Bluetooth - 2

- Bluetooth Security (2.1)
- Bluetooth 3.0 + HS
- Bluetooth Low Energy (4.0)
- Bluetooth 5.0

Review

- The network topology in Bluetooth
- The channel impairments – FHSS
- Media access in Bluetooth
- The state transition in Bluetooth?

Bluetooth History/Capabilities -1

Bluetooth 2.0 + EDR (Nov 4, 2004)

- **Enhanced Data Rates (EDR) bringing user data transfer**
- **rates of up to 2.1 Mbit/s.**
- **Reduced power consumption.**

Bluetooth 2.1 + EDR (July 26, 2007)

- **Specification improvements and feature enhancements**
- **Extended Inquiry Response**
- **Secure Simple Pairing**
-
  - **2008 – 1 billion Bluetooth chips shipped**

Bluetooth History/Capacities -2

Bluetooth 3.0 + HS (April 21, 2009)

- **BT itself remains 2.1 Mbit/s max**
- **Only with AMP(**Alternate MAC/PHY) **,Use of 802.11 b/g radio for High Speed data transferusing Bluetooth profiles**
- **Data rate 24Mbps for data;**
- **Approximately 8 times faster than EDR if no SCO connection**
- **active**
- **12Mbps with SCO (for voice);**
- **Approximately 4 times faster than EDR if SCO connectionactive**
- **Enhanced Power Control**

Bluetooth History/Capacities - 3

Bluetooth 4.0 (June, 2010) includes:

- **Classic Bluetooth**
  - **consists of legacy Bluetooth protocols**
- **Bluetooth high speed**
  - **is based on Wi-Fi**
- **Bluetooth low energy, (BLE), previously known as WiBree, is a subset to Bluetooth v4.0 with an entirely new protocol stack for rapid build-up of simple links.**

Bluetooth-Enabled Device Shipments Expected to Exceed 2 Billion in 2013

Bluetooth 4.0: Low Energy

How much energy does traditional Bluetooth use?

- **Traditional Bluetooth is *connection oriented*. When a device is connected, a link is maintained, even if there is no data flowing.**
- **Sniff modes allow devices to sleep, reducing power consumption to give months of battery life**
- **Peak transmit current is typically around 25mA**
- **Even though it has been independently shown to be lower power than other radio standards, it is still not low enough power for coin cells and energy harvesting applications**

What is Bluetooth Low Energy?

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

Basic Concepts of Bluetooth 4.0

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

Bluetooth low energy factsheet

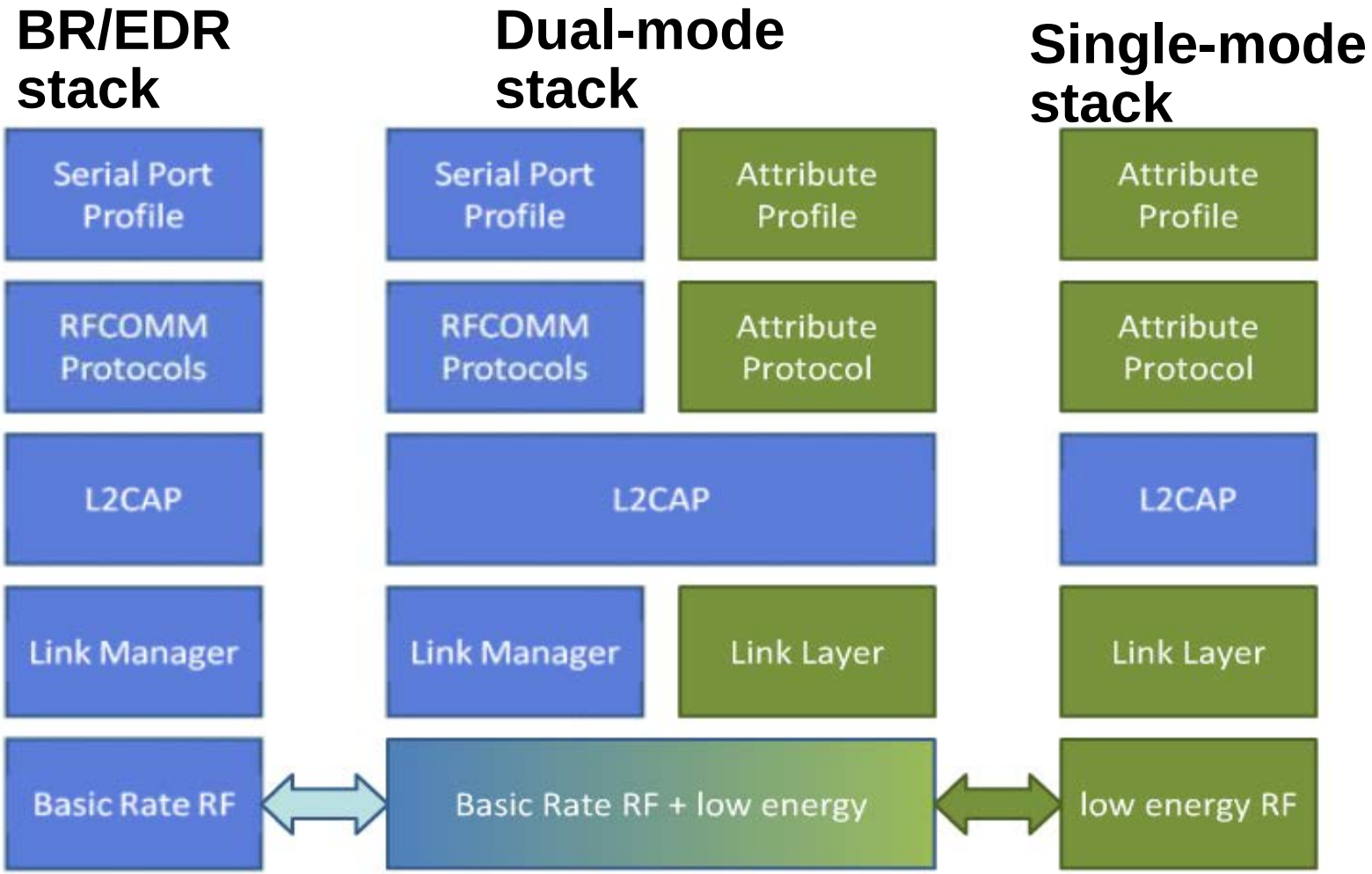
Range:	~ 150 meters open field
Output Power:	~ 10 mW (10dBm)
Max Current:	~ 15 mA
Latency:	3 ms
Topology:	Star
Connections:	> 2 billion
Modulation:	GFSK @ 2.4 GHz
Robustness:	Adaptive Frequency Hopping, 24 bit CRC
Security:	128bit AES CCM
Sleep current:	~ 1µA
Modes:	Broadcast, Connection, Event Data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

Bluetooth low energy factsheet #2

- **Data Throughput**
  - **For Bluetooth low energy, data throughput is not a meaningful parameter. It does not support streaming.**
  - **It has a data rate of 1Mbps, but is not optimized for file transfer.**
  - **It is designed for sending small chunks of data (exposing state)**

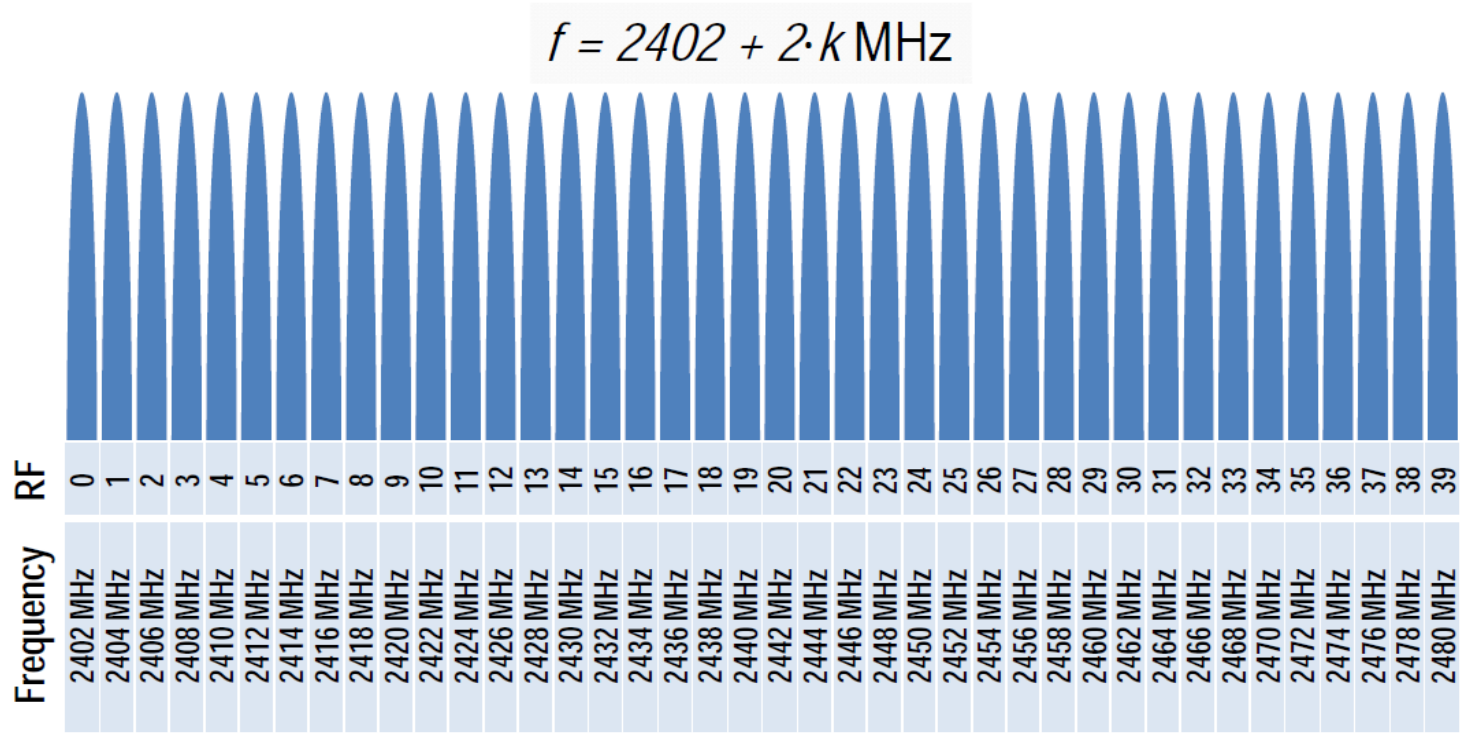
Device Modes

- **Dual mode + single modes**



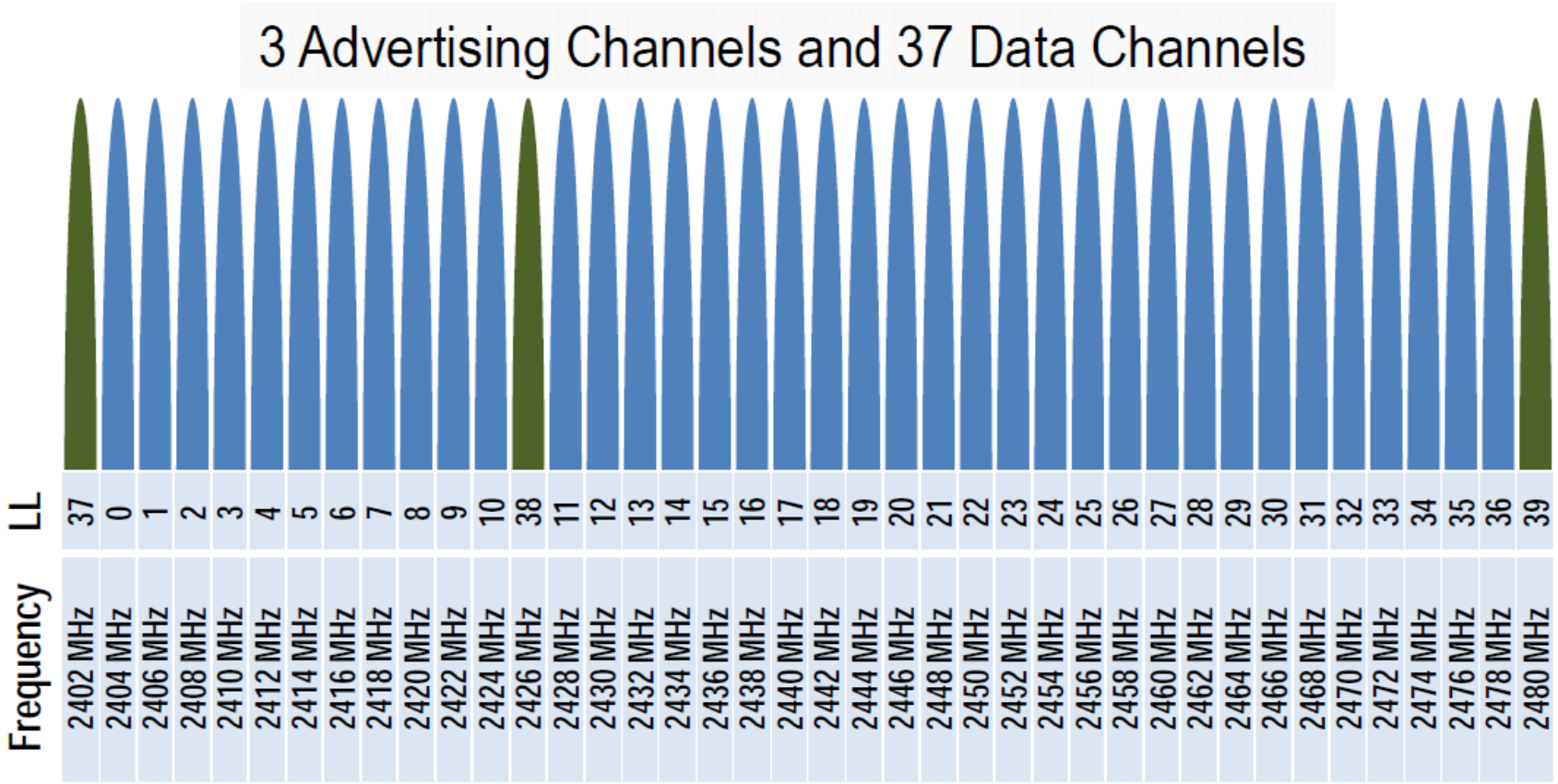
Physical Layer

- 2.4 GHz ISM band
- 1Mbps GFSK
  - Larger modulation index than Bluetooth BR (which means better range)
- 40 Channels on 2 MHz spacing



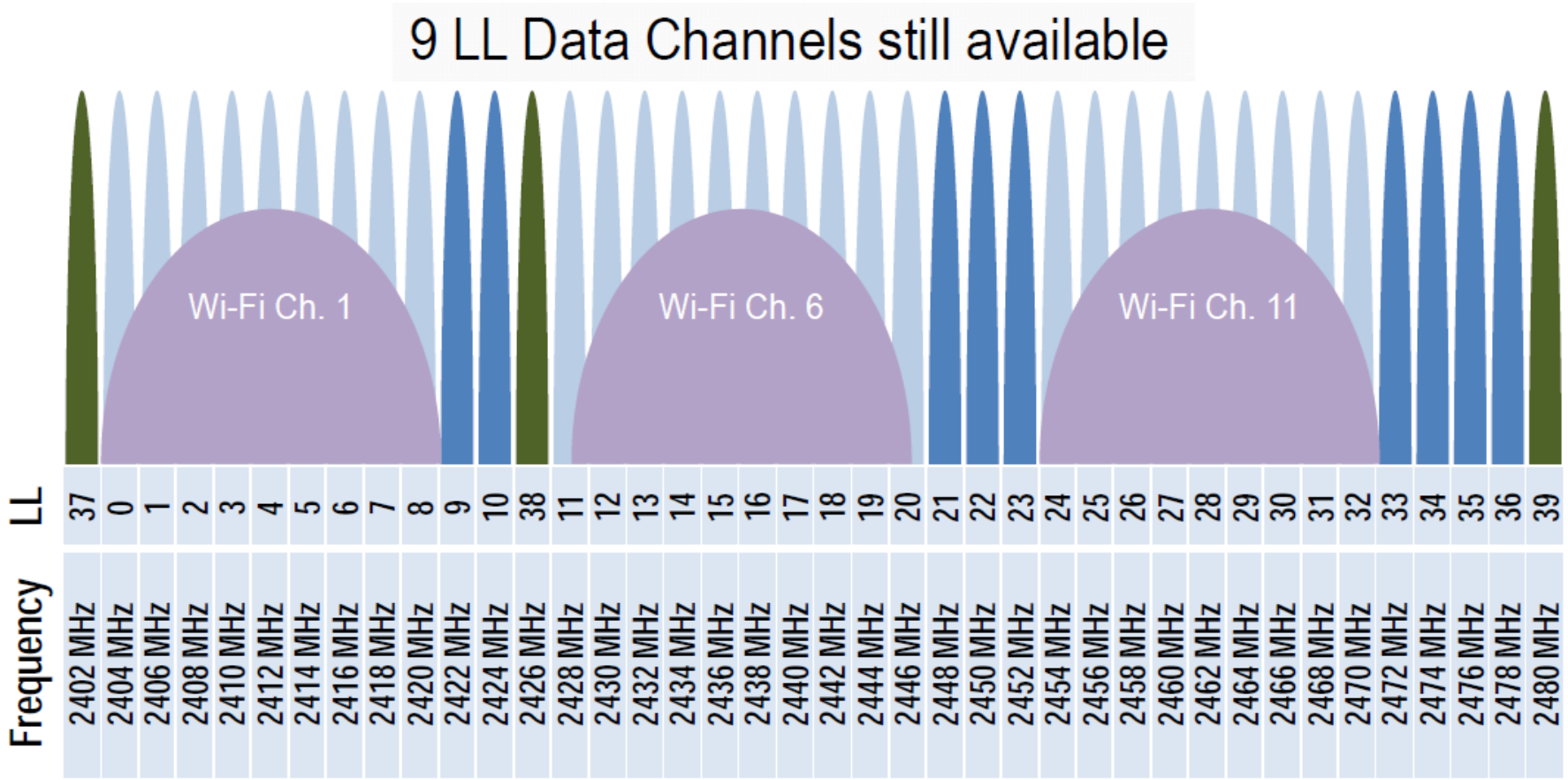
Physical Channels

- **Two types of channels**



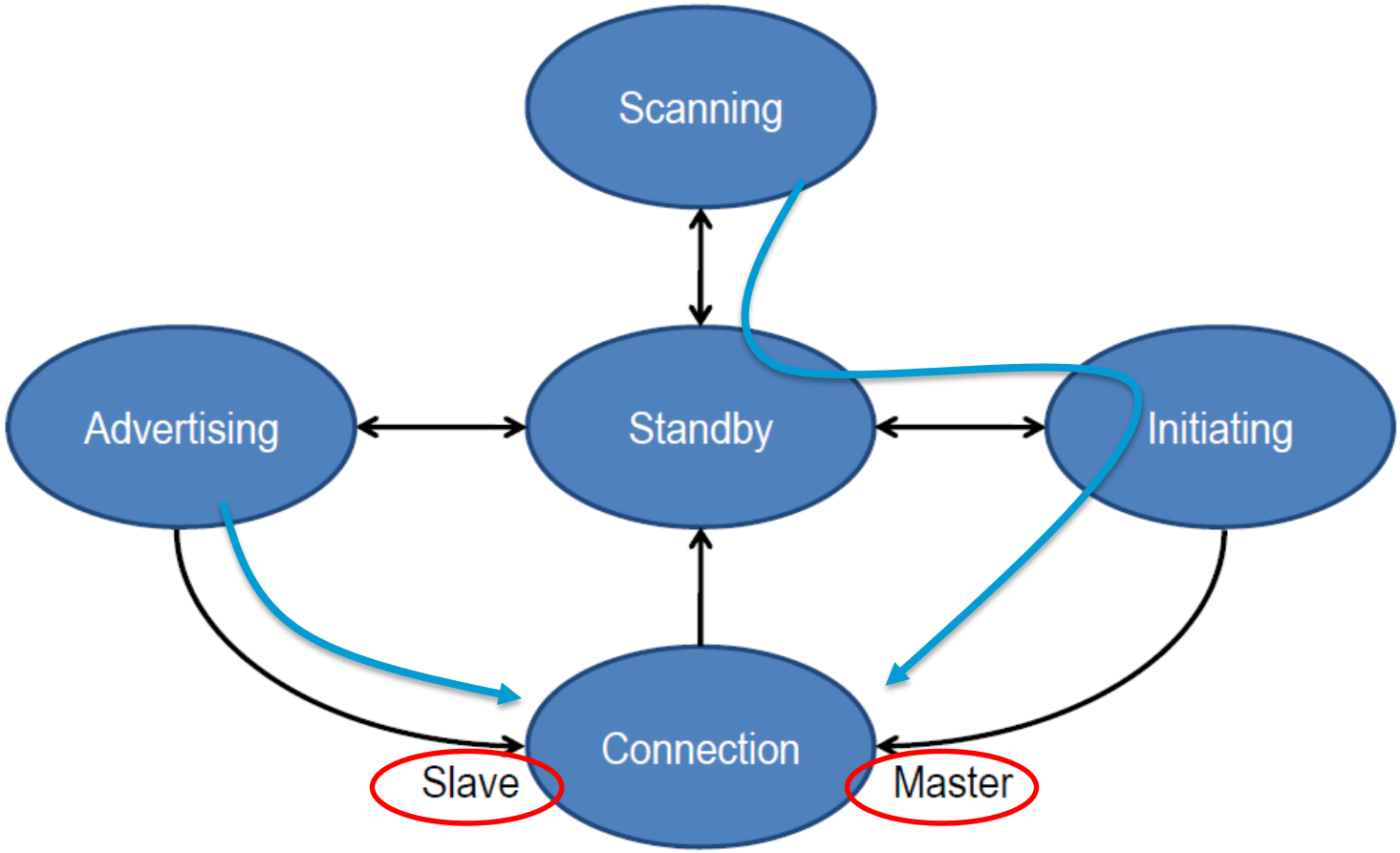
Physical Channels

- **Advertising channels avoid 802.11**

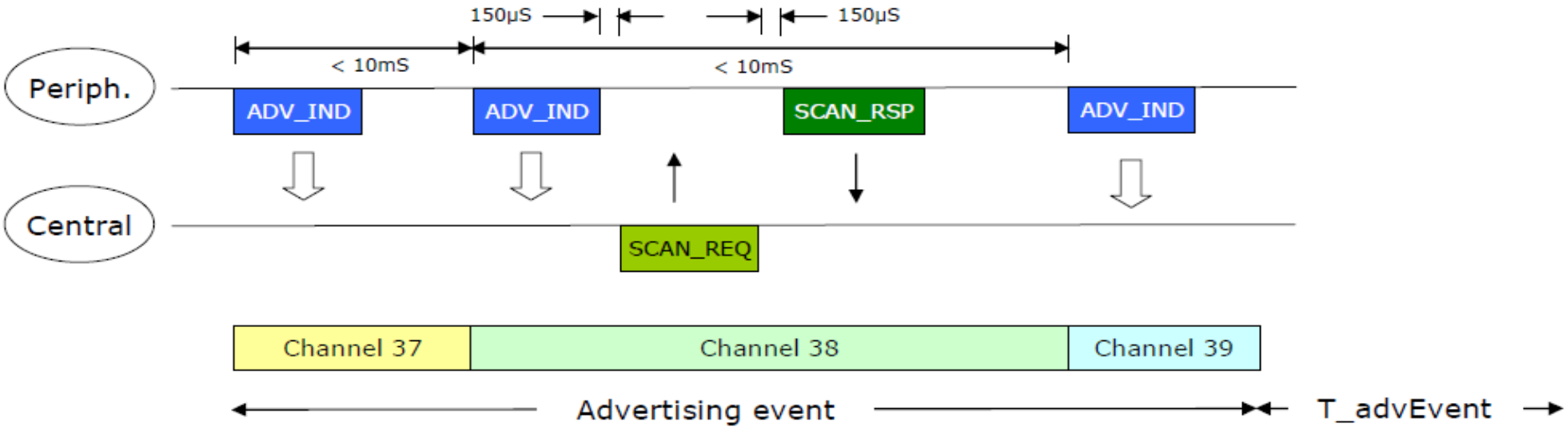


Link Layer

- **Link Layer state machine**

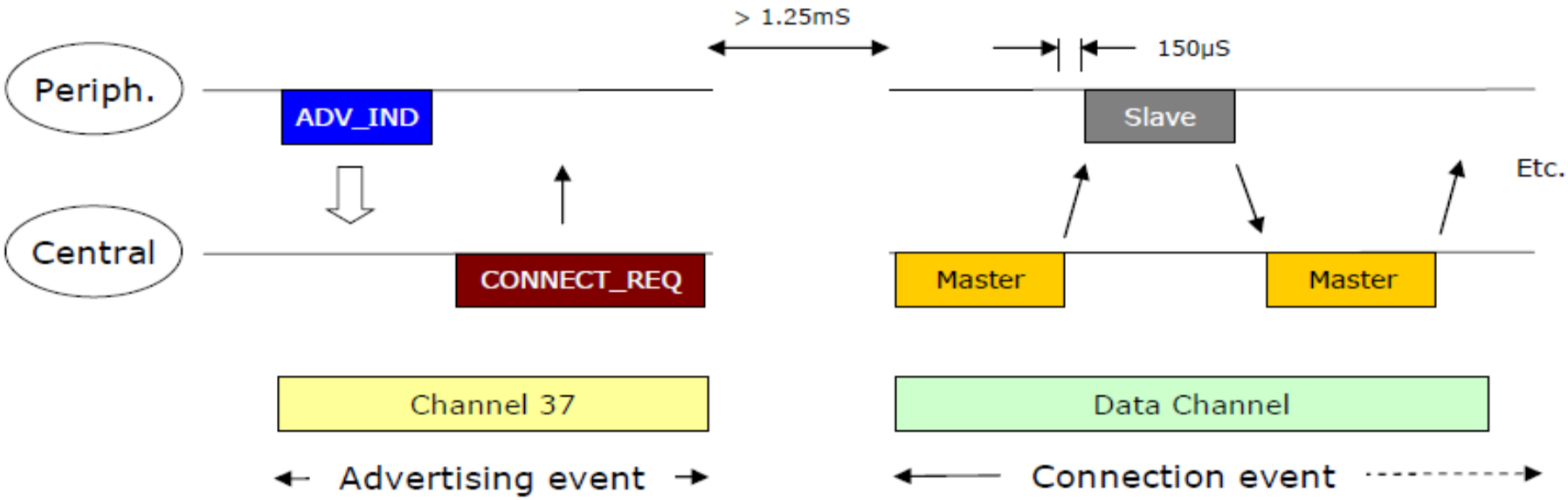


Advertising



- **Devices can advertise for a variety of reasons:**
  - **To broadcast promiscuously**
  - **To transmit signed data to a previously bonded device**
  - **To advertise their presence to a device wanting to connect**
  - **To reconnect asynchronously due to a local event**

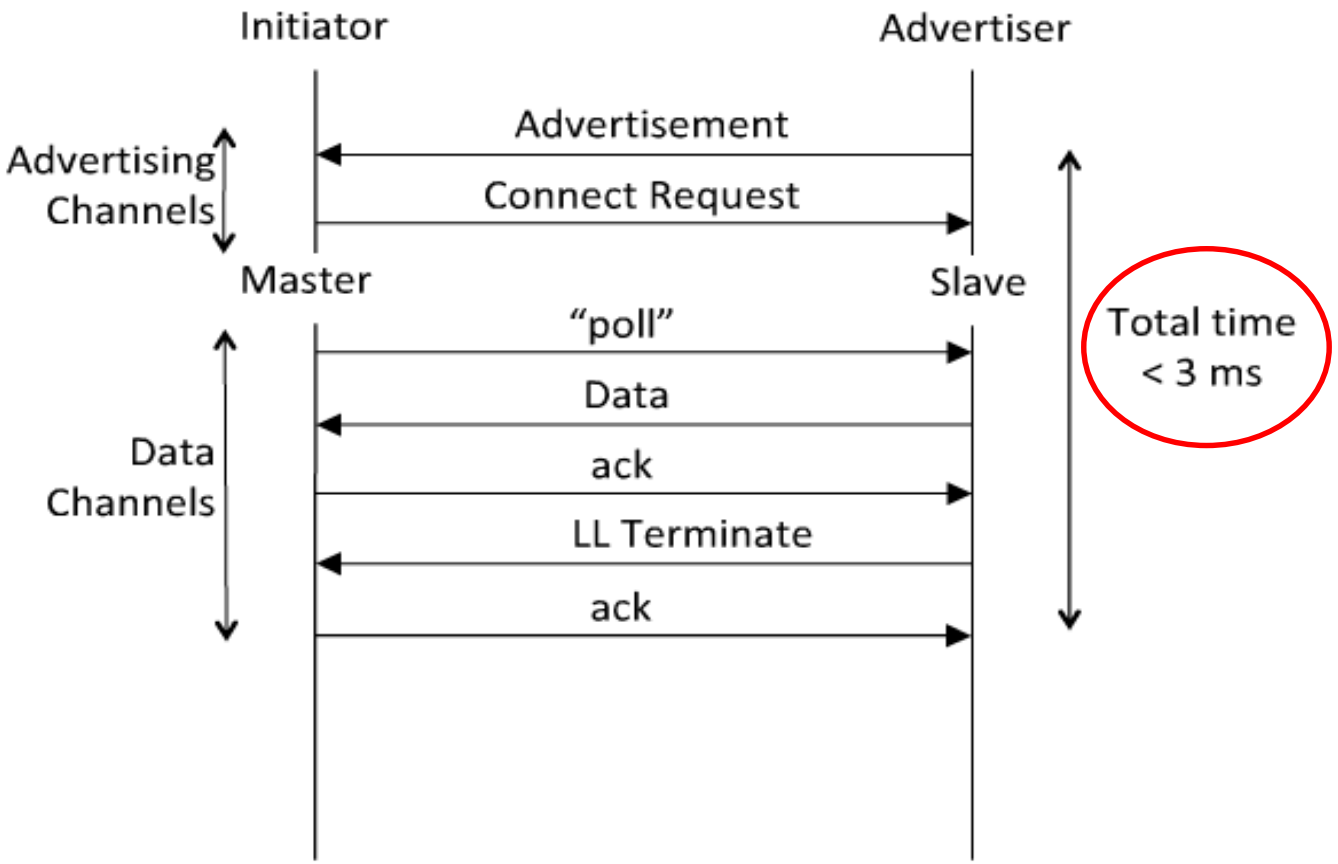
Data transactions



- **Once a connection is made:**
  - **Master informs slave of hopping sequence and when to wake**
  - **All subsequent transactions are performed in the 37 data channels**
  - **Transactions can be encrypted**
  - **Both devices can go into deep sleep between transactions**

Link Layer Connection

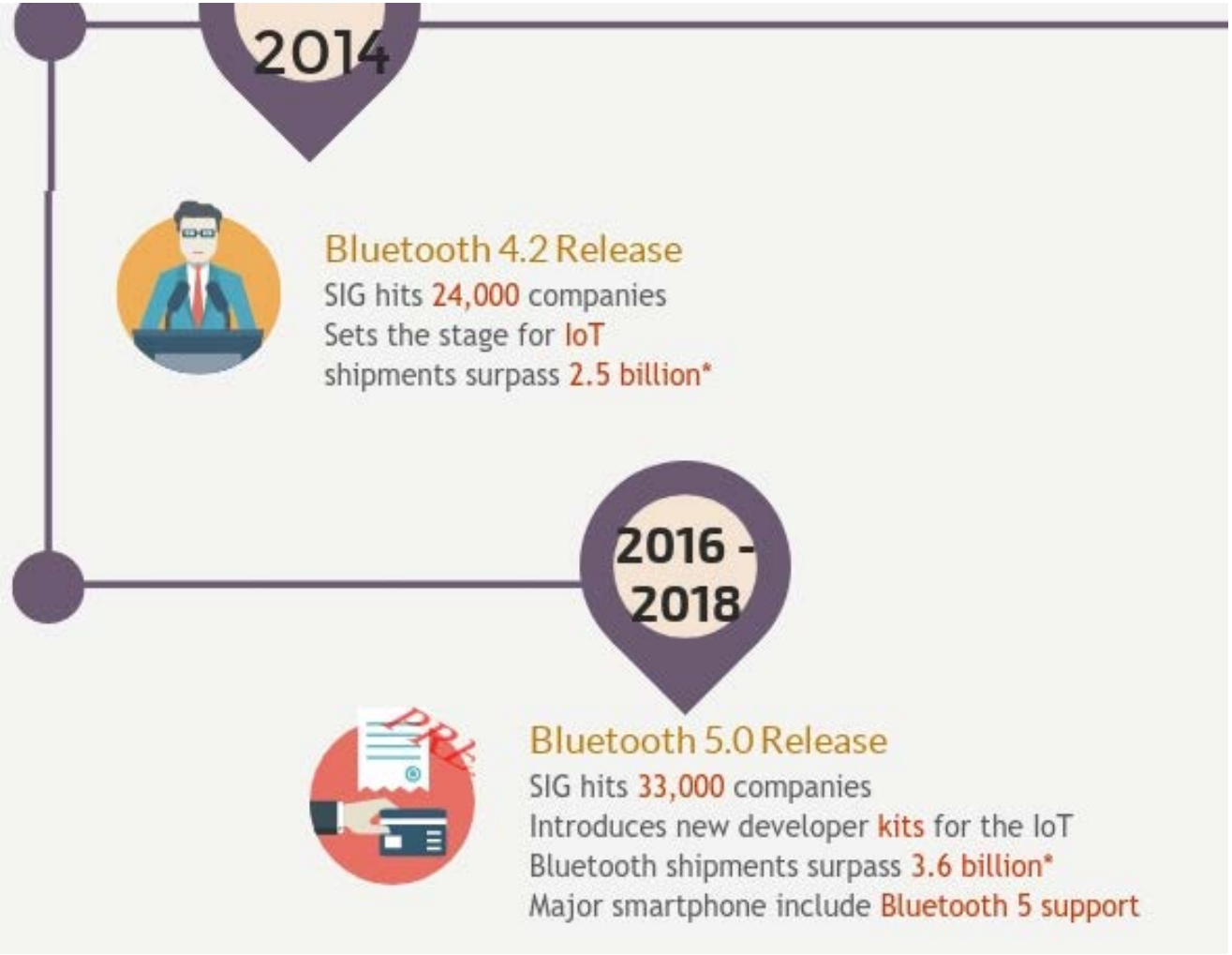
- **Very low latency connection**



How low can the energy get?

- From the previous slide, calculate energy per transaction
  - Assume an upper bound of 3ms per minimal transaction
  - Estimated TX power is 15mW (mostly TX power amp for 65nm chips)
  - For 1.5v battery, this is 10mA. 0.015W * 0.003 sec = 45 micro Joule
- How long could a sensor last on a battery?
  - An example battery: Lenmar WC357, 1.55v, 180mAh, $2-5
  - 180mAh/10mA = 18Hr = 64,800 seconds = 21.6M transactions
  - Suppose this sensor sends a report every minute 24x60 = 1440/day
  - For just the BT LE transactions, this is 21.6M/1440 =15,000 days, or > 40 years
  - This far exceeds the life of the battery and/or the product

Bluetooth Further Evolution



Bluetooth 4.2

Released on December 2, 2014, it introduces features for the Internet of Things.

The major areas of improvement are:
•Low Energy Secure Connection with Data Packet Length Extension
•Link Layer Privacy with Extended Scanner Filter Policies
•Internet Protocol Support Profile (IPSP) version 6 ready for Bluetooth Smart things to support connected home

Older Bluetooth hardware may receive 4.2 features such as Data Packet Length Extension and improved privacy via firmware upd

Bluetooth 5.0

The change is for the sake of "Simplifying our marketing, communicating user benefits more effectively and making it easier to signal significant technology updates to the market."

Age of IoT
≃ 48 Billion Devices

≃ 30% devices are forecasted to include Bluetooth technology By 2021

Major Improvements in Bluetooth 5.0

- 2x Speed
- 4x Range
- Maximum Transmit Power
- Low Energy Channel Selection Algorithm #2
- 8x Advertising Capacity
- High Duty Cycle Non-Connectable Advertising
- Slot Availability Mask (SAM)

2x Speed

- One of the major features in Bluetooth 5.0 is a new PHY.
- Bluetooth 4.x devices only support a single 1 Mbps PHY rate, but Bluetooth 5.0 devices are capable of supporting either the 1 Mbps or 2 Mbps PHY rates.
- By doubling the PHY rate, the amount of data that devices can transfer is almost doubled as shown in the table on next slide.
- Another benefit of the faster PHY is the reduced time required for transmitting and receiving data, which translates to a lower average current consumption.
- This is explained by the fact that more time can be spent in low-power sleep modes.

Comparison of 1M and 2M Bluetooth low energy PHYs

PHY	Symbol rate	Error detection	Range multiplier	PDU Length	Minimum packet time	Maximum packet time	Maximum throughput
1M	1M symbols/s	CRC	1 x	0 - 257 B	80 µs	2.12 ms	800 kbps
2M	1 M symbols/s	CRC	0.8 x	0 - 257 B	44 µs	1.064 ms	1438 kbps

- Doubling the throughput while providing low-power consumption will allow applications to provide faster data transfers for use cases like over-the-air (OTA) firmware upgrades or transmitting of days' worth of collected data from a sensor.

- It will also improve latency and responsiveness for time critical applications such as medical devices and security systems.

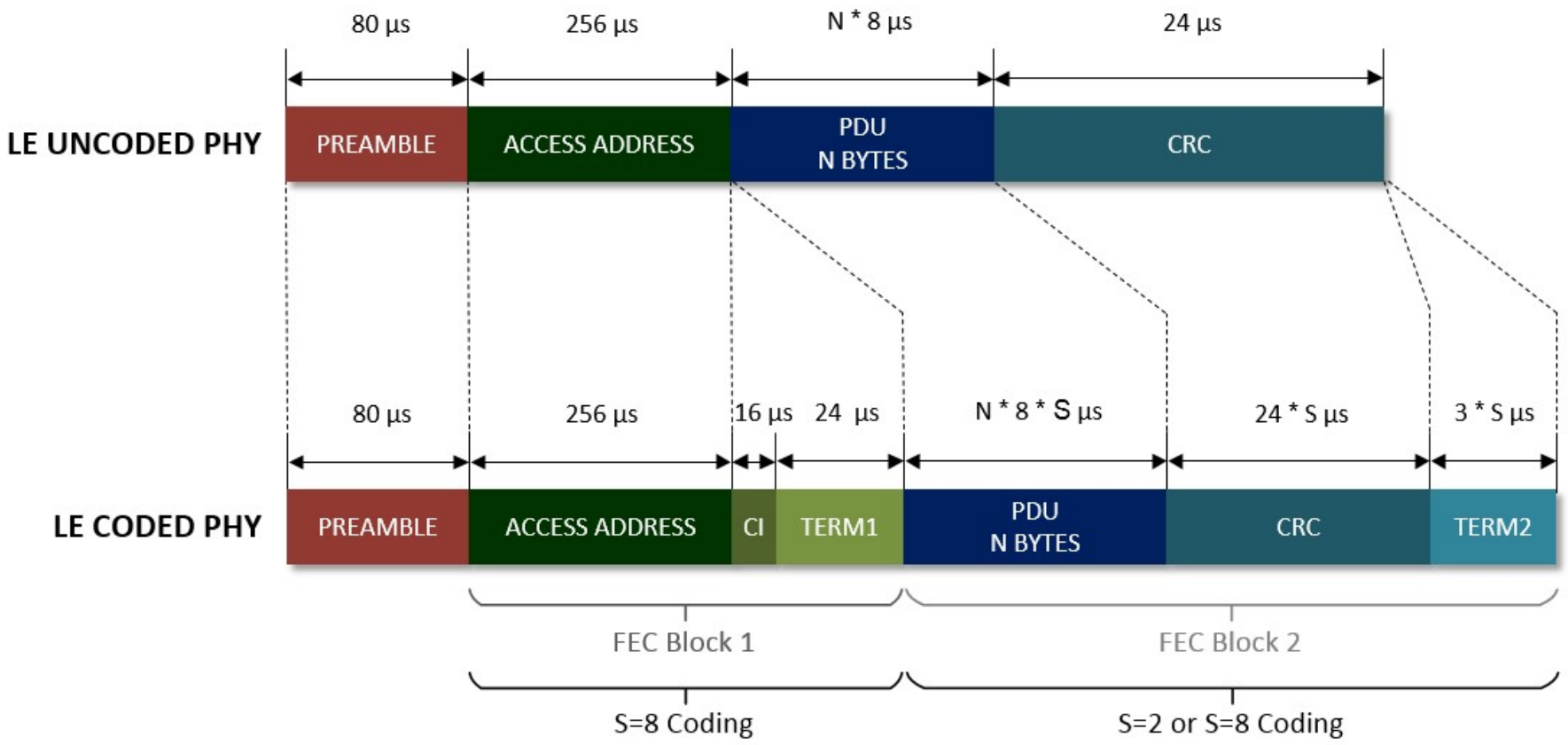
4x Range

- The LE long range feature of Bluetooth 5 can quadruple the range and deliver robust and reliable connections.
- This means that whole-house and building coverage, as well as new use cases for outdoor, industrial, and commercial applications will become a reality.
- Those are something Bluetooth has not been able to address earlier, or when it has, the range has been limited.

So, how can Bluetooth 5.0 provide 4x the range?

LE Codec PHY's

- In addition to the 2M PHY, Bluetooth 5.0 contains two additional optional PHYs called LE Coded PHYs.
- The LE Coded PHYs actually use the 1M PHY rate, but the actual payload is coded either with 500 kbps (S=2) or 125 kbps (S=8) rate, whereas the preamble and access address use the 1M coding.
- LE Coded PHY's also use a slightly different packet format versus the 1M and 2M PHYs.
- A coding indicator (CI) and TERM1 and TERM2 headers are added into the LE packet.
- Using the coded PHYs improves the RX sensitivity, which also means improved range.
- Typically, a 4-6 dB RX sensitivity improvement can be achieved using either the 500 kbps or 125 kbps PHY and this usually converts to a 2-4x range improvement.



Bluetooth 5.0 un-coded vs. coded PHY packet format

Maximum Transmit Power

- Maximum transmit power in Bluetooth 5.0 is defined to be +20 dBm, while in the Bluetooth 4X specification this level was defined at +10 dBm.
- Increasing the TX power by 10x of course can have a radical impact to the maximum range.
- Using a +20 dBm TX power with Bluetooth low energy technology is however not that straightforward.
- Different regulatory bodies do not allow transmit powers higher than 10 dBm due to the simplified hopping sequence and the small number of channels Bluetooth with low energy radios can use while advertising or in a connection.
- However, the Bluetooth 5 specification includes enhancements to both advertising and channel selection algorithms that make it possible to use more RF channels than Bluetooth 4.
- These enhancements may allow Bluetooth 5 devices to use higher than +10 dBm transmit power globally in the future, improving range and creating more robust connections.

Channel Selection Algorithm #2 (CSA#2)

- One of the new features is Channel Selection Algorithm #2 (CSA#2).
- It both improves the interference tolerance of the Bluetooth radio as well allows the radio to limit the minimum number of RF channels the radio can use in high interference environments.
- When limiting the minimum number of channels to 15 it should be possible to increase the TX power above the +10 dBm limit.

8x Advertising Capacity

- One of the major areas of improvement in the Bluetooth 5 specification is how Bluetooth advertisement (beaconing) works.
- The new specification contains significant updates to beaconing capabilities compared to previous versions of the specification.
- One of the basic improvements in Bluetooth 5 advertising is the Advertising Data Sets feature.
- It allows a single Bluetooth 5 device to send out multiple individual advertisement data sets with unique intervals and advertisement data.

Beacons

- At a basic level, beaconing is a way to deliver very short messages and track Bluetooth-enabled devices over a short distance, without the need for pairing between the beacon and the device.

- The only requirement is that the device, typically an Apple or Android smartphone or tablet, has an installed app dedicated to beaconing.

Slot Availability Masks

- Bluetooth 5 made some changes to help improve coexistence with other radio technologies on devices such as smartphones.
- Bluetooth uses the 2.4GHz ISM band and this is immediately adjacent to the Mobile Wireless Standard (MWS) bands, such as are used for LTE.
- There's potential for interference between the two systems, with transmissions from one desensitizing the receiver on the other.
- Bluetooth 5 introduces a system called Slot Availability Masks, which allows Bluetooth to indicate the availability of its time slots and to synchronize in an optimal manner with the use of the adjacent MWS bands.

Specifications or features	Bluetooth 5	Bluetooth 4.2
Speed	2x the data rate, Supports and 2 Mbps	Supports about 1 Mbps
Range	4x the range, Supports 40 meters in indoor enviroment	Supports 10 meters in indoor
Power Requirement	Low	High
Message Capacity	Large message capacity, About 255 bytes	Small message capacity, About 31 bytes
Robustness to operate in congested environment	More	Less
Battery Life	Longer	Less
Security Control	Better	Less Secure
Theoretical Data Throughput	2 Mbps, gives about 1.6 Mbps with overhead	1 Mbps
Reliability	High	Low
Digital Life	Better	Less better compare to Bluetooth 5
Support for IoT devices	Yes	No
Bluetooth Beacon	Beacons have become more popular due to increased range and speed	Beacons were less popular due to less speed/range.

Class Quiz

- What is the new PHY layer in Bluetooth 4.0?
- What is the link layer machine in Bluetooth 4.0?
- What is the new feature in Bluetooth 5.0?