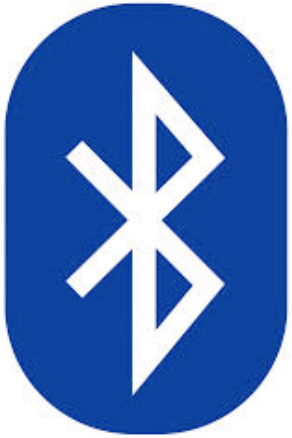


Bluetooth

Bluetooth Classic – Bluetooth 4

Bluetooth Low Energy – Bluetooth 5

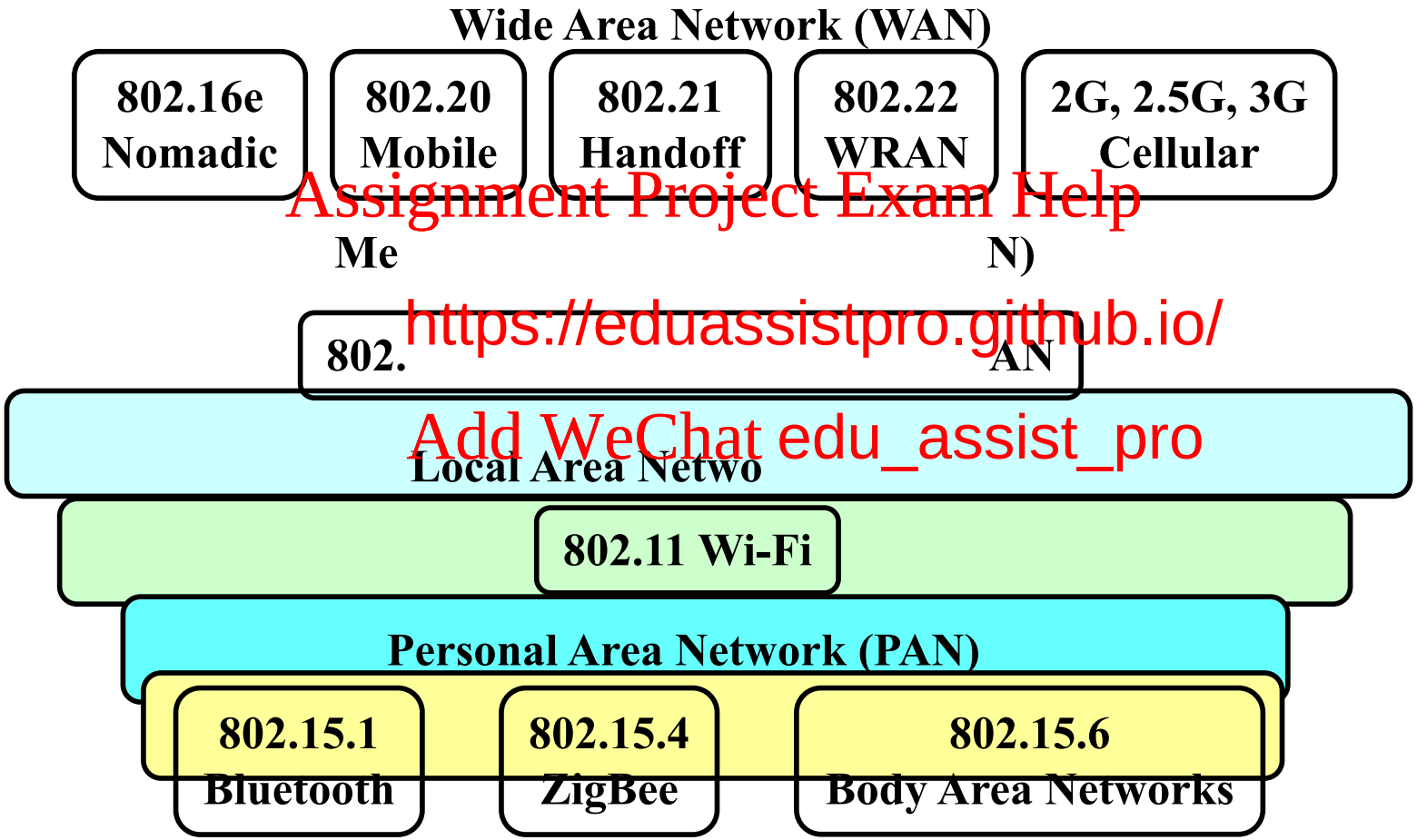
BLE

Overview

1. **Bluetooth History:** Wireless Personal Area Networks (WPANs) and IEEE 802.15 projects, Bluetooth Special Interest Group (SIG), Bluetooth Versions
2. **Bluetooth Markets and Applications**
3. **Bluetooth Cla**y, Channel Structure, Modulation an Hopping, Packet Format, Operating States, Pow Protocol Stack, Application Profiles
4. **Bluetooth Low Energy (BLE):** Channel Structure, Frequency Hopping, PHY, MAC
5. **Bluetooth 5:** PHY, Advertising, and Frequency Hopping Extensions

Wireless Personal Area Networks (WPANs)

- 10m or less



WPAN: Design Challenges

- **Battery powered**: Maximize battery life.
  A few hours to a few years on a coin cell.
- **Dynamic topologies**: Short duration connections and then device is turned off or goes to sleep
- **No infrastruct** ase station
- **Avoid Interfer** ed LAN devices
- **Simple and Extreme Interop** llions of devices.
  More variety than LAN or MAN
- **Low-cost**: A few dollars

IEEE 802.15 Projects

- **IEEE 802.15.1-2005**: **Bluetooth** 1.2
- **IEEE 802.15.4-2011**: Low Rate (250kbps) WPAN – **ZigBee**
- **IEEE 802.15.4f-2012**: PHY for Active **RFID**
- **IEEE 802.15.6-** king, Medical and entertainment. L
- **IEEE 802.15.7-2011**: Visible L nications

Bluetooth

Bluetooth SIG → IEEE 802.15.1 → Bluetooth SIG

- Started with Ericsson's Bluetooth Project in 1994 for radio-communication between cell phones over short distances
- Named after Danish king Herald Blåtand (=Bluetooth) (AD 940-981) who was fond of blueberries
- Intel, IBM, Nokia formed Bluetooth SIG in May 1998
- Version 1.0A of the specification in late 1999.
- IEEE 802.15.1 approved in early ed 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

Example of a Bluetooth Chipset

Bluetooth Versions

- **Bluetooth 1.1**: IEEE 802.15.1-2002
- **Bluetooth 1.2**: IEEE 802.15.1-2005. *Adaptive frequency hopping (avoid frequencies with interference)*
- **Bluetooth 2.0** + (Nov 2004): 3 Mbps using DPSK. For ed power due to reduced duty cyc
- **Bluetooth 4.0** (June 2010): Low ler devices requiring longer battery life (seve ew incompatible PHY. Bluetooth Smart or BLE
- **Bluetooth 5.0** (December 2016): Make BLE go faster and further.

The Rise of Bluetooth

Source: Bluetooth SIG

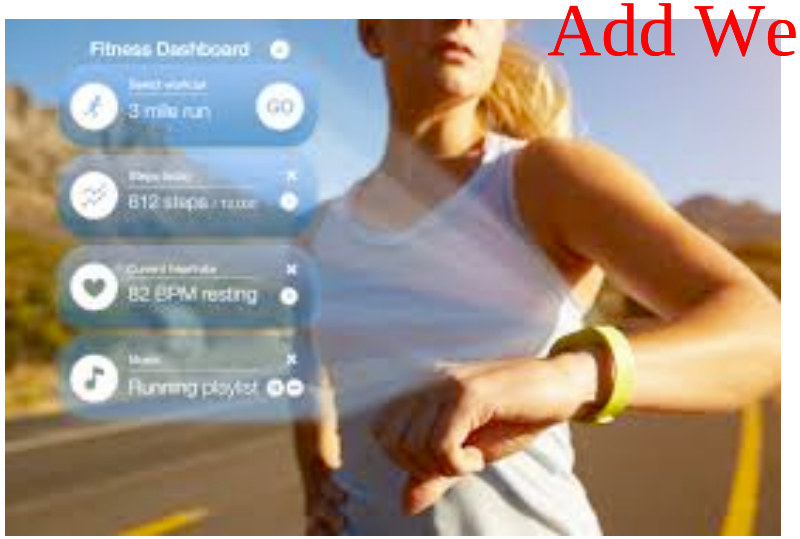
Bluetooth technology is factory installed in most new vehicles

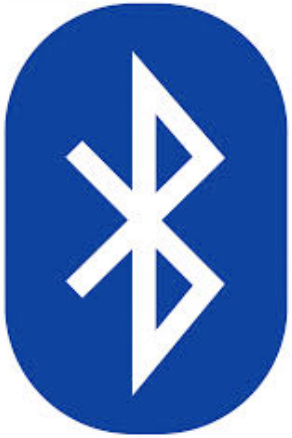
87%

OF NEW CARS

come standard with Bluetooth® technology

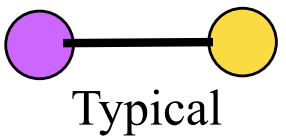
The Bluetooth

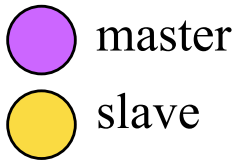


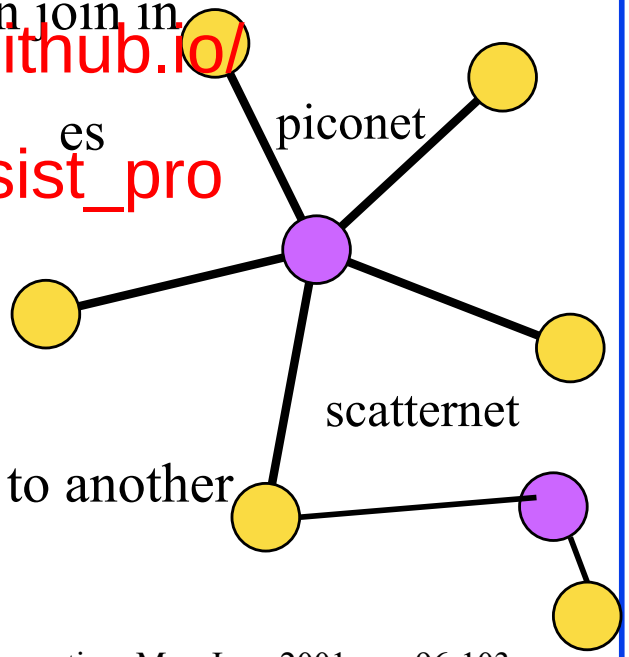


Bluetooth Network Topology: Piconet

- Piconet is formed by a master and many slaves (typically 1)
  - 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
- Any device can become a master (initiator becomes master)
- Each station gets an 8-bit parked address
  ⇒ 255 parked slaves/piconet
- A parked station can an join in more time.
- Slaves can only transmit/receive to/fro es cannot talk to another slave in the picon
- **Scatter net**: A device can participate in multiple Pico nets ⇒ Timeshare and must synchronize to the master of the current piconet. *Active* in one piconet, *parked* in another.
- Routing protocol not defined (a node can only talk to another node if within Bluetooth range of 10m)







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

Bluetooth Operating Spectrum

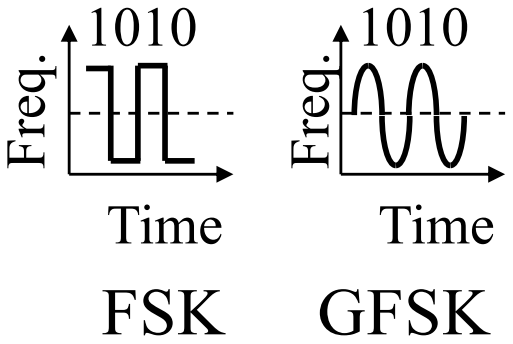
Bluetooth Channels

f_c = (2402+k) MHz; k = 0, 1, …, 78

k: channel index (79 1-MHz wide channels)

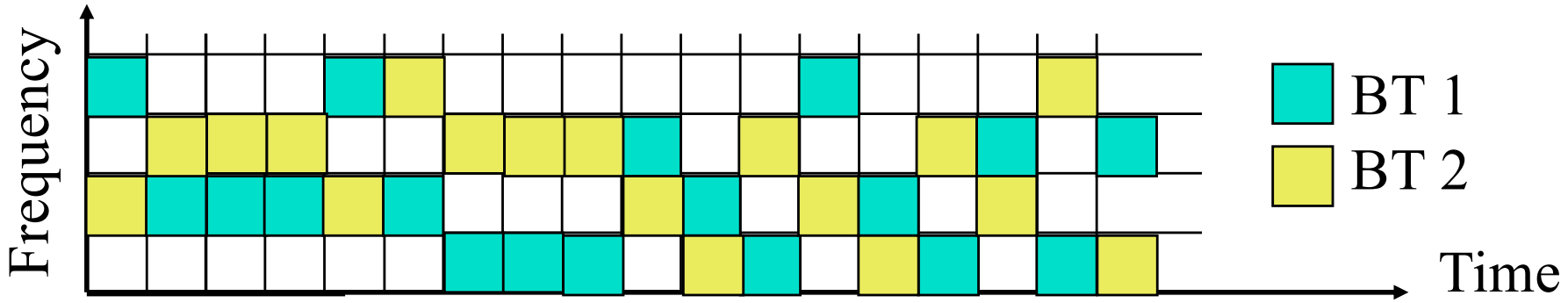
Modulation and Data Rate

- Basic rate (BR):
  - Binary Gaussian FSK (GFSK): 1 bit/symbol
  - Symbol duration = 1 μs: 1 Msps
  - Data rate: 1 Mbps
- Enhanced dat
  - Symbol duration is still 1 μ but
  - μ/4-DQPSK; 2 bits/symbol; 2 Mbps
  - 8DPSK: 3 bits/symbol; 3 Mbps



Frequency Hopping (1)

- Unlike WiFi, Bluetooth constantly switches channel within the same connection to avoid collisions with other nearby Bluetooth communications
- No two packets are transmitted on the same channel/frequency, but frequency is n dle of a packet transmission
- Such frequency switching is kno ency hopping



Frequency Hopping (2)

- Bluetooth connections are slotted: packet transmission can start only at the beginning of a time slot
- 625 μs slots using a 312.5 μs (3200Hz) clock (1 slot = 2 clock ticks)
- Time-division duplex (TDD)
  ⇒ Downstream (m slave-to-master) alternate
- Master starts in eve
- Slaves start in odd numbered slots onl
- Slaves can transmit right after receivi om master
- Packets = 1 slot, 3 slot, or 5 slots long
  - Enables master to start in even and slave in odd slots
- The frequency hop is skipped during a packet; frequency is hopped only at slot boundaries; at the beginning of the next slot after packet transmission/reception is complete; packet lengths may not align with slot boundaries

Frequency Hopping Illustrated

0 1 2 3 4 5

M=master, S = slave

Frequency Hopping Rate

1 frequency hop per packet: a packet can be 1,3, or 5 slot long (no hop in the middle of the packet); maximum FH rate = 1600Hz, minimum FH rate = 320Hz

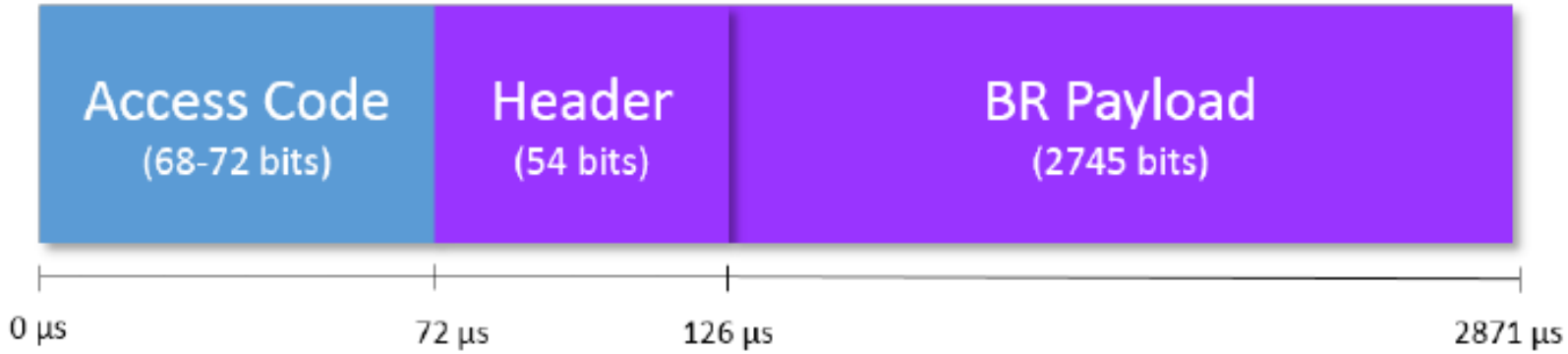
Example

- Consider a Bluetooth link where the *master* always transmits 3-slot packets. The transmission from the master is always followed up by a single-slot transmission from a *slave*. Assuming 625 μs slots, what is the effective frequency hopping rate (# of hopping per second)?

Answer: Given that fre in the middle of a packet transmission, we only op per 2 slots.

The effective hopping rate = $1/(2x625x10^{-6}$ s = 800Hz

Bluetooth Packet Format: Basic Rate (BR)



- Packets can be up to 5=3125 µs.
  - Maximum packe µs (@1Mbps)
  - Some *residual* slot-time cannot be 125)
- 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)+flow control (1b)+ack/nack (1b)+sequence number (1b)+header error check (8b)=18b, which is encoded using 1/3 rate FEC resulting in 54b

Example

- How many slots are needed to transmit a Bluetooth Basic Rate packet if the payload is (a) 400 bits, (b) 512 bits, and (c) 2400 bits. Assume that the non-payload portions do not change.
- Answer:
  - Bluetooth transmissions are 1, 3, or 5 slots (2, 4, 6, etc. not allowed)
  - Non-payload bits
  - Each slot can car
  - (a) 400b payload → 400+126 = 526b packet → 1 slot
  - (b) 512b payload → 512+126 = 638b packet → 2 slots would be sufficient, but will have to be padded for a 3-slot transmission (2-slot packets not allowed)
  - (c) 2400b payload → 2400+126 = 2526b packet → 5 slots

Bluetooth Packet Format: Enhanced Data Rate (EDR)

- Modulation changes within the packe[illegible] y a *guard interval lasting between 4.75 μs and 5.25 μs*
- GFSK for Access Code and Header
- μ/4-DQPSK (2Mbps) or 8DPSK (3Mbps) after guard interval
- EDR payload can accommodate more data than BR, but still fits within maximum 5-slot due to higher data rates

Bluetooth Address Format

company assigned						company id					
LAP						UAP		NAP			
0000	0001	0000	0000	0000	1100	0010	0111	1011	0011	0101	1001

LSB MSB

000666 = Roving Networks

- The Bluetooth de t address sent in the *access code* field of the packet head
- The first (most significant) 24 bits OUI (Organization Unique Identifier) or the Company ID
- The main purpose of the Bluetooth address is for identification and authentication, but
- The address is also used to seed the frequency hopping pseudorandom generator, to synchronize master and slave clocks, and to pair devices.

Frequency Hopping with Pseudorandom Number Generator

- In Bluetooth Classic, FH is defined by a pseudorandom generating algorithm seeded with the following values
  - UAP and LAP of the master device address, and
  - Bits 1-26 of the
- The pseudorand itself after 2^{27} hops
  - Would take 23.3 hours@16 eat!
  - In practice the pseudorandom sequence is never repeated

Bluetooth is both Time and Frequency Synchronised

Illustration of Pseudorandom FH

Collision with WiFi: fixed (non-adaptive) hopping

Collision Avoidance via Adaptive FH (AFH)

- Mark interfering channels as *bad channels*
- Avoid bad channels; hop between *good channels* only
- Minimum available (go channels to hop = 20 (79-20=59 channels can marked as bad)
- AFH available only during Connected state (i.e., when two devices are exchanging data)

AFH Illustration: hopping only between good channels

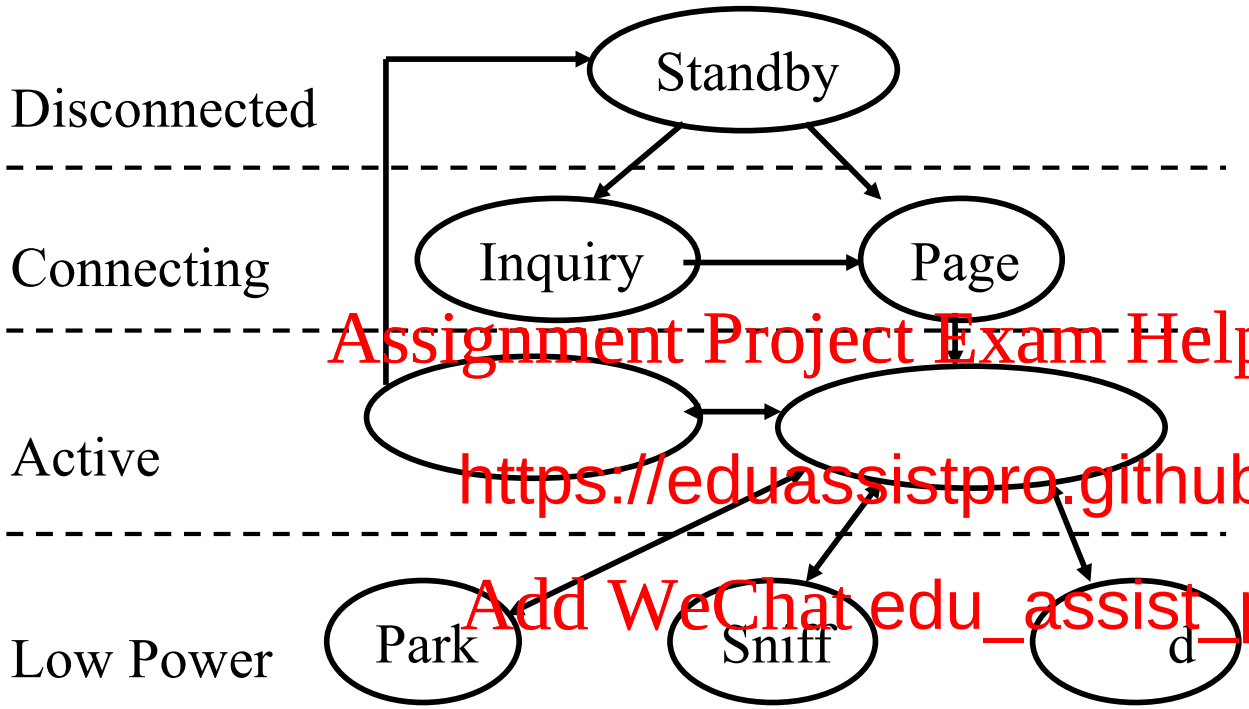
Channel assessment: RSSI/SNR, PER (left to chipset vendor; not specifid in standard)

- Black: used (by another piconet)
- White: available (good to use)
- Yellow: Bad

Channel Map

Master updates the map dynamically and sends it to slaves

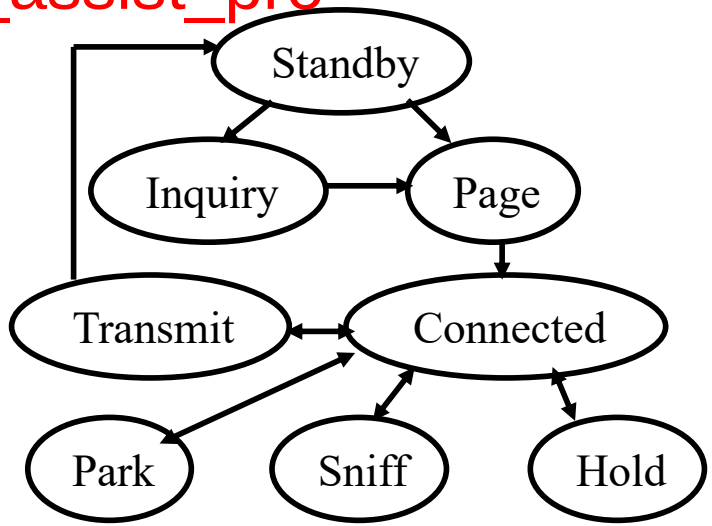
Bluetooth Operational States



- 8 distinct states grouped under 4 high-level states
- **Standby**: Initial state
- **Inquiry**: Master broadcasts an inquiry packet. Slaves scan for inquiries and respond with their address and clock after a random delay (CSMA/CA)

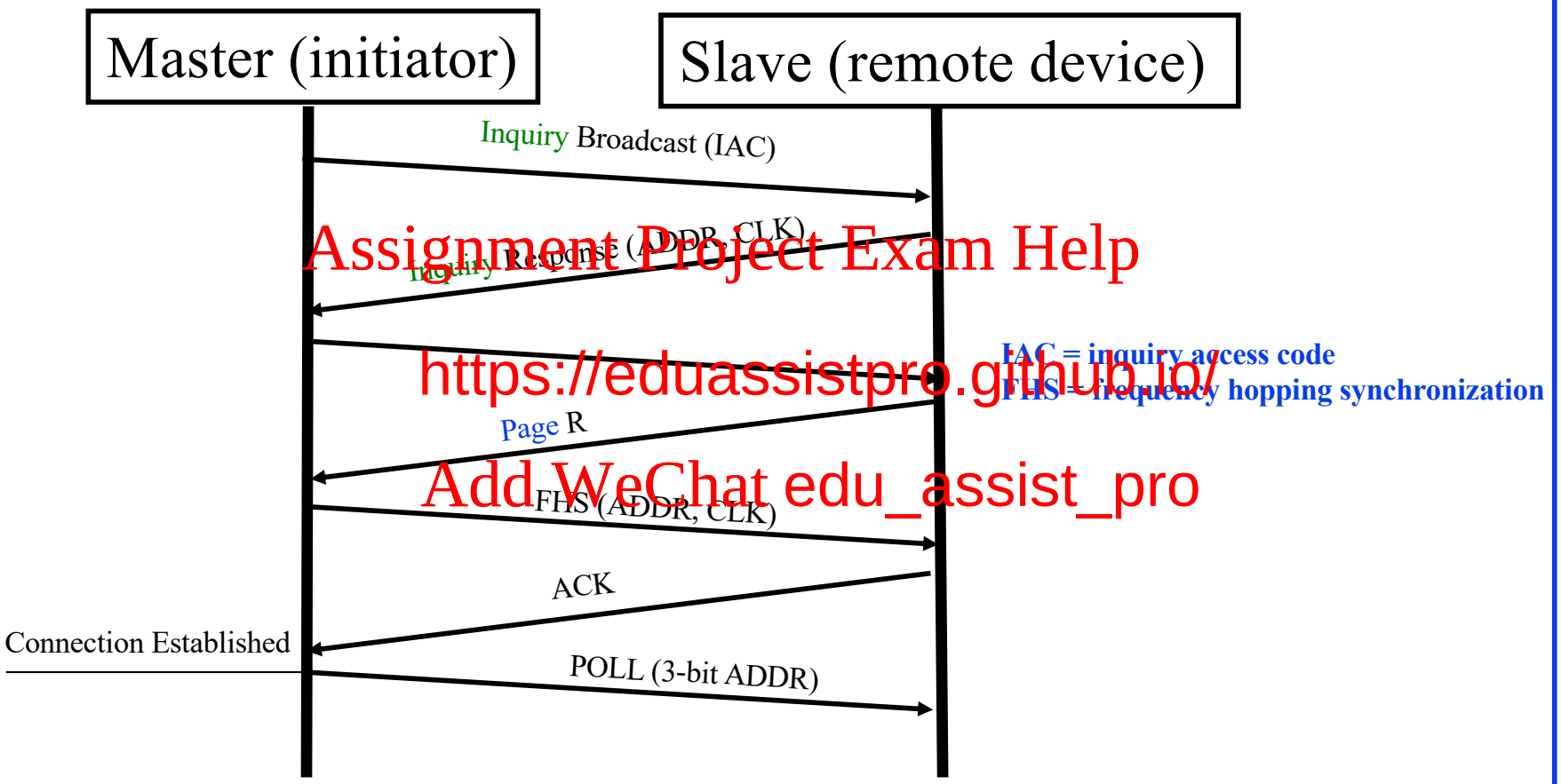
Bluetooth Operational States (Cont)

- **Page**: Master in page state invites a slave device to join the piconet. Slave enters page response state and sends page response to the master.
- Master informs slave about its *clock* and *address* so that slave can participate in piconet.
- **Connected**: A short 3-bit logical address (*member address* within *control header* field) is assig
- **Transmit**: station is t ket



Bluetooth Connection Establishment Procedure

Inquiry and Paging Flow Diagram



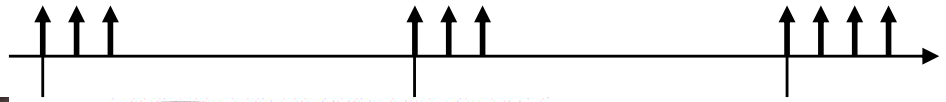
Bluetooth Connection Establishment Procedure
Inquiry and Paging Frequency Hopping

- Inquiry/page hopping sequence
  - Hop over 32 subset of 79 channels/frequencies (to speedup)
  - 32 is divided into two 16-channel *trains*
  - For inquiry, each train is repeated 256 times before *switching* to the other train; must have 3 train switches (1st → 2nd → 1st → 2nd): each train effectively repeated 256 x 2 ti
  - Master sends two i rent frequencies per slot (hops in the middle of the slot; hops fre µs!), and listens for responses (both frequencies in the fall speedup) → eventually 2 frequencies covered in 2 slots
- Connection establish time
  - 16 x 625 µs = 10 ms for completing a train once
  - Inquiry time (maximum) = 256 x 4 x 10 ms = 10.24 s
  - There is an additional paging time

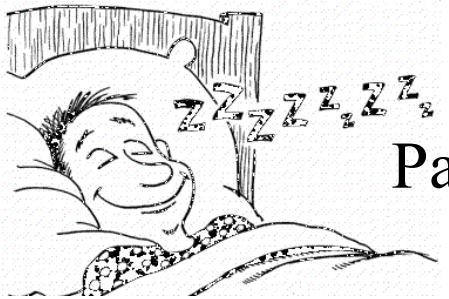
Power Saving Modes in Bluetooth

Three inactive (power-saving) states:

1. **Hold**: Go inactive for a single short period and become active after that
2. **Sniff**: Low-power mode. Slave listens periodically after fixed sniff intervals.
3. **Park**: Very Low-power mode. Gives up its 3-bit active member address and gets an . Wake up periodically and listen to beaco f beacons periodically

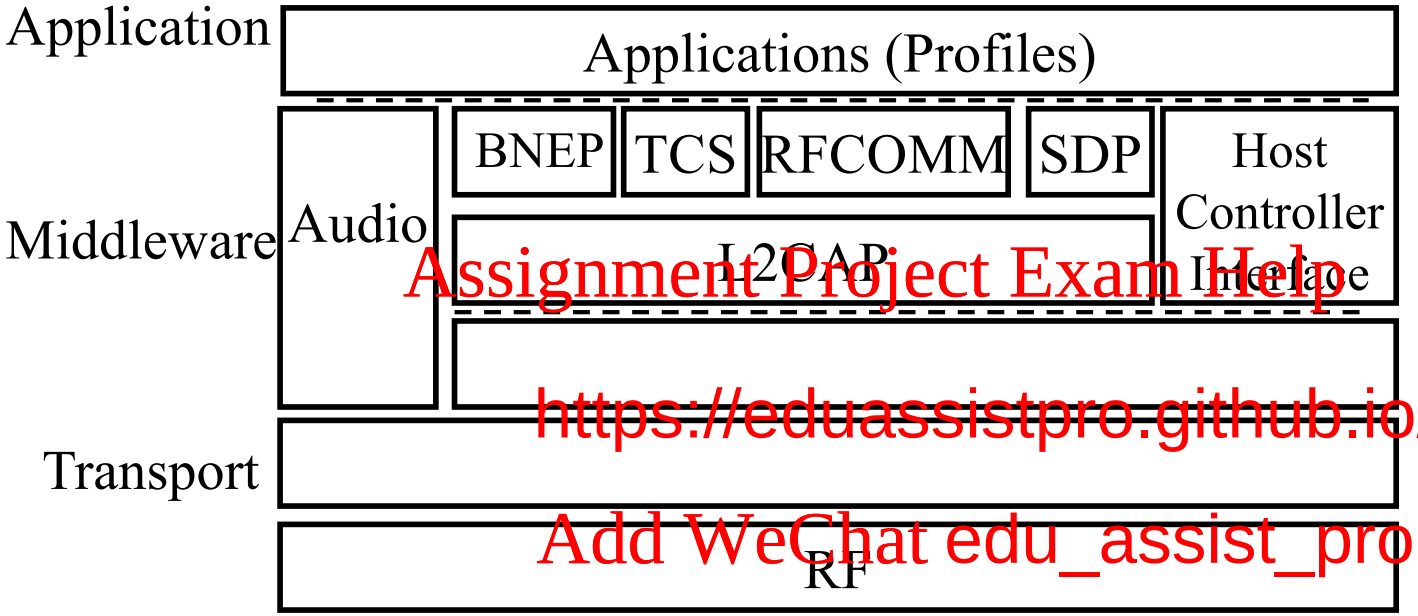


Sniff

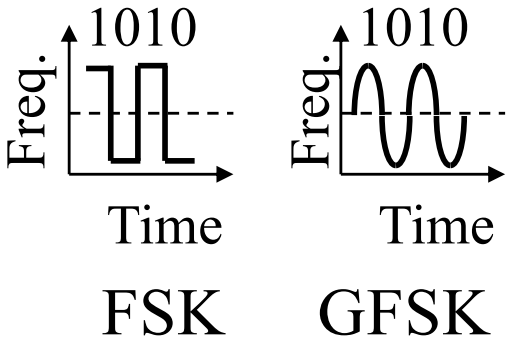


Park

Bluetooth Protocol Stack

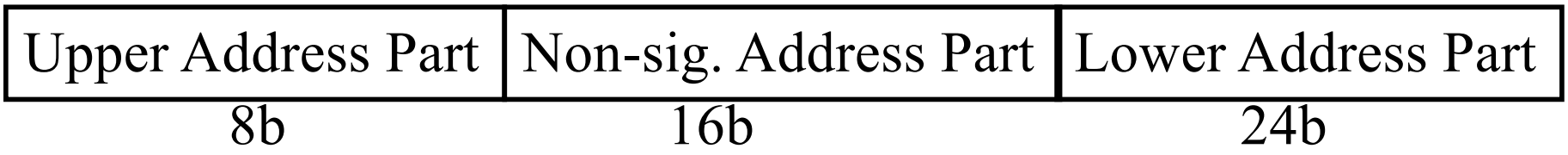


- **RF**: Gaussian Frequency Shift Keying (GFSK) modulation
- **Baseband**: Frequency hop selection, connection, MAC



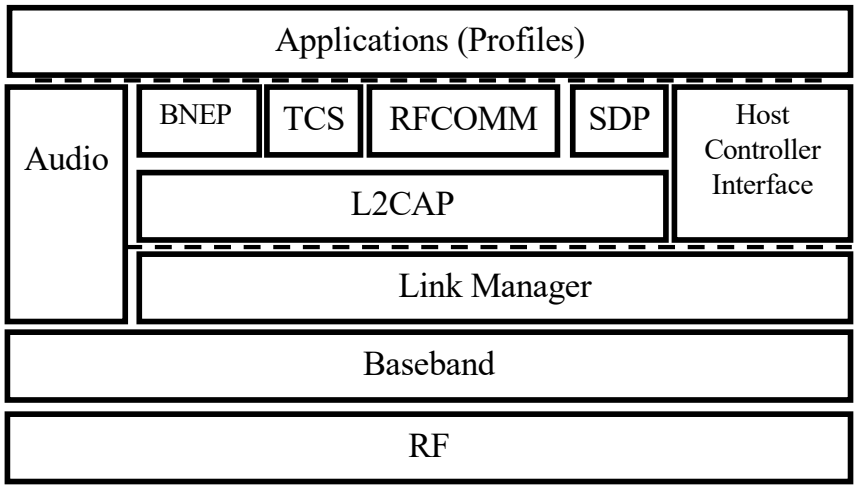
Baseband Layer

- Each device has a 48-bit IEEE MAC address
- 3 parts:
  - Lower address part (LAP) – 24 bits
  - Upper address part (UAP) – 8 bits
  - Non-significa 6 bits
- UAP+NAP = Organizationally tifier (OUI) from IEEE
- LAP is used in identifying the piconet and other operations
- Clock runs at 3200 cycles/sec or 312.5 µs (twice the hop rate)



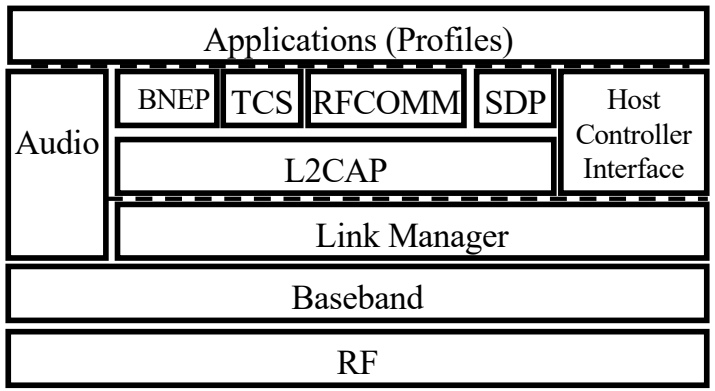
Bluetooth Protocol Stack (Cont)

- **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 Int** face to Bluetooth chip. Allows same softwar
- **RFCOMM Layer**: P
  - Sets up a connection to another RF
- **Service Discovery Protocol (SDP):** Devices can discover the services offered and their parameters
  - E.g., Bluetooth keyboard,
  - Bluetooth mouse
  - Bluetooth headset
  - …



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 s** N): Call control including group mana call forwarding, and group calls)
  - Telephony has both audio and cont
  - Bluetooth telephone very popular in cars
- **Application Profiles**: Set of algorithms, options, and parameters
  - To support specific applications



Application Profile Examples

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

With IoT, the list is expected to grow rapidly over the ming years

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

Connecting a wireless keyboard with HID Bluetooth profile

Bluetoo gy (BLE)

a. etooth 4

Bluetooth LE or BLE

- **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 y
- **Simple**: Star topology. No scatter …
- **Lower cost** than Bluetooth classi
- New protocol design based on Nokia's **WiBree** technology
  Shares the same 2.4GHz radio as Bluetooth
  ⇒ Dual mode chips
- Most smartphones (iPhone, Android, …) have dual-mode chips

BLE Channels

- 40 2MHz-wide channels: 3 (37,38,39) for advertising and 37 (0-36) for data
- Advertising channels specially selected to avoid interference with popular default WiFi channels (1,6,11)

BLE Advertising Channels Avoiding Popular WiFi Channels

BLE Modulation and Data rate

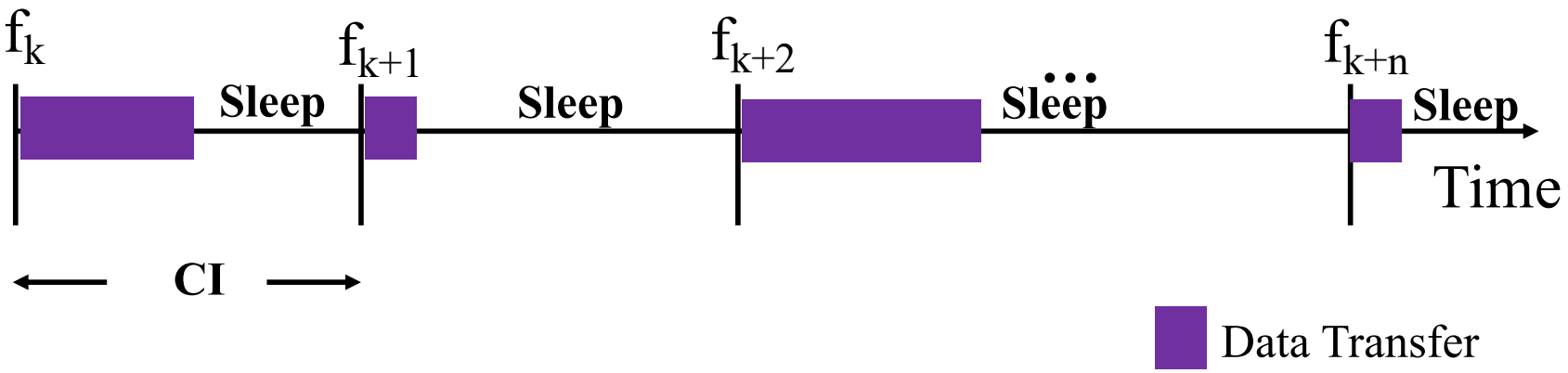
- Binary GFSK over 2MHz channel: More significant frequency separations for '0' and '1' allows longer range with low power
  - Note that with B dwidth is only 1MHz, so frequency separa
- 1 million symbols per second → a rate

Benefit of Advertising Channels

- BLE simplifies discovery and broadcasting by using only three advertising channels (instead of 32 channels for inquiry/paging in BT Classic)
- A BLE device ing beacons on these 3 channel about the device, so other devices can connec also broadcast some sensor data
- Data channels are used to exchange data bidirectionally between two devices

Connection Events and Connection Intervals

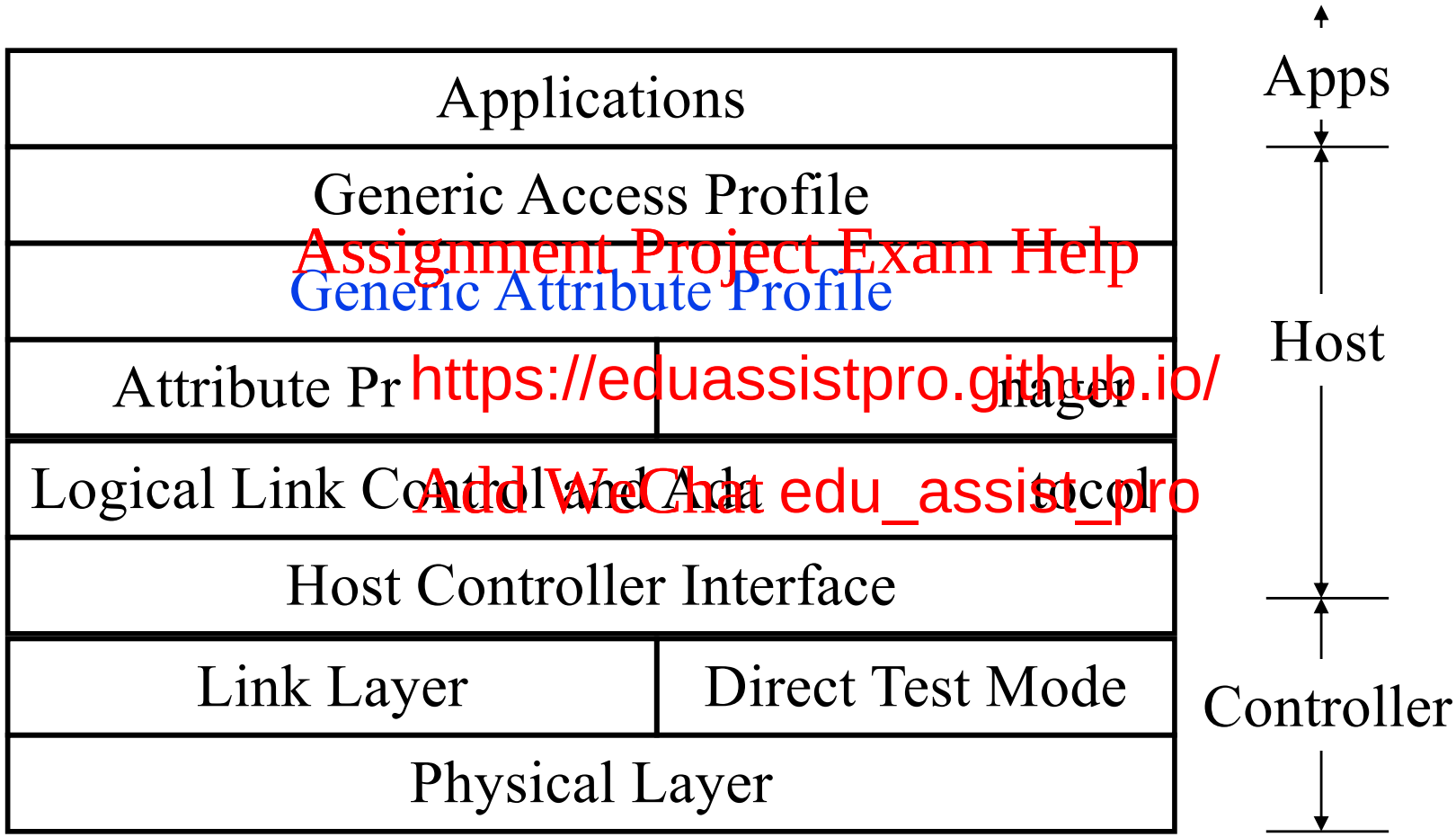
- In BLE connections, devices wake up periodically after every connection interval (CI) time; transmit some data (connection event) and then go back to sleep until the next connection event
- Send a short blank packet if no data to send during a connection event
- More than one packet can be sent during a connection event
- Connection interval t s and is negotiated during connection set up
- Hop frequency (switch to different dat each event



BLE Frequency Hopping Algorithm
a.k.a Algorithm #1

- *Fixed* hopping instead of *pseudorandom*
- $f_{k+1} = (f_k + h) \bmod 37$
  - Where h (hop increment) is a fixed value negotiated during connection setup
  - Note: Data chann
- Example hopping 0 → 20 → 30 → 3 → 13
- Adaptive FH: If the hopping land channel, the channel is remapped to a *good* c a channel *remapping* algorithm

Bluetooth Smart Protocol Stack

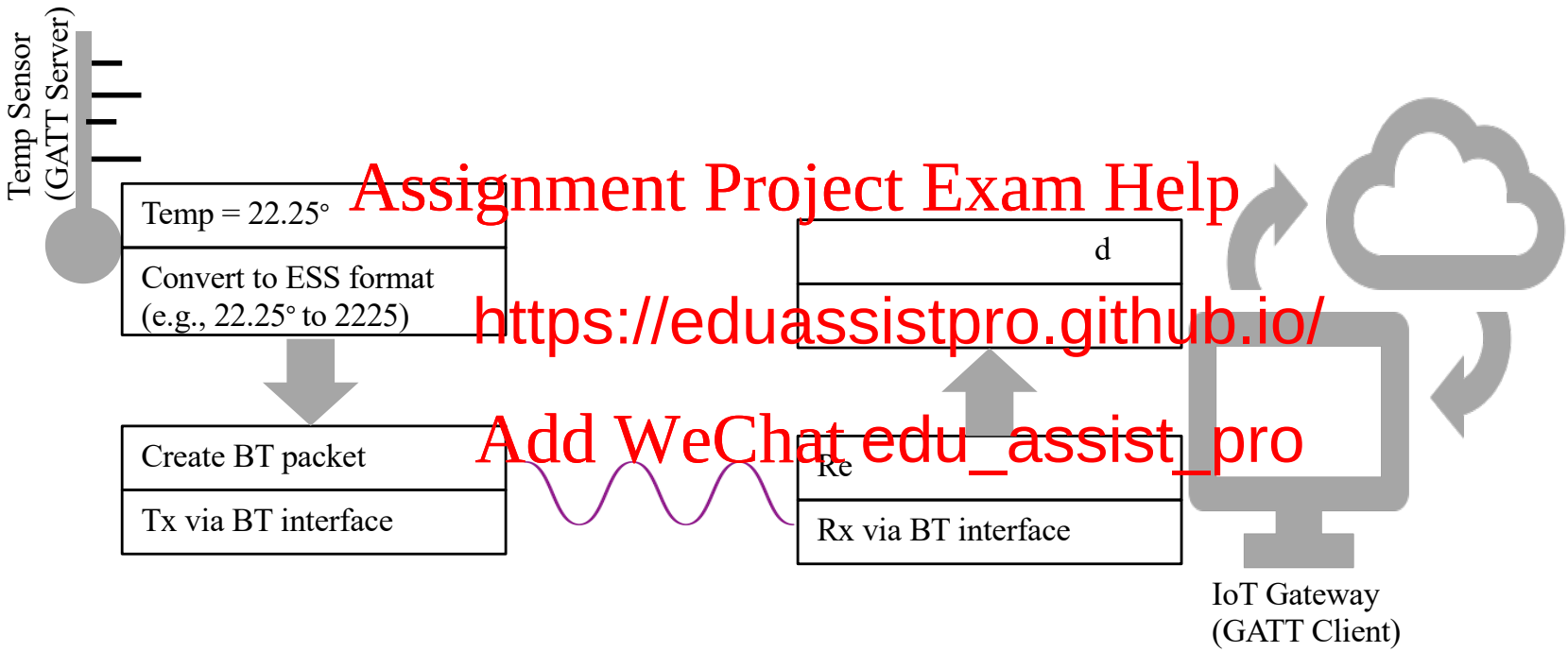


Generic Attribute (GATT) Profile

- Defines data formats and interfaces with the Attribute Protocol
  - Define attributes instead of applications (a major difference from Bluetooth Classic); temperature, pressure, heart rates are examples of attributes
  - New applications can be supported by using appropriate attributes
- Type-Length-Value (TLV) encoding is used
- Each attribute has a 16-bit Universally Unique ID (UUID) standardized by Bluetooth SIG
  - 2^{16}=65 thousand un
- 128-bit UUID if assigned by a manufac
  - Manufacturers can define their own attributes and still interoperate
- Allows any client to find a server, read/write data
  Allows servers to talk to generic gateways
- Allows security up to AES-128
- Each to encode in XML
- Makes profile (application) development easier

Example of BLE GATT services and characteristics

Temperature sensing using BLE: environmental sensing service profile



Bluetooth Gateway Devices

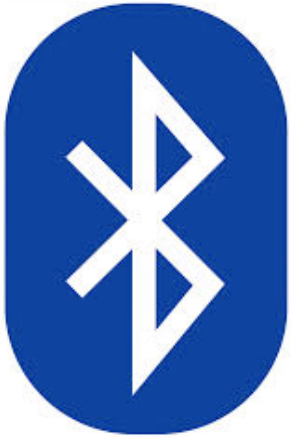
- A gateway device helps connect a Bluetooth device to the Internet. Smart phone, Tablets, PC, …
- A generic app can forward the data to the URL sent by the device

Bluetooth Smart Applications

- Proximity: In car, In room 303, In the mall
- Locator: Keys, watches, Animals
- Health devices: Heart rate monitor, physical activities monitors, therm
- Sensors: Temp s, tire pressure
- Remote control: Open/close on lights

Beacons

- Advertizing based on proximity
- Peripherals (your phone) broadcasts its presence if Bluetooth is turned on
- Primary aim of these broadcasts is to allow device discovery
- Advertising pack nd max 27B of payload with mul terns
  - May include signal strength
- iPhones can send/received iBeaco
- Can be used for customized advertising, indoor location, geofencing
- PayPal uses this to identify you. You can pay using a PIN and your phone.



Bluetooth 5

Bluetooth 5: Motivation

- BLE (Bluetooth 4) was great in terms of reducing energy consumption and extending battery life
- BLE, however, could not support high data rate applications, such as audio and file transfer (e.g., quick firmware updates), and the range was [illegible] w IoT applications
- Bluetooth 5 exten [illegible] r (2x) and longer range (4x) Bluetooth without co [illegible] the battery life; advertising is also improved
- Bluetooth 5 is seen as a significant new milestone in the evolution of Bluetooth; expected to support many new markets in home and industrial automation, health and fitness tracking, and so on.

Bluetooth 5: Major Improvements

- Two new PHYs: one for 2x higher speed and the other for 4x longer range than BLE 4
- New Advertising
- Improved freq

Benefits and use cases for 2x speed

- Quick firmware updates for millions of home and industrial automation devices
- Sports and fitness wearable multi-dimensional and buffered data uploads to edge/cloud
- Medical device d EEG, …
- Higher spectral e ted 2.4GHz space

PHY: 2M

- Two mega symbols per sec: symbol duration = 500ns
  - Symbol duration reduced by half from BLE 4
- Binary GFSK, but with higher frequency deviation to combat inter-symbol interference arising from shorter symbols:
  - Frequency deviat to denote '1' or '0' in FSK > 370kHz (

PHY: Coded

- 1 Mega symbols per sec: the same as in BLE 4
- However, to increase the range, data is coded with FEC; two coding rates
  - ½: cuts data rate by half → 500Kbps; 2x range increase against BLE 4
  - ¼: → 250Kbps; 4
- BLE 4 and BT Cl FEC (*not coded*)

Advertising Extensions

- Motivation: Bluetooth beacons is a major advertising use case
- BLE 4 typically allow just ID or URL to be advertised in the beacon due to limited advertising packet size (31 bytes payload) and heavy load on advertising channels
  - BLE 4 uses ch rtising; all beacon have to be tran nels
- Bluetooth 5 allows advertising p 255 B payload
  - Devices and products can advertise many more things and status, such as a fridge can advertise its contents, temperature, expiry dates of sensitive items, etc.

Advertising Extension: Channel Offload

- Only header is transmitted over advertising channels and the actual payload is offloaded to a data channel
- Note: BLE 4 reserves data channels only for data transfers during Connection Events when connections are established; Channel offload a els in connectionless manner

Advertising Extension: Packet Chaining

- Chain multiple 255B packets together to carry a very large advertising message

Frequency Hopping Extension

- BLE 4 supports only a simple hopping algorithm
  - Algorithm #1: fixed hopping increment only
- Fixed hopping increment limits the number of possible seque
- Bluetooth 5 sup hopping like the BT Classic
  - Algorithm #2: large number of sequences possible

Summary

1. Bluetooth Classic uses frequency hopping over 79 1-MHz channels with 1, 3, and 5-slot packets.
2. Bluetooth 4 is designed for short broadcasts by sensors. 40 2-MHz channels are used with 3 channels reserved for advertising and 37 used for data transfers.
3. BT Classic uses flat application profiles to support different types of communication services, which requires different ap ifferent types of sensing and communications.
4. BLE has a hierarchical ser measurements into a given service type, which scales for large variety of dev expected in the IoT era.
5. Bluetooth 5 extends BLE to support higher data r nge. It also has an improved advertising structure that allows advertisement of more comprehensive information and contents.