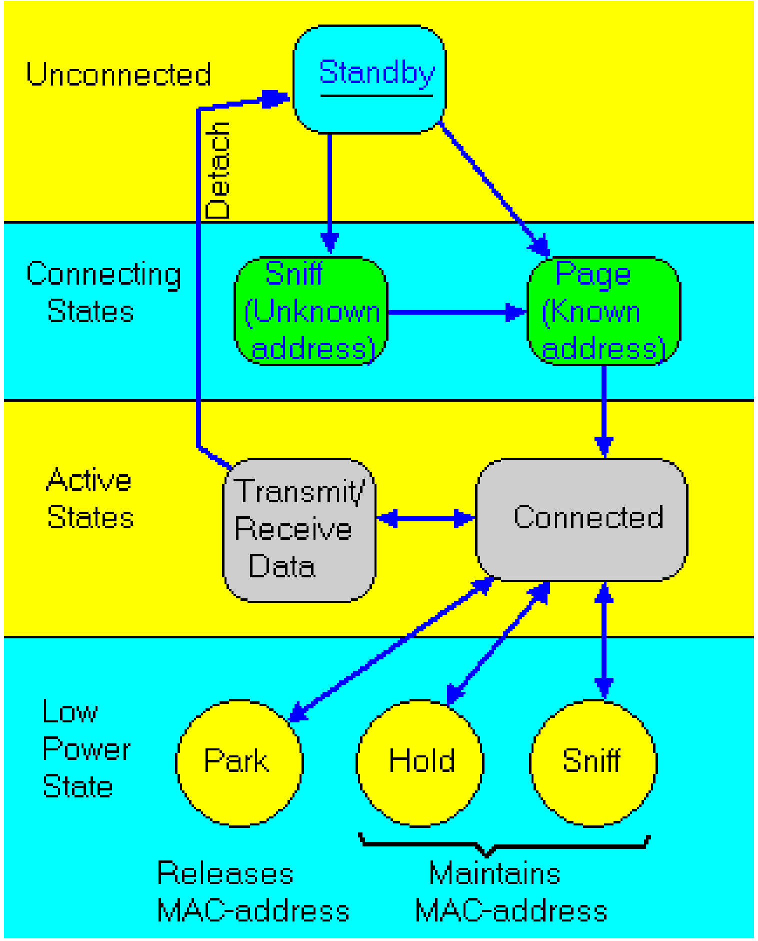
BB: Channel Control: BT Basics

- Access procedures and Hop selection:
  - Either “Page”, “Inquire”, or “Scan” (Page or Inquiry): Five Hopping sequences are defined for the 79-hop system:
    - A page hopping sequence (PHS): 32 unique frequencies distributed equally over the 79 hops
    - A page-response sequence (PRS): 32, 1-1 correspondence to the current PHS
    - An inquiry sequence (IHS): 32 unique frequencies distributed equally over the 79 hops
    - An inquiry-response sequence (IRS): 32, 1-1 correspondence to the current IHS
    - A channel hopping sequence (CHS): All the 79 frequencies used in a long sequence based on the master ID

Consecutive transmissions of paging & inquiring are performed on different frequencies (of the 32) every 312.5us, i.e., double the nominal hop-rate

BB: Channel Control: BT Basics

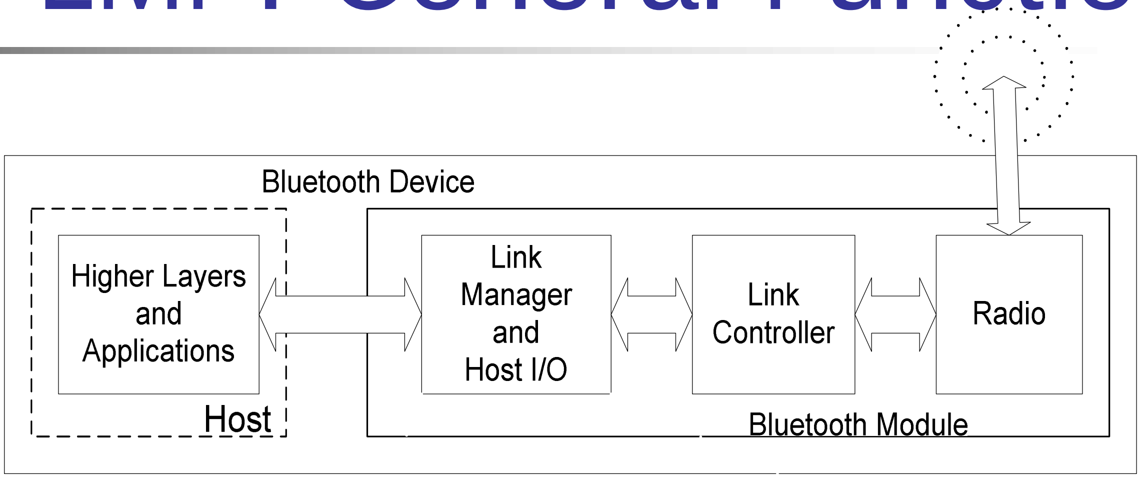
- Summary of “States”:
  - Initiating node will be a master
  - A slave may join an ongoing piconet after scanning (page or inquiry) and possibly master/slave switch
  - Master/slave switch: two-step process:
    - 1. TDD switch of master/slave
    - 2. Piconets switch of the two

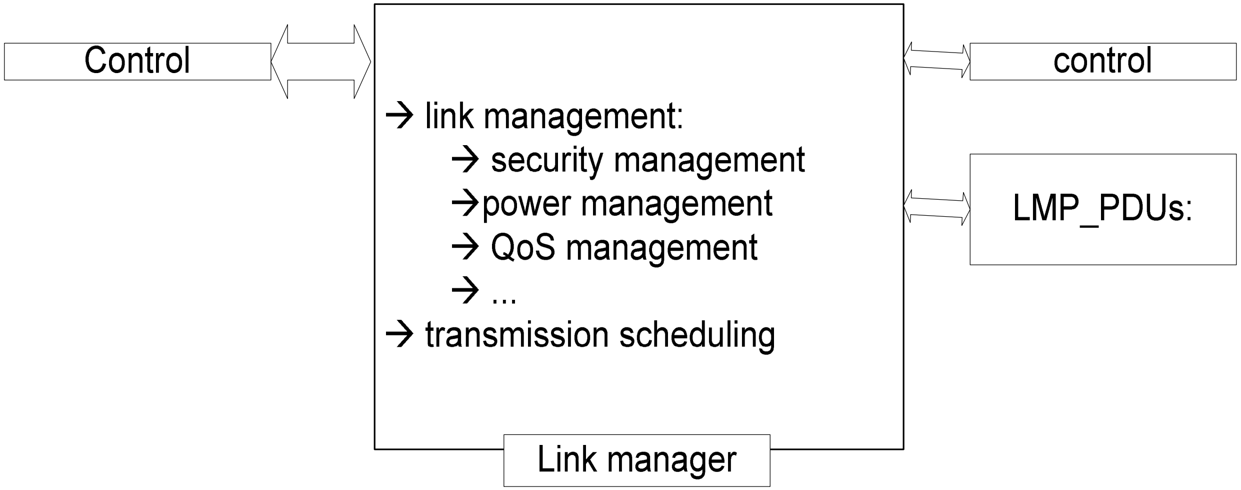


We will come back to the “low power states” under the “power management” by the LM

LM and LMP: General Function

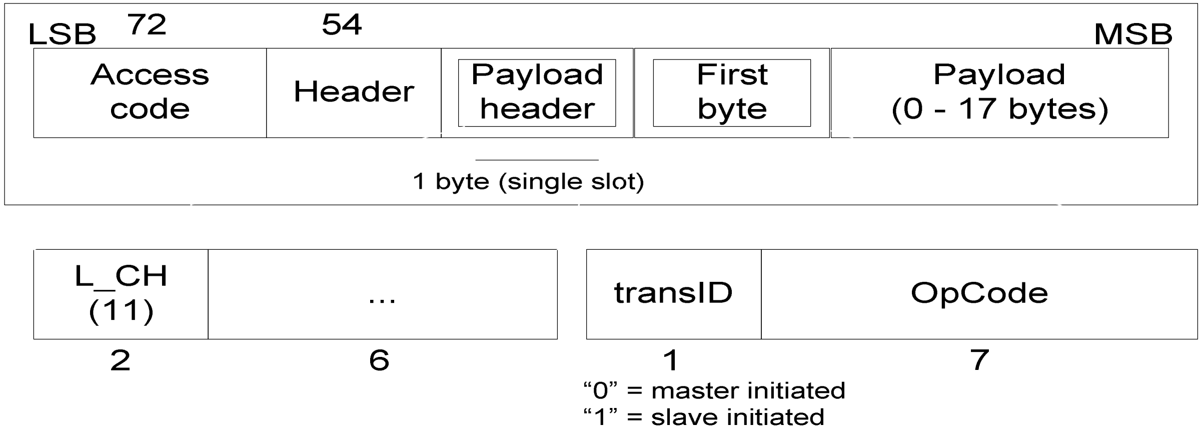
- LM does the following:
  - Set up and control BT-link between devices via LMP_PDUs: Security, power-control, QoS
  - LMP does not carry application data, either communicate with the LM of another device or it sends control signals to its own BB & radio layers





LM and LMP: General Function

- LMP_PDUs are carried in the payload of ACL (DM1 or DV) packets whose “payload” header has the two L_CH bits set to “11”
- Connection establishment and Detachment:
    - A device may issue a LMP_*host_connection_req* PDU,
    - If accepted, negotiation starts between the two LMs on parameters on the link. After that, a LMP_*setup_complete* PDUs **must** be exchanged between the two devices to allow non-LMP_PDUs to flow ...
    - To terminate, any device can send a **non-contested** LMP_*detach* PDU, with a reason parameter explaining why link is to be terminated



LSB 72 54 MSB

Access code | Header | Payload header | First byte | Payload (0 - 17 bytes)

1 byte (single slot)

L_CH (11) | ... | transID | OpCode

2 6 1 7

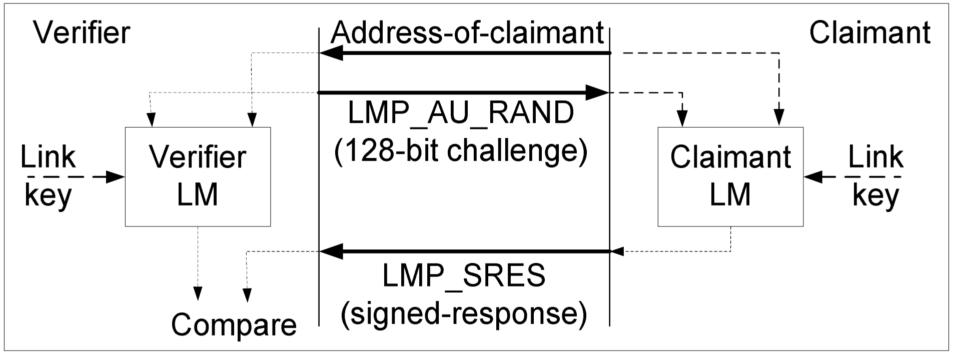
“0” = master initiated
“1” = slave initiated

LM and LMP: Security

- Security measures in RF environment is essential
- Device authentication is mandatory and link encryption is optional
- Security is presented in the BB part of the specification but setup, negotiation and configuration are the function of the LMs
- Authentication can be uni- or bidirectional
- Public-key and certificate schemes are not appropriate for low-level ad-hoc networks since they require the support of a trusted authentication agencies (third-part). They can be implemented at higher layers

LM and LMP: Authentication

- Challenge-response transaction that depends on a shared secret (secret-key)
- The claimant-address, AU_RAND, and a 128-bit shared secret link-key form the input to produce a 32-bit signed-response and a 96-bit authenticated cipher offset (ACO)
- The ACO is used for encryption



- The secret link-key is generated in an initialization phase (pairing-up or associating two devices)
- Once the 128-bit link-key is generated, it resides in hardware and is not accessible by the user, and automatic authentication can be done
- For N units, Nx(N-1)/2 link-keys required
- To authorize initialization, user has to enter identical PIN in both devices

LM and LMP: Link Encryption

- 1-bit stream cipher, whose implementation is specified in specs
- Encryption applies only to “payload” of the BB_PDUs (link property: SCO and ACL) and is symmetric (i.e., applies in both directions)
- The payload bits are modulo-2 added to a binary keystream
- Size of encryption key is negotiable to match application requirements (max. 128 bits)
- Encryption-key is derived from the “link-key”, the ACO (so authentication must precedes encryption), and a master-generated random number
- Start: LMP_*encryption_mode_req* PDU (with a parameter distinguishing a point-to-point or broadcast encryption. In broadcast, a master key is created to be used by all devices)
- If accepted: devices exchange LMP_*encryption_key_size_req* PDUs

LM and LMP: Power Management

- Level of handling packets
  - Tx-side: sending only useful data
    - If only link control information needs to be exchange, NULL packets will be used
    - NACK is implicit on no-reply, i.e., no transmission if no link control or data to be exchange
    - If there is data to be sent, payload length is "adapted" so that only valid bytes are sent (using the "LENGTH" field in "payload header")
  - Rx-side: listening only to your data
    - If no valid access-code is found, transceiver return to sleep
    - If access-code is valid, then if HEC fails, unit will return to sleep after the packet header
    - A valid header will indicate if a payload will follow and how many slots
    - A slave not addressed in the first slot of a multi-slot packet, may go to sleep for the remaining slots. This is read from the "TYPE" code

Two levels are used:
(1) Packet-level and
(2) Connection-level

LM and LMP: Power Management

The "active" mode is the highest power and fastest response

The "hold" mode frees the slave to do other things like scanning, paging, inquiring, or attending other piconets, or simply saving power

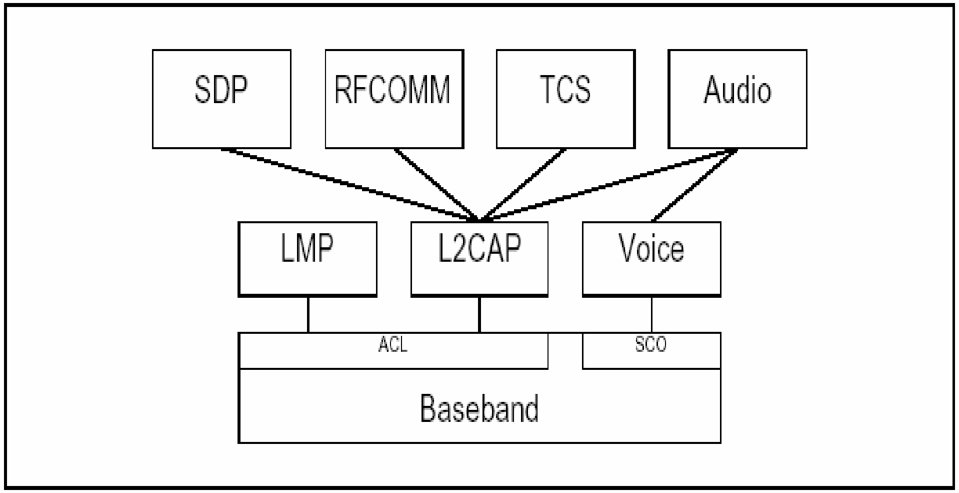
- "connection" state level: four modes are defined
  - Active: previous-slide (level of handling packets)
  - Sniff: a slave listen to master only during designated sniff intervals (which is programmable depending on application)
  - Hold: does not receive any ACL packet and listen only to determine if it should be active again
  - Park: stop listening and give up its AM_ADDR. It remains in synch with the FH pattern by listening to a special beacon signal sent by the master to all parked slaves (broadcast)
  - In all cases, a master may force a slave in a mode, or alternatively, either the slave or the master may request that the slave enters a mode
  - In sniff & hold, any SCO transmissions will still occur as scheduled (but not in park)

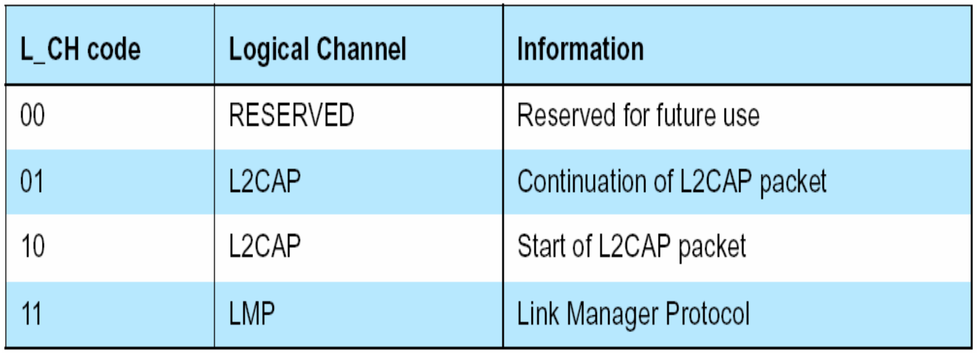
LM and LMP: QoS (for ACL)

- To control the minimum bandwidth of an ACL traffic (or the maximum access-delay of ACL BB_PDUs), the polling-interval, T_{poll}, (max time between subsequent master-to-slave transmissions) can be adjusted as needed
- Polling-interval is guaranteed in active mode except when there are collisions with page, page-scan, inquiry, inquiry-scan
- Master can force change by LMP_*quality_of_service* PDU (contains T_{poll})
- A slave (or the master) may request to change the polling-interval by LMP_*quality_of_service_req* PDU (Only the master can set the T_{poll} depending on its bandwidth availability)

L2CAP (only for ACL packets)

- Lower transport protocols are optimized to deal with the hostility of the RF medium, power consumption, security, regulatory issues, ...
- This lead to a small size BB_PDUs compared to the Internet packets
- Therefore, adaptation layer is needed
- L2CAP channels: Each endpoint of a channel (a device's L2CAP layer) is assigned a unique 16-bit local channel identifier (CID). Each endpoint is uniquely associated with a "payload recipient entity", which could be in the L2CAP or at higher layers

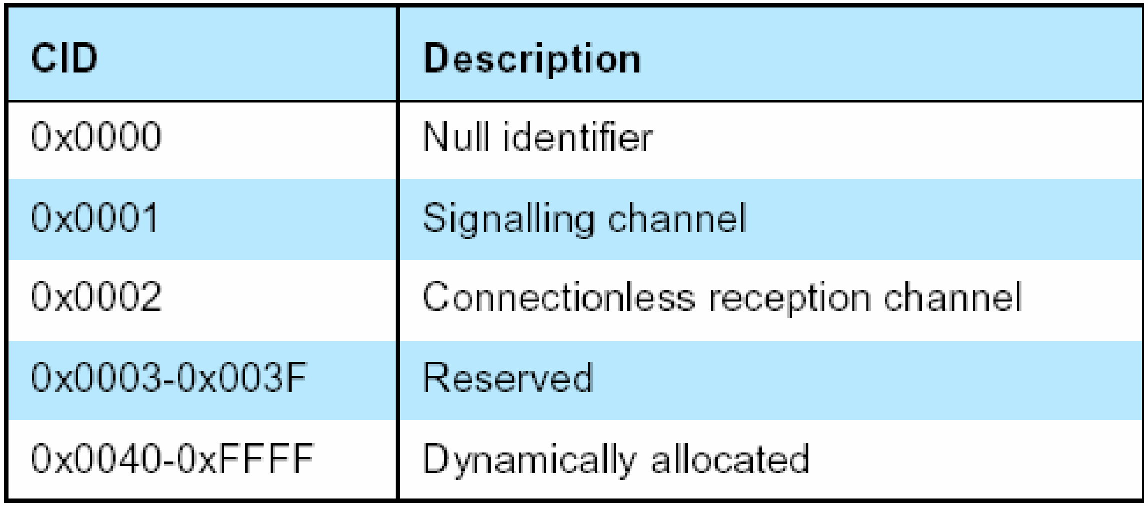




L_CH code	Logical Channel	Information
00	RESERVED	Reserved for future use
01	L2CAP	Continuation of L2CAP packet
10	L2CAP	Start of L2CAP packet
11	LMP	Link Manager Protocol

L2CAP

- The CIDs:

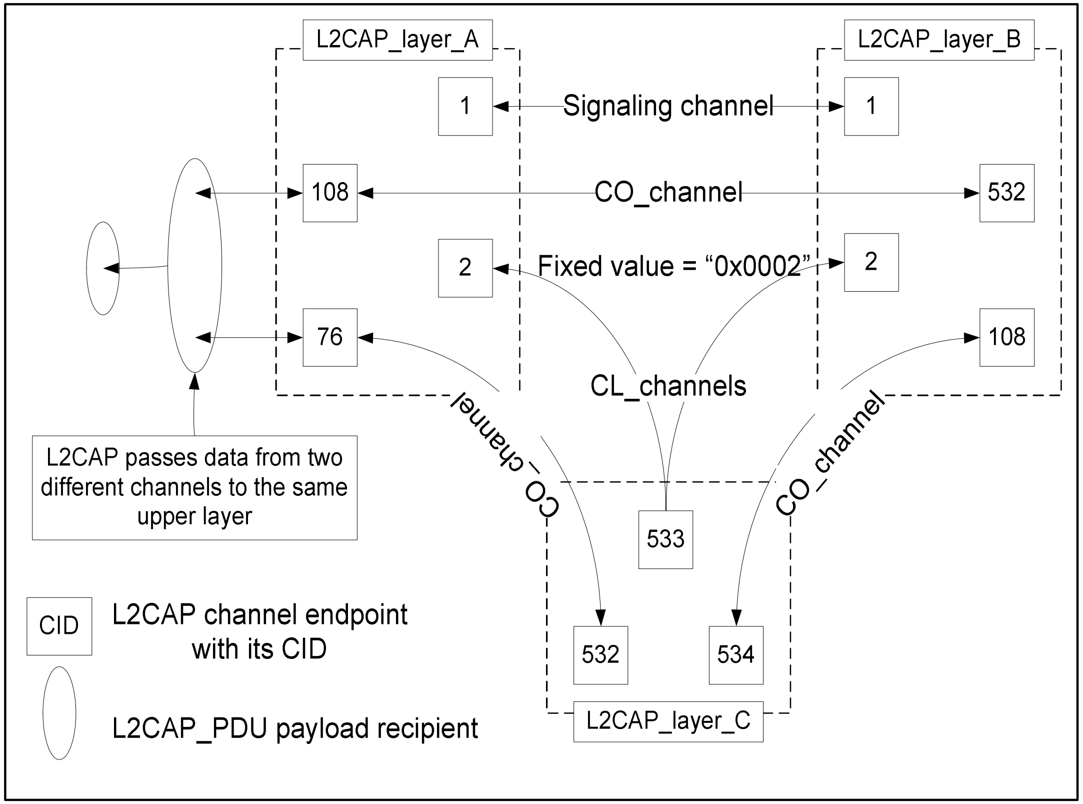


CID	Description
0x0000	Null identifier
0x0001	Signalling channel
0x0002	Connectionless reception channel
0x0003-0x003F	Reserved
0x0040-0xFFFF	Dynamically allocated

L2CAP

- The L2CAP layer provides:
  - Higher-layer protocol multiplexing
  - Facility to help segmentation & reassembly (length information)
  - exchange of QoS information
  - no reliability
  - Two L2CAP_PDUs: CL & CO (CO includes signaling and is the basis of QoS)
  - Signaling commands, configuration options and commands ...

The different types L2CAP channels defined: Signaling, CO, CL



Host Controller Interface (HCI)

- HCI is a standardized interface (with corresponding communication protocol) between the host controller (on the BT module) and the host
- The capabilities of the HCI define what can be achieved by BT technology
- Largest section of the specification, however, it is “optional” in the sense that a device may not implement a HCI and still be compliant!
- One of the advantages of HCI is that the “host” device can sleep and wakes up only if a Bluetooth connection arrives

HCI: Packet classes

- Packet HCI_PDU classes
  - Command HCI_PDU: used by “host” to control “module” and monitor status
  - Event HCI_PDU: used by “module” to inform “host”
  - Data HCI_PDU: used by both to forward traffic
- Configuring modules
- Inquiring and paging

HCI: Command & Event HCI_PDU

1024 possible commands for each group of the 64 possible groups, resulting in a total of 65, 536 possible commands

Some groups:
1.Vender-specific
(debugging)
2. Reserved

- The Command HCI_PDU contains:
  - OpCode (2 bytes): 6-bits=OpCode group subfield (OGF); 10-bits=OpCode command subfield (OCF) identifies a specific HCI command within the particular OGF. Groups include:

    (1) Link control, (2) Link policy, (3) Host controller & BB, (4) info parameters, (5) status parameters
  - Payload_Length field (1 byte): total length in bytes of the following parameters
  - (variable-size) sequence of fields for the various parameters of this command
- Similarly for the Event HCI_PDU:
  - Event_Code (1 byte):
  - Payload_Length field (1 byte):
  - (variable-size) sequence of fields for the various parameters of this event

HCI: Configuring module (command)

UTF = Unicode Transformation Format

- Configuring commands to inquire a local module or a remote device: e.g.,
  - HCI version, LMP version, manufacturer name, ...
  - UTF-8 encoded name (global): up to 248 bytes long
  - Device class
  - Voice settings, ...
- Other configuration commands include:
  - Setting operational parameters of the module, such as providing a “link-key” for authentication
  - Configuring the module’s operational status and related parameters, such as activating and setting the parameters for low power modes
  - Depending upon the command, module registers will be read or set, link manager may execute an LMP transaction, the link controller may change state and execute a page, and so on.

HCI: Inquiring (Discovering other devices) and Inquiry scan (Becoming discoverable)

- The inquiry process is fully controlled by the HCI: e.g.,
  - The host uses the HCI_Inquiry command to initiate an inquiry
  - The module utilizes a HCI_Inquiry_Result event to respond to an inquiry from the host
- The device allows others to discover it by conducting inquiry scan, listening for the IAC for repeated short bursts of about 10ms each, every 1.28s (or max. 2.56s)

HCI: Paging (Initiating connections) and Paging scan (Receiving connections)

- The paging process is fully controlled by the HCI: e.g.,
  - The host uses the HCI_Create_Connection command to initiate paging (containing all needed information to establish a connection)
- The device allows others to connect to it by conducting paging scan, listening for the access code (based on its own ID) for repeated short bursts of about 10ms, every 1.28s (or max. 2.56s)

The Future Bluetooth

- That was Bluetooth 1.1
- There is a medium-rate Bluetooth 1.2
  - Rates of 2 to 3 Mbps
- There is a high-rate Bluetooth 2.0: (~by 2004)
  - Expected to support gross rates of 4, 8, and 12 Mbps
  - Will offer new communications modes on top of the “1.1” specs, non-hopping narrow band and distributed MAC protocol
  - Faster response times, built-in QoS, broadcast/multicast support
  - Operates over the same 10-meter distance (peak power is expected to be doubled)
  - Expected cost of Bluetooth 2.0 chip sets is not more than 20% more than the current Bluetooth chips

News article information

The End.

- Thank you.