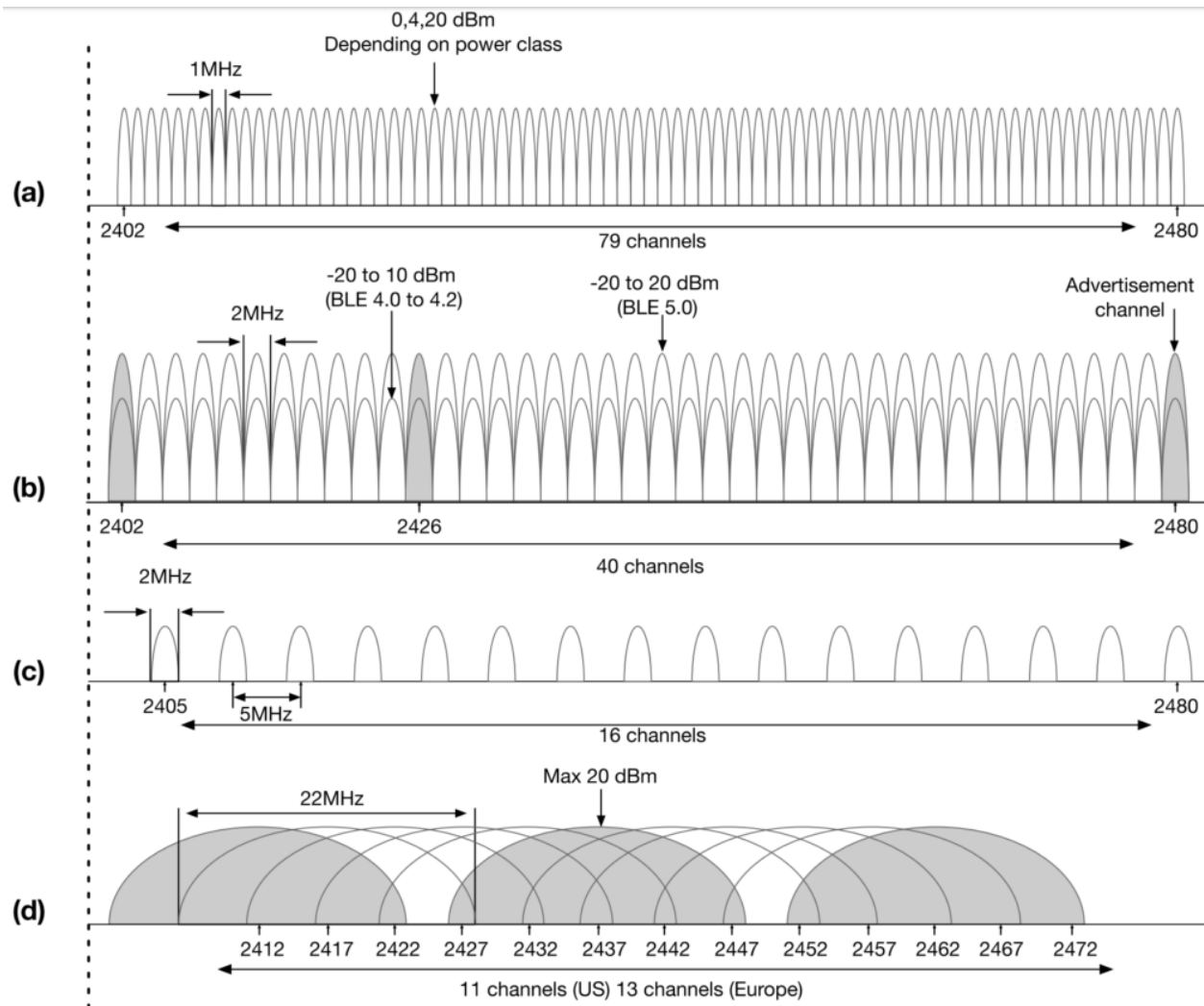




Bluetooth spectrum (comparison)



(a) Traditional Bluetooth; 79 channels with 1MHz width

(b) BLE (4.0-4.2 and 5.0); 40 channels 2MHz wide; 3 'advertisement channels'

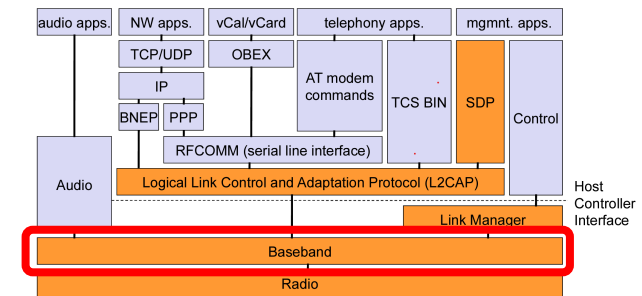
(c) 16 channels used by IEEE 802.15.4 based networks (e.g. ZigBee)

(d) IEEE 802.11b™ DSS channels; 22MHz wide channels



Baseband in Bluetooth

- Manages physical channels and logical lines
 - Controls device addressing, channel control, power-saving operations, and flow control and synchronization among devices
 - Implements TDD aspects: master and slave switch in communications
- Works closely with Link controller:
 - Manages link (a)synchronism
 - Controls paging and inquiries
 - Controls power save modes





Baseband link types

- Polling-based (TDD) frame transmissions

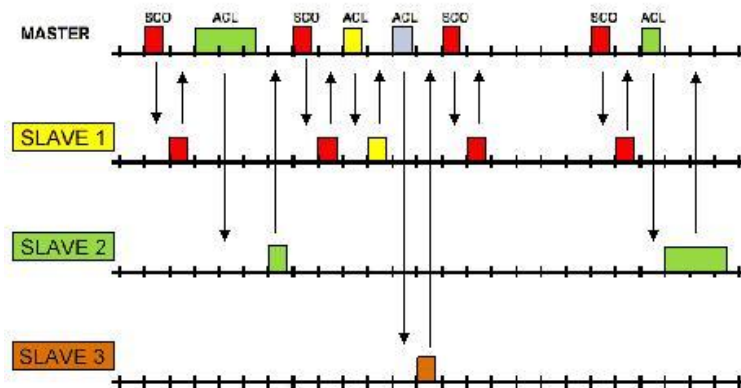
- 1 slot: 0.625 μ S (max 1600 slots/sec)
- Master/Slave slots (even-/odd-numbered slots)
- Polling: master always “polls” slaves

- Synchronous Connection-Oriented (SCO) link

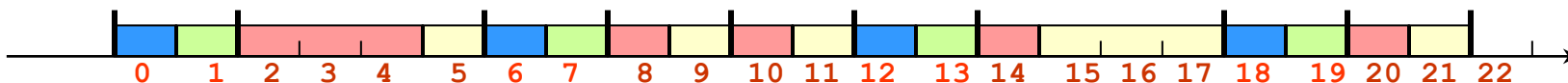
- “Circuit-switched”
 - Periodic single-slot frame assignment
- Symmetric 64Kbps full-duplex

- Asynchronous Connection-Less (ACL) link

- Frame switching
- Asymmetric bandwidth
 - Variable frame size (1-5 slots)
 - max. 721 kbps (57.6 kbps return channel)
 - 108.8 - 432.6 kbps (symmetric)

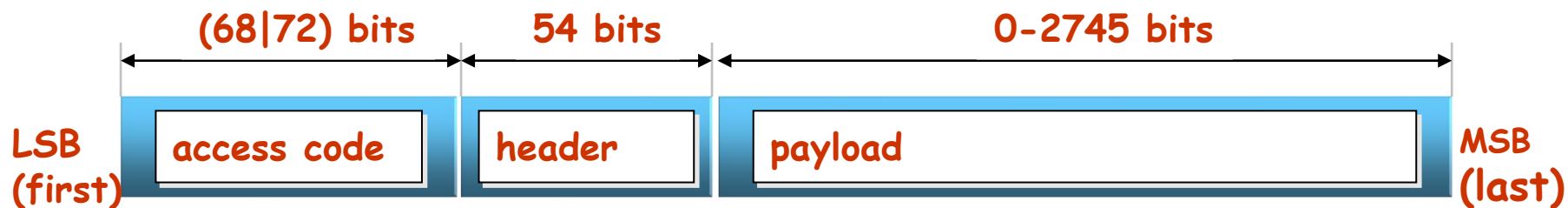


	SCO	ACL
Master		
Slave		





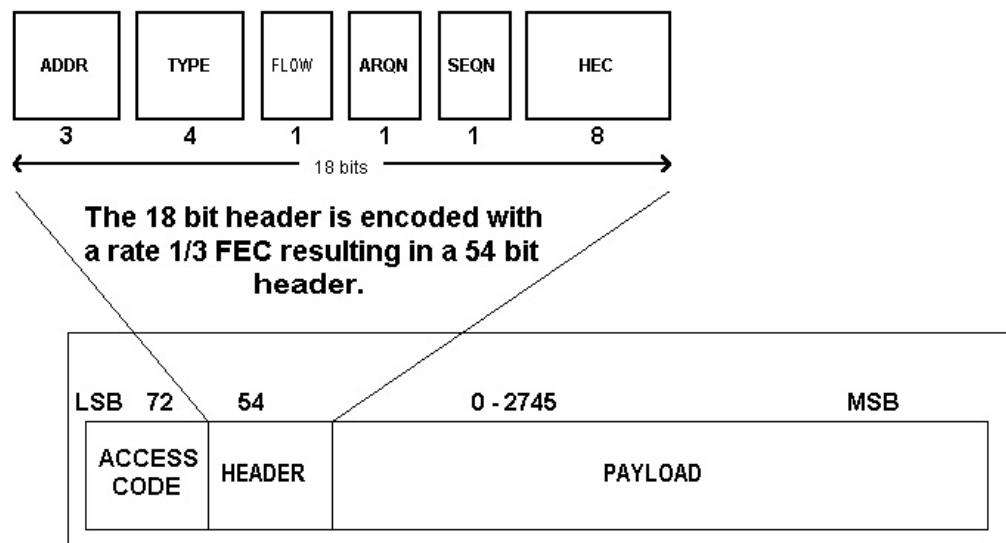
Baseband Frame



- **Access Code:** time synchronization, offset, paging, inquiry
 - 3 types:
 - Channel Access Code (CAC), piconet identification, synchronization, DC offset
 - Device Access Code (DAC), paging and replies
 - Inquiry Access Code (IAC), inquiries (GIAC, general; DIAC, dedicated)
- **Header:** packet acknowledgement and numbering, flow control, slave address, error checking
- **Payload:** voice, data or both (DV packets)
 - When data, the payload has an additional internal header



Baseband Packet



ADDR	000 is for broadcasting
TYPE	16 types Also specifies the length of the packet Dependent on the type of connection, i.e., ACL or SCO
FLOW	If the buffer in the recipient is full, a STOP (0) is sent A GO (1) is sent for indicating that more data packets can be received
ARQN	ACK (1) is sent if the data is successfully received A NAK (0) is sent if data was not received or contains errors
SEQN	Determines the sequence of received packet
HEC	Value to check for the integrity of the header information



Packets: Common

TYPE	NAME	#	DESCRIPTION
Common	ID	1	Carries device access code (DAC) or inquiry access code (IAC).
	NULL	1	NULL packet has no payload. Used to get link information and flow control. Not acknowledged.
	POLL	1	No payload. Acknowledged. Used by master to poll the slaves to know whether they are up or not.
	FHS	1	A special control packet for revealing Bluetooth device address and the clock of the sender. Used in page master response, inquiry response and frequency hop synchronization. 2/3 FEC encoded.
	DM1	1	To support control messages in any link type. can also carry regular user data. Occupies one slot.



Packets: Synchronous Connection-Oriented (SCO)

SCO	HV1	1	Carries 10 information bytes. Typically used for voice transmission. 1/3 FEC encoded.
	HV2	1	Carries 20 information bytes. Typically used for voice transmission. 2/3 FEC encoded.
	HV3	1	Carries 30 information bytes. Typically used for voice transmission. Not FEC encoded.
	DV	1	Combined data-voice packet. Voice field not protected by FEC. Data field 2/3 FEC encoded. Voice field is never retransmitted but data field can be.



Packets : Assynchronous Connection-Less (ACL)

ACL	DM1	1	Carries 18 information bytes. 2/3 FEC encoded.
	DH1	1	Carries 28 information bytes. Not FEC encoded.
	DM3	3	Carries 123 information bytes. 2/3 FEC encoded.
	DH3	3	Carries 185 information bytes. Not FEC encoded.
	DM5	5	Carries 226 information bytes. 2/3 FEC encoded.
	DH5	5	Carries 341 information bytes. Not FEC encoded.
	AUX1	1	Carries 30 information bytes. Resembles DH1 but no CRC code.



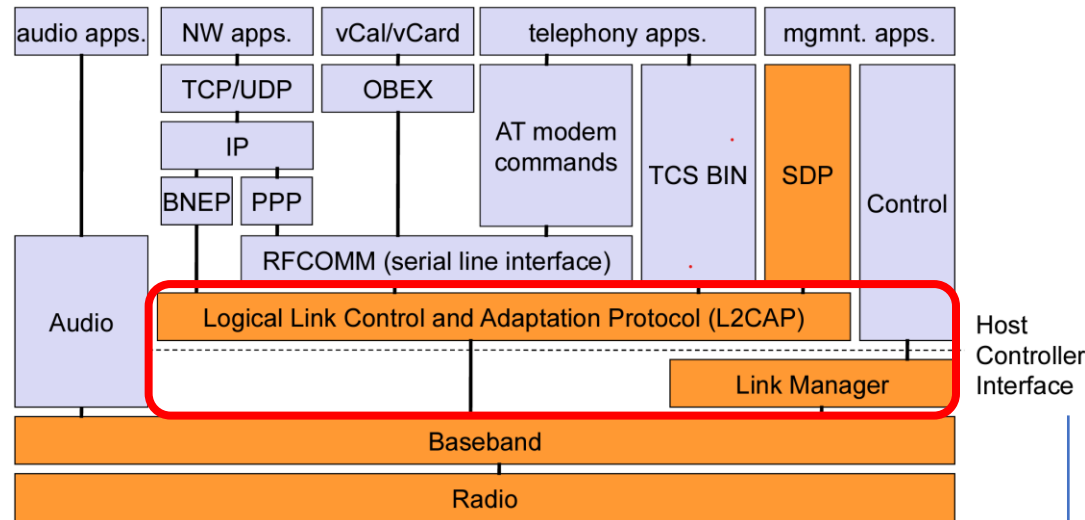
Adaptation protocols

- Link Manager

- Carries out link setup above baseband, with authentication, link configuration and other protocols
 - Support protocol multiplexing
 - BT may support other protocols besides IP
 - Segmenting and reassembly

- Link Layer Control & Adaptation (L2CAP)

- Link control protocol, provides connection-oriented and connectionless data services to upper layer protocols
 - Handles ACL and SCO connections
 - Handle QoS specifications per connection (logical channel)
 - Manages concepts as “group of connections”



- Host Controller Interface (HCI)

- Allows command line access to the baseband layer and LM for control and status information
 - Current interfaces: USB; UART; RS-232
- Made up of three parts:
 - HCI firmware, HCI driver, Host Controller Transport Layer



Host-Controller Interface (HCI)

- Specifies all interactions between a host and a Bluetooth radio controller
- Defines how commands, events, asynchronous and synchronous data packets are exchanged
- HCI Packet Types
 - Command (0x01)
 - Each command is assigned a 2 byte Opcode which it's divided into two fields, called the OpCode Group Field (OGF) and OpCode Command Field (OCF)
 - Asynchronous Data (0x02)
 - Synchronous Data (0x03)
 - Events (0x04)

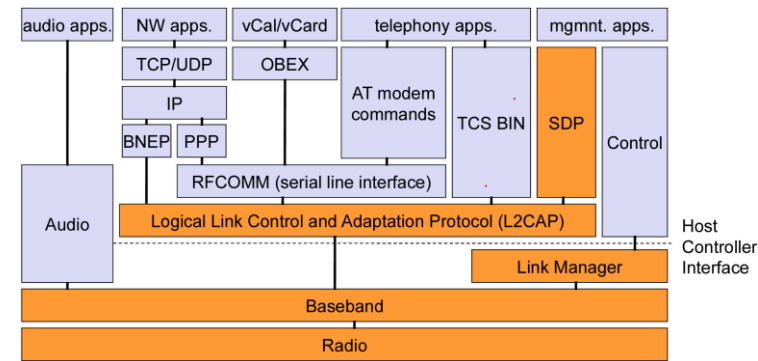
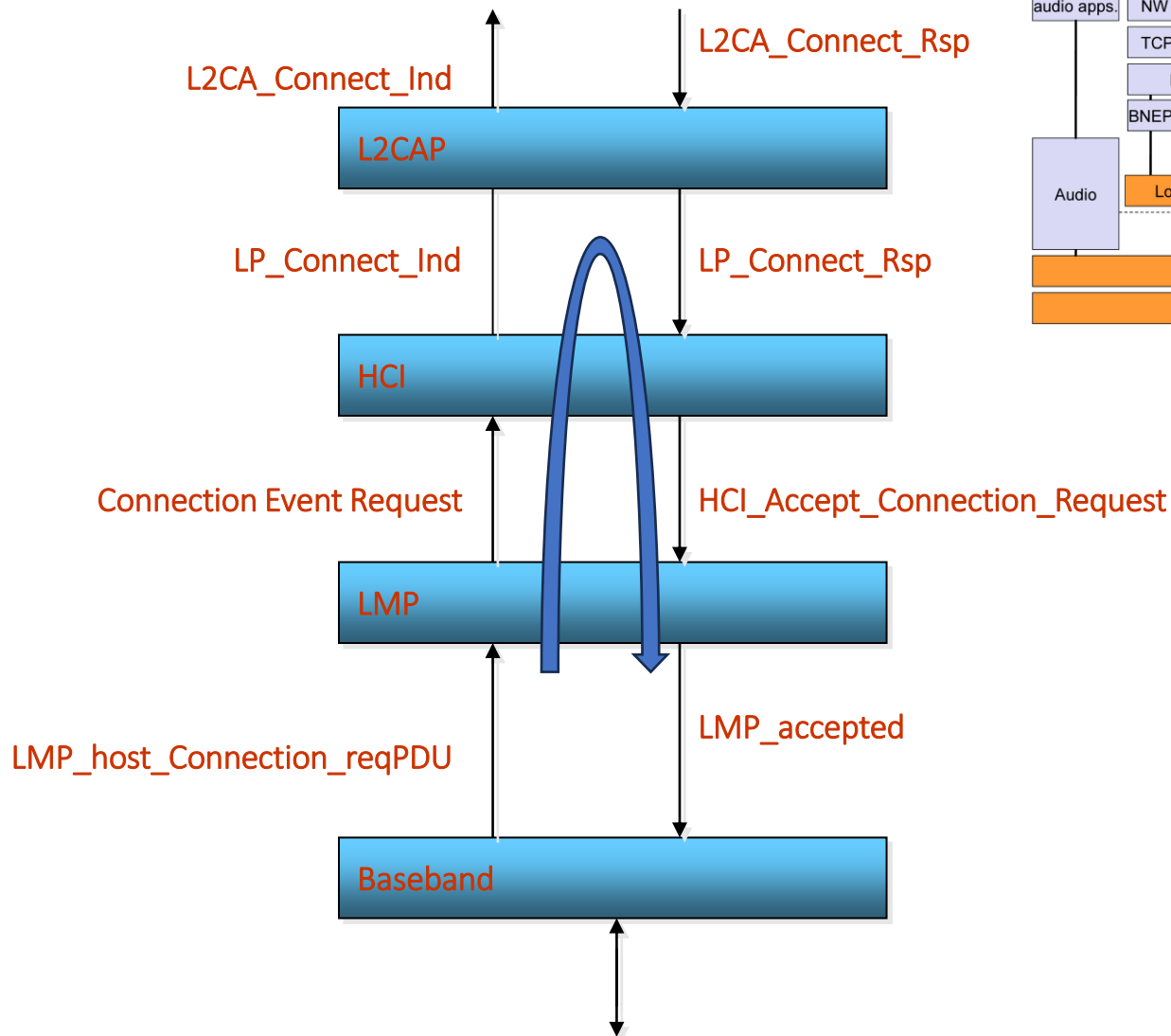
See Bluetooth Lab guide Annexes for packet formats

Complete list of HCI Commands, Events and Error Codes:

https://lisha.ufsc.br/teaching/shi/ine5346-2003-1/work/bluetooth/hci_commands.html

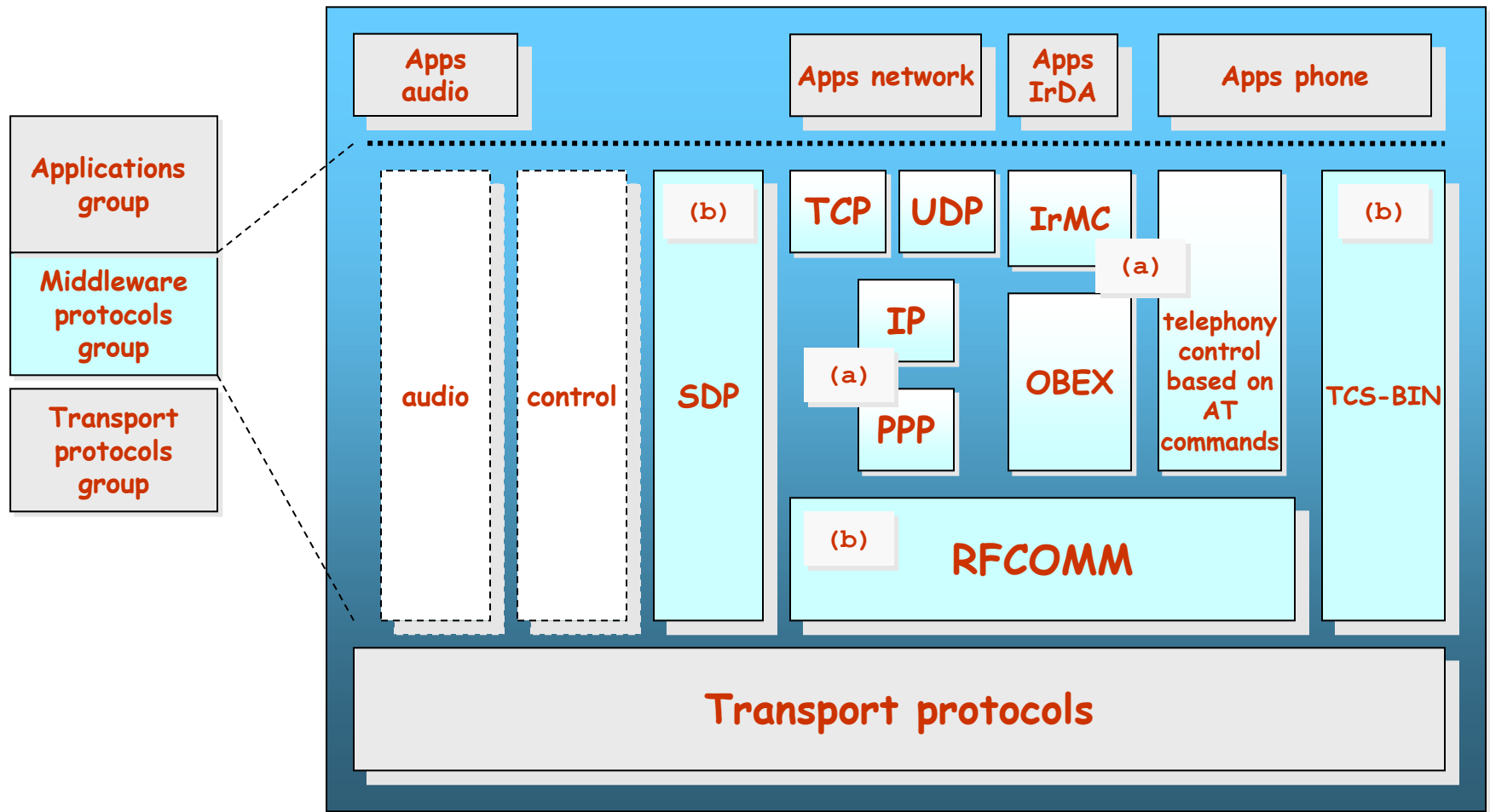


Interlayer communication





Protocols (middleware)



Protocol reuse

BT aims to reuse older protocols (e.g. WAP, OBEX-IrDA)

Interaction with applications and phones, as commonly done before

a: common protocol
b: Bluetooth dedicated protocol


SDP: Service Discovery Protocol

OBEX: Facilitates binary transfers between BT devices

TCP-BIN: Telephony-control protocol binary (call control)



Middleware

- **Service Discovery Protocol (SDP)**
 - Provides a way for applications to detect which services are available and their characteristics
 - Protocol question  answer
 - Search and browsing of services
 - Defines a format for service registry
 - Information provided by the service *attributes*, a name (ID) + value
 - IDs can be universal (UUID)



Middleware

- **RFCOMM** (Serial Port Emulation Protocol)
 - Based on GSM TS07.10
 - Emulates a serial port, supporting all traditional applications that were able to use a serial port
 - Supports multiple ports over a single physical channel between two devices
- **Telephony Control Protocol Spec (TCS)**
 - Handles call control (setup, release)
 - Group management for gateways, serving multiple devices
 - Audioconference, e.g.



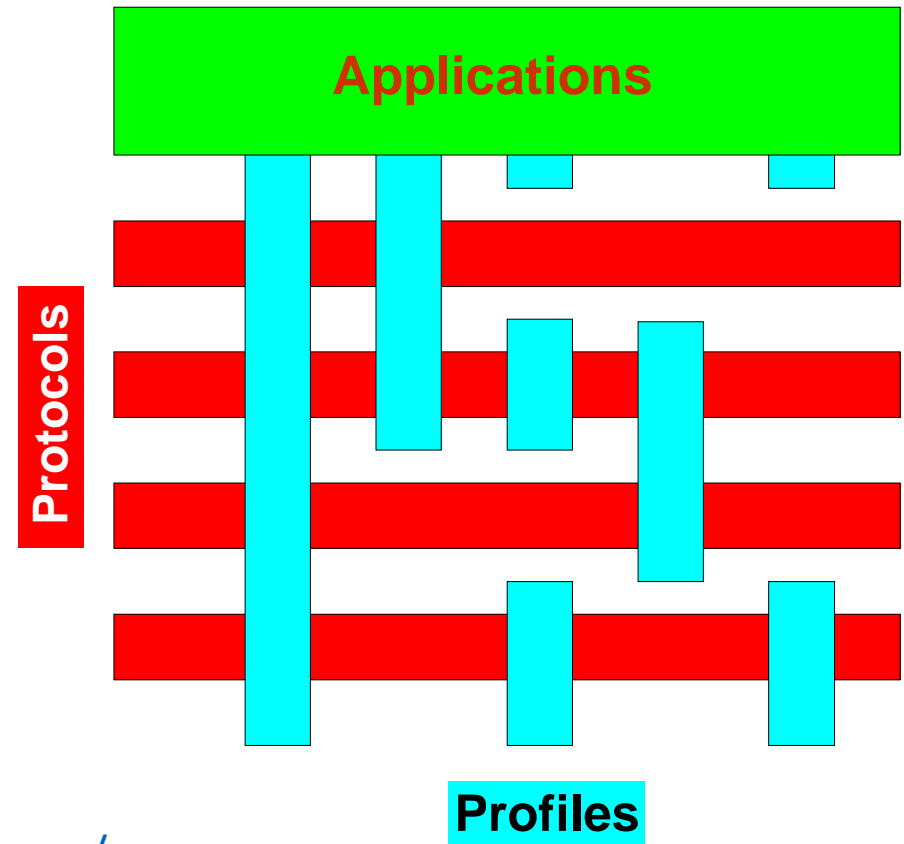
Outline

- Bluetooth networks
- Piconet operation
 - Inquiry
 - Paging
- Bluetooth stack
- Profiles and security
- BT 4.0 BLE



Interoperability: Profiles

- Profile: base for BT interoperability (BT too much flexible!)
- “vertical cut” in Bluetooth stack
- A given usage model (typical solution)
- Each BT device supports one or more profiles



<https://www.bluetooth.com/specifications/specs/>



Profiles (v.1)

- Generic Access
 - Profile SDA (*Service Discovery Application*)
 - Profiles for serial port, including:
 - Profile Dial-up
 - Profile Fax
 - Profile Headset
 - LAN Access (uses PPP)
 - Profile for generic object exchange (OBEX)
 - File transfer
 - Data synchronization
 - Push-pull
- Profile of cordless phone (TCS-BIN)
 - Profile interphone
 - Profile Cordless Telephony

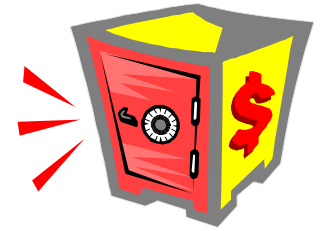


Profiles (v.2)

- **Advanced Audio Distribution Profile (A2DP)**
 - Dual-channel audio stream through a stereo headset
 - Can also be used to make calls, and users can switch between music and calls at the touch of a button
- **Audio/Video Remote Control Profile (AVRCP)**
 - Provides a standard interface to control TVs, hi-fi equipment, and so forth
 - A single remote control (or other device) to control all the AV equipment to which a user has access
 - Defines how to control characteristics of streaming media (pausing, stopping, and starting playback and volume control)
- **Hands-Free Profile (HFP)**
 - Use a gateway device to place and receive calls for a hand-free device
 - Example: vehicle using a mobile phone as a gateway device. Car's audio system and an installed microphone are used instead of the phone's audio



Bluetooth: security



- Devices can be:
 - “Trusted”
 - “Untrusted”
 - Also “unknown” devices
- Services security types:
 - Open services – cypher only
 - Authentication only – machine ID
 - Authentication and authorization (ID+explicit service grant)
- Levels of security:
 - Mode 1
 - No security
 - Mode 2
 - Security guaranteed at service level
 - Mode 3
 - Security guaranteed at link level

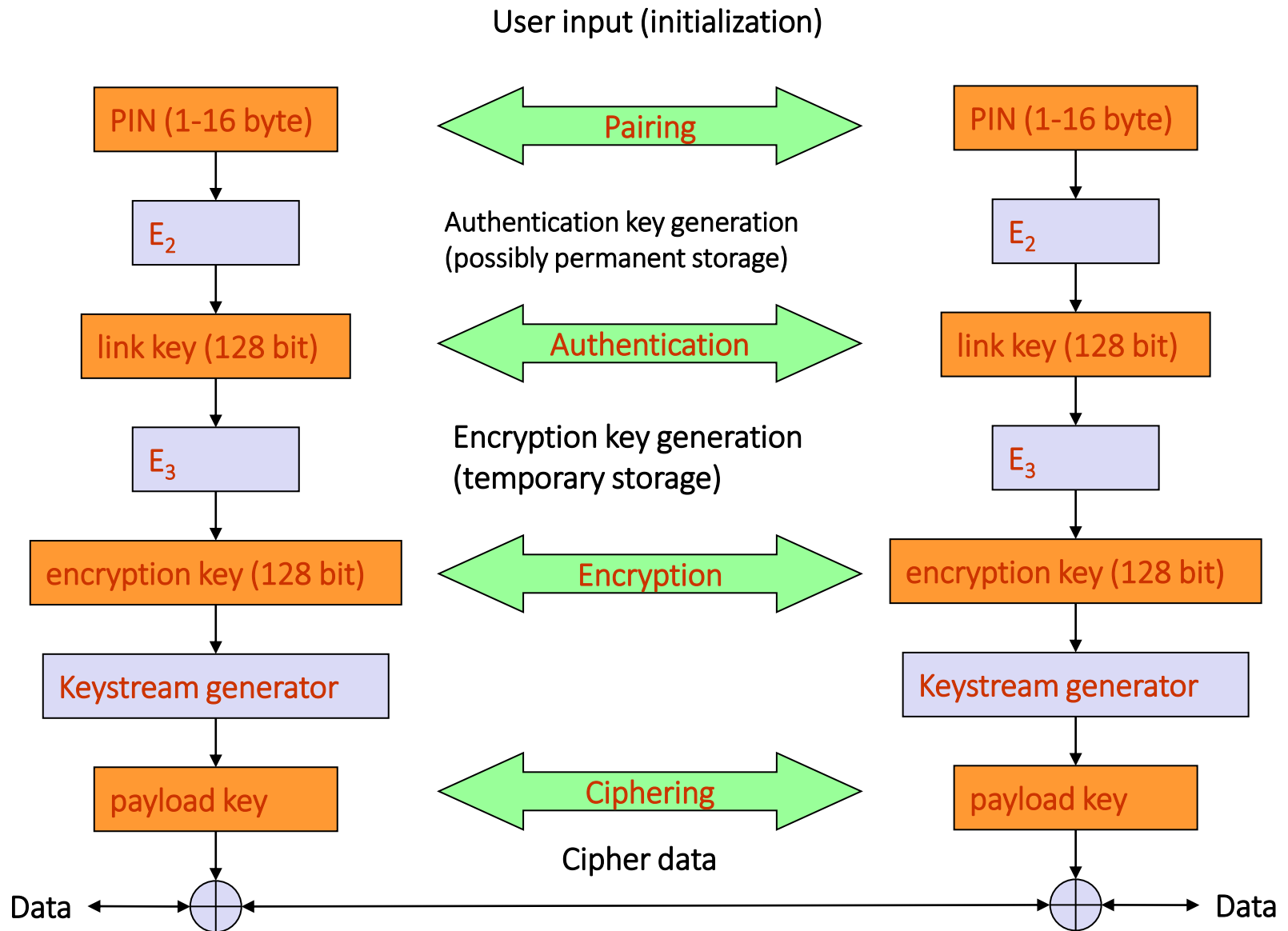


Bluetooth: security features

- Mechanisms used in BT for security
 - Fast frequency hopping
 - Low range
 - Authentication
 - Two way challenge/response mechanism
 - Cypher (to ensure privacy)
 - Data between two devices can be encrypted
 - Keys used
 - Cypher size configurable (0-16bytes) by the devices, but there are security constraints (government)
 - Keys using standard well-known algorithms
- Security initialization – device pairing
 - PIN (user input)
 - Shared key



Security





Outline

- Bluetooth networks
- Piconet operation
 - Inquiry
 - Paging
- Bluetooth stack
- Profiles and security
- BT 4.0 BLE



Bluetooth 4.0: Low Energy





Short range wireless application areas

	Voice	Data	Audio	Video	State
Bluetooth ACL/HS		Y	Y		
Bluetooth SCO/eSCO	Y				
Bluetooth low energy (BLE)					Y
Wi-Fi	(VoIP)	Y	Y	Y	
Wi-Fi Direct	Y	Y	Y		
ZigBee					Y

State = low bandwidth, average/low latency data

Low Power



What is Bluetooth Low Energy (BLE)?

- Bluetooth Low Energy is an open, short range radio technology
 - Blank sheet of paper design
 - Different to Bluetooth classic (BR/EDR)
 - Optimized for ultra low power
 - Enable coin cell battery use cases
 - < 20mA peak current
 - < 5 uA average current



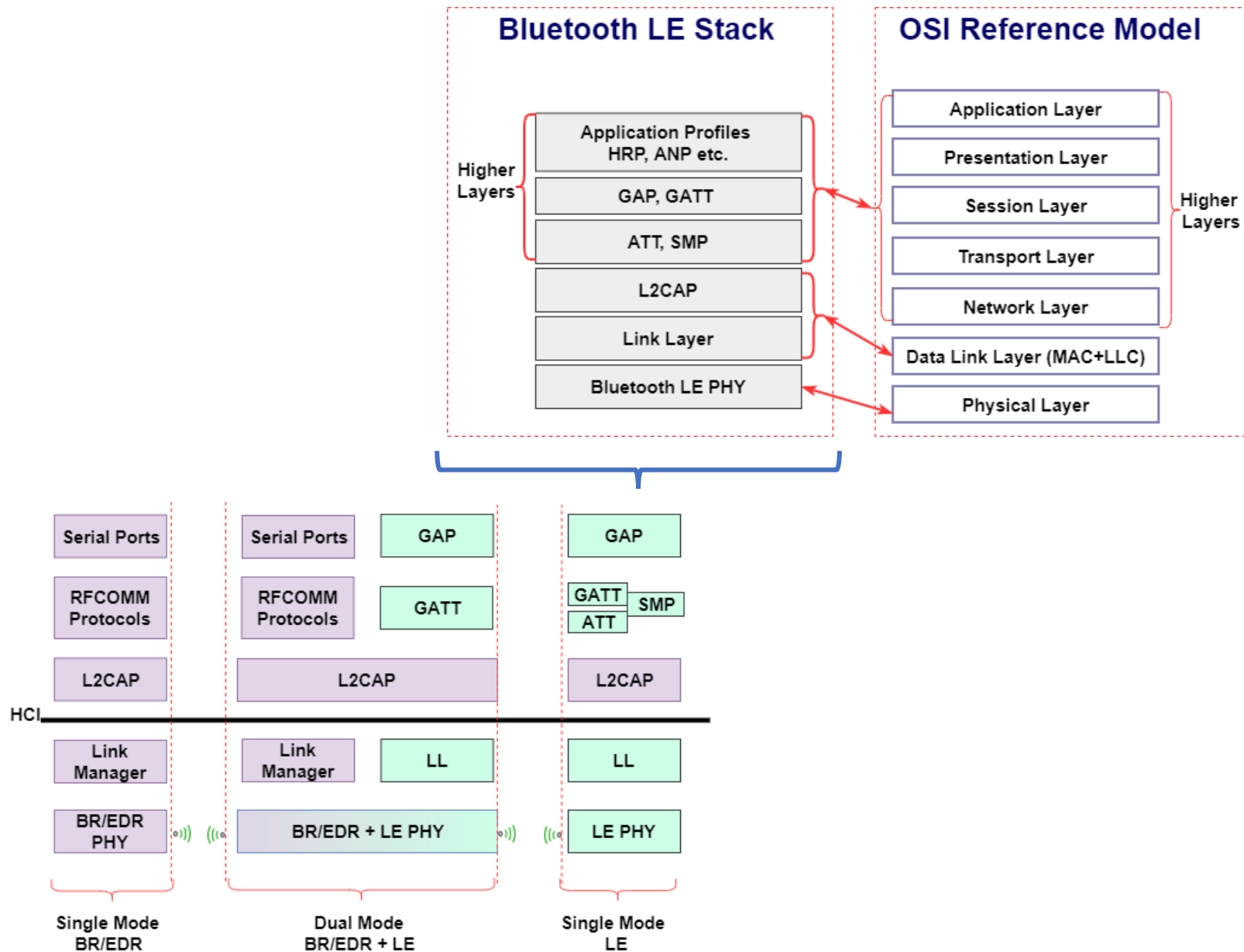


Basic concepts of BLE

- Everything is optimized for lowest power consumption
 - Short packets reduce TX peak current
 - Short packets reduce RX time
 - Less RF channels to improve discovery and connection time
 - Simple state machine
 - Single protocol
 - Needs a gateway for Internet access
 - Etc.



BLE Protocol Stack





Bluetooth Low Energy factsheet

Range:	~ 150 meters open field
Output Power:	~ 10 mW (10dBm)
Max Current:	~ 15 mA
Latency:	3 ms
Topology:	Star
Connections:	> 2 billion
Modulation:	GFSK @ 2.4 GHz
Robustness:	Adaptive Frequency Hopping, 24 bit CRC
Security:	128bit AES CCM
Sleep current:	~ 1μA
Modes:	Broadcast, Connection, Event Data Models, Reads, Writes