ECEN 5823-001

Internet of Things Embedded Firmware

Lecture #9

25 September 2018

Be Boulder.

University of Colorado Boulder

BLE assignment demo

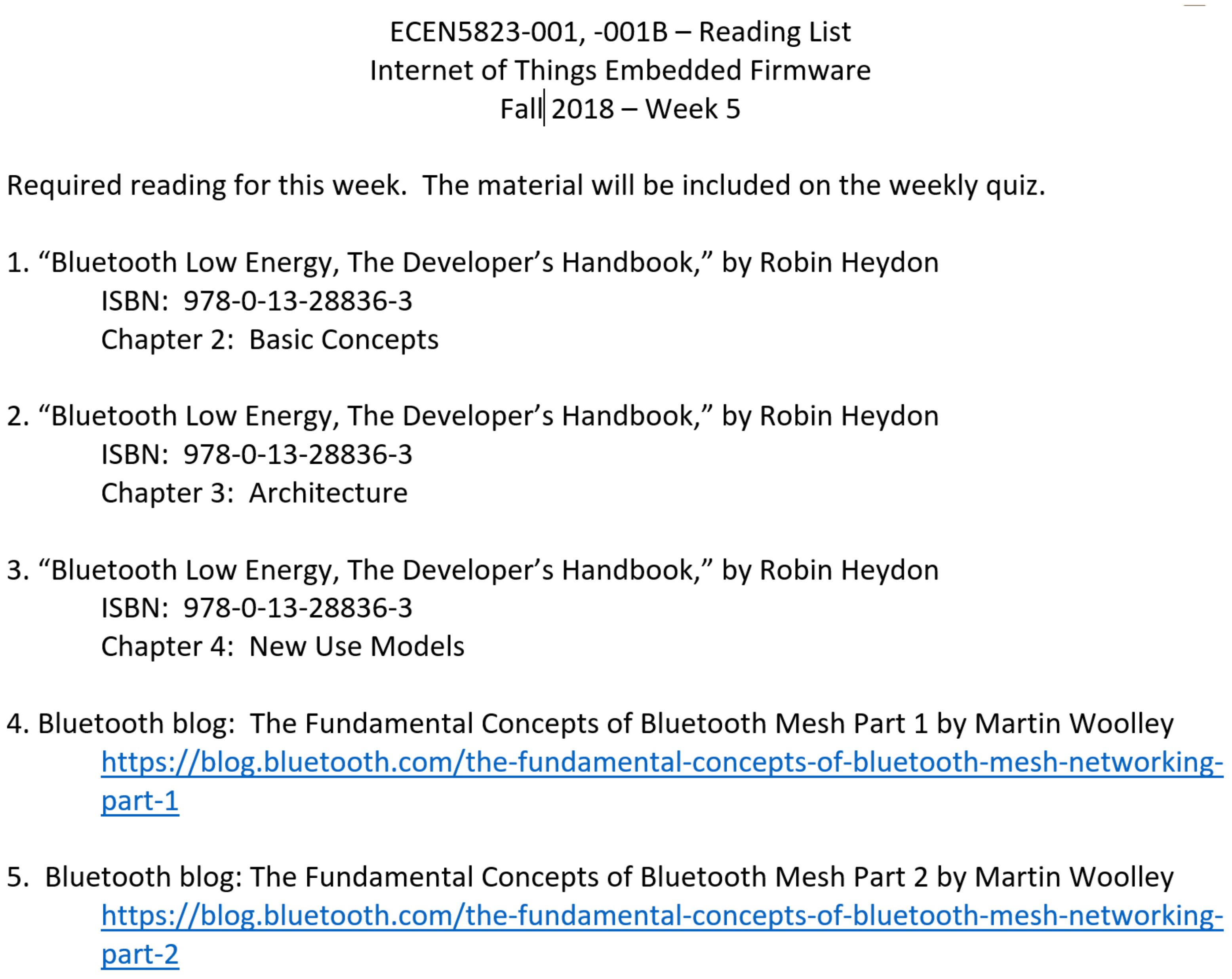
Agenda

- HTP BLE demo
- Class Announcements
- Reading Assignment
- I2C Load Power Management Rubric
- Quiz 4 review
- Bluetooth Low Energy / Smart

Class Announcements

- Quiz #5 is due at 11:59 on Sunday, September 30th, 2018
- Homework #3: HTP BLE Assignment is due on Sunday, September 30th, at 11:59pm
- Allowing resubmissions of I2C Load Power Management assignment
  - Must notify by end of today, Tuesday the 25th, to Gunj and Vipul whether you are planning to submit an updated project by end of Wednesday, September 26th
  - They will only be grading one of your project
  - If you choose the submission date of Wednesday the 26th, your score starts at 8 instead of 10
- Mid-term will be held in class on Thursday, October 18th

Reading assignment



ECEN5823-001, -001B – Reading List
Internet of Things Embedded Firmware
Fall 2018 – Week 5

Required reading for this week. The material will be included on the weekly quiz.

1. “Bluetooth Low Energy, The Developer’s Handbook,” by Robin Heydon
   ISBN: 978-0-13-28836-3
   Chapter 2: Basic Concepts

2. “Bluetooth Low Energy, The Developer’s Handbook,” by Robin Heydon
   ISBN: 978-0-13-28836-3
   Chapter 3: Architecture

3. “Bluetooth Low Energy, The Developer’s Handbook,” by Robin Heydon
   ISBN: 978-0-13-28836-3
   Chapter 4: New Use Models

4. Bluetooth blog: The Fundamental Concepts of Bluetooth Mesh Part 1 by Martin Woolley
   https://blog.bluetooth.com/the-fundamental-concepts-of-bluetooth-mesh-networking-part-1

5. Bluetooth blog: The Fundamental Concepts of Bluetooth Mesh Part 2 by Martin Woolley
   https://blog.bluetooth.com/the-fundamental-concepts-of-bluetooth-mesh-networking-part-2

I2C Load Power Management Rubric

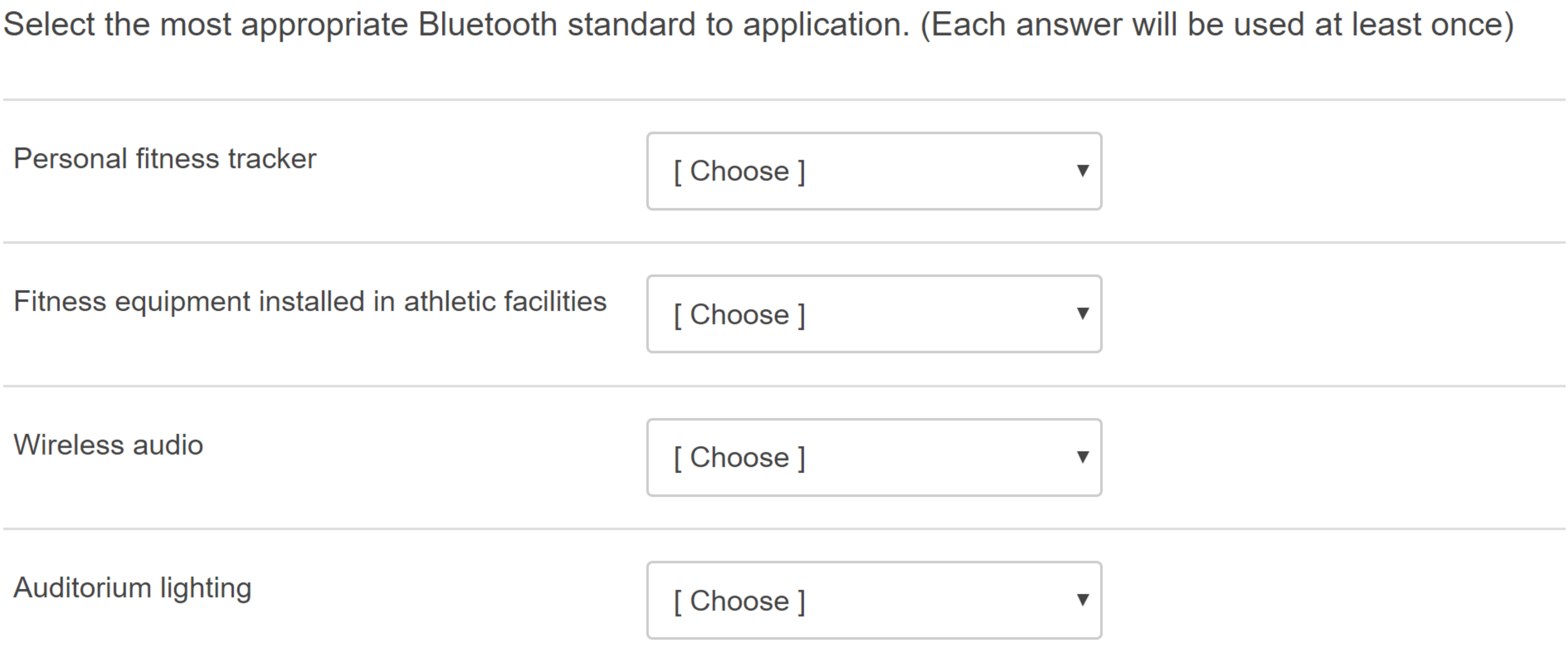
1. Total points for this exercise is 10 points
    a. 2.0 pts for the questions
    b. 8.0 pts of the code

2. Question scoring. Max score is 2.0 pts.
    a. Question 1: Will not score due to multiple ways to implement
    b. Question 2: < 3uA (1.0 pts)
    c. Question 3: Not scoring due to different ways of measuring
    d. Question 4: 87-90ms (1.0 pts)

3. Functional code delivered per exercise. Max score is 5.0 pts.
    a. Measured Period of measurements = 2.0s (1.0 pts)
    b. Length of POR of Si7021 = 80mS (1.0 pts)
    c. Total time once LPM On to going Off ~ 87-90mS (1.0 pts)
    d. Length of conversion time = 7-10mS (1.0 pts)
    e. Function temperature output being read via I2C (1.0 pts)
    f. Current will Load Power Management Off < 3uA (1.0 pts)
    g. Verify LPM being turned ON and OFF (1.0 pts)
    h. Program is written to use a scheduler to service interrupts (1.0 pts)

4. Best Practices
    a. Lack of Silicon Labs IP statement for sleep routines (-1.0 pts)
    b. Not following course documentation practices (-1.0 pts)

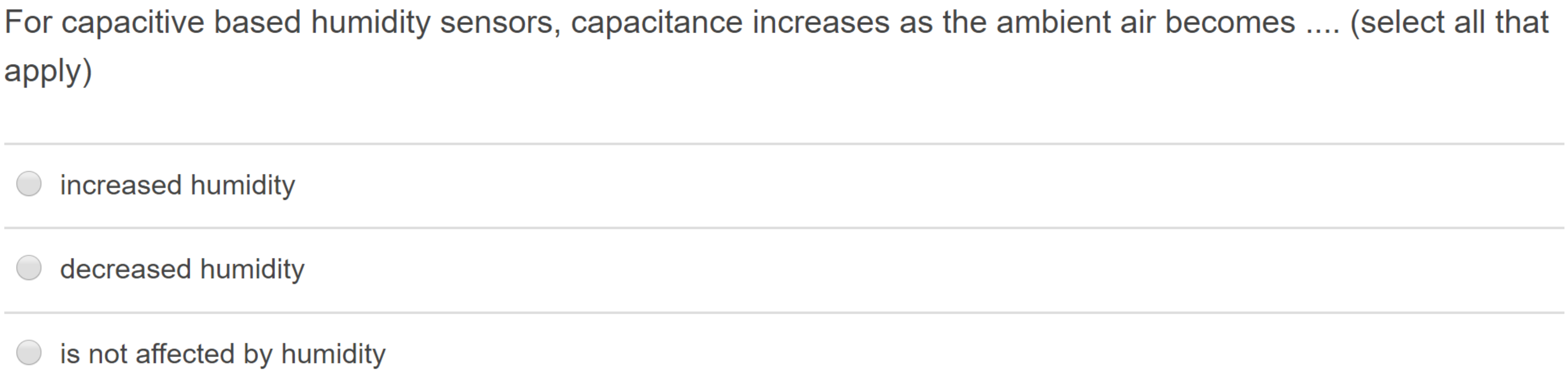
Quiz 4 review



Select the most appropriate Bluetooth standard to application. (Each answer will be used at least once)

Personal fitness tracker	[Choose] ▾
Fitness equipment installed in athletic facilities	[Choose] ▾
Wireless audio	[Choose] ▾
Auditorium lighting	[Choose] ▾

Quiz 4 review



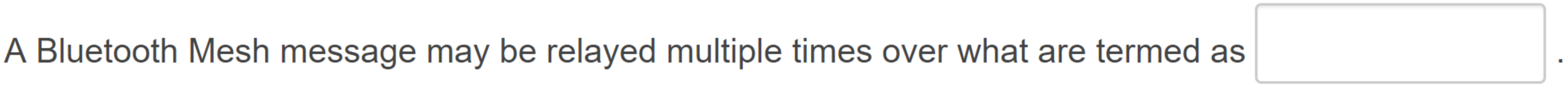
For capacitive based humidity sensors, capacitance increases as the ambient air becomes .... (select all that apply)

○ increased humidity

○ decreased humidity

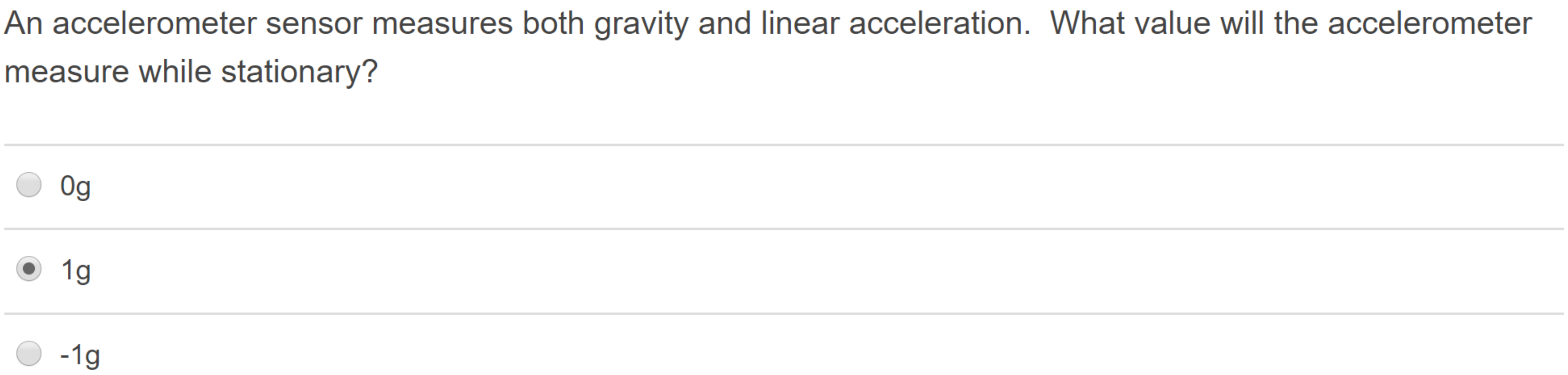
○ is not affected by humidity

Quiz 4 review



A Bluetooth Mesh message may be relayed multiple times over what are termed as ________ .

Quiz 4 review



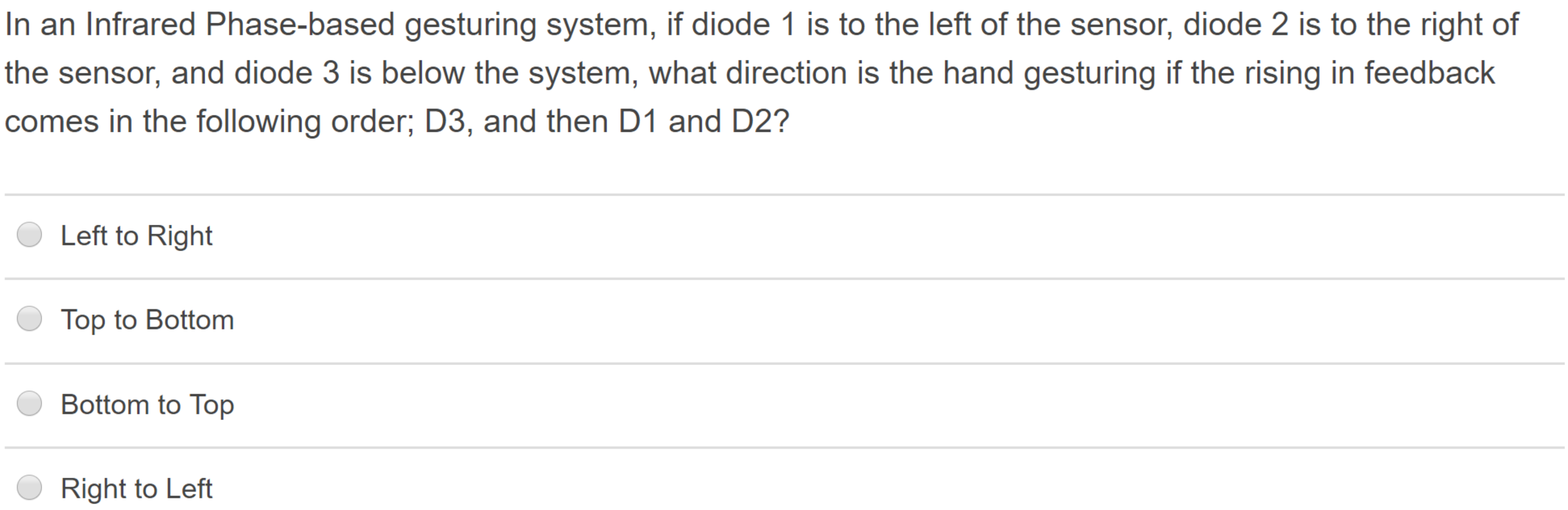
An accelerometer sensor measures both gravity and linear acceleration. What value will the accelerometer measure while stationary?

○ 0g

● 1g

○ -1g

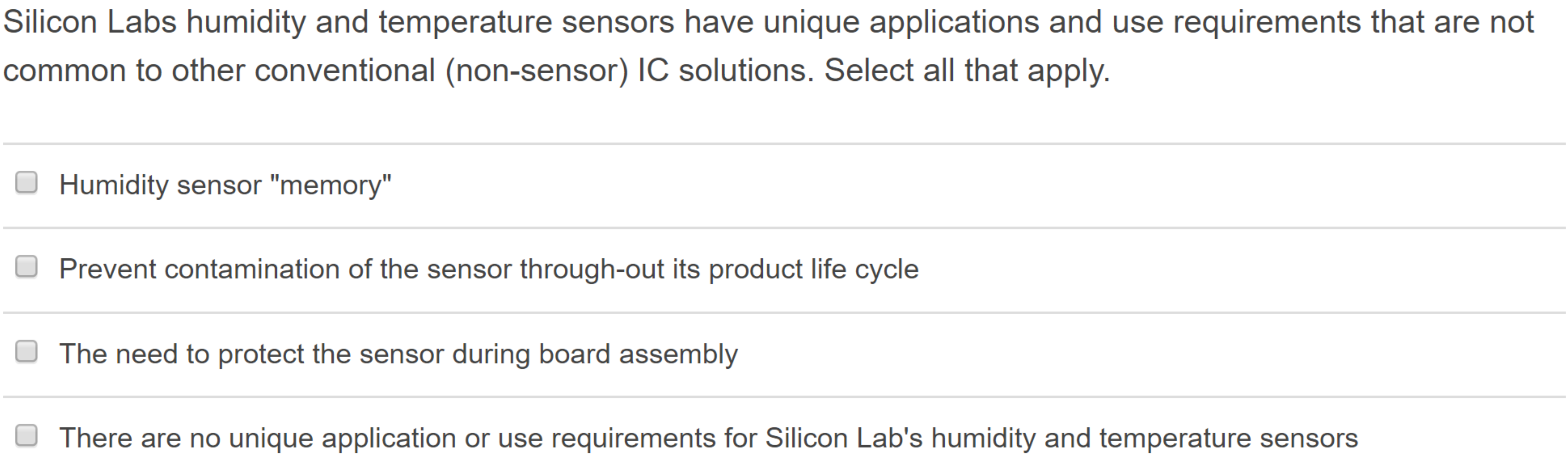
Quiz 4 review



In an Infrared Phase-based gesturing system, if diode 1 is to the left of the sensor, diode 2 is to the right of the sensor, and diode 3 is below the system, what direction is the hand gesturing if the rising in feedback comes in the following order; D3, and then D1 and D2?

- ○ Left to Right
- ○ Top to Bottom
- ○ Bottom to Top
- ○ Right to Left

Quiz 4 review



Silicon Labs humidity and temperature sensors have unique applications and use requirements that are not common to other conventional (non-sensor) IC solutions. Select all that apply.

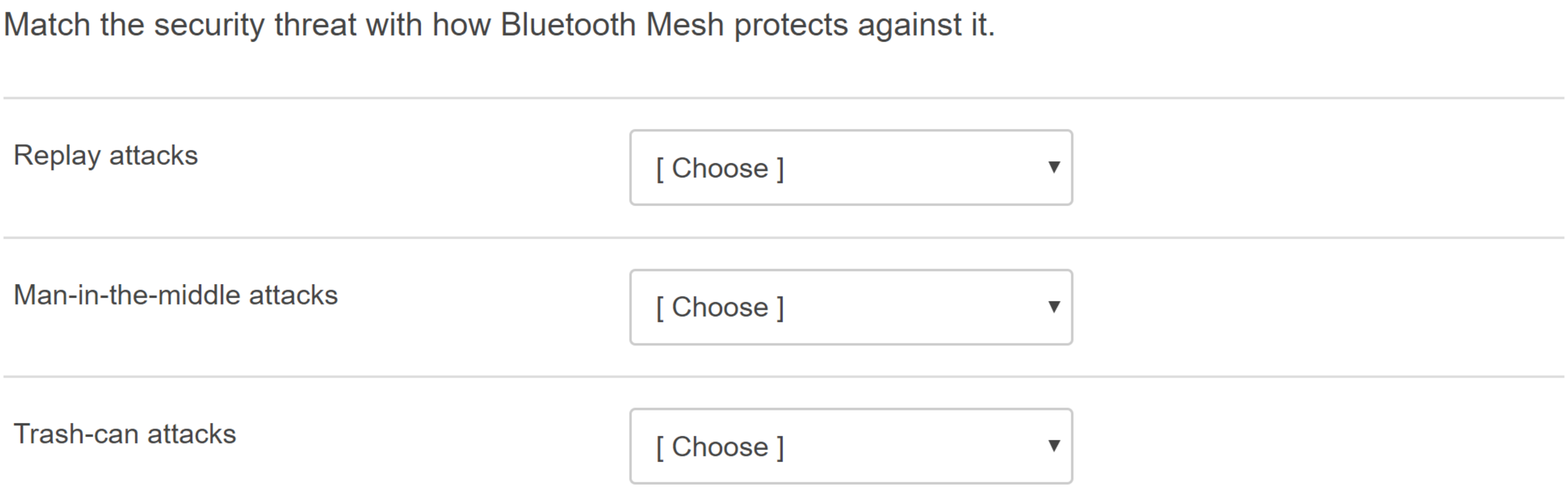
□ Humidity sensor "memory"

□ Prevent contamination of the sensor through-out its product life cycle

□ The need to protect the sensor during board assembly

□ There are no unique application or use requirements for Silicon Lab's humidity and temperature sensors

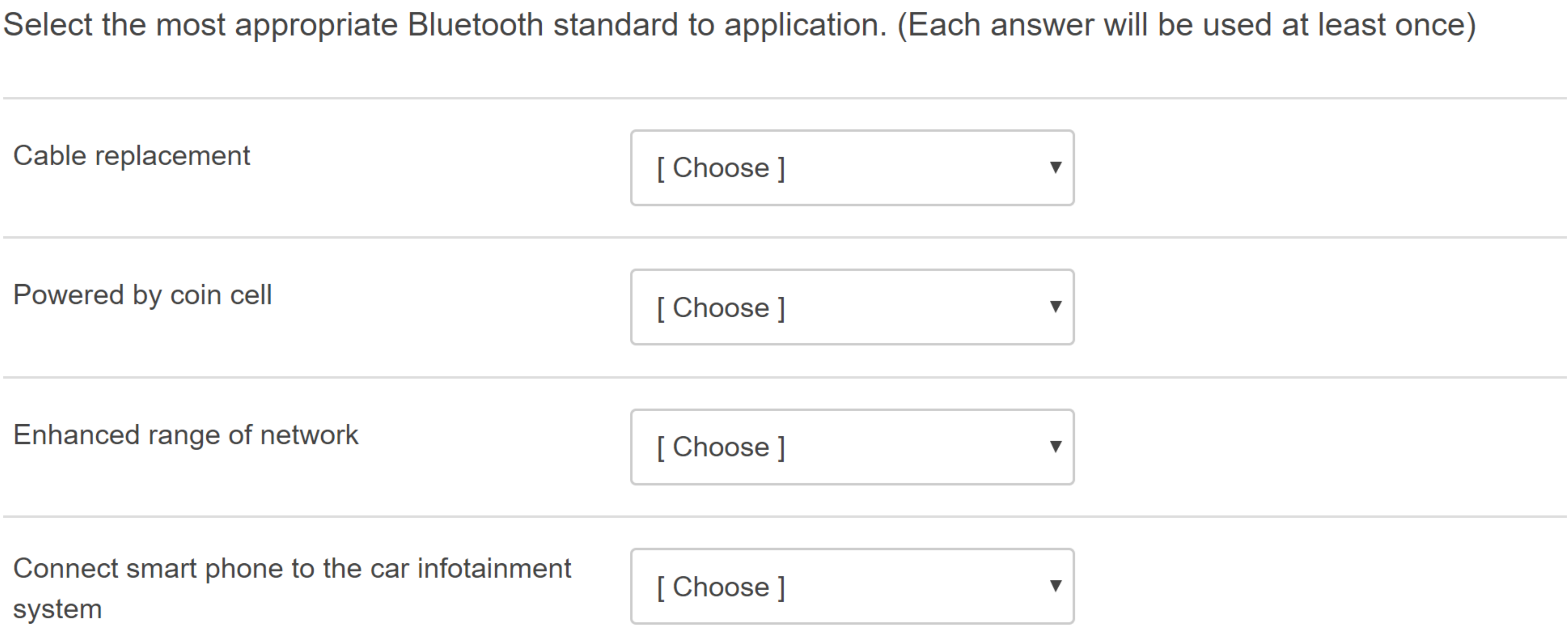
Quiz 4 review



Match the security threat with how Bluetooth Mesh protects against it.

Replay attacks	[Choose] ▼
Man-in-the-middle attacks	[Choose] ▼
Trash-can attacks	[Choose] ▼

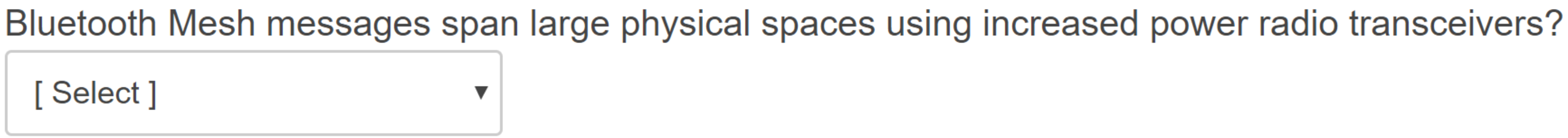
Quiz 4 review



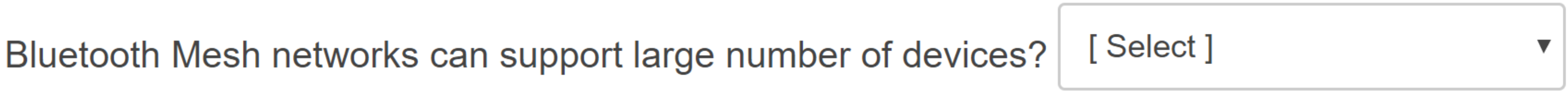
Select the most appropriate Bluetooth standard to application. (Each answer will be used at least once)

Cable replacement	[Choose] ▾
Powered by coin cell	[Choose] ▾
Enhanced range of network	[Choose] ▾
Connect smart phone to the car infotainment system	[Choose] ▾

Quiz 4 review

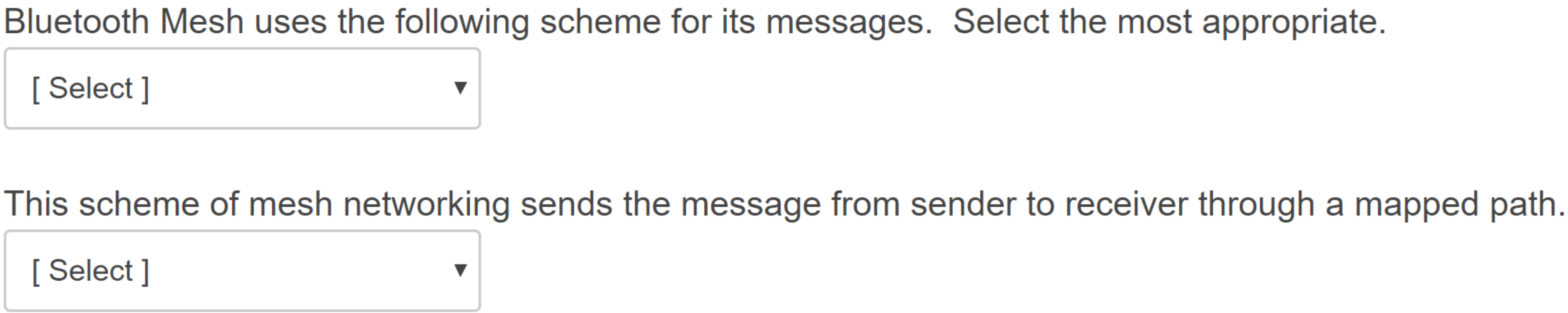


Bluetooth Mesh messages span large physical spaces using increased power radio transceivers?



Bluetooth Mesh networks can support large number of devices?

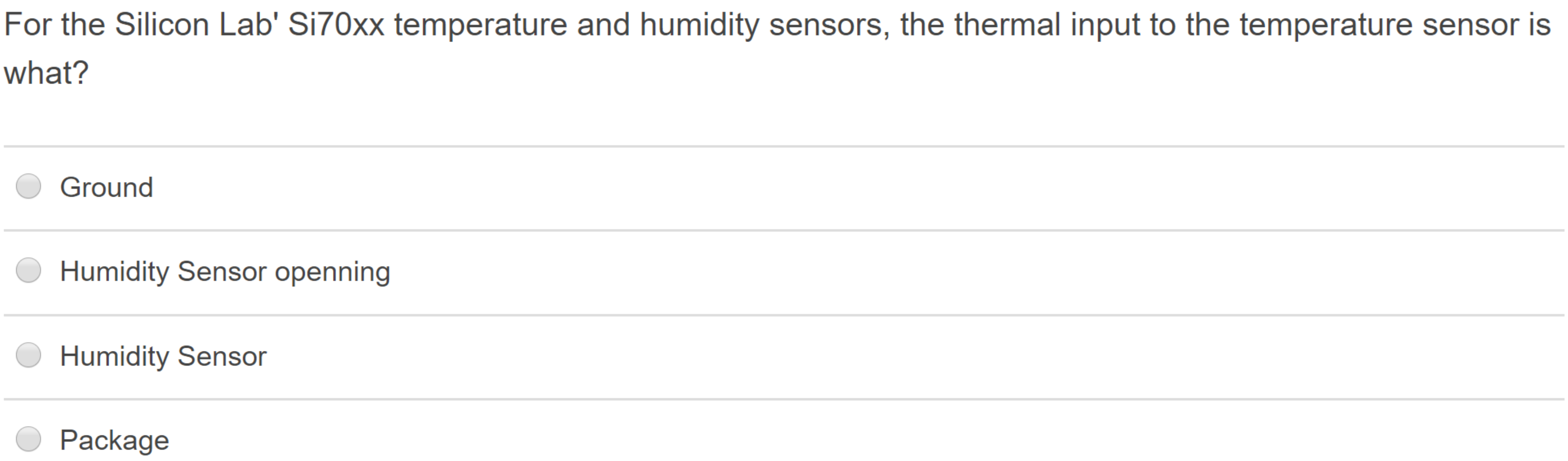
Quiz 4 review



Bluetooth Mesh uses the following scheme for its messages. Select the most appropriate.

This scheme of mesh networking sends the message from sender to receiver through a mapped path.

Quiz 4 review



For the Silicon Lab' Si70xx temperature and humidity sensors, the thermal input to the temperature sensor is what?

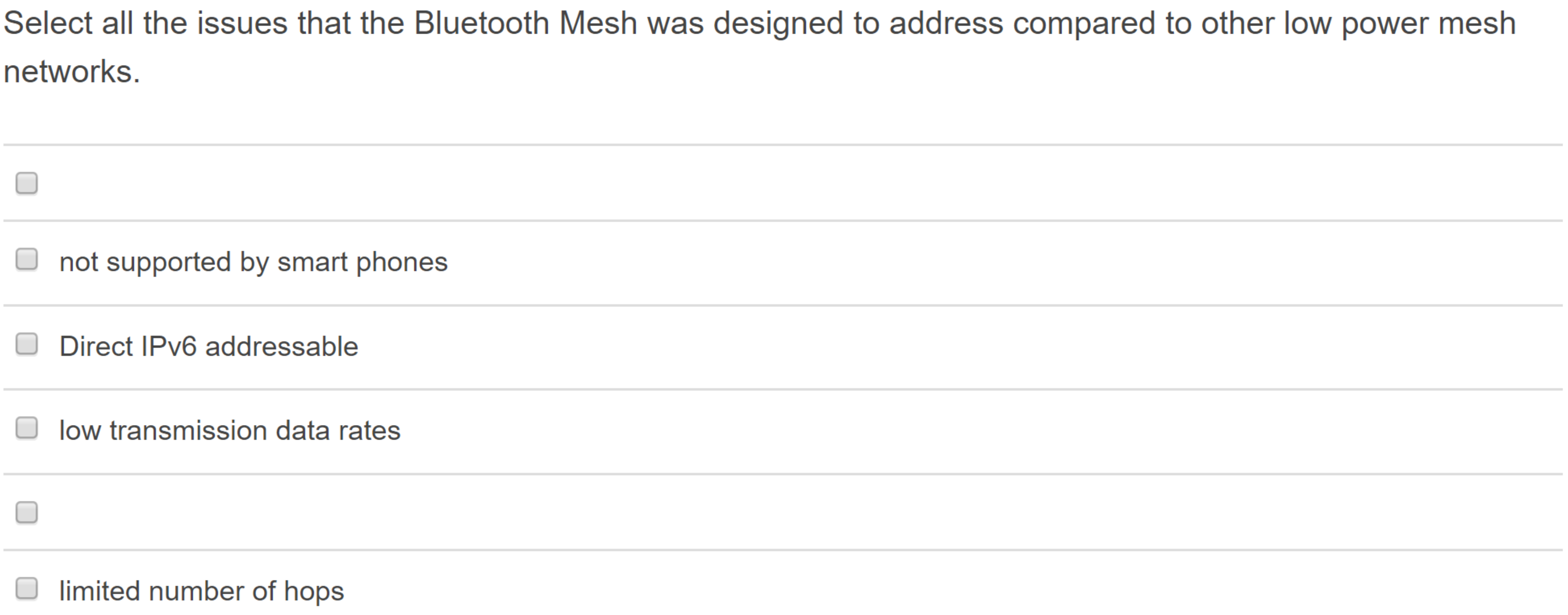
○ Ground

○ Humidity Sensor openning

○ Humidity Sensor

○ Package

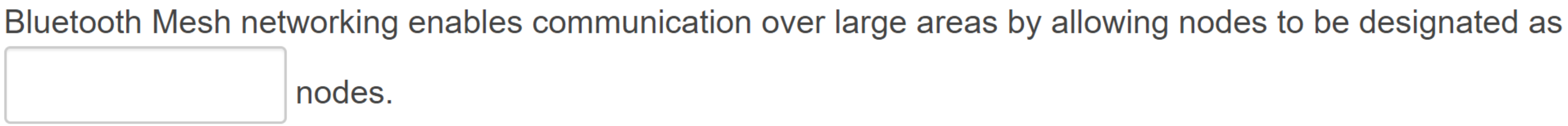
Quiz 4 review



Select all the issues that the Bluetooth Mesh was designed to address compared to other low power mesh networks.

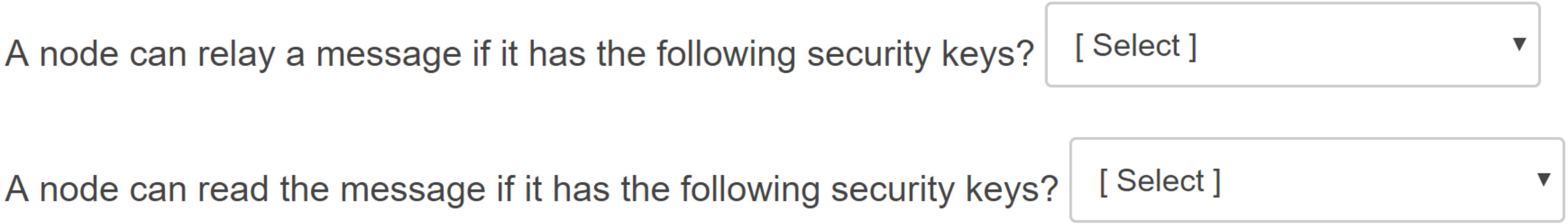
- □
- □ not supported by smart phones
- □ Direct IPv6 addressable
- □ low transmission data rates
- □
- □ limited number of hops

Quiz 4 review



Bluetooth Mesh networking enables communication over large areas by allowing nodes to be designated as □ nodes.

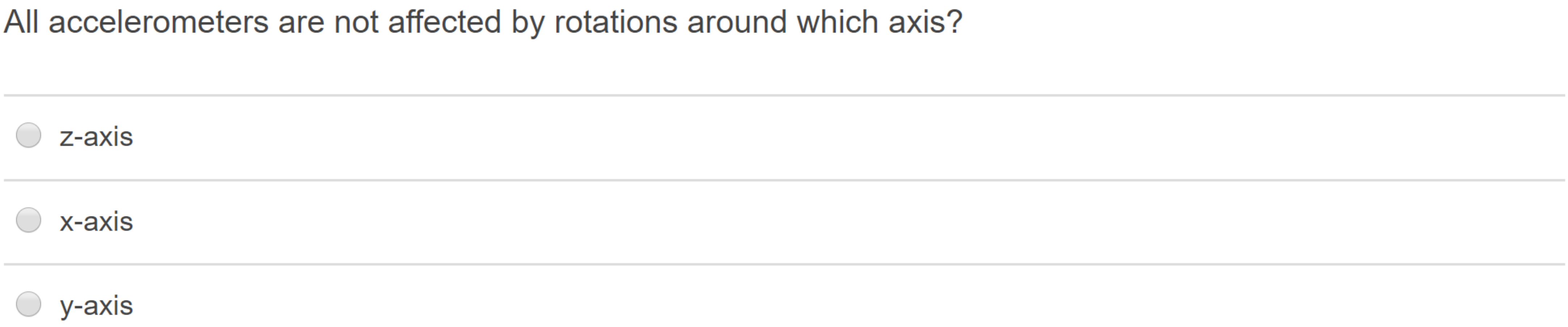
Quiz 4 review



A node can relay a message if it has the following security keys? [Select] ▾

A node can read the message if it has the following security keys? [Select] ▾

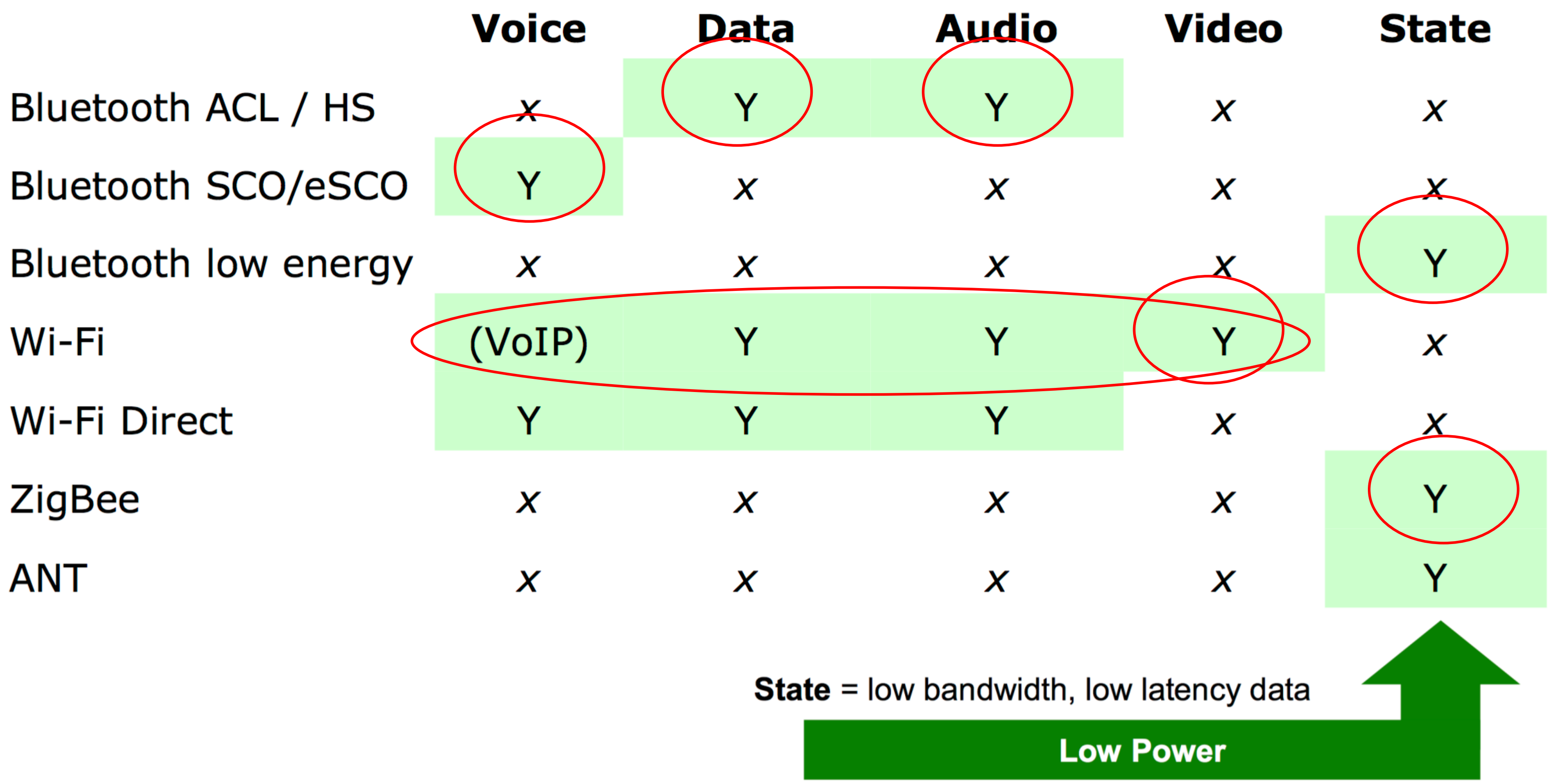
Quiz 4 review



All accelerometers are not affected by rotations around which axis?

- ○ z-axis
- ○ x-axis
- ○ y-axis

Bluetooth Low Energy / Smart



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

State = low bandwidth, low latency data

CSR: Bluetooth 4.0 Low Energy
http://chapters.comsoc.org/vancouver/BTLER3.pdf

Bluetooth Low Energy / Smart

- What is traditional Bluetooth Classic used for?
  - Mobile phones, including ‘smart phones’
  - Wireless controllers for video games
  - Voice headsets and “Car kits”
  - Stereo speakers
  - PCs
  - M2M applications
    - credit card readers
    - industrial automation

Think of replacing wires

- Bluetooth Classic is mainly or more commonly used for Human I/O applications!

CSR: Bluetooth 4.0 Low Energy
http://chapters.comsoc.org/vancouver/BTLER3.pdf

Bluetooth Low Energy / Smart

- Bluetooth Classic energy usage?
  - Bluetooth Classic is *connection oriented*
  - When a device is connected, a link, "pseudo wire," 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 Bluetooth Classic 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

CSR: Bluetooth 4.0 Low Energy
http://chapters.comsoc.org/vancouver/BTLER3.pdf

Bluetooth BLE - What is Bluetooth Low Energy?

- What are some of the goals of this new radio, new protocol stack, new profile architecture?
- It’s designed to run from coin cells
- It is a radio standard enabling the Internet of Things
- Features:
  - Mostly new PHY; some parts derived from the Basic Rate (BR) radio
  - New advertising mechanism, for ease of discovery & connection
  - Asynchronous connection-less MAC: used for low latency, fast transactions (e.g. 3ms from start to finish)
  - New Generic Attribute Profile to simplify devices and the software that uses them.
  - Asynchronous Client / Server architecture
- Designed to be LOWEST cost and EASY to implement

CSR: Bluetooth 4.0 Low Energy
http://chapters.comsoc.org/vancouver/BTLER3.pdf

BLE - fact sheet

Range:	~ 150 meters open field
Output Power:	~ 10mW (10dBm)
Max Current:	~ 15mA
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

What specification commonly found in communications protocols or standards that is missing?

Specification

Implementation specific

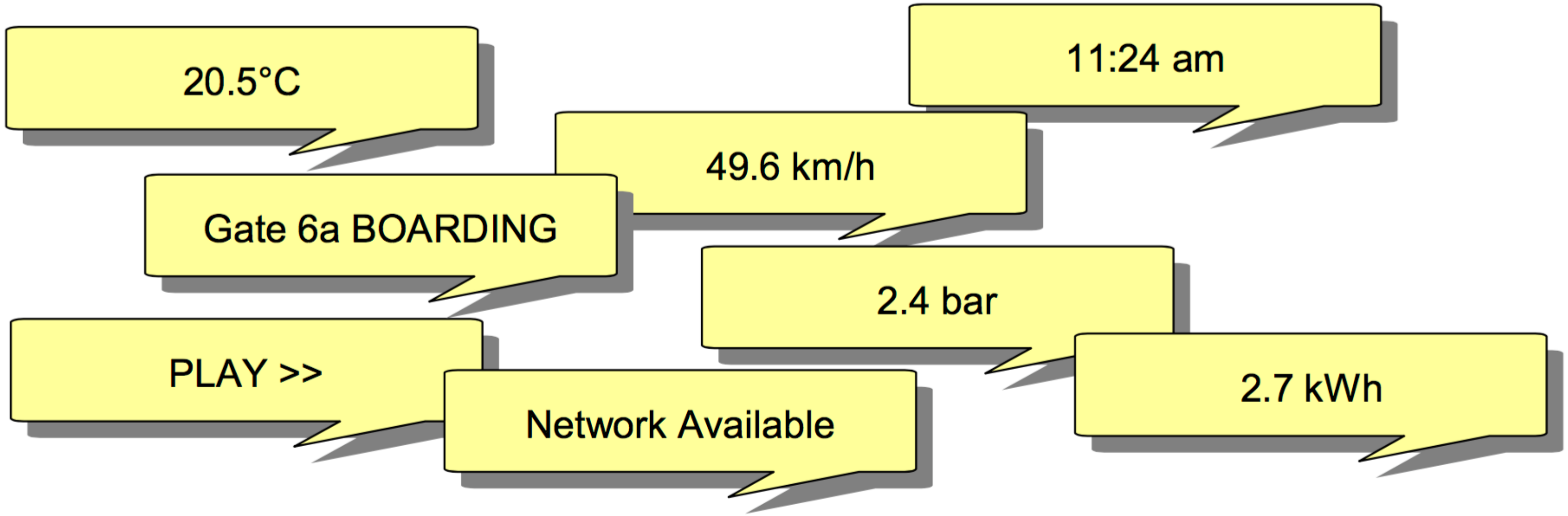
CSR: Bluetooth 4.0 Low Energy
http://chapters.comsoc.org/vancouver/BTLER3.pdf

BLE – fact sheet

- Data through put is missing
  - Data throughput is not a meaningful parameter for BLE
  - It does not support streaming
  - It has a data rate of 1Mbps, but is not optimized for file transfer.
- What type of data is BLE designed to transmit?
  - It is designed for sending small chunks of data (exposing state).

CSR: Bluetooth 4.0 Low Energy
http://chapters.comsoc.org/vancouver/BTLER3.pdf

BLE – Exposing state



- It’s good at small, discrete data transfers
- Data can be triggered by local events
- Data can be read at any time by a client
- Interface model is very simple (GATT)
- Not targeted for Human I/O

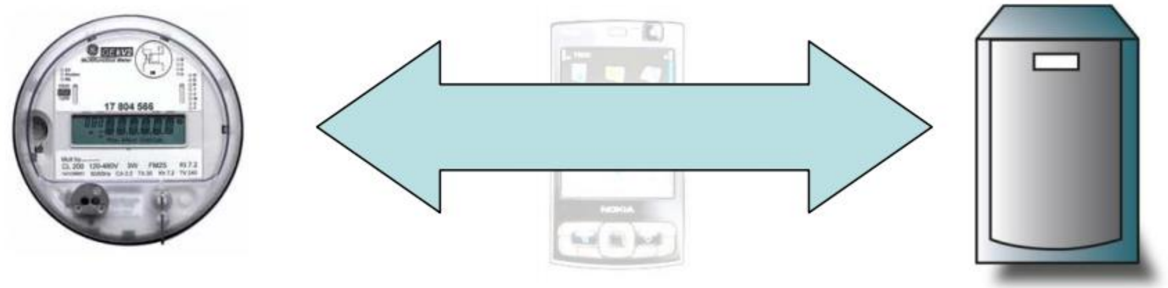
These examples do not include what type of common I/O devices. What are they?

CSR: Bluetooth 4.0 Low Energy
http://chapters.comsoc.org/vancouver/BTLER3.pdf

Bluetooth Low Energy is about ~~generic~~ gateways

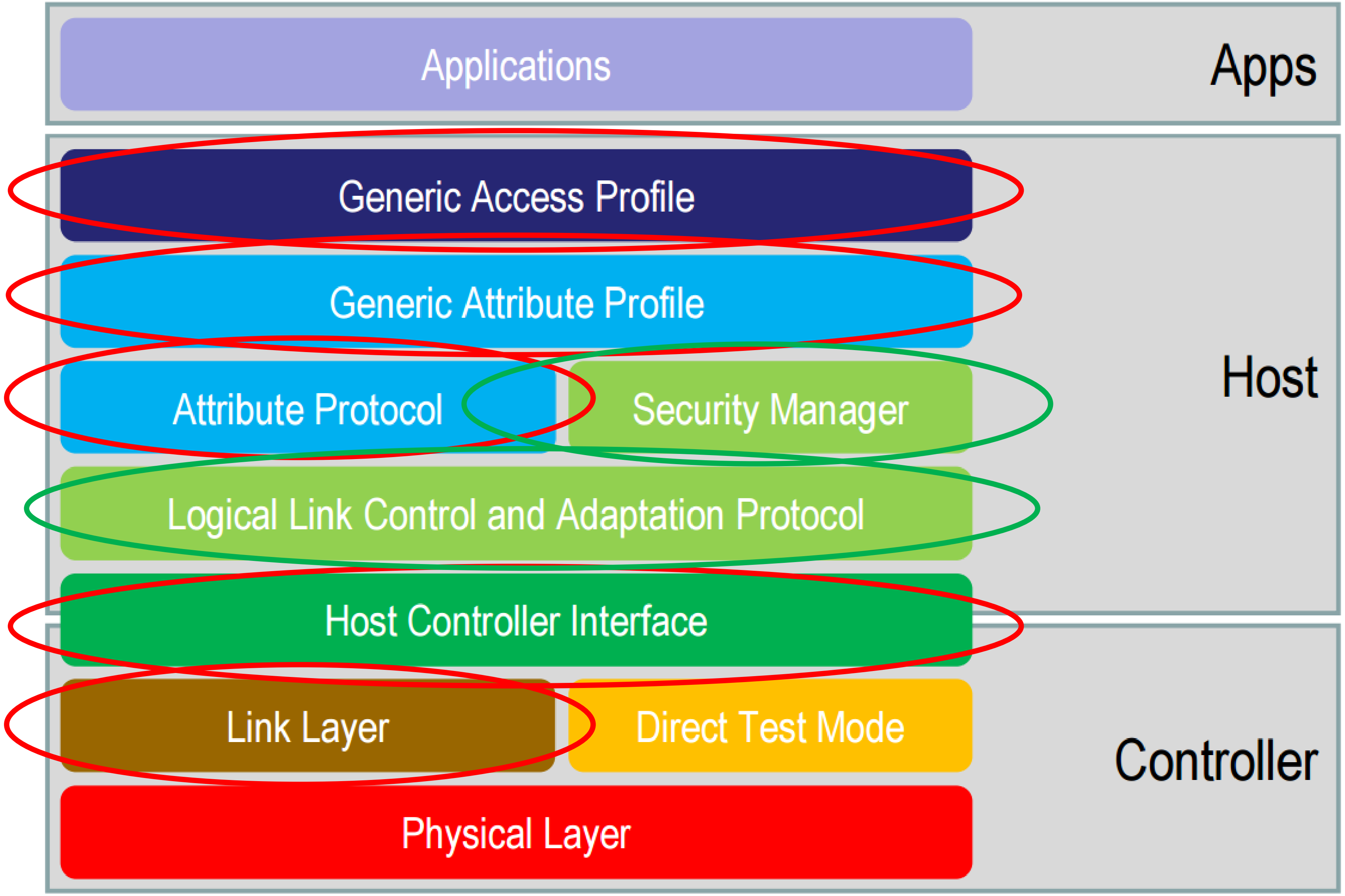
Currently, hardware or vendor specific

- Devices that support Bluetooth low energy Gateway functionality provide a transparent pipe from a device to an IP address
- Middleware at the IP address can access the device directly as if it were a collector talking to it locally
- The Gateway device plays no part other than in acting as a pipe



CSR: Bluetooth 4.0 Low Energy
http://chapters.comsoc.org/vancouver/BTLER3.pdf

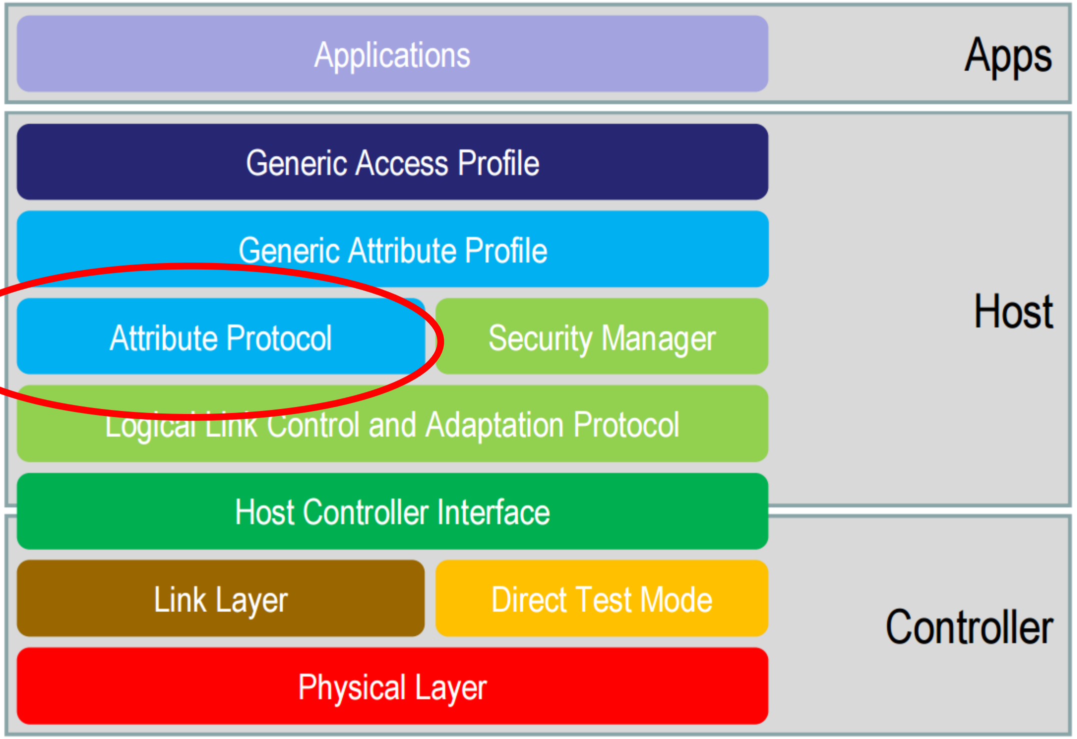
BLE: Stack



CSR: Bluetooth 4.0 Low Energy
http://chapters.comsoc.org/vancouver/BTLER3.pdf

BLE: Attribute Protocol

- Only one protocol which is used for name discovery, service discovery, and for reading and writing information required to implement a given use case
- Defines a set of rules for accessing data on a peer device
  - The data is stored on an attribute server in "attributes" that an attribute client can read and write
  - The client sends requests to the server, and the server responds with response messages



Bluetooth 4.0 Low Energy
http://chapters.comsoc.org/vancouver/BTLER3.pdf
Bluetooth Low Energy: The Developer's Handbook By Robin Heydon

BLE: The Attribute Protocol

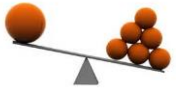
- What types of BLE message are there (six types)?
  - Requests sent from client to the server
  - Responses sent from the server to the client in reply to request
  - Commands sent from the client to the server that have no response
  - Notifications sent from the server to the client that have no confirmation
  - Indications sent from the server to the client
  - Confirmations sent from the client to the server in reply to an indication
- Who can initiate communications?
  - Communications can be initiated by both the client and the server

BLE: The Attribute Protocol

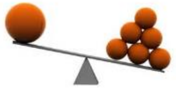
- Attributes are addressed, labeled bits of data
  - Each attribute has a unique handle that identifies that attribute
  - Type that identifies the data stored in the attribute
  - And a value
- For example, an attribute with type Temperature that has a value of 20.5C could be contained within an attribute with the handle 0x01CE
- The Attribute Protocol does not define any attribute types, although it does define that some attributes can be grouped, and their groups can be discovered via the Attribute Protocol
- The Attribute Protocol also defines that some attributes have permissions:
  - To allow a client to read or write an attribute's value
  - Or, to only allow access to the value of the attribute if the client has been authenticated itself or has been authorized by the server
- The Attribute Protocol is mostly stateless
  - Each individual transaction such as a read request and read response does not cause state to be saved on the server
  - The one exception is the prepare and execute write request. These store a set of values that are to be written in the server and then executed all in sequence in a single transaction

BLE: Asymmetric Design

- A major philosophy of the Bluetooth Low Energy Architecture



  - Devices with smaller energy sources be given less to do
  - Conversely, devices with larger energy sources be given more to do
- A fundamental assumption is the most resource-constraint device will be the one to which all others are optimized



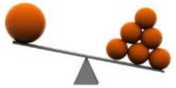
  - Advertising is less energy consuming than scanning
  - A slave has less energy than a master
    - A master has to manage the piconet timing, the adaptive frequency hopping set, encryption, and many other complex procedures

BLE: Asymmetric Design

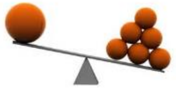
- At the Generic Attribute Protocol Layer, the two type of devices are:
    - Client
        - Determines what data the server has and how to use it
        - The client sends request to the server for data
    - Server
        - The Server holds data
        - Similar to the slave at the Link Layer, the server just does what it is told
- The security architecture works on a key distribution scheme by which the slave device gives a key to the master device to remember
    - The burden is on the master to remember the bonding information, not the slave
- This implies the most resource-constraint device will want to be the advertisers, slaves, and servers
- Conversely, the devices with the most resources will be the scanners, masters, and clients

BLE: Asymmetric design

- Client-Server Architecture:
  - An IP address could have been specified to be given to each BLE device, but the simplest of IP stack takes more memory and energy than is desired on resourced constrained devices



    - The most resource-constraint device will be the one to which all others are optimized
  - The client-server architecture makes possible smart gateways to connect the very efficient low-energy slaves to the internet

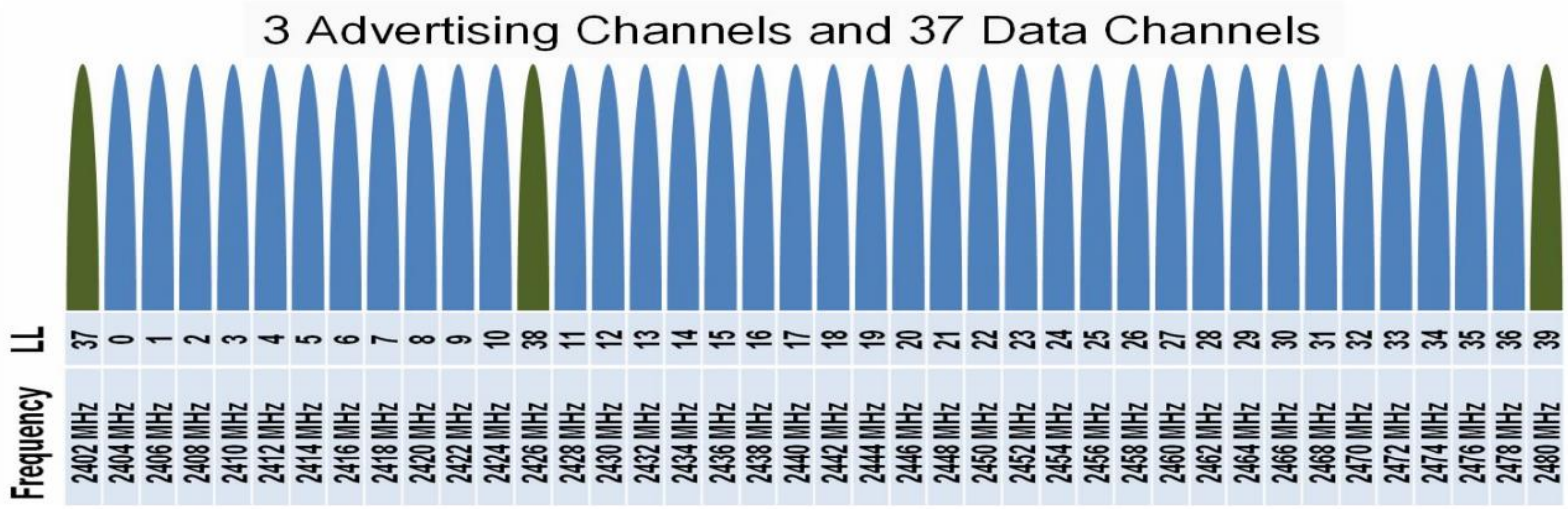


    - The client, the more resource abundant device, can connect and handle the IP protocol
    - While, the server is just the repository of data
  - Full Internet security can be provided between the client to the gateway where the gateway performs access control, firewall, and authorization of the client before granting access to anything beyond the gateway
    - These gateways, routers and access points, are proven technologies used today

BLE: The Radio

- Why would the advertising channels be spread out over the frequency spectrum?
- Why are the frequency channels not ordered from 0 to the left to 39 to the right?

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

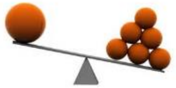


LL	Frequency
37	2402 MHz
0	2404 MHz
1	2406 MHz
2	2408 MHz
3	2410 MHz
4	2412 MHz
5	2414 MHz
6	2416 MHz
7	2418 MHz
8	2420 MHz
9	2422 MHz
10	2424 MHz
38	2426 MHz
11	2428 MHz
12	2430 MHz
13	2432 MHz
14	2434 MHz
15	2436 MHz
16	2438 MHz
17	2440 MHz
18	2442 MHz
19	2444 MHz
20	2446 MHz
21	2448 MHz
22	2450 MHz
23	2452 MHz
24	2454 MHz
25	2456 MHz
26	2458 MHz
27	2460 MHz
28	2462 MHz
29	2464 MHz
30	2466 MHz
31	2468 MHz
32	2470 MHz
33	2472 MHz
34	2474 MHz
35	2476 MHz
36	2478 MHz
39	2480 MHz

CSR: Bluetooth 4.0 Low Energy
http://chapters.comsoc.org/vancouver/BTLER3.pdf

BLE: The Radio

- Adaptive Frequency Hopping (AFH):
  - A technology where only a subset of available frequencies are used
  - Robust by detecting sources of interference quickly, and adapting to avoid them in the future
  - Quickly recovers from dropped packets caused by interference quickly by hopping to a new channel
- Short Range and Low Power:
  - Transmit power should be kept as low as possible
  - Receive sensitivity should be relatively high to pick up the transmitted signals
  - Transmit power and Receive amplification should match the device resources appropriately
    - Dual-Mode devices with larger batteries can transmit at a higher power
    - Dual-Mode devices with larger batteries can increase the gain of the receiver



BLE: Adaptive Frequency Hopping

Another representations of the BLE Advertising and Data Channels

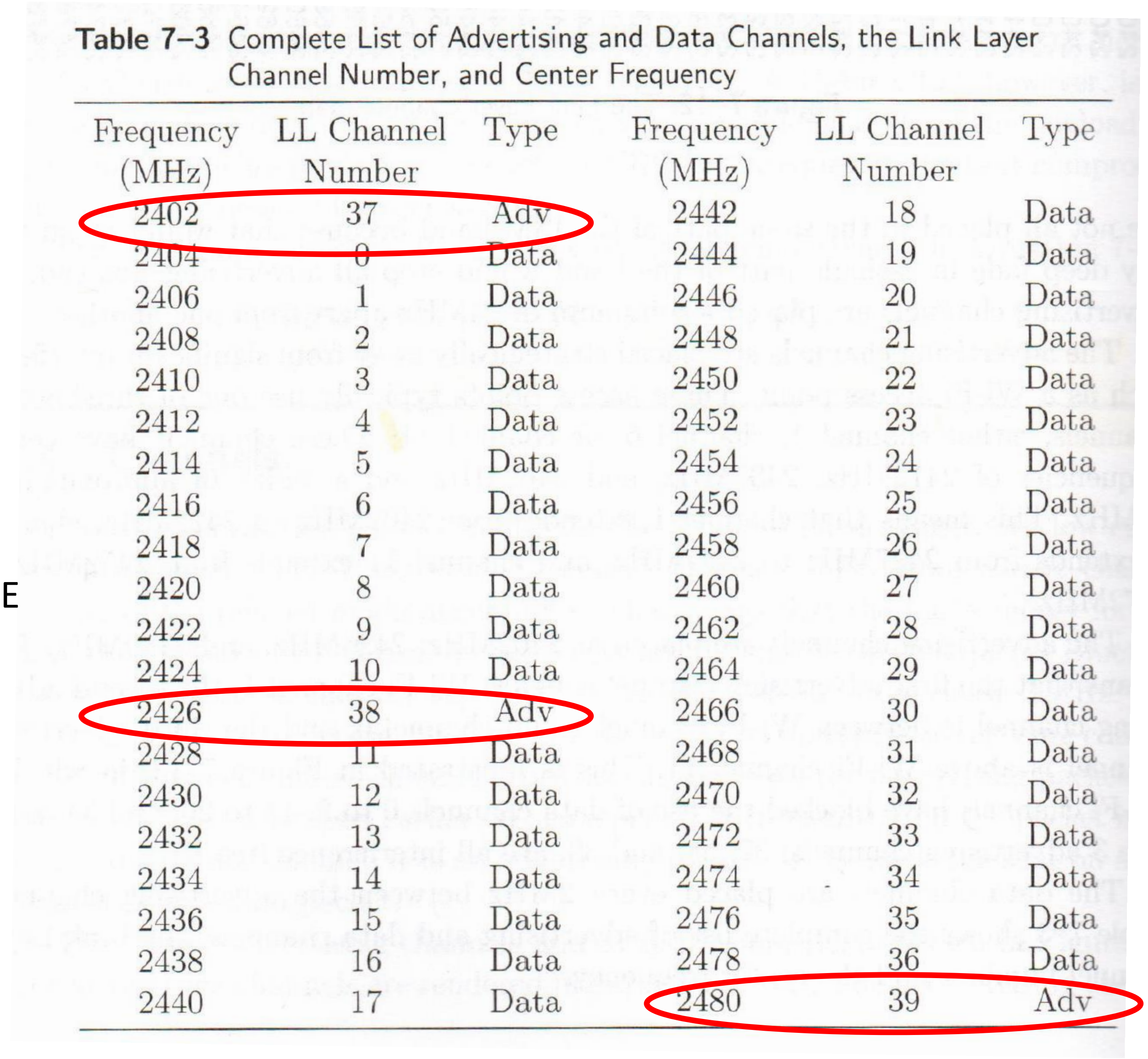


Table 7–3 Complete List of Advertising and Data Channels, the Link Layer Channel Number, and Center Frequency

Frequency (MHz)	LL Channel Number	Type	Frequency (MHz)	LL Channel Number	Type
2402	37	Adv	2442	18	Data
2404	0	Data	2444	19	Data
2406	1	Data	2446	20	Data
2408	2	Data	2448	21	Data
2410	3	Data	2450	22	Data
2412	4	Data	2452	23	Data
2414	5	Data	2454	24	Data
2416	6	Data	2456	25	Data
2418	7	Data	2458	26	Data
2420	8	Data	2460	27	Data
2422	9	Data	2462	28	Data
2424	10	Data	2464	29	Data
2426	38	Adv	2466	30	Data
2428	11	Data	2468	31	Data
2430	12	Data	2470	32	Data
2432	13	Data	2472	33	Data
2434	14	Data	2474	34	Data
2436	15	Data	2476	35	Data
2438	16	Data	2478	36	Data
2440	17	Data	2480	39	Adv

Bluetooth Low Energy: The Developer's Handbook
By Robin Heydon

BLE: Adaptive Frequency Hopping Managing Interference and Coexistence

- WiFi access point typically use one of three 802.11 channels
- BLE Advertising channels are strategically placed to not be interfered by these WiFi channels (1, 6, and 11)
- Three advertising channels are designed into the BLE specification to provide robustness
- Without an effective advertising channel, BLE would not be an effective wireless network

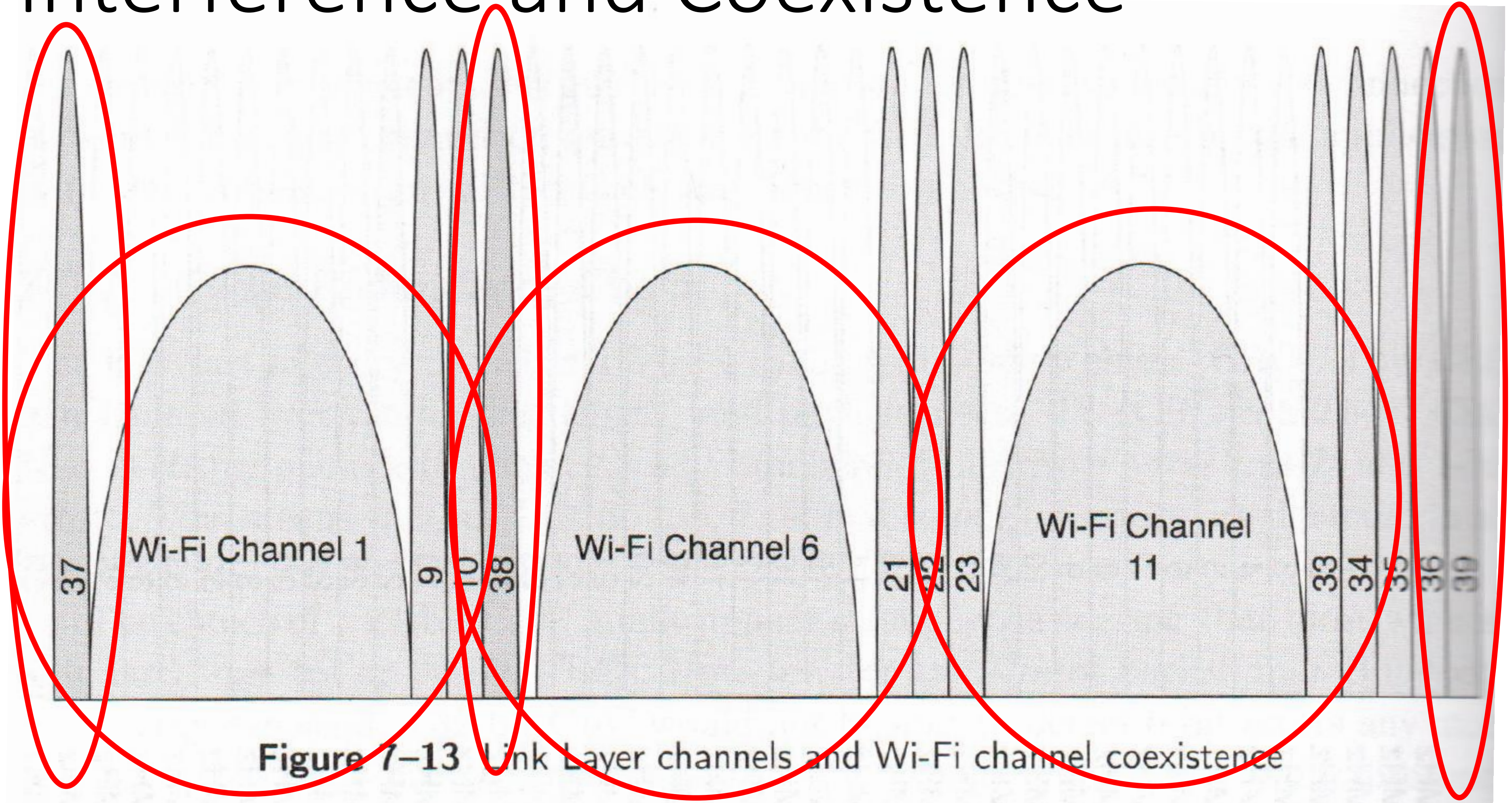


Figure 7–13 Link Layer channels and Wi-Fi channel coexistence

BLE: Frequency Hopping

- When in data connection, a frequency-hopping algorithm is used. Since there are 37 data channels which is a prime number, the hopping sequence is very simple
  - f_{n+1} = (f_n+hop) mod 37
  - The hop value can range from 5 to 16
  - This will result in every frequency be used with equal priority
- Notice, that the advertising channel numbers are greater than 37, so they will never be used in the data connection hop sequence

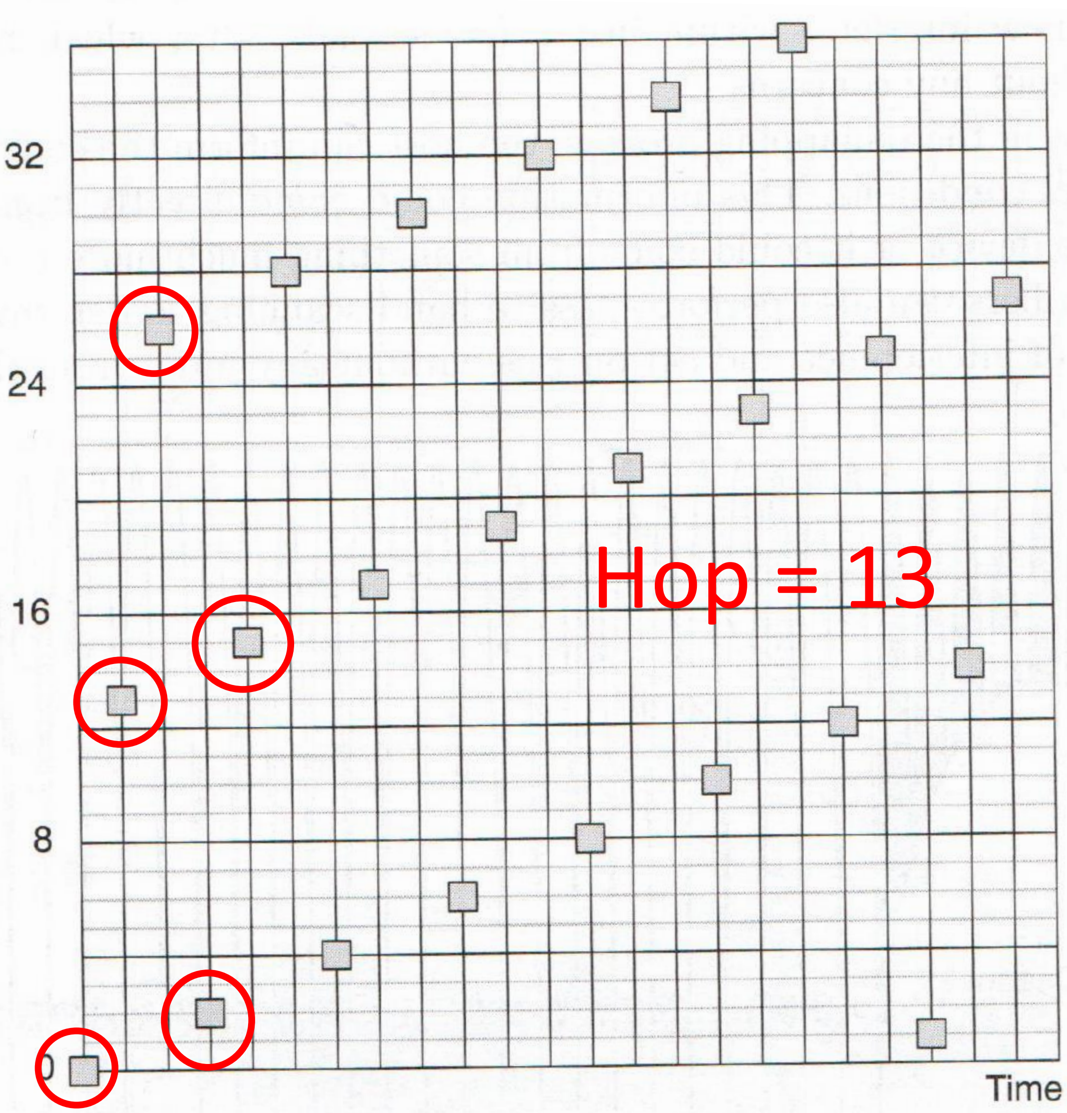


Figure 7–14 Frequency hopping of data channels over time

Bluetooth Low Energy: The Developer's Handbook
By Robin Heydon

BLE: Adaptive Frequency Hopping

- Adaptive frequency hopping makes it possible for a given packet to be remapped from a known bad channel to a know good channel
- In the example to the right, the data channels 0-8 are known bad channels due to the WiFi Channel 1 interference
- Channels 0-8 should be remapped to channels 9-36

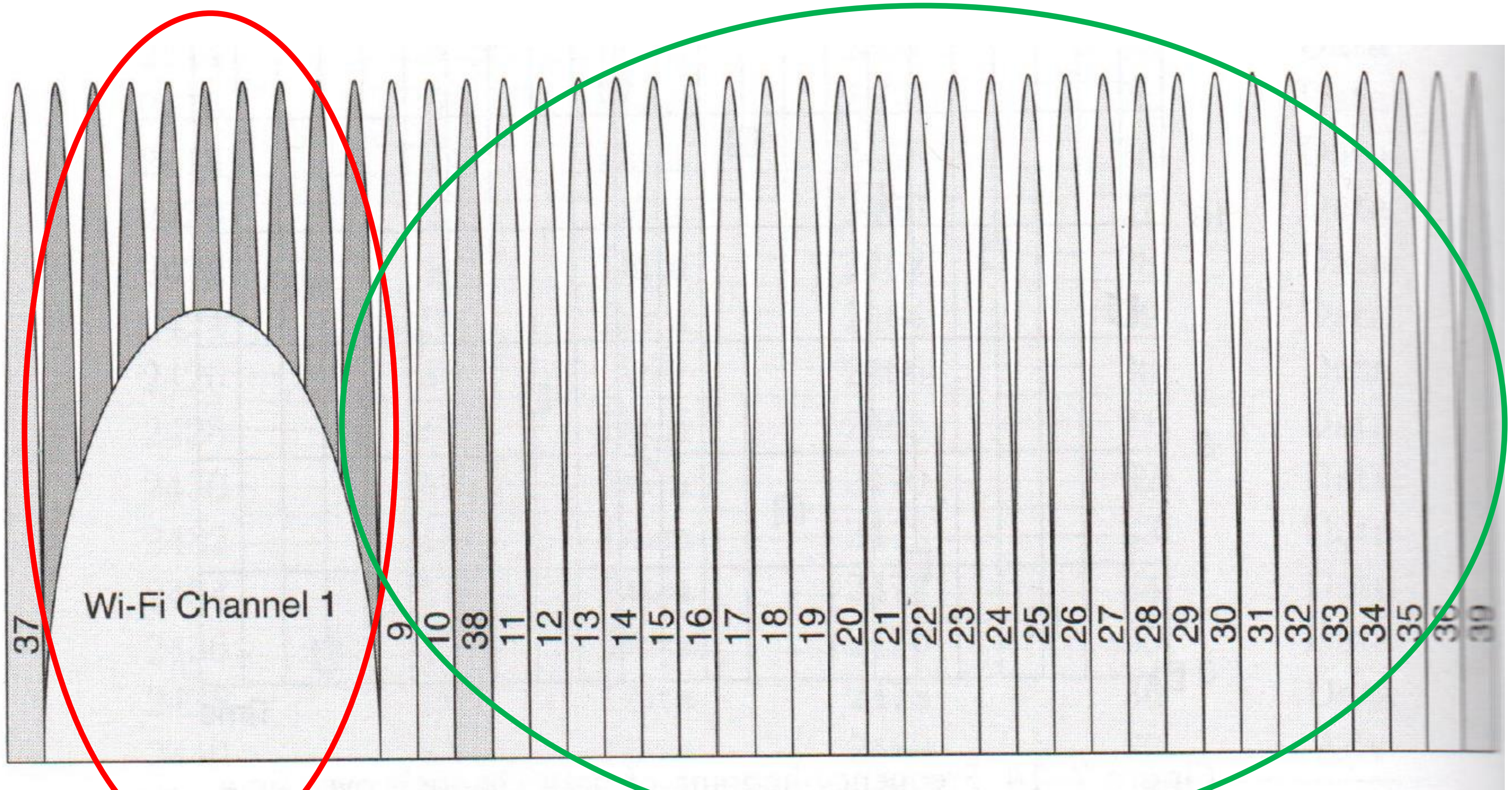


Figure 7–15 Link Layer adaptive frequency-hopping bad channels with Wi-Fi channel 1

Bluetooth Low Energy: The Developer's Handbook
By Robin Heydon

BLE: Adaptive Frequency Hopping

Hop = 13

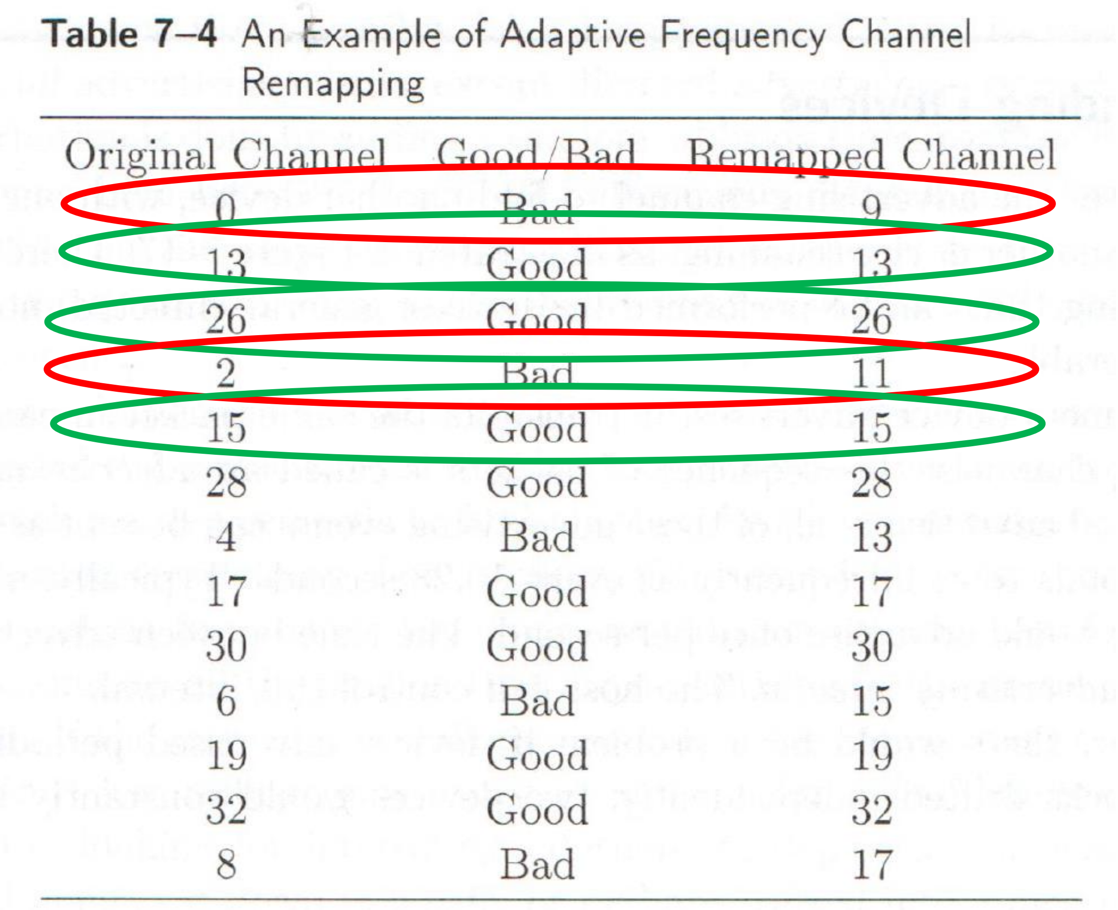


Table 7–4 An Example of Adaptive Frequency Channel Remapping

Original Channel	Good/Bad	Remapped Channel
0	Bad	9
13	Good	13
26	Good	26
2	Bad	11
15	Good	15
28	Good	28
4	Bad	13
17	Good	17
30	Good	30
6	Bad	15
19	Good	19
32	Good	32
8	Bad	17

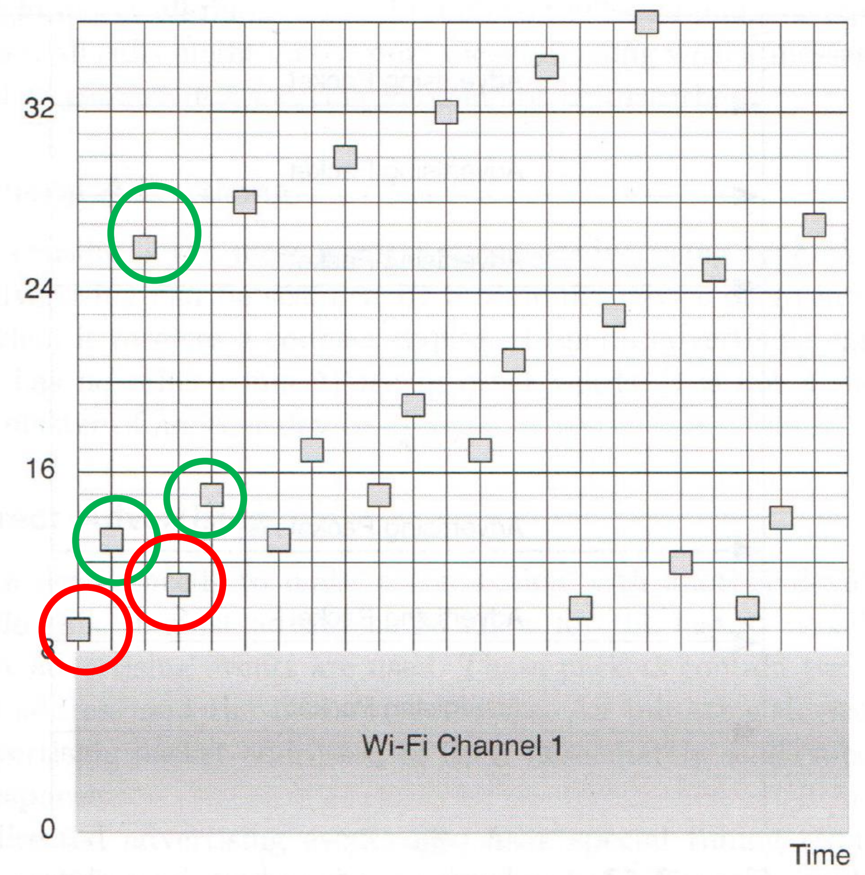


Figure 7–16 Adaptive frequency-hopping remapping

BLE: Time is Energy

Energy = Power x Time

- Optimizing a number of important and repetitive action is a must
  - Discovering devices
  - Connecting to devices
  - Sending data

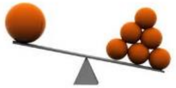
➢Reducing the time for these activities

  ➢Reduces the energy consumed for these activities

    ➢Lengthening the battery life

BLE: Time is Energy (Advertising)

- Advertising to be discovered requires a device to transmit a very short message 3 times per second and listen immediately afterwards if it wants to connect
- Three transmits are done, one per advertising frequency channel, for robustness.
  - If the advertising channels was just one frequency band, if that frequency became blocked or a lot of interference, devices would not be able to connect
  - If the number of channels was much higher than 3, such as 16, then the device would spend more time and energy by having its radio on 5x+
- Searching for a device that is transmitting requires the radio to be on a long period of time which requires more energy than the advertising device
  - Thus, the device that typically has more resources, larger battery, is listening and will become the master
  - The advertiser will normally be the smaller device with the smaller battery and become the slave

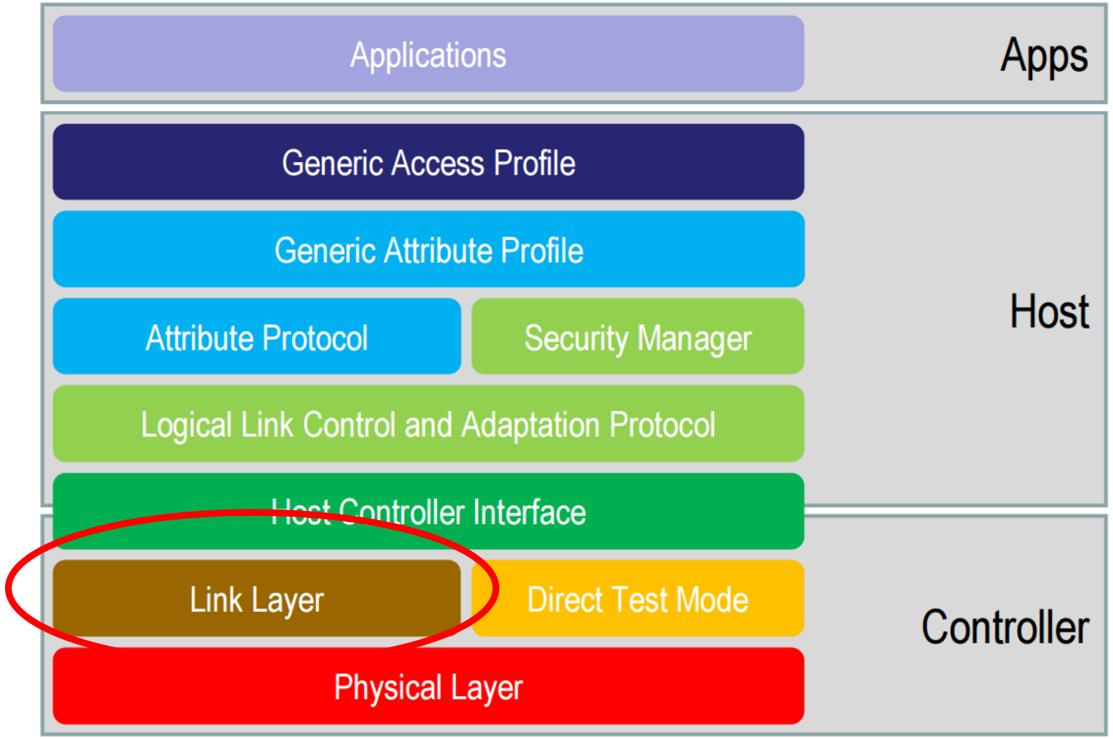


BLE: Time is Energy (Packet size)

- What are three good reasons for short radio packets?
  - Efficient encoding allows short packets to transmit as much as larger packets faster using less energy
  - Restricting the radio devices to only use short packets removes the requirement of constantly recalibrating the radio within the controller due to internally heating while the radio is operational
  - Short packets reduces peak power consumption which enables more energy to be taken out of the battery

BLE: Link Layer

- Two types of Link Layer Channels:
  - Advertising channels
    - Broadcast data
    - Advertise that they are connectable and discoverable
    - Scan
    - Initiate connections
  - Data channels
    - Only used once a connection has been established
    - And, only when data needs to flow



CSR: Bluetooth 4.0 Low Energy
http://chapters.comsoc.org/vancouver/BTLER3.pdf
Bluetooth Low Energy: The Developer's Handbook By Robin Heydon

BLE: Link Layer packet structure

- Basic packet structure is the same for both advertising channels and data channels
  - A minimum of 80 bits of addressing, header, and check information for every packet
- The packets are optimized to increase their robustness by using an 8-bit preamble that is sufficiently large to allow the receiver to synchronize bit timing and set the radio's automatic gain control
- A 32-bit access address that is fixed for advertising packets, but can be completely random and private for data packets
- An 8-bit header packet to describe the contents of the packet
- An 8-bit length field to describe the payload length
- 0-296 bit payload
- And, a 24-bit cyclic redundancy check (CRC) value to ensure that there are not bit errors in the received packet

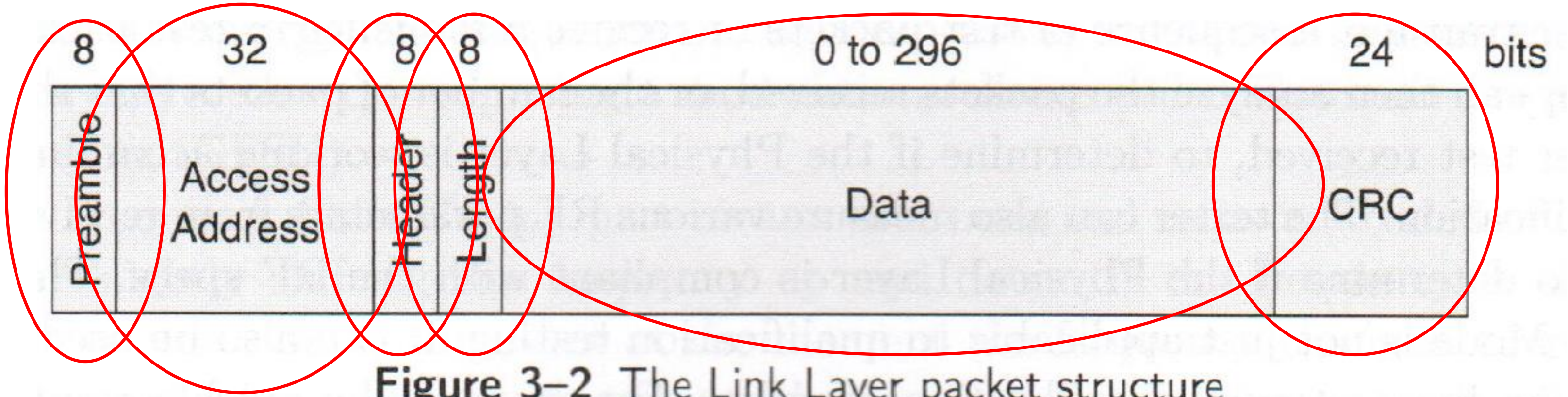
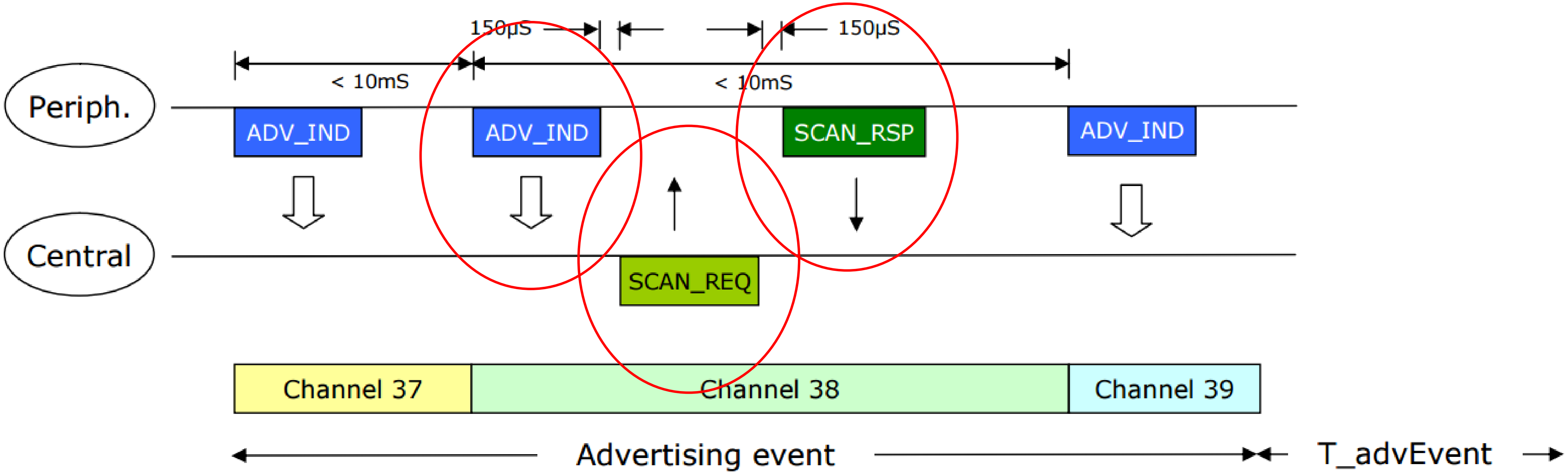


Figure 3–2 The Link Layer packet structure

Bluetooth Low Energy: The Developer's Handbook
By Robin Heydon

BLE: 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

CSR: Bluetooth 4.0 Low Energy
http://chapters.comsoc.org/vancouver/BTLER3.pdf