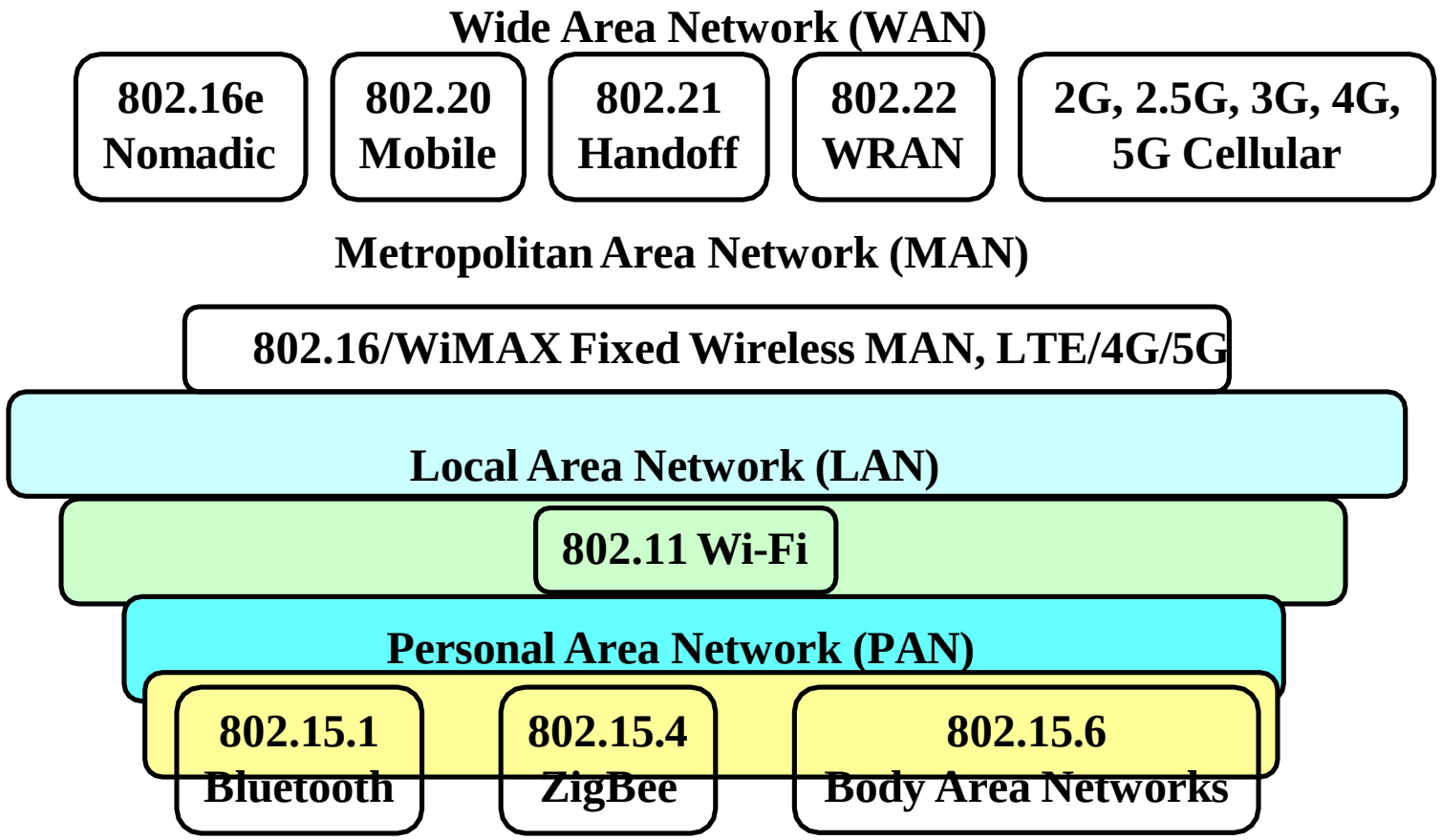
Overview

1. Bluetooth: Packet Format, Energy Management
2. Bluetooth Protocol Stack, Application Profiles
3. Bluetooth LE: Protocol Stack, PHY, MAC
4. Bluetooth and Wi-Fi Coexistence

Wireless Personal Area Networks (WPANs)



Bluetooth

- Started with Ericsson's Bluetooth Project in 1994 for radio-communication between cell phones over short distances
- Intel, IBM, Nokia, Toshiba, formed Bluetooth SIG in May 1998
- Version 1.0A of the specification came out in late 1999.
- IEEE 802.15.1 approved in early 2002 is based on Bluetooth Later versions handled by Bluetooth SIG directly
- Key Features:
  - Lower Power: 10 mA in standby, 50 mA while transmitting
  - Cheap: $5 per device
  - Small: 9 mm^2 single chips

Bluetooth Versions

- **Bluetooth 1.1**: IEEE 802.15.1-2002
- **Bluetooth 1.2**: IEEE 802.15.1-2005. Completed Nov 2003. Adaptive frequency hopping (avoid frequencies with interference).
- **Bluetooth 2.0** + Enhanced Data Rate (EDR) (Nov 2004): 3 Mbps using DPSK. For video applications. Reduced power due to reduced duty cycle
- **Bluetooth 2.1** + EDR (July 2007): Secure Simple Pairing to speed up pairing
- **Bluetooth 3.0**+ High Speed (HS) (April 2009): 24 Mbps using WIFI PHY + Bluetooth PHY for lower rates
- **Bluetooth 4.0** (June 2010): Low energy. Smaller devices requiring longer battery life (several years). New incompatible PHY. Bluetooth Smart or BLE
- **Bluetooth 4.1**: 4.0 + Core Specification Amendments (CSA) 1, 2, 3, 4
- **Bluetooth 4.2** (Dec 2014): Larger packets, security/privacy, IPv6

Ref: ITL, "Security of Bluetooth Systems and Devices," http://csrc.nist.gov/publications/nistbul/august-2012_itl-bulletin.pdf

Bluetooth 5

$$P(dBm)=10\cdot\log10(P(mW))$$

- June/December 2016
- Enhanced Bluetooth low energy
- Supports many more devices at low energy, e.g., headphones,
- Dual-audio: two headphones playing two streams
- 2X Data rate using a new modulation ⇒ 2 Mbps

Or 4X range 800 ft using a special coding (Good for beacons) Long-Range mode allows 1.6 km at 125 kbps

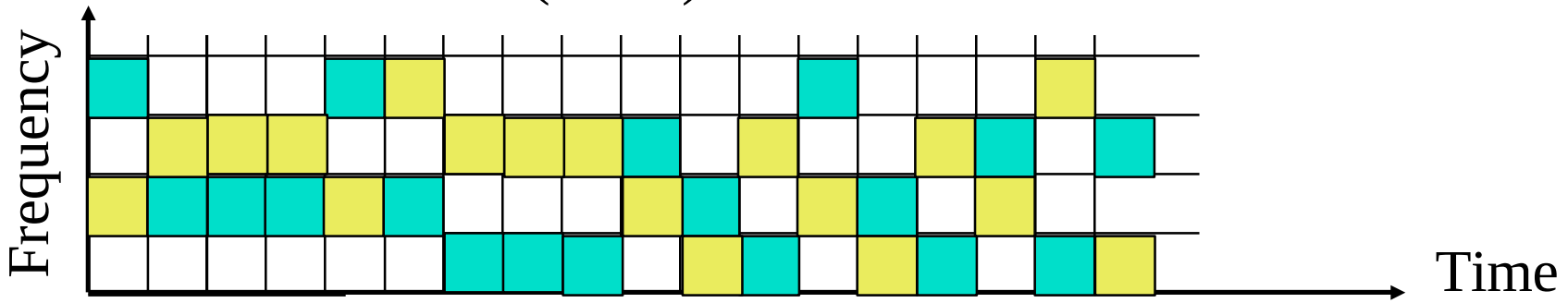
- compression allows CD quality audio over 1 Mbps. Bluetooth 5.0 allows better quality using 2 Mbps.
- +20 dBm transmit power in LE mode ⇒ Good for bursts
- Both ends must be Bluetooth 5 to benefit. Backward compatible with older devices using older modes

Ref: Madhur Bhargava, " IoT Projects with Bluetooth Low Energy," Packt Publishing, August 2017, 278 pp.,

ISBN:978-1-78839-683-7 (Safari Book).

Bluetooth: Details

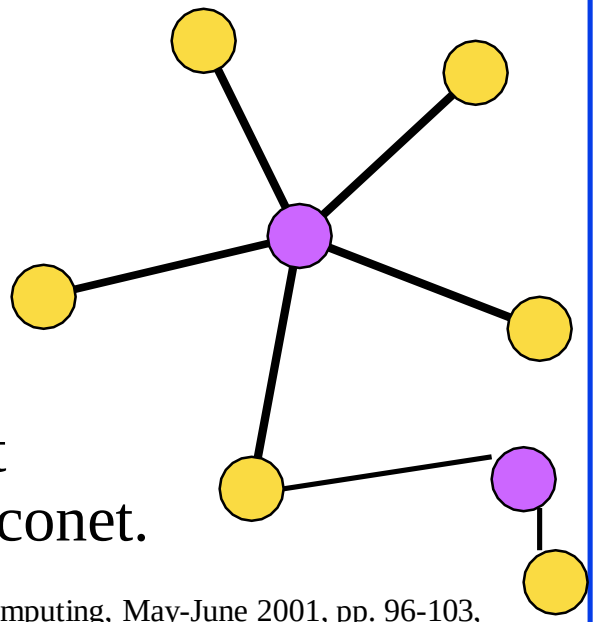
- **Frequency Range:** 2401 - 2480 MHz
  (total 79 MHz band) 23 MHz in some countries, e.g., Spain
- **Data Rate:** 1 Mbps
- **Radio Frequency hopping:** 1600 times/s ⇒ 625 us/hop
- **Security:** Challenge/Response Authentication. 128b Encryption
- **TX Output Power:**
  - Class 1: 20 dBm Max. (0.1W) – 100m
  - Class 2: 4 dBm (2.5 mW)
  - **Class 3**: 0 dBm (1mW) – 10m



Ref: http://www.bluetooth.com/, http://www.bluetooth.org/, http://grouper.ieee.org/groups/802/15/index.html _

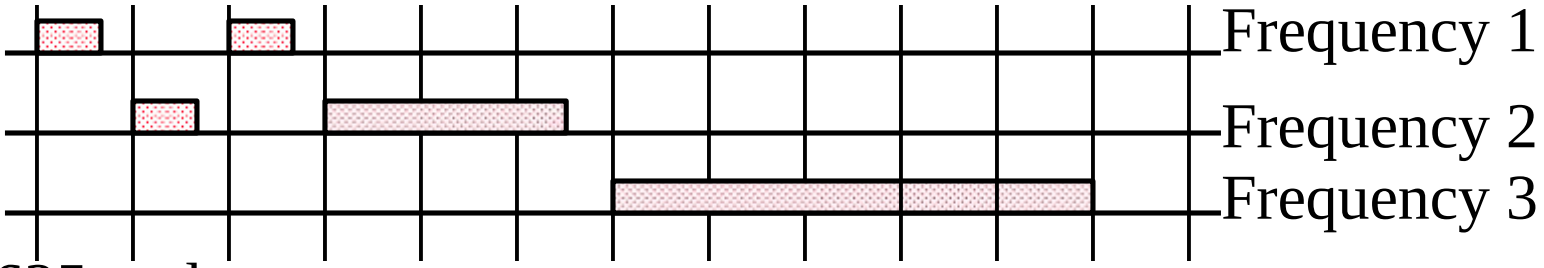
Piconet

- Piconet is formed by a master and many slaves
  - Up to 7 active slaves.
    Slaves can only transmit when requested by master
  - Up to 255 Parked slaves
- Active slaves are polled by master for transmission
- Each station gets a 8-bit parked address
  $\Rightarrow$ 255 parked slaves/piconet
- The parked station can join in 2us.
- Other stations can join in more time.
- **Scatter net**: A device can participate in multiple Pico nets $\Rightarrow$ Timeshare and must synchronize to the master of the current piconet.



Ref: P. Bhagwat, "Bluetooth Technology for short range wireless Apps," IEEE Internet Computing, May-June 2001, pp. 96-103, bluetooth.pdf (Must read)

Frequency Hopping Sequences



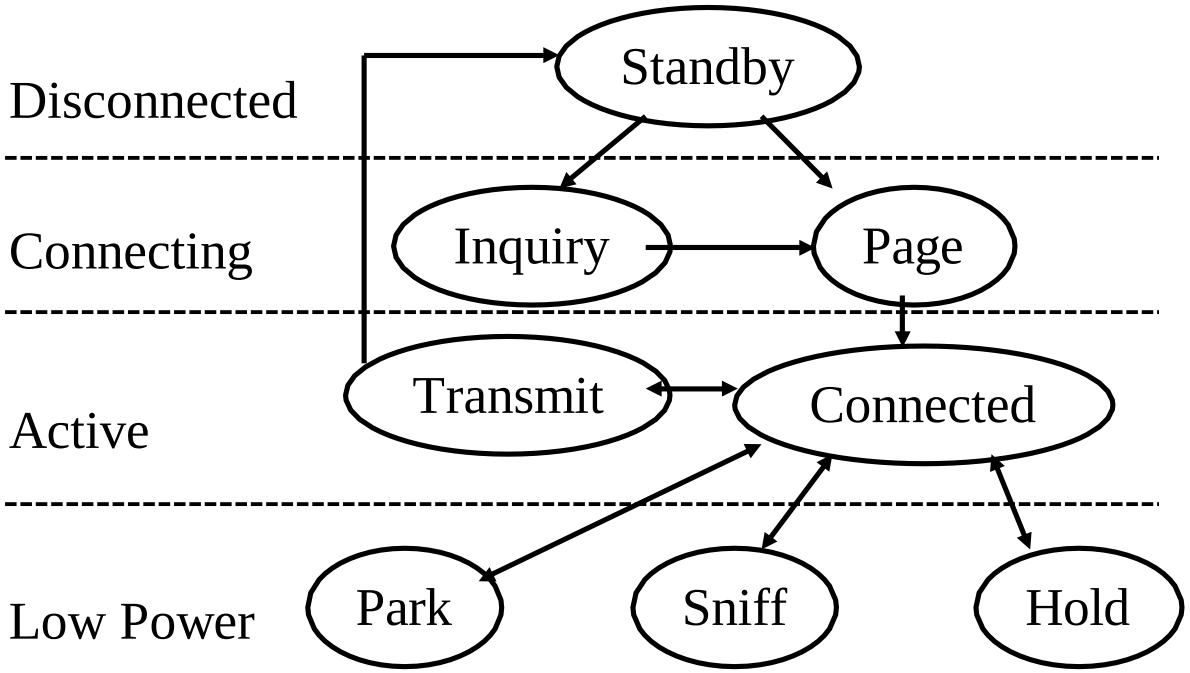
- 625us slots
- Time-division duplex (TDD)
  ⇒ Downstream and upstream alternate
- Master starts in even numbered slots only.
- Slaves start in odd numbered slots only
- Slaves can transmit in one slot right after receiving a packet from master
- Packets = 1 slot, 3 slot, or 5 slots long
- The frequency hop is skipped during a packet.

Bluetooth Packet Format

Access Code	Baseband/Link Control Header	Data Payload
72b	54b	0-2745b

- Packets can be up to five slots long. 5 slots =3125 bits.
- Access codes:
  - Channel access code identifies the piconet
  - Device access code for paging requests and response
  - Inquiry access code to discover units
- Header: member address (3b), type code (4b)(V/A/C), flow control(1b)), ack/nack (1b), sequence number(1b), and header error check (8b) 18b
- Synchronous traffic has periodic reserved slots.
- Other slots can be allocated for asynchronous traffic

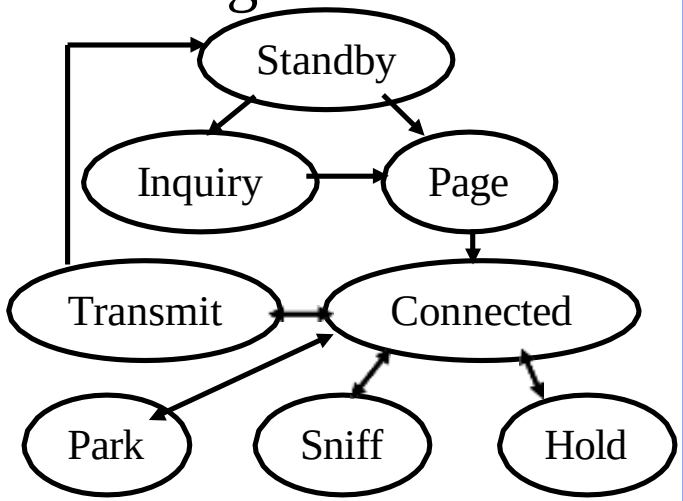
Bluetooth Operational States



- **Standby**: Initial state
- **Inquiry**: Master sends an inquiry packet. Slaves scan for inquiries and respond with their address and clock after a random delay (CSMA/CA)

Bluetooth Operational States (Cont)

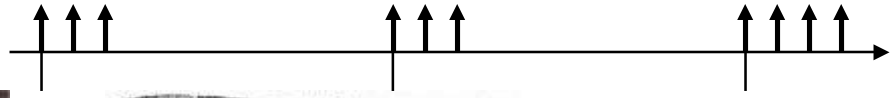
- **Page**: Master in page state invites devices to join the piconet. Page message is sent in 3 consecutive slots (3 frequencies). Slave enters page response state and sends page response including its device access code.
- Master informs slave about its clock and address so that slave can participate in piconet. Slave computes the clock offset.
- **Connected**: A short 3-bit logical address is assigned
- **Transmit**:



Energy Management in Bluetooth

Three inactive states:

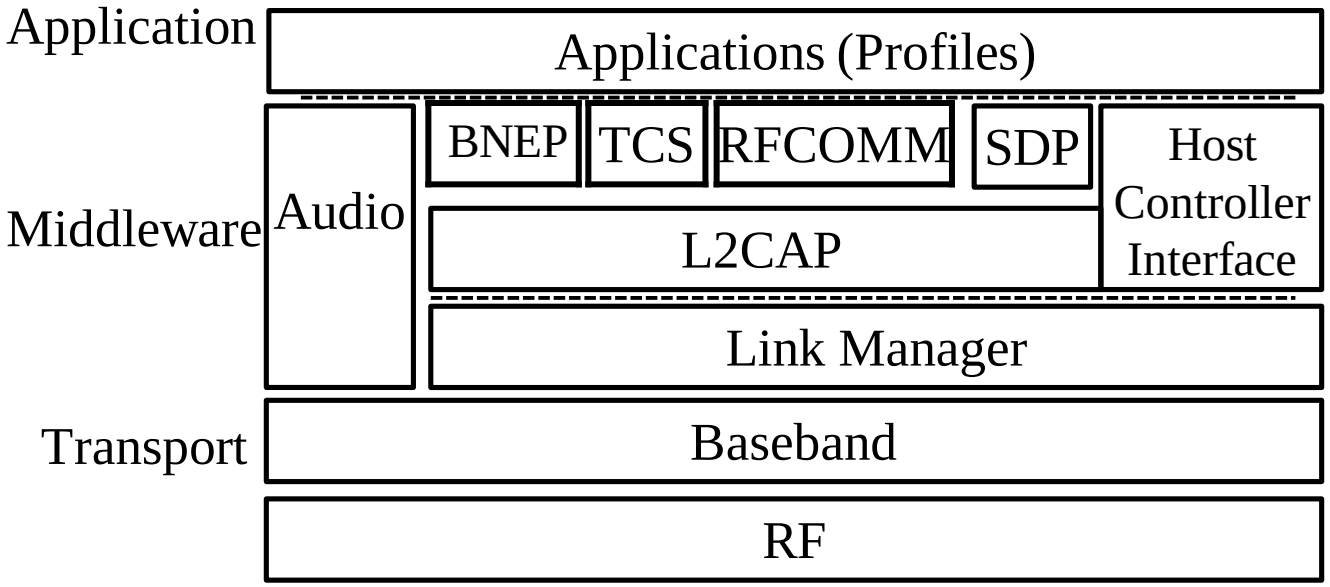
1. **Hold**: No Asynchronous Connection List (ACL). Synchronous Connection Oriented (SCO) continues.
   Node can do something else: scan, page, inquire
2. **Sniff**: Low-power mode. Slave listens after fixed sniff intervals.
3. **Park**: Very Low-power mode. Gives up its 3-bit active member address and gets an 8-bit parked member address. Wake up periodically and listen to beacons. Master broadcasts a train of beacons periodically



Sniff

Park

Bluetooth Protocol Stack



- **RF**: Frequency hopping Gaussian Frequency Shift Keying (GFSK) modulation
- **Baseband**: Frequency hop selection, connection, MAC

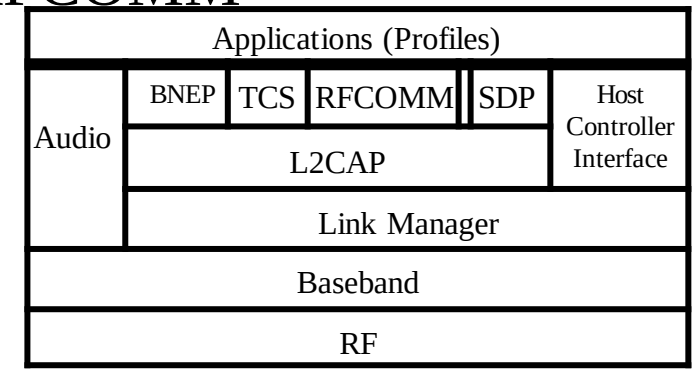
Baseband Layer

- Each device has a 48-bit IEEE MAC address
- 3 parts:
  - Lower address part (LAP) – 24 bits
  - Upper address part (UAP) – 8 bits
  - Non-significant address part (NAP) - 16 bits
- UAP+NAP = Organizationally Unique Identifier (OUI) from IEEE
- LAP is used in identifying the piconet and other operations

Upper Address Part	Non-sig. Address Part	Lower Address Part
8b	16b	24b

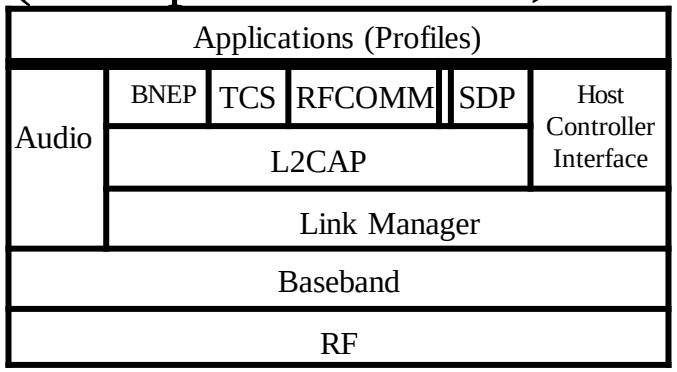
Bluetooth Protocol Stack (Cont)

- **Link Manager:** Negotiate parameters, Set up connections
- **Logical Link Control and Adaptation Protocol (L2CAP)**:
  - Protocol multiplexing
  - Segmentation and reassembly
  - Controls peak bandwidth, latency, and delay variation
- Host **Controller Interface**: Chip independent interface to Bluetooth chip. Allows same software to run on all chips.
- **RFCOMM Layer**: Presents a virtual serial port
  - Sets up a connection to another RFCOMM
- **Service Discovery Protocol (SDP):** Devices can discover the services offered and their parameters



Bluetooth Protocol Stack (Cont)

- **Bluetooth Network Encapsulation Protocol (BNEP):** To transport Ethernet/IP packets over Bluetooth
- **IrDA Interoperability protocols**: Allow existing IrDA applications to work w/o changes. IrDA object Exchange (IrOBEX) and Infrared Mobile Communication (IrMC) for synchronization
- **Audio** is carried over 64 kbps over SCO links over baseband
- **Telephony control specification binary (TCS-BIN)**: Call control including group management (multiple extensions, call forwarding, and group calls)
- **Application Profiles**: Set of algorithms, options, and parameters.



Application Profile Examples

- Headset Profile
- Global Navigation Satellite System Profile
- Hands-Free Profile
- Phone Book Access Profile
- SIM Access Profile
- Synchronization Profile
- Video Distribution Profile
- Blood Pressure Profile
- Cycling Power Profile
- Find Me Profile
- Heart Rate Profile
- Basic Printing Profile
- Dial-Up Networking Profile
- File Transfer Profile

Ref: Bluetooth SIG, "Adopted Bluetooth Profiles, Services, Protocols and Transports," https://www.bluetooth.org/en-us/specification/adopted-specifications

Bluetooth Smart

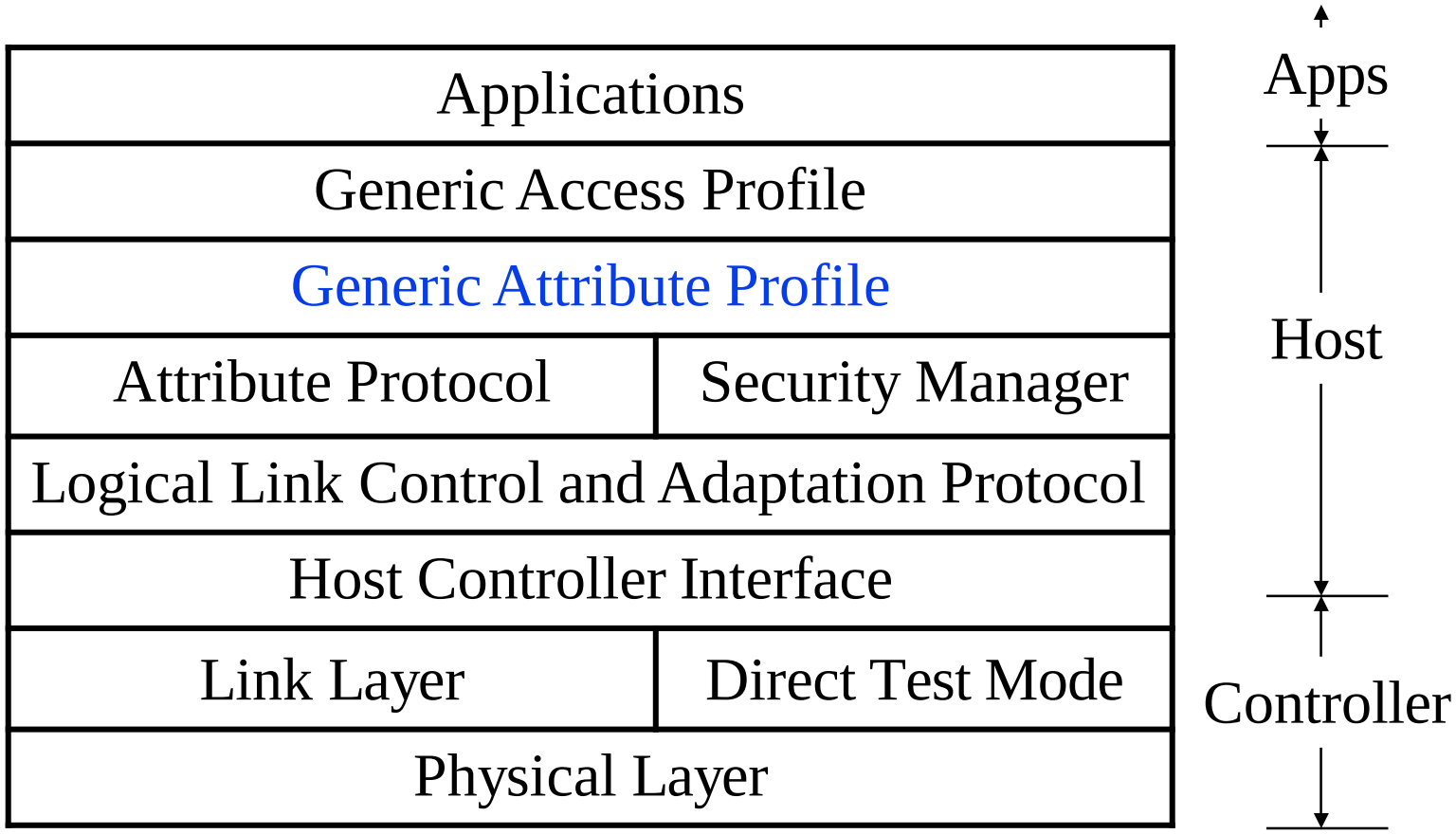
- **Low Energy**: 1% to 50% of Bluetooth classic
- **For short broadcast**: Your body temperature, Heart rate, Wearables, **sensors**, automotive, industrial.
  Not for voice/video, file transfers, …
- **Small messages**: 1Mbps data rate but throughput not critical.
- **Battery life**: In years from coin cells
- **Simple**: Star topology. No scatter nets, mesh, …
- **Lower cost** than Bluetooth classic
- New protocol design based on Nokia's **WiBree** technology
  Shares the same 2.4GHz radio as Bluetooth
  ⇒ All new smart phones (iPhone, Android, …) have dual-mode chips

Bluetooth Smart PHY

- 2.4 GHz. 150 m open field
- Star topology
- 1 Mbps Gaussian Frequency Shift Keying
  Better range than Bluetooth classic
- Adaptive Frequency hopping. 40 Channels
  with 2 MHz spacing.
- 3 channels reserved for advertising and 37 channels for data
- Advertising channels specially selected to avoid interference with Wi-Fi channels

Ref: J. Decuir, “Bluetooth 4.0: Low Energy,” 2010,
https://californiaconsultants.org/wp-content/uploads/2014/05/CNSV-1205-Decuir.pdf

Bluetooth Smart Protocol Stack



Ref: J. Decuir, "Bluetooth 4.0: Low Energy," 2010,
https://californiaconsultants.org/wp-content/uploads/2014/05/CNSV-1205-Decuir.pdf

Bluetooth Gateway Devices

- A gateway device helps connect a Bluetooth device to the Internet. Smart phone, Tablets, PC, …
- A generic app can forward the data to the URL sent by the device

Bluetooth Smart Applications

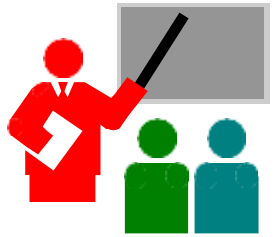
- Proximity: In car, In room, In the mall
- Locator: Keys, watches, Animals
- Health devices: Heart rate monitor, physical activities monitors, thermometer
- Sensors: Temperature, Battery Status, tire pressure
- Remote control: Open/close locks, turn on lights

Ref: E. Vlugt, “Bluetooth Low Energy, Beacons and Retail,” Verifone White paper, 2013, 12 pp., https://www.slideshare.net/verifone/bluetooth-low-energy-beacons-and-retail-final

Beacons

- Advertising based on proximity
- Peripherals (your phone) broadcasts its presence if Bluetooth is turned on
- Primary aim of these broadcasts is to allow device discovery and indoor navigation
- iOS7 iPhones can send/received iBeacons
- Can be used for customized advertising, indoor location, geofencing
- Google is promoting Eddystone beacons which requires only a browser (not another app) to discover proximity using beacons

Summary



1. Bluetooth basic rate uses frequency hoping over 79 1-MHz channels with 1, 3, 5 slots packets.
2. Three inactive states: hold, sniff, park. Has a fixed set of applications called "Profiles"
3. Bluetooth and WIFI co-exist by time-sharing or adaptive frequency notching
4. Bluetooth Smart is designed for short broadcasts by sensors. 40 2-MHz channels with 3 channels reserved for advertising. One or two-message exchanges
5. Generic attribute profile allows new applications using UUID for data types

Homework 11

- Submit answer to the following Problem:
  Assume that in one slot in Bluetooth 256 bits of payload could be transmitted. How many slots are needed if the payload size is (a) 512 bits, (b) 728 bits, and (c) 1024 bits. Assume that the non-payload portions do not change.

Reading List: Bluetooth

- Madhur Bhargava, " IoT Projects with Bluetooth Low Energy," Packt Publishing, August 2017, 278 pp., ISBN:978-1-78839-683-7 (Safari Book).
- Kevin Townsend, Carles Cufí, Akiba, Robert Davidson, "Getting Started with Bluetooth Low Energy," O'Reilly Media, Inc., May 2014, 180 pp., ISBN:978-1-4919-4951-1 (Safari Book), Chapter 2.
- J. Decuir, “Bluetooth 4.0: Low Energy,” 2010, 62 pp., https://californiaconsultants.org/wp-content/uploads/2014/05/CNSV-1205-Decuir.pdf
- E. Vlugt, “Bluetooth Low Energy, Beacons and Retail,” Verifone White paper, 2013, 12 pp., https://www.slideshare.net/verifone/bluetooth-low-energy-beacons-and-retail-final
- P. Bhagwat, "Bluetooth Technology for short range wireless Apps," IEEE Internet Computing, May-June 2001, pp. 96-103, http://ieeexplore.ieee.org/xpl/abstractKeywords.jsp?arnumber=935183

References

- Bluetooth SIG, http://www.bluetooth.com/lowenergy
- Bluetooth SIG, “BLUETOOTH 4.1 Features and Technical Description,” 2013, https://www.bluetooth.org/en-us/Documents/Bluetooth%204.1%20Technical%20Description.pdf
- Bluetooth SIG, "Adopted Bluetooth Profiles, Services, Protocols and Transports," https://www.bluetooth.org/en-us/specification/adopted-specifications
- http://whatis.techtarget.com/definition/Bluetooth-20EDR
- ITL, "Security of Bluetooth Systems and Devices," http://csrc.nist.gov/publications/nistbul/august-2012_itl-bulletin.pdf
- E. Ferro and F. Potorti, ""Bluetooth and Wi-Fi wireless protocols: a survey and a comparison", Volume: 12 Issue: 1, Pages: 12-26, IEEE Wireless Communications, 2005, http://ieeexplore.ieee.org/iel5/7742/30466/01404569.pdf?tp=&arnumber=1404569&isnumber=30466