Wireless Protocols for IoT Part I: Bluetooth and Bluetooth Smart

Raj Jain
Professor of CSE
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this class lecture are available online at:
http://www.cse.wustl.edu/~jain/cse574-22/

Student Questions

Overview

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

Note: This is one in a series of lectures on WPANs. ZigBee and other networks are discussed in subsequent lectures.

Student Questions

Bluetooth

- ❑ Started with Ericsson's Bluetooth Project in 1994 for radio-communication between cell phones over short distances
- ❑ Named after Danish king Herald Blatand (AD 940-981) who was fond of blueberries
- ❑ Intel, IBM, Nokia, Toshiba, and Ericsson 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 were handled by Bluetooth SIG directly
- ❑ Key Features:
  - ➢ Lower Power: 10 mA on standby, 50 mA while transmitting
  - ➢ Cheap: $5 per device
  - ➢ Small: 9 mm^2 single chips

Student Questions

❑ Is Bluetooth transmission secure?

Yes. But in most wireless technologies (both Wi-Fi and Bluetooth), the initial connections require clear broadcasts. That gives away your privacy.

See Slide 11-31 on Beacons used by businesses to determine who you are.

Bluetooth Versions

- ❑ **Bluetooth 1.1**: IEEE 802.15.1-2002
- ❑ **Bluetooth 1.2**: IEEE 802.15.1-2005. Completed Nov 2003. Extended SCO, Higher variable rate retransmission for SCO + **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 Wi-Fi PHY + Bluetooth PHY for lower rates
- ❑ **Bluetooth 4.0** (June 2010): Low energy. Smaller devices require 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 frames, security/privacy, IPv6 profile

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

Student Questions

❑Can you explain what SCO is?

Yes, later in Slide 11-16.

❖You listed Bluetooth1.1-4.2, so do we need to be familiar with all these and their features?

Yes, key features.

Bluetooth 5

- ❑ 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

- ❑ 8X broadcast capacity by changing the advertising procedure. 255B instead of 31B with v4.2
- ❑ aptX 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).

Student Questions

❑Why is version 5 at 2 Mbps when version 3.0 on the previous slide said 24 Mbps?

This is "Low energy."

❑What new modulation is being used?

Gaussian Frequency Shift Keying (GFSK) vs. older Differential Quadrature Phase-Shift Keying (DQPSK).

❑Can one device with Bluetooth 4 and another device with BLE communicate?

Yes. It is a matter of implementation. New features will not be there in older devices, but newer ones will use older protocols when needed.

Bluetooth 5

- ❑ 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

- ❑ 8X broadcast capacity by changing the advertising procedure. 255B instead of 31B with v4.2
- ❑ aptX 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).

Student Questions

❑Do two devices have to use the same Bluetooth protocol for communication, regardless of what version?

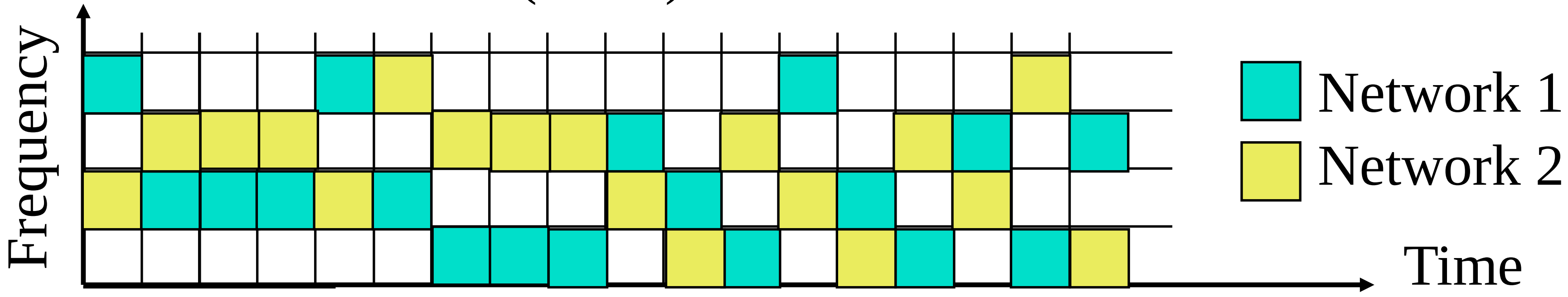
Yes. The version is negotiated first.

❑What is the most common use of Bluetooth?

Headsets

Bluetooth: Details

- **Frequency Range:** 2402 - 2480 MHz
  (total 79 MHz band) 23 MHz in some countries, e.g., Spain
- **Data Rate:** 1 Mbps using 1 MHz (Nominal) 720 kbps (User)
- **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

Student Questions

- ❑ Given that frequency hopping doesn't sense the spectrum, is there a lot of interference?

Not really. With 79 channels, the probability of colliding is 1/79^2 or $\approx 10^{-4}$*.*

- ❑ At each time slot, we use only 1 MHz of the whole available 79 MHz, but we may change the frequency at each time slot. Correct?

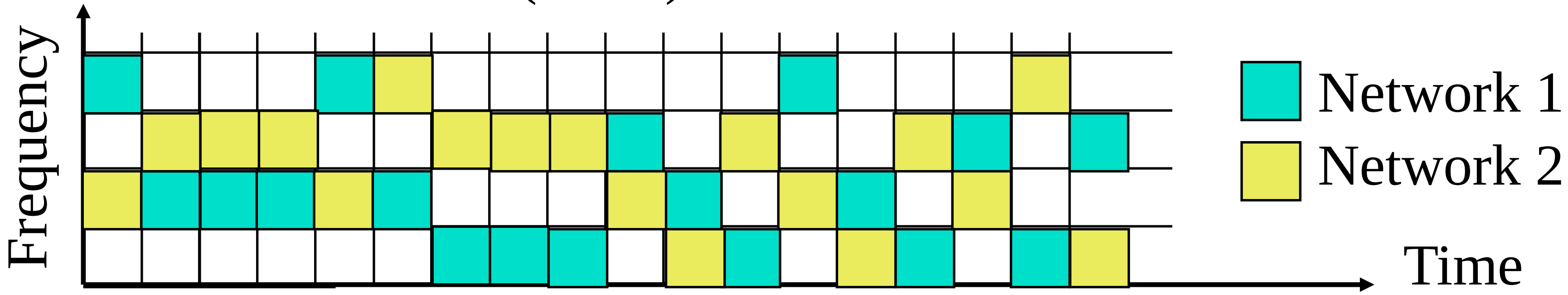
Yes.

- ❑ How can the receiver know which 1 mHz channel to switch to for reception given constant frequency hopping?

Using pseudorandom number generation. If you start with the same seed, you get the same sequence.

Bluetooth: Details

- **Frequency Range:** 2402 - 2480 MHz (total 79 MHz band) 23 MHz in some countries, e.g., Spain
- **Data Rate:** 1 Mbps using 1 MHz (Nominal) 720 kbps (User)
- **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

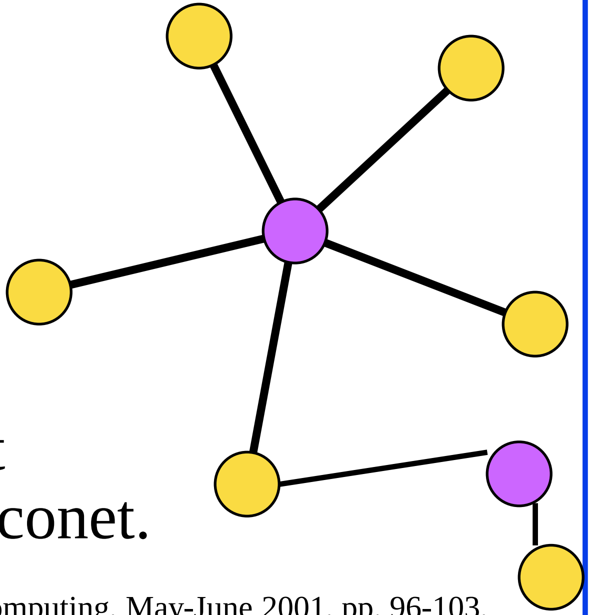
Student Questions

❖ How did we calculate 625us/hop?

1/1600 = 625

Piconet

- ❑ Piconet is formed by a master and many slaves
  - ➢ Up to 7 active slaves.
    Slaves can only transmit when requested by the master
  - ➢ Up to 255 Parked slaves (See Slide 11-11)
- ❑ Master polls active slaves for transmission
- ❑ Each station gets an 8-bit parked address
  ⇒ 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 ⇒ 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)

Student Questions

- ❑ Is a Piconet specific to bluetooth, or do other protocols use similar networks?

This is quite common amont IoT protocols. We will see similar (bigger networks) in ZigBee. The names are different.
In Wi-Fi we call these Service Set and need a dedicated Access Point.

- ❑ In scatter net, does the device need to synchronize with two masters or just one?

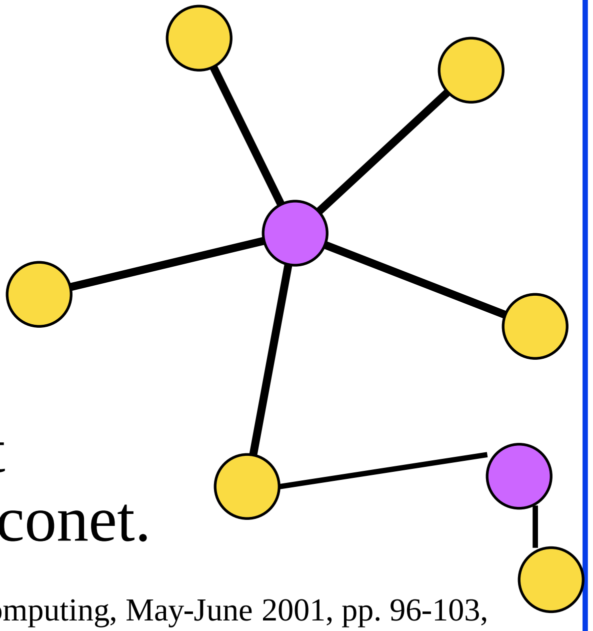
Synchronize to the master it is talking to at the moment, like working two jobs.

- ❑ Could two devices make up a piconet?

Yes. That's the most common case.

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 (See Slide 11-11)
- ❑ Active slaves are polled by master for transmission
- ❑ Each station gets a 8-bit parked address
  ⇒ 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 ⇒ 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)

Student Questions

❑Can a node simultaneously be both master and slave in a piconet? If not, should it form by making two channels or something?

Masters can easily speak to the slaves. There is no need to be a slave. However, in a scatter net, you may be a slave in one and a master in another.

❖Can you explain point 4?

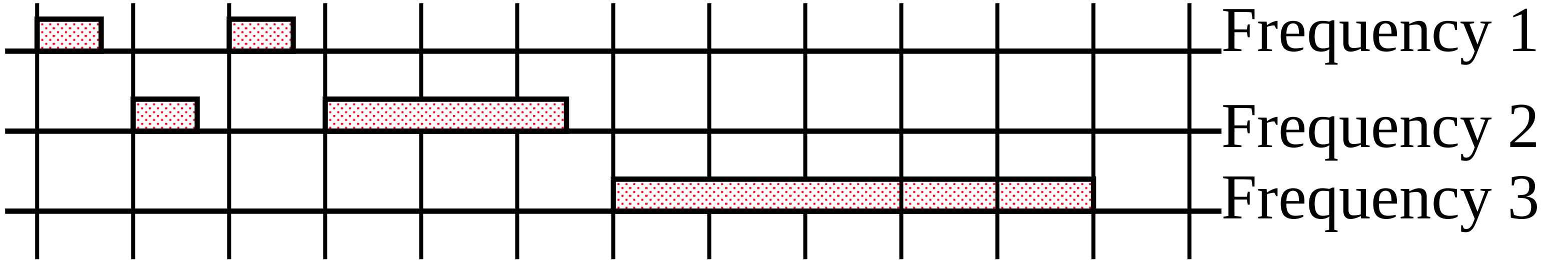
Parked stations have 8-bit addresses, and their info is already with the master.

❖Point 1, part two, do you mean inactive instead of parked?

Parked do not have 3-bit addresses. Actives have 3-bit addresses. They include those transmitting, sniffing, or on hold. I meant parked.

Q on 8c

Frequency Hopping Sequences



- ❑ 625 μs slots using a 312.5 μs clock
- ❑ 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 frame from the master
- ❑ Frames = 1 slot, 3 slot, or 5 slots long
- ❑ The frequency hop is skipped during a frame.

Student Questions

❑ "How is the frequency hop coordinated?

Frequency hopping uses a pseudo-random number generated. Two nodes that use the same parameters and seed will generate the same sequence of numbers. The nodes interchange the parameters and seed on connection initialization.

❑ What happens in the event of a frequency collision with another bluetooth transmission?

The collision is limited to one frequency hop or less. Then they go on different ways.

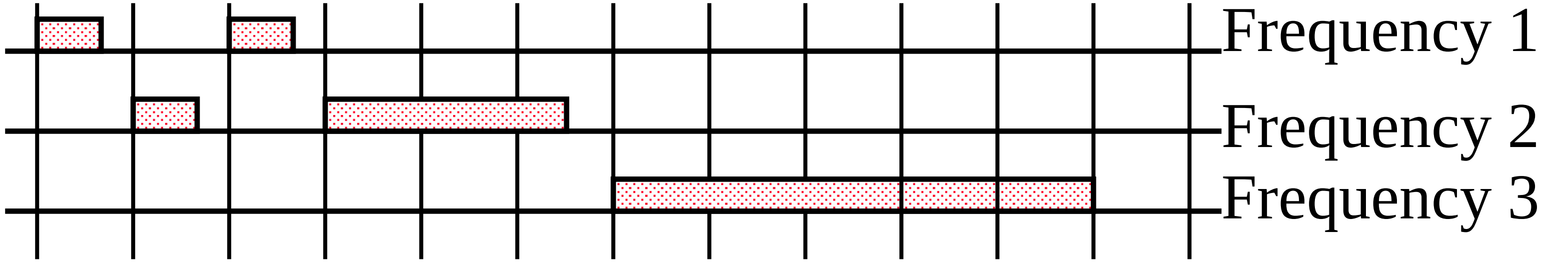
❑ Does it mean that slaves start their transmission in odd-numbered slots and continue for 1, three, or five consecutive slots?

Yes.

❑ In the picture, which one is the master node?

The figure shows three frequencies, not stations. It is all one station. It could be master or slave, depending on whether the first slot is even or odd-numbered.

Frequency Hopping Sequences



- 625 μs slots using a 312.5 μs clock
- 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 frame from master
- Frames = 1 slot, 3 slot, or 5 slots long
- The frequency hop is skipped during a frame.

Student Questions

- Are the masters and slaves the frequencies themselves? So would the master be Frequency 2 in the example image?

No. The figure shows only frequency hopping by one station.

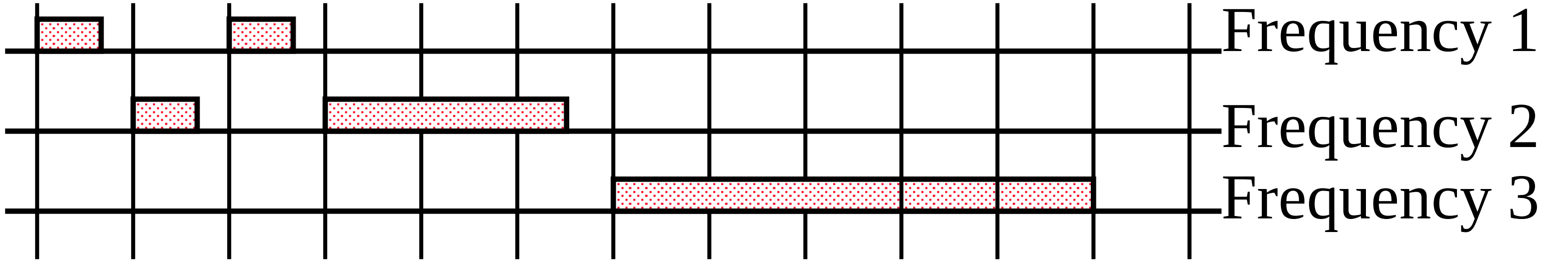
- Does this mean that the master always transmit in even numbers only?

No. They start in even numbered slots. They may continue for 1, 3 or 5 slots.

- Is BLE still following this even/odd-slot scheme for master/slaves? It seems inefficient.

Yes.

Frequency Hopping Sequences



- 625 µs slots using a 312.5 µs clock
- 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 frame from the master
- Frames = 1 slot, 3 slot, or 5 slots long
- The frequency hop is skipped during a frame.

Student Questions

- Will the seed of the hopping sequence generator first be sent to the slaves?

It is told at connection setup.

- Can the frame length be non-integer like what it is in the picture? If so, is that OK if it is close to an even-number length?

The frames can be fractional in length. But slots are aligned, and the transmissions start at slot boundaries only, regardless of the previous transmission.

❖Can a frame size be larger than 5 slots?

Frames larger than 5 slots are sent in multiple frames.

Q on 9a

Bluetooth Frame Format

Access Code	Baseband/Link Control Header	Data Payload
72b	54b	0-2744b

- Frames can be up to five slots long. Five slots =3125 us.
- 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, ack/nack (1b), sequence number, and header error check (8b) 18b. Header is encoded using 1/3 rate FEC resulting in 54b
- Synchronous traffic has periodic reserved slots.
- Other slots can be allocated for asynchronous traffic

Student Questions

❑Do units mean other Bluetooth devices?

Yes.

❑In this slide, you said if we have a 3-slot frame, we can multiply by 3/5 and get about 1200. Why do we not use 3125 * 3/5 = 1875?

Yes. Your calculation is correct.

❖What layer is this?

MAC

❖3125 bit or Microsecond?

Microseconds

❖Point 3, can you break down the 54b?

(3+4+1+1+1+8)×3=18×3=54

Q on 9b

Bluetooth Frame Format

Access Code	Baseband/Link Control Header	Data Payload
72b	54b	0-2744b

- Frames can be up to five slots long. Five slots =3125 us.
- 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, ack/nack (1b), sequence number, and header error check (8b) 18b Header is encoded using 1/3 rate FEC resulting in 54b
- Synchronous traffic has periodic reserved slots.
- Other slots can be allocated for asynchronous traffic

Student Questions

❖Is the Bluetooth frame format the same for every generation of Bluetooth?

Yes, but EDR adds a few extra fields in the data.

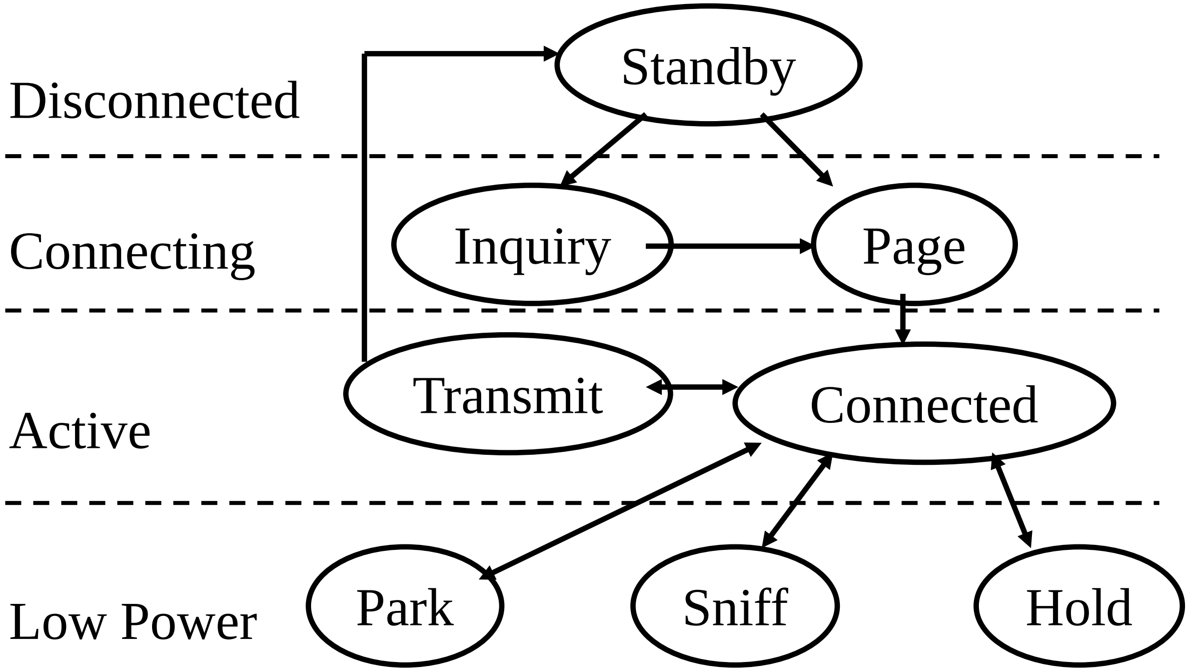
❖Can you explain why five slots=3125 bits?

3125 us. Each slot is 625 us.

❖Could you go over how the slots and frames work? How can the header have 126 bits, the payload is 0-2745 bits, but five slots have a max of 3125 bits. I'm just having a hard time figuring out the math of it.

3125 bits has been corrected to 3125 us. 2745 bits has been corrected to 2744 bits. The maximum frame is 2870 bits. There can be some gaps after the frames.

Bluetooth Operational States



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

Student Questions

- Is there a handshake involved between the page state and the connected state? what information does the master and slave exchange?

Several messages are exchanged including the type of service.

- While on Hold, could that be when a device connects to another master to communicate with it?

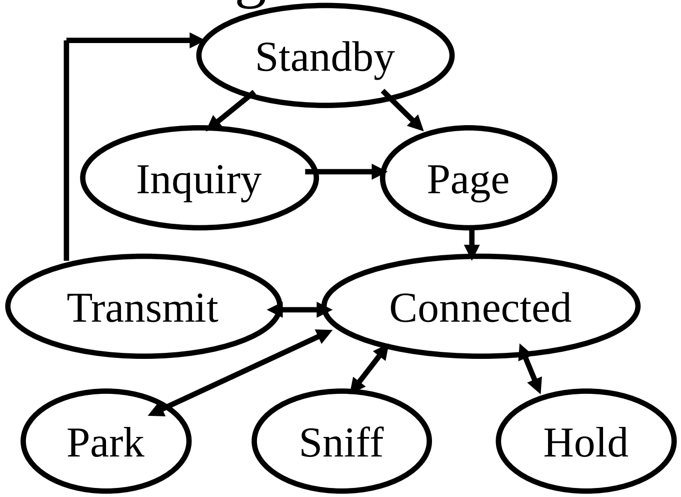
Yes. It could.

- Can a device be connected to more than one master at a time?

No. But in scatter nets, it timeshares between two masters.

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 the page response state and sends the page response, including its device access code.
- Master informs slave about its clock and address so that slave can participate in the piconet. Slave computes the clock offset.
- **Connected**: A short 3-bit logical address is assigned
- **Transmit**:



Student Questions

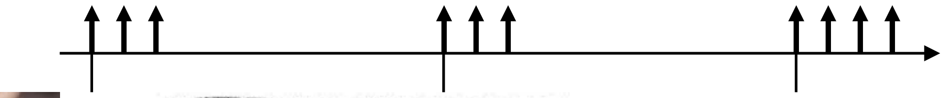
❑What is the clock offset?

Offset=How far is your tick from the master's tick?

Energy Management in Bluetooth

Three inactive states:

1. **Hold**: No Asynchronous Connection List (ACL). Synchronous Connection Oriented (SCO) continues.
   A 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. It 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

Student Questions

□Do applications control what state the Bluetooth device is in? Does the application profile specify this?

Yes, applications follow the needs of the user.

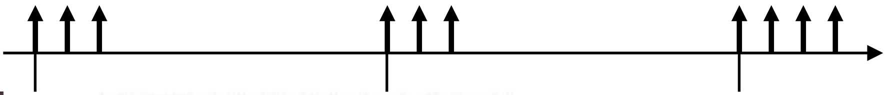
□How could the nodes know they should turn to sniff or park state? Can a node in the sniff state turn to the park state?

Yes, that's what they do. Like sleep and hibernate states in computers.

Energy Management in Bluetooth

Three inactive states:

1. **Hold**: No Asynchronous Connection List (ACL). Synchronous Connection Oriented (SCO) continues.
   The 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. It 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

Student Questions

❑What do you mean by "slaves listen after fixed sniff intervals"?

They set an alarm and go to sleep.

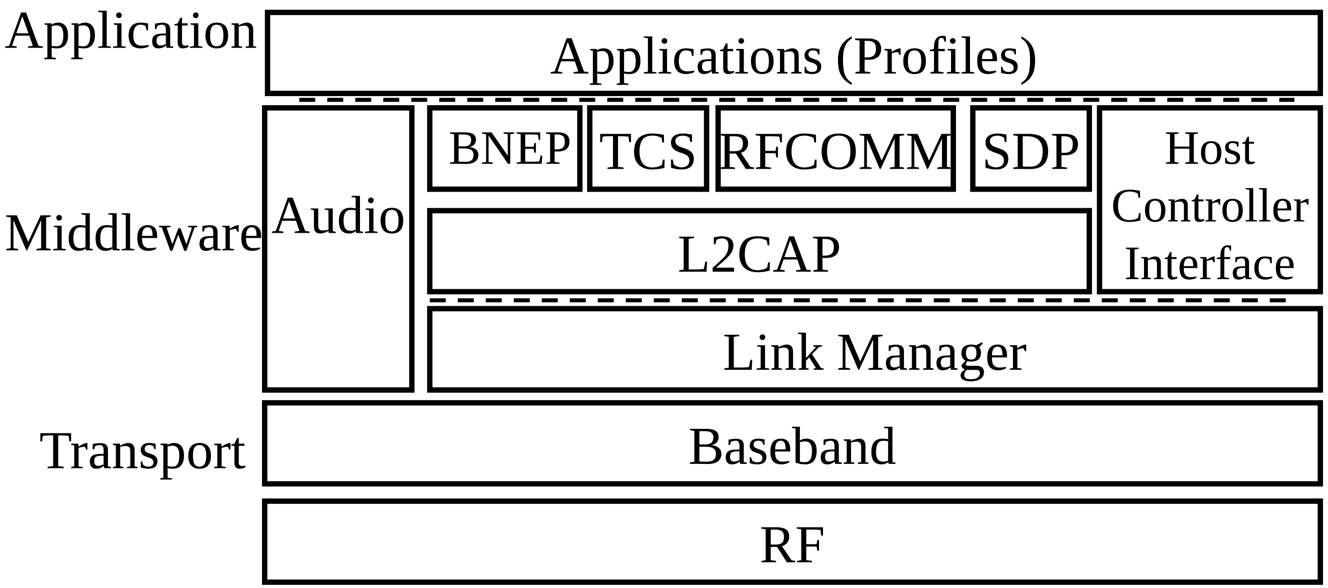
❑ Is the only difference between sniff and park that they do not give up their address in a sniff?

The sleep intervals are different.

❑Is the difference between park and standby (disconnected) only the 8-bit parked member address?

Standby=Disconnected

Bluetooth Protocol Stack



Application

Applications (Profiles)

Middleware

Audio

BNEP

TCS

RFCOMM

SDP

Host Controller Interface

L2CAP

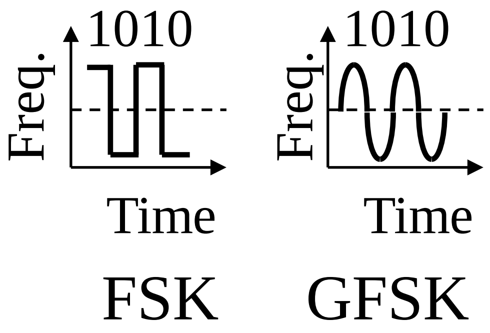
Link Manager

Transport

Baseband

RF

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



Student Questions

❑ Why does Audio Middleware not need a Link Manager?

Audio was given a fast path since it is the most latency sensitive application and was the primary application in the beginning.

❑ How is the security of Bluetooth compared to Wi-Fi?

Wi-Fi security is more mature. Bluetooth is catching up. See "Beacons" at end of this lecture about violation of privacy.

❑Based on the diagram, GFSK seems to make less sense than normal FSK? Why use it?

Frequency shift is not visible from the diagram. GFSK is claimed to have lower power utilization.

Baseband Layer

- ❑ Each device has a 48-bit IEEE MAC address
- ❑ three 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
- ❑ Clock runs at 3200 cycles/sec or 312.5 μs (twice the hop rate)

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

Student Questions

❑What part of the addresses is pre assigned and what is not?

All 48-bits are assigned to a device. In IEEE 802 addresses, the first 24 bits indicate the manufacturer.

❑What is the implication or the effect of the 5th point?

Slot is two clock cycles long.

❑How do we make all devices have a unique MAC Address? How about non-IEEE devices?

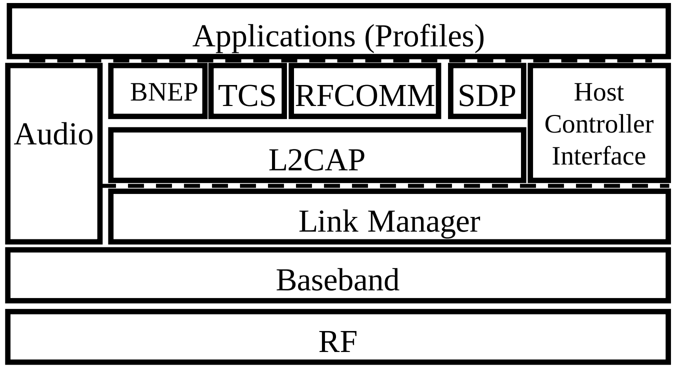
There are no Non-IEEE Bluetooth devices. IEEE does allow global and local addresses.

❑What do UAP and NAP identify?

NAP is used for some functions.

Bluetooth Protocol Stack (Cont)

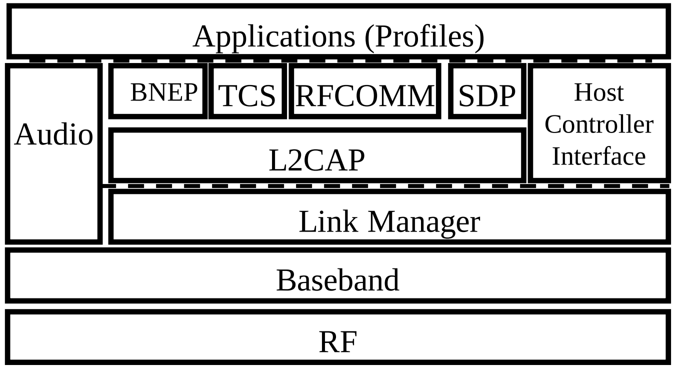
- **Link Manager:** Negotiate parameters, Set up connections
- **Logical Link Control and Adaptation Protocol (L2CAP)**:
  - Protocol multiplexing
  - Segmentation and reassembly
  - Controls peak bandwidth, latency, and delay variation
- Host **Controller Interface**: Chip-independent interface to Bluetooth chip. Allows the 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



Student Questions

Bluetooth Protocol Stack (Cont)

- **Bluetooth Network Encapsulation Protocol (BNEP):** To transport Ethernet/IP frames 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.



Student Questions

- What are the SCO links over the baseband?

Synchronous Connection Oriented (SCO) operation is used for voice/video. Fixed slot positions are reserved in both directions. Provides a circuit-switched link-like service. Asynchronous operations are used for data and control.

End of Part 1

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

Student Questions

- ❑ With profiles, can you only make applications based on the predefined profiles, or can you make new profiles as needed?

Any changes in profiles need to be approved by Bluetooth SIG, otherwise, different manufacturers devices will not interoperate. New profiles are being added by the SIG regularly.

Bluetooth Smart

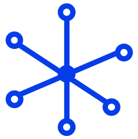
- **Low Energy**: 1% to 50% of Bluetooth classic
- **For short broadcast**: Your body temperature, Heart rate, Wearables, **sensors**, automotive, industrial.
  Not for voice/video, file transfers, …
- **Small messages**: 1Mbps data rate but throughput not critical.
- **Battery life**: In years from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

Student Questions

- Why did Bluetooth use 2.4GHz frequency? Isn't this band already crowded by Wi-Fi?

When Bluetooth started there was not much choice. Also others would have been more expensive.

- What does star topology mean?

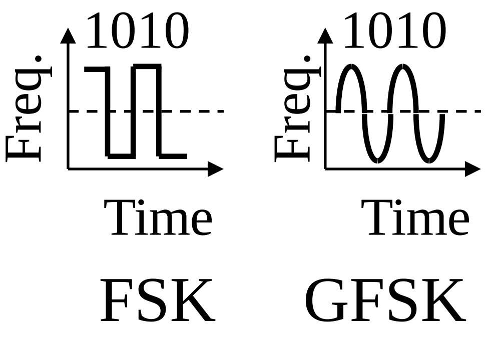


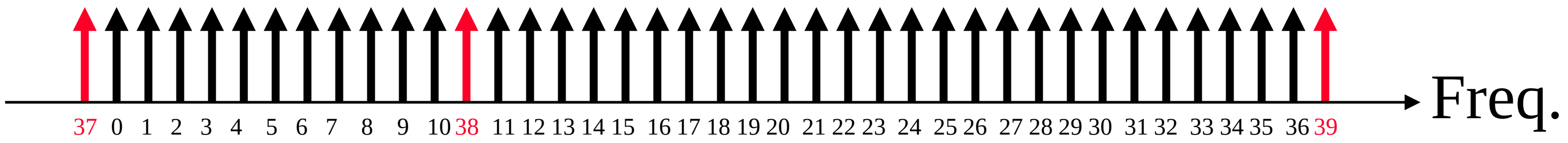
- Is Bluetooth smart the rebranded version of WiBree?

Yes.

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

Student Questions

- ❑ Can you clarify what advertising is vs Data?

Explained in the next slide.

- ❑ Could you explain what adaptive frequency hopping is? What makes it "adaptive," and how is that different than how Bluetooth Classic frequency hops?

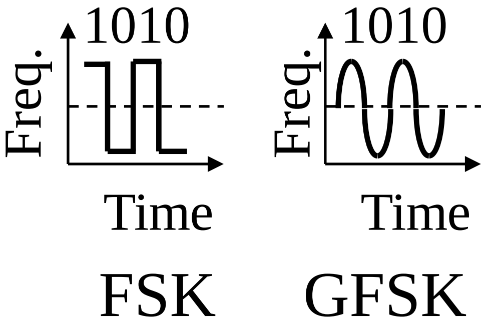
The device exchanges a "Slot Availability Mask (SAM)" listing channels with low interference, and then both hop on this subset. Useful when a node is already using a set of channels for Wi-Fi.

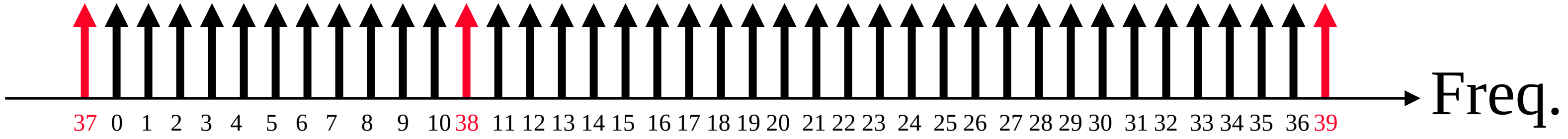
- ❑ Till which Bluetooth version that 79 channels instead of 40 are used for hopping.

V4

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

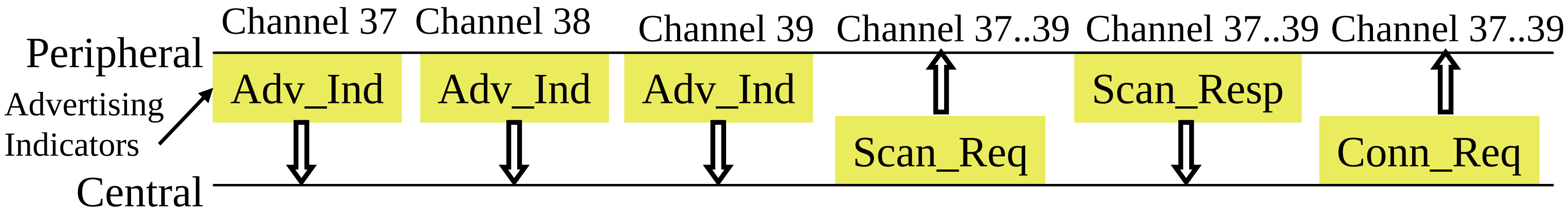
Student Questions

- Most phones can only use Bluetooth at a short distance; does it set a limit, or it because the field is not open enough?

There is a power limit, no distance limit. Open fields help.

Bluetooth Smart MAC

- ❑ Two Device Types: “**Peripherals**” are simpler than “**central.**”
- ❑ Two PDU Types: Advertising, Data
- ❑ **Non-Connectable Advertising**: Broadcast data in clear
- ❑ **Discoverable Advertising**: Central may request more information. Peripheral can send data without connection
- ❑ **General Advertising**: Broadcast presence wanting to connect. Central may request a short connection.
- ❑ **Directed Advertising**: Transmit signed data to a previously connected master



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

Student Questions

- ❑ I see the Con_Req across multiple channels- how does the Peripheral/Central ensure only one connection is made?

One channel is sufficient. However, if there are many nodes, it may become overloaded.

- ❑ If these advertising messages are broadcast on all three advertising channels how do we prevent collisions between two devices, or is the probability of collisions low enough to ignore?

Advertisements are done only one channel at a time. Not simultaneously on all 3 channels.

- ❑ For discoverable advertising, is the data still broadcast, or is it just sent to the requesting central device?

Requesting central device

- ❑ What's "Adv_Ind"?

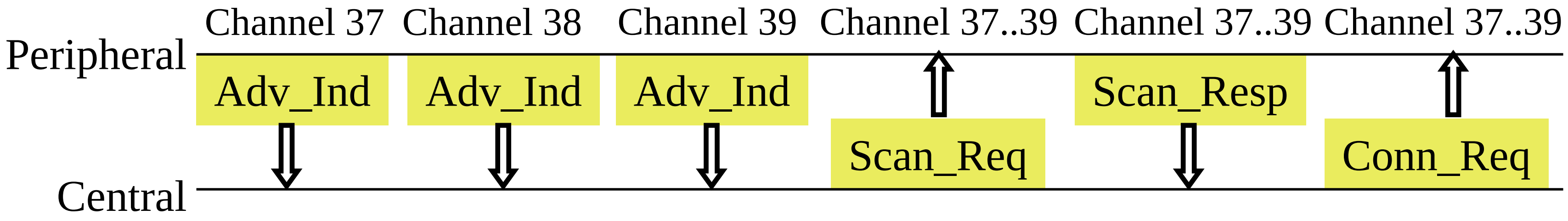
Advertising Indicators (broadcasts)

- ❑ Do peripherals mean slaves?

Yes

Bluetooth Smart MAC

- ❑ Two Device Types: "**Peripherals**" are simpler than "**central.**"
- ❑ Two PDU Types: Advertising, Data
- ❑ **Non-Connectable Advertising**: Broadcast data in clear
- ❑ **Discoverable Advertising**: Central may request more information. Peripheral can send data without connection
- ❑ **General Advertising**: Broadcast presence wanting to connect. Central may request a short connection.
- ❑ **Directed Advertising**: Transmit signed data to a previously connected master



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

Student Questions

❑What are central and peripheral devices? Are they related to the master and slave?

Yes.

❑When is discoverable advertising being used (after or before connection), and for what purpose?

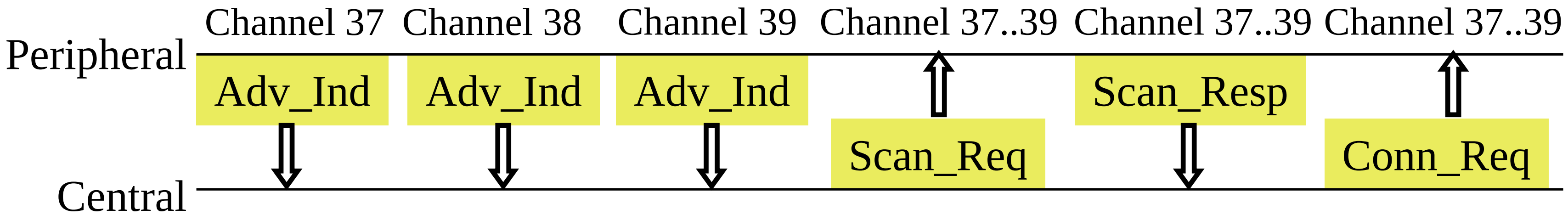
To identify each other and for capability negotiation during connection.

❑Is it correct that signed data is accessible by anyone as long as they have the public key?

The signature can be verified by anyone using Public Key. But the data can still be encrypted before or after the signature.

Bluetooth Smart MAC

- ❑ Two Device Types: "**Peripherals**" are simpler than "**central.**"
- ❑ Two PDU Types: Advertising, Data
- ❑ **Non-Connectable Advertising**: Broadcast data in clear
- ❑ **Discoverable Advertising**: Central may request more information. Peripheral can send data without connection
- ❑ **General Advertising**: Broadcast presence wanting to connect. Central may request a short connection.
- ❑ **Directed Advertising**: Transmit signed data to a previously connected master



Channel 37 Channel 38 Channel 39 Channel 37..39 Channel 37..39 Channel 37..39

Peripheral

Adv_Ind Adv_Ind Adv_Ind Scan_Req Scan_Resp Conn_Req

Central

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

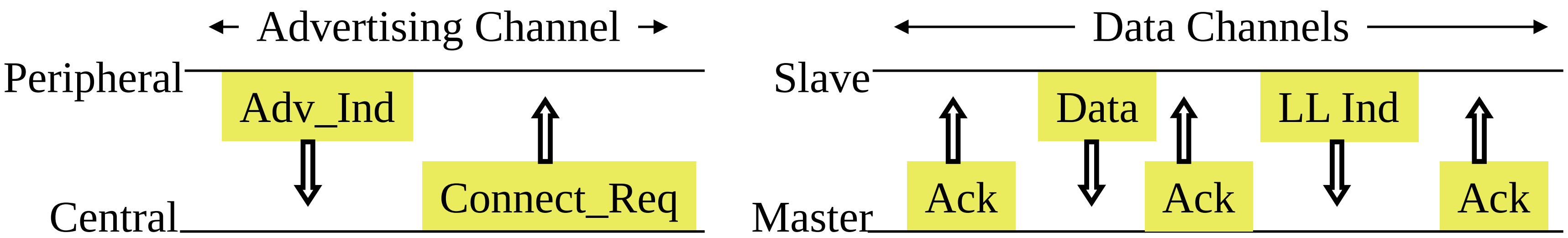
Student Questions

❑ Does the master always broadcast the same information at three advertising channels?

One of the three

Bluetooth Smart MAC (Cont)

- ❑ After connecting, the master tells the slave about the hopping sequence and wake-up cycle
- ❑ All subsequent data transfers in 37 data channels
- ❑ Both devices can sleep between transactions
- ❑ Data can be encrypted.
- ❑ ~3 μs per transaction, 15 μW Power = 10 μA using 1.5V
  ⇒ 30μAs/transaction
  ⇒ 21.6 M transactions using 180 μAh battery
  ⇒ 41.1 years with one transaction/minute



← Advertising Channel →
Peripheral
Adv_Ind
Connect_Req
Central
← Data Channels →
Slave
Data
LL Ind
Ack
Ack
Ack
Master

Student Questions

❑The slides say ms, mW, and mA, but in the video, you say uW, uA. Which ones are correct?

PowerPoint bug. It changes the font to the installed font if the symbol font is unavailable.
Symbol μ = Times New Roman m

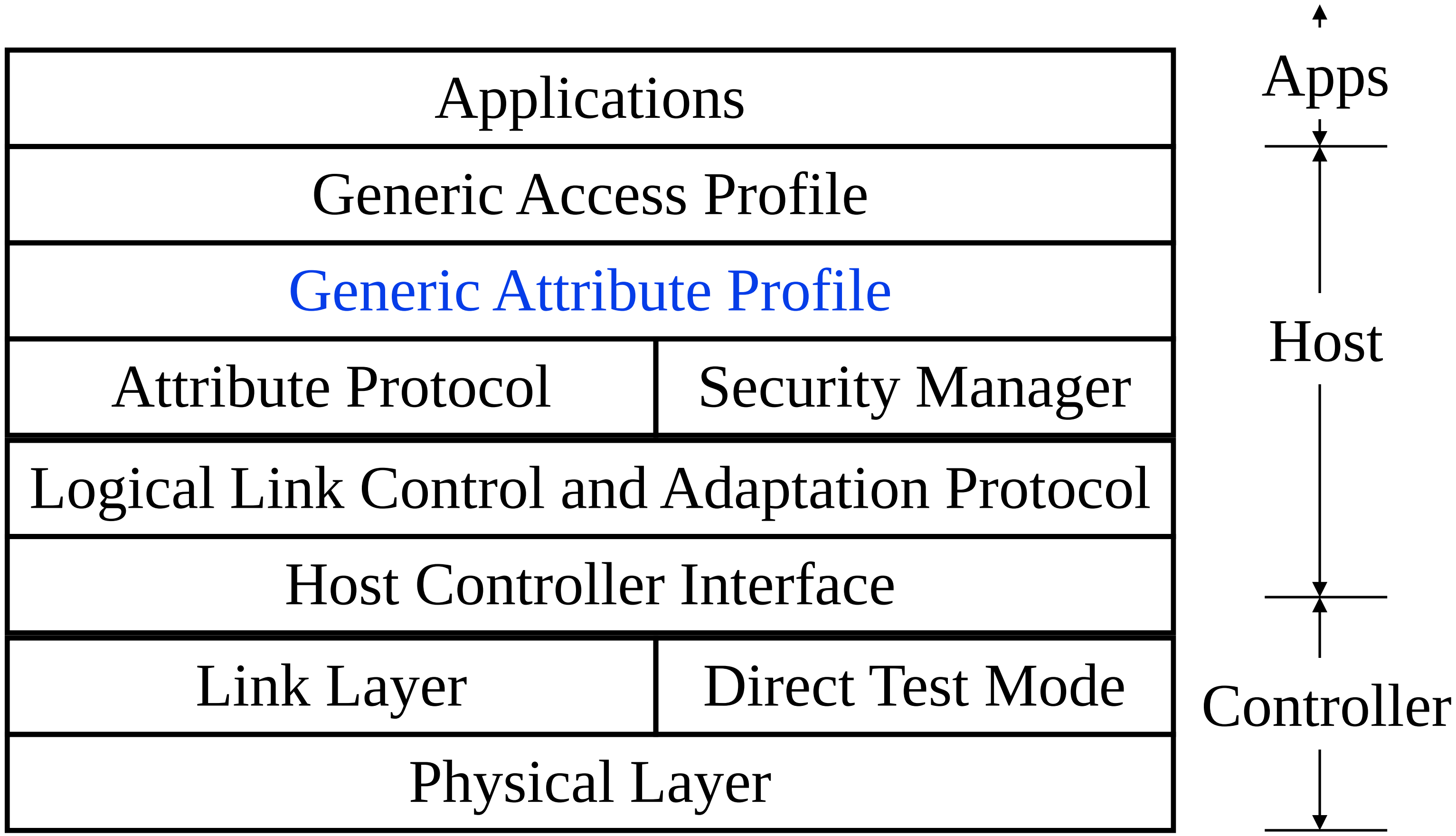
❑In point 4, which 'm' is micro and which is milli? In the video you were not sure about units.

All m's are micro.

❑What's "LL End"?

Logical Link Termination Indicator

Bluetooth Smart Protocol Stack



Applications

Generic Access Profile

Generic Attribute Profile

Attribute Protocol | Security Manager

Logical Link Control and Adaptation Protocol

Host Controller Interface

Link Layer | Direct Test Mode

Physical Layer

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

Student Questions

❑Is the Serial interface not exposed for the Bluetooth smart protocol stack?

The serial wireless interface is called an antenna connector.

❑Is Generic Access Profile the whole standby --> inquiry --> page --> connect procedure?

Profiles are databases, not protocols.

Generic Attribute (GATT) Profile

- ❑ Defines data formats and interfaces with the Attribute Protocol
- ❑ Type-Length-Value (TLV) encoding is used
- ❑ Each attribute has a 16-bit Universally Unique ID (UUID) standardized by Bluetooth SIG
- ❑ 128-bit UUID if assigned by a manufacturer
- ❑ 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

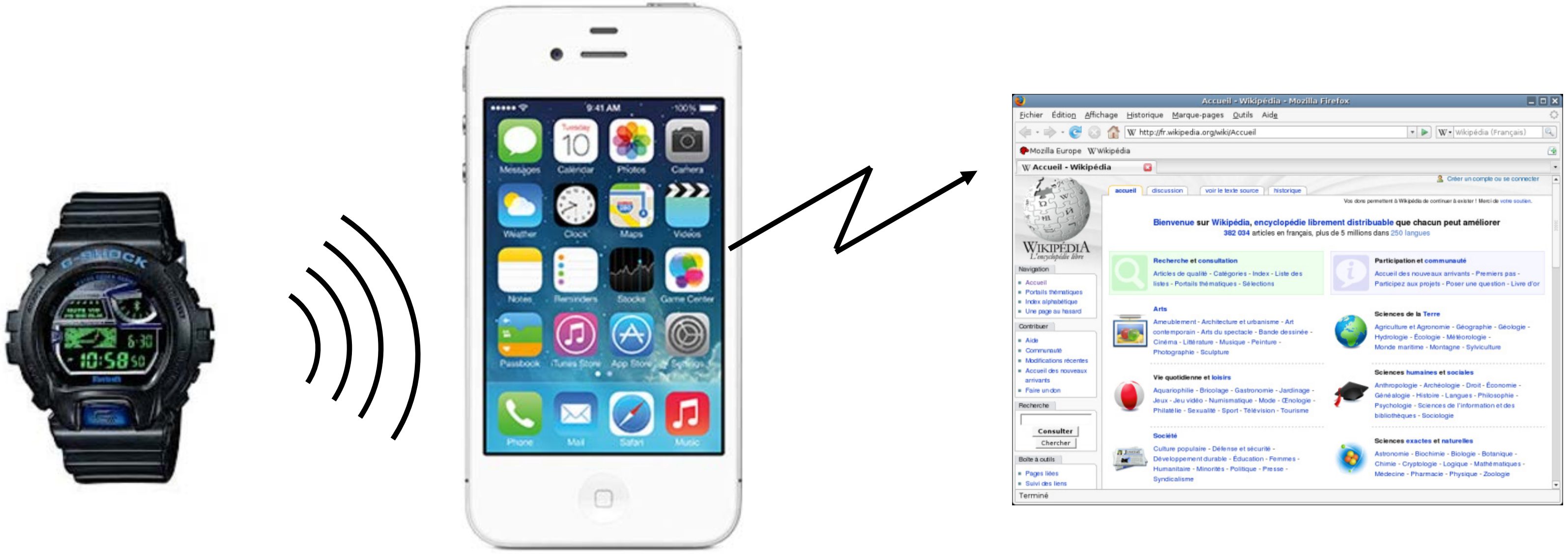
Student Questions

❑UIDs that SIG created cannot be changed, but those created by a manufacturer could be changed in the future. For instance, we might have multiple 128-bit UIDs that refer to the same attribute.

This can occur since manufacturers' UIDs are independently set. However, manufacturers publish their UIDs to avoid this.

Bluetooth Gateway Devices

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



Student Questions

❑It seems that many Bluetooth devices have the problem that the gateway devices restrict their functions. The same connection requires double-checking on the phone; the remote access requires the app to be in the front end, which is annoying. Is that common, or are there any solutions?

This is up to the application/OS interface designers and implementers. This may be done to avoid accidental connections. Not a part of the standards.

Bluetooth Smart Applications

- Proximity: In the car, In room 303, 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

Student Questions

Beacons

- ❑ Advertising based on proximity
- ❑ Peripherals (your phone) broadcast their presence if Bluetooth is turned on
- ❑ Primary aim of these broadcasts is to allow device discovery and indoor navigation
- ❑ Advertising frames consist of a header and max 27B of payload with multiple TLV-encoded data items
  - ➢ May include signal strength ⇒ Distance
- ❑ iOS7 iPhones can send/receive iBeacons
- ❑ Can be used for customized advertising, indoor location, geofencing
- ❑ PayPal uses this to identify you.
  You can pay using a PIN and your phone.
- ❑ Google is promoting Eddystone beacons, which require only a browser (not another app) to discover proximity using beacons

Student Questions

- ❑ Is this similar to how NFC works?

NFC does not advertise. It is more like a storage than networking. You can read the card numbers within 2 cm.

- ❑ How can locations be calculated using bluetooth? Is it similar to cell tower triangulation?

Yes. Recently they have added "Angle of Arrival" too.

- ❑ Are there any rules about privacy? Can stores collect data on me as I walk around? These days on websites, you have to accept data collection via cookies.

European Privacy Global Data Privacy (GDPR) Law requires permission on websites and allows deletion on request. No US law. But on the Internet, the provider does not know whether you are in Europe or not. No laws on advertising.

Beacons

- ❑ Advertising based on proximity
- ❑ Peripherals (your phone) broadcast their presence if Bluetooth is turned on
- ❑ Primary aim of these broadcasts is to allow device discovery and indoor navigation
- ❑ Advertising frames consist of a header and max 27B of payload with multiple TLV-encoded data items
  - ➢ May include signal strength ⇒ Distance
- ❑ iOS7 iPhones can send/receive iBeacons
- ❑ Can be used for customized advertising, indoor location, geofencing
- ❑ PayPal uses this to identify you. You can pay using a PIN and your phone.

- ❑ Google is promoting Eddystone beacons, which require only a browser (not another app) to discover proximity using beacons

Student Questions

❑How is geofencing implemented using just the iBeacons?

i is for Apple iPhone/iPad/i…

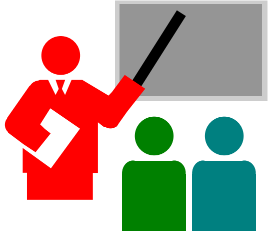
❑Is iBeacon different from the general Bluetooth beacons?

May have been customized but standards compliant.

❑How far do the Beacon broadcasts reach?

There is no distance limit. Only Power limit, generally up to 30 m in open spaces.

Summary



1. Bluetooth basic rate uses frequency hopping over 79 1-MHz channels with 1, 3, and 5 slots frames.
2. Three inactive states: hold, sniff, park. It 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

Student Questions

❑Do BLE and Bluetooth 5 use 1/3/5-slot frames transmitted in even or odd-numbered time slots?

YES

❑Assume a device has a 2-slot frame. Can the frame be continuously transmitted without frequency hopping?

Yes, in 3-slots.

❑When Bluetooth is turned on, can any information be retrieved from the device?

Generally, no information other than name and MAC address is broadcast. But hackers have found ways to sneak in connections.

Homework 11

- ❑ Submit an answer to the following problem: Assume that 256 bits could be transmitted in one slot in Bluetooth. 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.

Student Questions

❑ Is the non-payload portion always a fixed length or is it a fixed percentage of the total message length?

Fixed length.

❖ What are the answers here? Not yet graded on Canvas.

We will go over the answers at the end of this session.

End of Q

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

Student Questions

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

Student Questions

References (Cont)

- P. McDermott-Wells, "What is Bluetooth?", Volume 23, Issue 5, Page(s):33 - 35, IEEE Potentials, 2005, http://ieeexplore.ieee.org/iel5/45/29958/01368913.pdf?tp=&arnumber=1368913&isnumber=29958
- K.V.S.S.S.S. Sairam, N. Gunasekaran, and S.R. Redd, "Bluetooth in wireless communication" Volume 40, Issue 6, Page(s):90 - 96, IEEE Communications Magazine, June 2002, http://ieeexplore.ieee.org/iel5/35/21727/01007414.pdf?tp=&arnumber=1007414&isnumber=21727
- B. Chatschik, "An overview of the Bluetooth wireless technology", Volume 39, Issue 12, Page(s):86 - 94, IEEE Communications Magazine, 2001, http://ieeexplore.ieee.org/iel5/35/20896/00968817.pdf?tp=&arnumber=968817&isnumber=20896

Student Questions

References (Cont)

- Martin Wooley, “Bluetooth Core Specification Version 5.1 Feature Overview,” Bluetooth SIG, December 2020, https://www.bluetooth.com/wp-content/uploads/Files/Specification/1901_Feature_Overview_Brief_FINAL.pdf
- Martin Wooley, “Bluetooth Core Specification Version 5.2 Feature Overview,” Bluetooth SIG, December 2020, https://www.bluetooth.com/wp-content/uploads/2020/01/Bluetooth_5.2_Feature_Overview.pdf
- Martin Wooley, “Bluetooth Core Specification Version 5.3 Feature Enhancements,” Bluetooth SIG, June 2021, https://www.bluetooth.com/wp-content/uploads/2021/01/Bluetooth_5.3_Feature_Enhancements_Update.pdf

Student Questions

Acronyms

ACL	Asynchronous Connection List
AD	Advertisement
AES-128	Advanced Encryption Standard w 128-bit keys
BIN	Binary
BLE	Bluetooth Low Energy
BNEP	Bluetooth Network Encapsulation Protocol
CAP	Connection Access Profile
CSA	Core Specification Amendment
dBm	Deci-bel milli-watt
DPSK	Differential Phase Shift Keying
EDR	Enhanced Data Rate,
FEC	Forward Error Correction
FSK	Frequency Shift Keying
GATT	Generic Attribute
GFSK	Gaussian Frequency Shift Keying
GHz	Giga Hertz
HS	High Speed,

Student Questions

Acronyms (Cont)

IBM	International Business Machines
ID	Identifier
IEEE	Institution of Electrical and Electronics Engineers
iOS	Apple’s iDevices Operating System
Ind	Indicator
IoT	Internet of Things
IP	Internet Protocol
IPv6	Internet Protocol version 6
IrDA	Infrared Data Association
IrMC	Infrared Mobile Communications
IrOBEX	Infrared Object Exchange
LAN	Local Area Network
LAP	Lower address part
LE	Low Energy
LL	Logical Link
MAC	Media Access Control
MAN	Metropolitan Area Network

Student Questions

Acronyms (Cont)

MHz	Mega Hertz
mW	milli Watt
NAP	Non-significant address part
OUI	Organizationally Unique Identifier
PAL	Protocol Adaptation Layer
PC	Personal Computer
PDU	Protocol Data Unity
PHY	Physical Layer
PIN	Personal Identification Number
RF	Radio Frequency
RFCOMM	Radio Frequency Communication
RFID	Radio Frequency Identifier
SCO	Synchronous Connection Oriented
SDP	Service Discovery Protocol
SG	Study Group
SIG	Special Interest Group

Student Questions

Acronyms (Cont)

SIM	Subscriber Identity Module
TCS	Telephony Control Specification
TDD	Time-division duplex
TLV	Type-Length-Value
TV	Television
TX	Transmit
UAP	Upper address part
UCD	Unicast Connectionless Data
URL	Uniform Resource Locator
UUID	Universally Unique Identifier
µW	Micro-Watt
WAN	Wide Area Network
WBS	Wide Band Speed
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WPAN	Wireless Personal Area Networks

Student Questions

Acronyms (Cont)

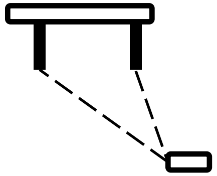
WRAN	Wireless Regional Area Network
XML	Extensible Markup Language

Student Questions

Bluetooth 5.1

- Bluetooth 5.1 in January 2019 (2 years after 5.0)

1. **Direction Finding:** Angle of Arrival (AoA) and Angle of Departure (AoD) for locating devices and indoor positioning. One of the two devices should have multiple antennas.



2. **Attribute caching:** Faster connections
3. **Randomized Advertising Channel Selection:** Removed strict sequencing between 37, 38, 39 ⇒ Avoids collisions

4. **Periodic Advertising Sync Transfer**: Allows one device (smartphone) to pass on info on another device (TV) to a low-energy companion (smartwatch) ⇒ Lower energy consumption on the companion

Ref: Martin Wooley, "Bluetooth Core Specification Version 5.1 Feature Overview," Bluetooth SIG, December 2020, https://www.bluetooth.com/wp-content/uploads/Files/Specification/1901_Feature_Overview_Brief_FINAL.pdf

Student Questions

Bluetooth 5.2

- Bluetooth 5.2 in December 2019

1. **Enhanced Attribute Protocol (EATT):** Allows multiple applications to operate simultaneously by interleaving transactions.
2. **Low-Energy Power Control**: Allows monitoring quality and requesting power level changes ⇒ Saves battery
3. **Low-Energy Isochronous Channels**: Time-synchronized unicast or broadcast ⇒ Allows audio to multiple devices
4. **Low-Energy Audio**: Uses LE Isochronous channels with special features for hearing aids. Can customize for different locations: theatres, conferences, lecture halls, airports, …

Ref: Martin Wooley, "Bluetooth Core Specification Version 5.2 Feature Overview," Bluetooth SIG, December 2020, https://www.bluetooth.com/wp-content/uploads/2020/01/Bluetooth_5.2_Feature_Overview.pdf

Student Questions

Bluetooth 5.3

- Bluetooth 5.3 in July 2021. Many products are on the market.

1. **Periodic Advertisement**: Do not interrupt the host application if the data is the same as before, e.g., temperature from thermostats
2. **Encryption Key Size Control**: Devices can specify the minimum key length requirement to the controller
3. **Connection Subrating**: Allows quickly changing parameters after periodic wakeup
4. **Channel Classification Enhancement**: Devices also can send Slot Availability Mask (SAM) to the controller.

Ref: Martin Wooley, "Bluetooth Core Specification Version 5.3 Feature Enhancements," Bluetooth SIG, June 2021, https://www.bluetooth.com/wp-content/uploads/2021/01/Bluetooth_5.3_Feature_Enhancements_Update.pdf

Student Questions

Scan This to Download These Slides

Raj Jain
http://rajjain.com

http://www.cse.wustl.edu/~jain/cse574-22/j_11ble.htm

Student Questions

Related Modules

CSE567M: Computer Systems Analysis (Spring 2013),
https://www.youtube.com/playlist?list=PLjGG94etKypJEKjNAa1n_1X0bWWNyZcof

CSE473S: Introduction to Computer Networks (Fall 2011),
https://www.youtube.com/playlist?list=PLjGG94etKypJWOSPMh8Azcgy5e_10TiDw

Recent Advances in Networking (Spring 2013),
https://www.youtube.com/playlist?list=PLjGG94etKypLHyBN8mOgwJLHD2FFIMGq5

CSE571S: Network Security (Fall 2011),
https://www.youtube.com/playlist?list=PLjGG94etKypKvzfVtutHcPFJXumyyg93u

Video Podcasts of Prof. Raj Jain's Lectures,
https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw

Student Questions