Physical and Link Layers Protocols- IEEE 802.15.4e/g

- The IEEE frequently makes amendments to the core 802.15.4 specification, before integrating them into the next revision of the core specification.

- When these amendments are made, a lowercase letter is appended. Two such examples of this are 802.15.4e-2012 and 802.15.4g-2012, both of which are especially relevant to the subject of IoT.
  - Both of these amendments were integrated in IEEE 802.15.4-2015 but are often still referred to by their amendment names.
  - IEEE 802.15.4g-2012 is also an amendment to the IEEE 802.15.4-2011 standard, and just like 802.15.4e-2012, it has been fully integrated into the core IEEE 802.15.4-2015 specification.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

Physical and Link Layers Protocols- IEEE 802.15.4e/g

- The focus of IEEE 802.15.4g-2012 as an amendment to the IEEE 802.15.4-2011 is the smart grid or, more specifically, smart utility network communication.
- This technology applies to IoT use cases such as the following:
  - Distribution automation and industrial supervisory control and data acquisition (SCADA) environments for remote monitoring and control
  - Public lighting
  - Environmental wireless sensors in smart cities
  - Electrical vehicle charging stations
  - Smart parking meters
  - Micro grids
  - Renewable energy

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

Physical and Link Layers Protocols- IEEE 802.15.4e/g

- While the IEEE 802.15.4e-2012 amendment is not applicable to the PHY layer, it is pertinent to the MAC layer.

- This amendment enhances the MAC layer through various functions, which may be selectively enabled based on various implementations of the standard.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

Physical and Link Layers Protocols- IEEE 802.15.4e/g

- The 802.15.4e-2012 MAC amendment is quite often paired with the 802.15.4g-2012 PHY.

- The main difference between 802.15.4 and 802.15.4g is the payload size, with 802.15.4g supporting up to 2047 bytes and 802.15.4 supporting only 127 bytes.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

Physical and Link Layers Protocols- IEEE 802.15.4e/g

- IEEE 802.15.4e and 802.15.4g- Physical layer
  - In IEEE 802.15.4g-2012, the original IEEE 802.15.4 maximum payload size of 127 bytes was increased to 2047 bytes.
  - Fragmentation is no longer necessary at Layer 2 when IPv6 packets are transmitted over IEEE 802.15.4g MAC frames.
  - The error protection was improved in IEEE 802.15.4g by evolving the CRC from 16 to 32 bits.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

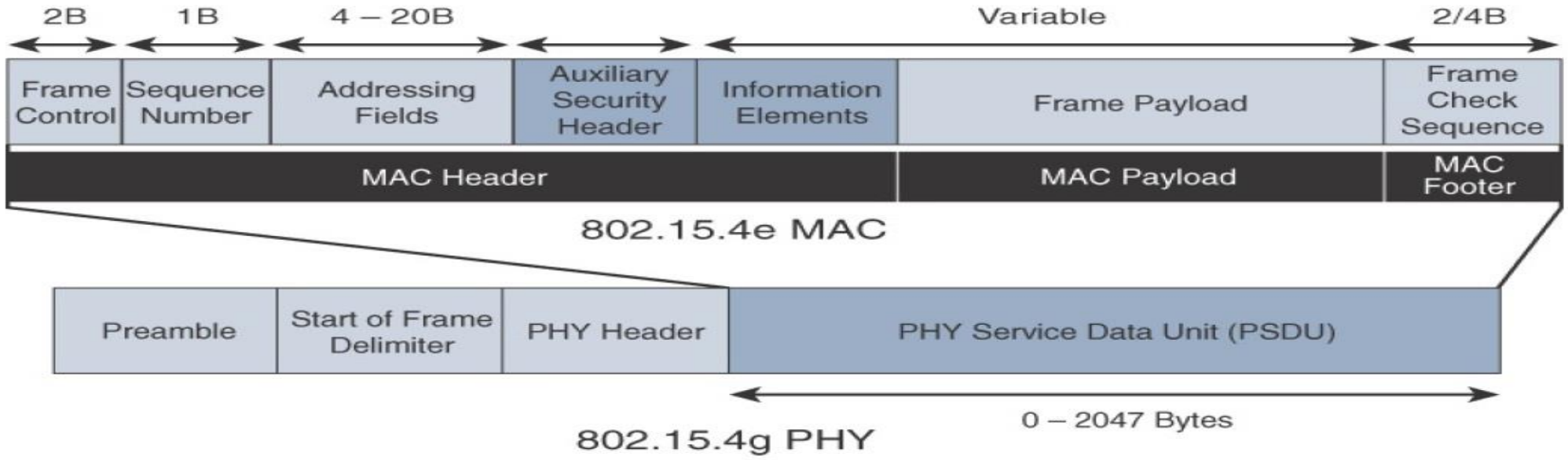
Physical and Link Layers Protocols- IEEE 802.15.4e/g

- IEEE 802.15.4e and 802.15.4g- MAC layer
  - IEEE 802.15.4g/e MAC Frame Format
    - The main difference between 802.15.4 and 802.15.4g frame format is the payload size, with 802.15.4g supporting up to 2047 bytes and 802.15.4 supporting only 127 bytes.
    - The other difference is the presence of the Auxiliary Security Header and Information Elements (IE) field.
      - The Auxiliary Security header provides for the encryption of the data frame.
      - the IE field contains one or more information elements that allow for additional information to be exchanged at the MAC layer.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

Physical and Link Layers Protocols- IEEE 802.15.4e/g

- IEEE 802.15.4e and 802.15.4g- MAC layer
  - IEEE 802.15.4g/e MAC Frame Format



* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

Physical and Link Layers Protocols- IEEE 802.15.4e/g

- IEEE 802.15.4e and 802.15.4g
  - Topology
    - Mesh

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

History of BLE

- Bluetooth LE was originally introduced under the name Wibree by Nokia in 2006

- It was merged into the main Bluetooth standard in 2010, when the Bluetooth Core Specification Version 4.0 was adopted

- iPhone 4S was the first ever commercial device to include BLE

* "Bluetooth Low Energy: An insight", Robert Bosch Centre for Cyber-Physical Systems

Bluetooth Low Energy

- Universal short-range wireless Capability
- 2.4 GHz ISM Band
- Available globally for unlicensed users
- Achievable data-rate of 0.2 Mbit/s
- Used mainly for low-powered devices and IoT to collect sensor data
- Low power requirements, operating for "months or years"
- Small size and low cost
- Compatibility with a large installed base of mobile phones, tablets and computers

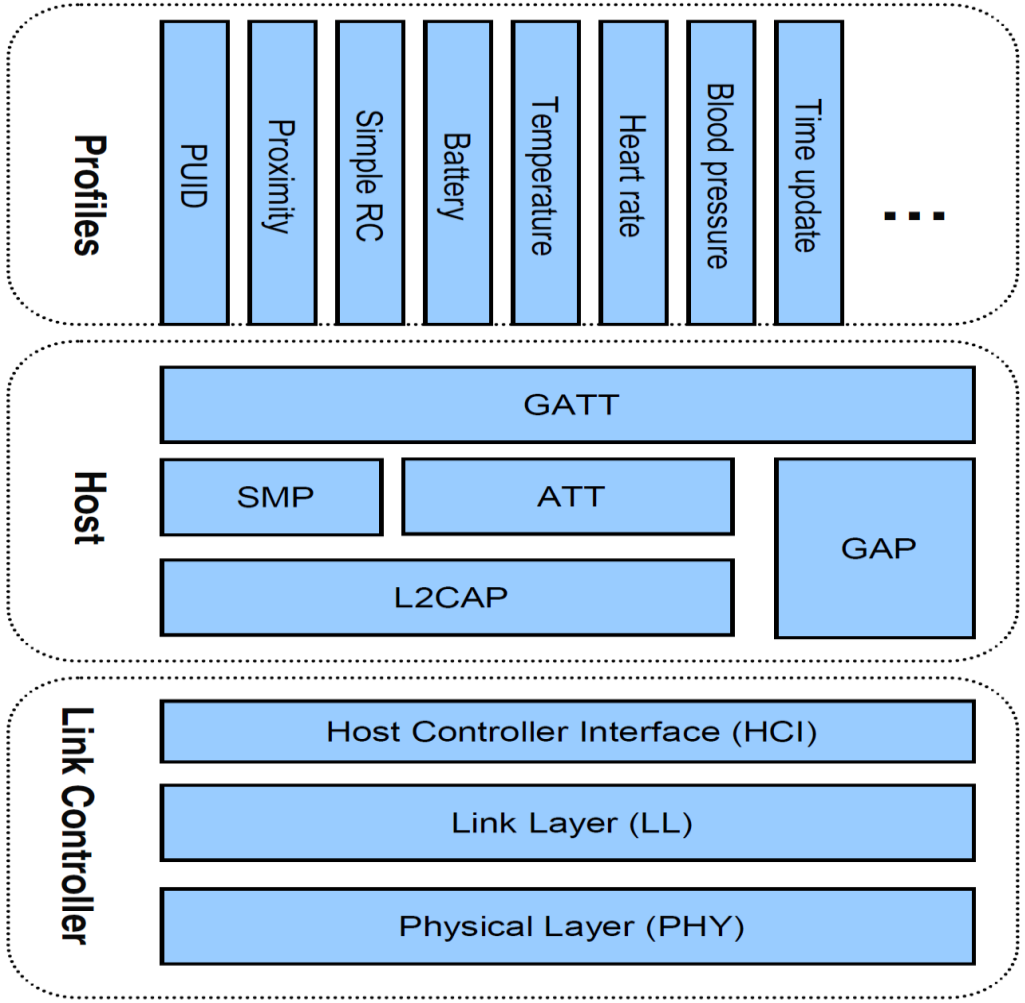
* Bluetooth Low Energy: An insight, Robert Bosch Centre for Cyber-Physical Systems

Physical and Link Layers Protocols- BLE

- Bluetooth Low Energy (BLE)/ Bluetooth Smart
  - BLE has a relatively shorter range and consumes lower energy as compared to competing protocols.
  - The BLE protocol stack is similar to the stack used in classic Bluetooth technology.
  - It has two parts:
    - Controller
      - The physical and link layer are implemented in the controller
      - The controller is typically a SOC (System on Chip) with a radio.
    - Host
      - The functionalities of upper layers are included in the host.

* Internet of Things: Architectures, Protocols, and Applications, Hindawi, 2017

Bluetooth Low Energy System Architecture



* Bluetooth low energy, Nordic semiconductor, 2010

Bluetooth Low Energy

- **Physical layer** – *transmits / receive bits*
- **Link layer** – *packets and control*
- **Logical Link Control and Adaptation Protocol (L2CAP)** – *Link multiplexor*
- **Generic Access Profile (GAP)** – *Discovery and link management*
- **Security Manager Protocol (SMP)** – *Link security*
- **Attribute Protocol (ATT)** – *Protocol for accessing data*
- **Attribute Profile (GATT)** – *Data (attribute) organization*
- **Profiles** – *Application specific protocol for communication between devices*

* Bluetooth low energy, Nordic semiconductor, 2010

Physical and Link Layers Protocols- BLE

- Bluetooth Low Energy (BLE)/ Bluetooth Smart
  - BLE does not support data streaming. Instead, it supports quick transfer of small packets of data (packet size is small) with a data rate of 1Mbps.
  - There are two types of devices in BLE:
    - Master
      - The master acts as a central device that can connect to various slaves.
    - Slave
      - Therefore, to save energy, slaves are by default in sleep mode and wake up periodically to receive packets from the master.

* Internet of Things: Architectures, Protocols, and Applications, Hindawi, 2017

Physical and Link Layers Protocols- BLE

- Bluetooth Low Energy (BLE)/ Bluetooth Smart
  - The differences between BLE and classic Bluetooth:
    - In classic Bluetooth, the connection is on all the time even if no data transfer is going on.
    - The classic Bluetooth supports 79 data channels (1MHz channel bandwidth) and a data rate of 1 million symbols/s
    - BLE supports 40 channels with 2MHz channel bandwidth (double of classic Bluetooth) and 1 million symbols/s data rate.
    - BLE supports low duty cycle requirements as its packet size is small and the time taken to transmit the smallest packet is as small as 80 μs.
    - The BLE protocol stack supports IP based communication also.

* Internet of Things: Architectures, Protocols, and Applications, Hindawi, 2017

Technical Specification	Classic Bluetooth technology	Bluetooth low energy technology
Distance/Range	100 m (330 ft)	50 m (160 ft)
Over the air data rate	1–3 Mbit/s	1 Mbit/s
Application throughput	0.7–2.1 Mbit/s	0.27 Mbit/s
Active slaves	7	Not defined; implementation dependent
Security	56/128-bit and application layer user defined	128-bit AES with Counter Mode CBC-MAC and application layer user defined
Robustness	Adaptive fast frequency hopping, FEC, fast ACK	Adaptive frequency hopping, Lazy Acknowledgement, 24-bit CRC, 32-bit Message Integrity Check
Latency (from a non-connected state)	Typically 100 ms	6 ms
Total time to send data (det.battery life)	100 ms	3 ms, <3 ms
Voice capable	Yes	No
Network topology	Scatternet	Star-bus
Power consumption	1 as the reference	0.01 to 0.5 (depending on use case)
Peak current consumption	<30 mA	<15 mA
Service discovery	Yes	Yes
Profile concept	Yes	Yes
Primary use cases	Mobile phones, gaming, headsets, stereo audio streaming, automotive, PCs, security, proximity, healthcare, sports & fitness, etc.	Mobile phones, gaming, PCs, watches, sports and fitness, healthcare, security & proximity, automotive, home electronics, automation, Industrial, etc.

Bluetooth low energy- PHY layer

- 40 RF Channels
  - 3 FIXED Channels for Advertising
  - 37 Dynamic Channels:
    - Used to send application data and Adaptively Frequency Hopped

* Bluetooth low energy, Nordic semiconductor, 2010

Bluetooth low energy- Link layer- Package Structure

- All packets have same structure
  - Preamble – 01010101 or 10101010
  - Access Address – correlated 32 bit sequence
  - Payload – actual data
  - CRC – 24 bit CRC for robust bit error detection
  - CRC calculated over Payload

Preamble	Access Address	Payload	CRC
1 byte	4 bytes	2 to 39 bytes	3 bytes

* Bluetooth low energy, Nordic semiconductor, 2010

Modulation Technique: Adaptive Frequency Hopping Spread Spectrum

- Resists Interference and multi-path effects
- Provides a form of multiple access among co-located devices in different piconets
- Total Bandwidth of 80 MHz is divided into 40 channels of 2 MHz each
- FH occurs by jumping from one frequency to other using a pseudo-random sequence
- Hopping sequence shared across entire piconet

* "Bluetooth Low Energy: An insight", Robert Bosch Centre for Cyber-Physical Systems

BLE L2CAP

- Advertisement
- Scanning
- Connection Establishment

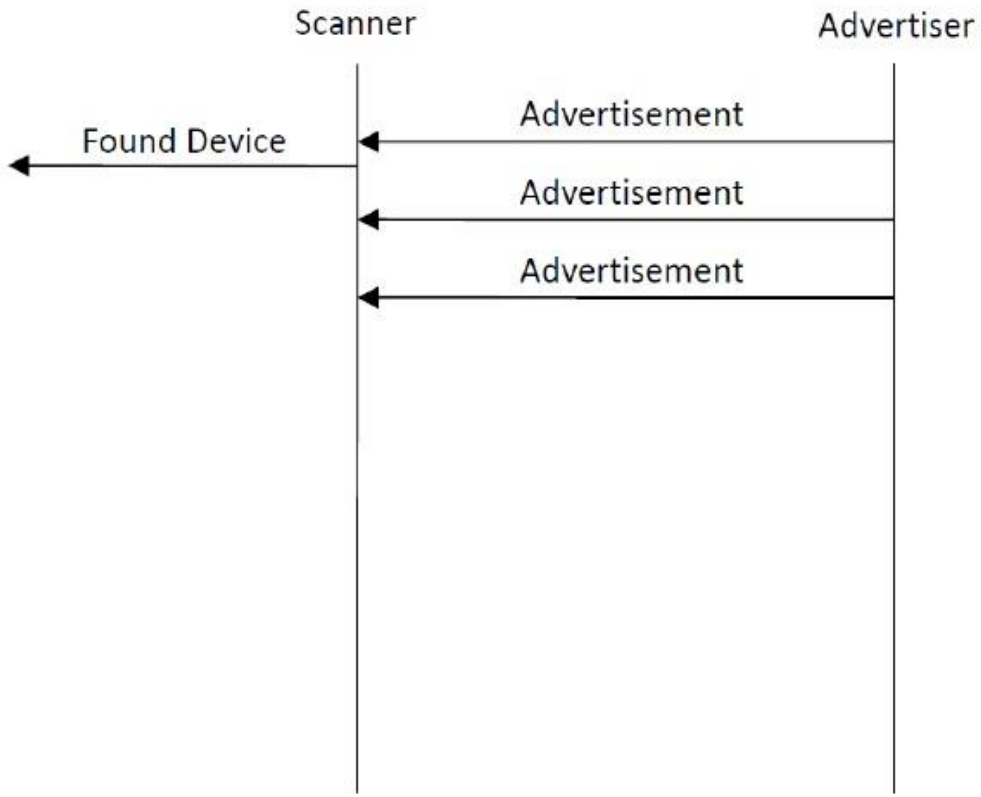
* "Bluetooth Low Energy: An insight", Robert Bosch Centre for Cyber-Physical Systems

BLE L2CAP - Advertisement

- Provides a way for devices to broadcast their presence
- Allows connection to be established
- Broadcast data like the list of supported services, device name and TX Power Level
- Device will send advertising broadcast packets to one or multiple advertisement channels, which remote devices will pick up.

* "Bluetooth Low Energy: An insight", Robert Bosch Centre for Cyber-Physical Systems

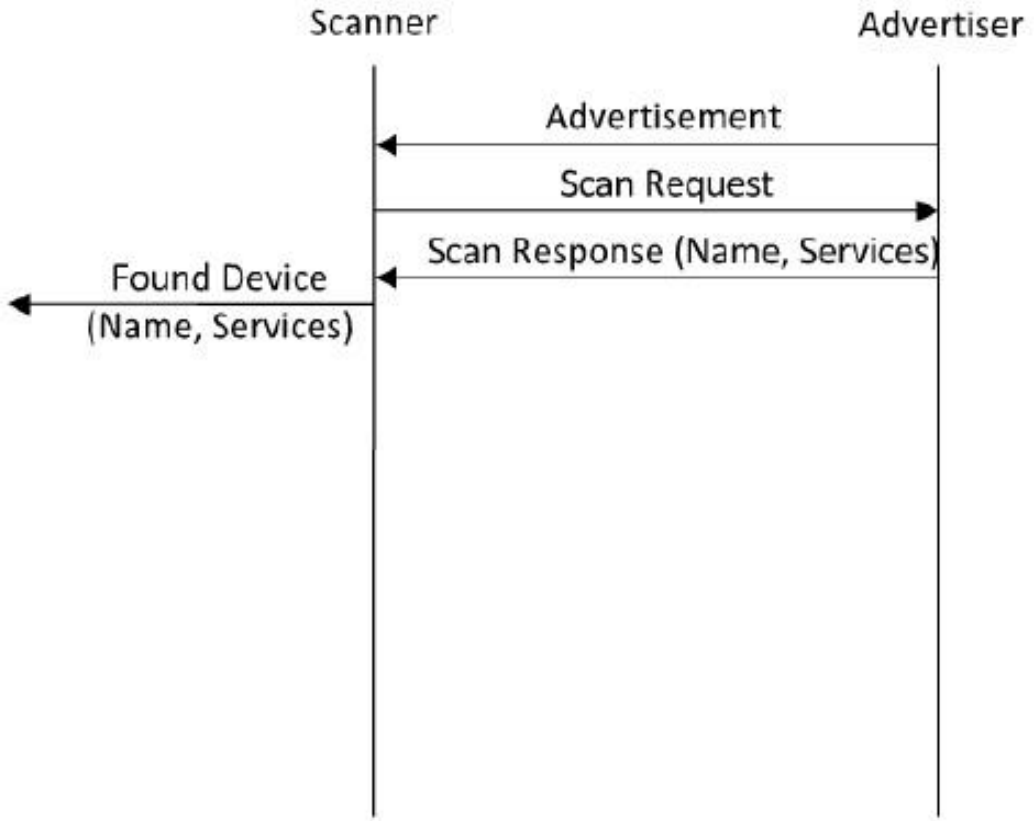
BLE L2CAP – Advertisement- Passive Scanning



Bluetooth low energy advertisement

* "Bluetooth Low Energy: An insight", Robert Bosch Centre for Cyber-Physical Systems

BLE L2CAP – Active Scanning



Active scanning

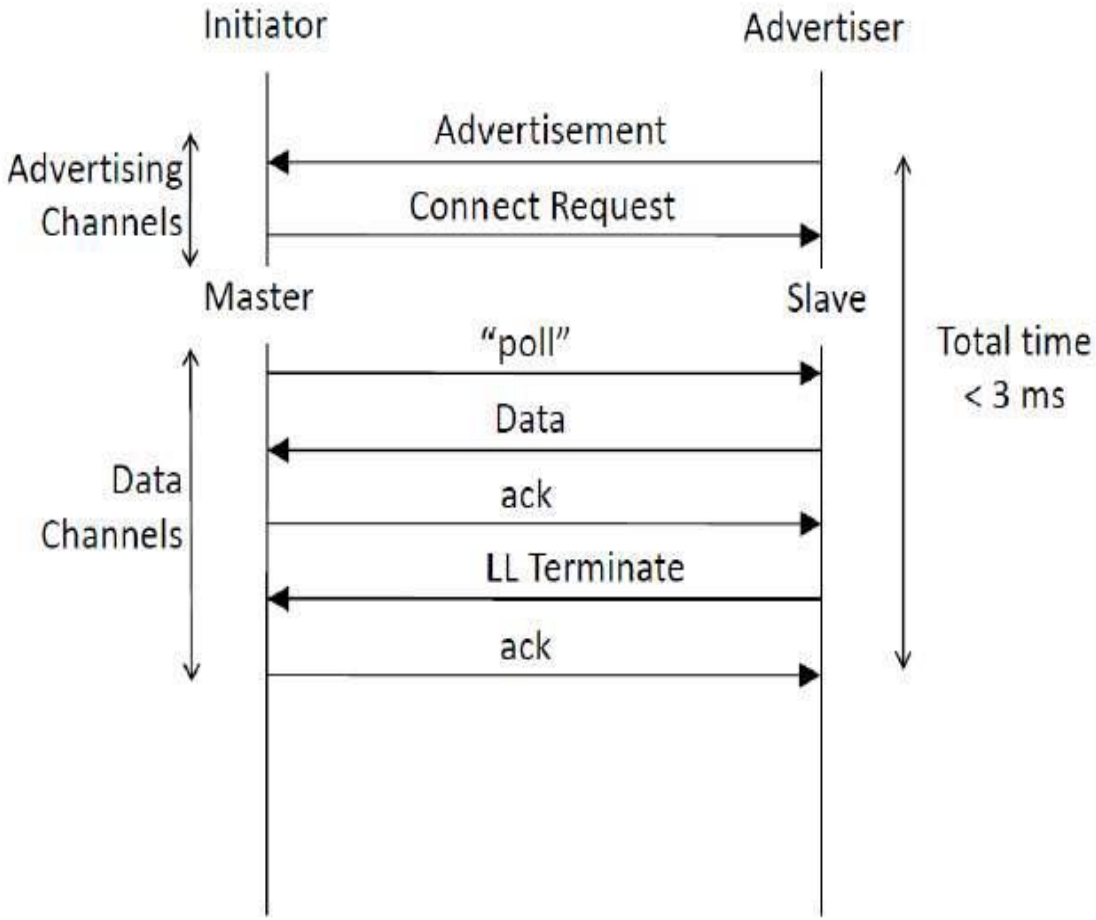
* "Bluetooth Low Energy: An insight", Robert Bosch Centre for Cyber-Physical Systems

BLE Advertising Parameters

Parameter	Values	Description
Advertisement Interval	20 mSec to 10240 mSec	Interval between advertisement packets
Advertisement channels	37, 38 & 39	RF Channel used to transmit
Discoverability Mode	Not Discoverable Generic Discoverable Limited Discoverable Broadcast	How the advertiser visible to other devices
Connect ability mode	Not connectable Directly connectable Undirected connectable	Defines if advertiser can be connected or not
Payload	0 – 31 Byte	Data byte can be included in advertisement packet

* "Bluetooth Low Energy: An insight", Robert Bosch Centre for Cyber-Physical Systems

BLE L2CAP – Connection



Connection, transmission of packet, and connection termination

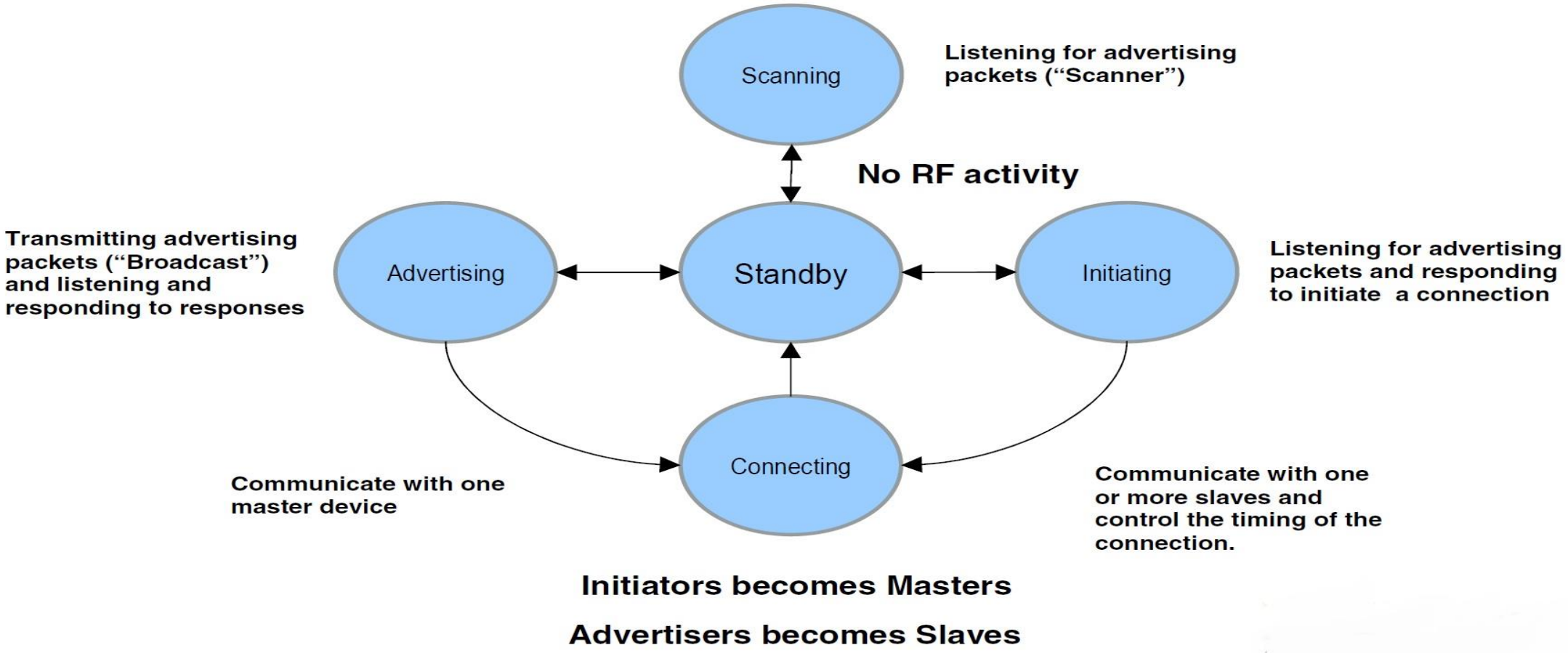
* "Bluetooth Low Energy: An insight", Robert Bosch Centre for Cyber-Physical Systems

BLE L2CAP – Network Topology

- Advertiser
  - Broadcasts advertisement packets
- Scanner
  - Only listen for advertisements, can connect to advertiser
- Slave
  - Device connected to master
- Master
  - Device connected with one or more slaves
  - Master can connect upto 4 – 8 slaves at a time
- Hybrid
  - Device advertise and scan at the same time
  - Connected to a master and advertise or scan simultaneously

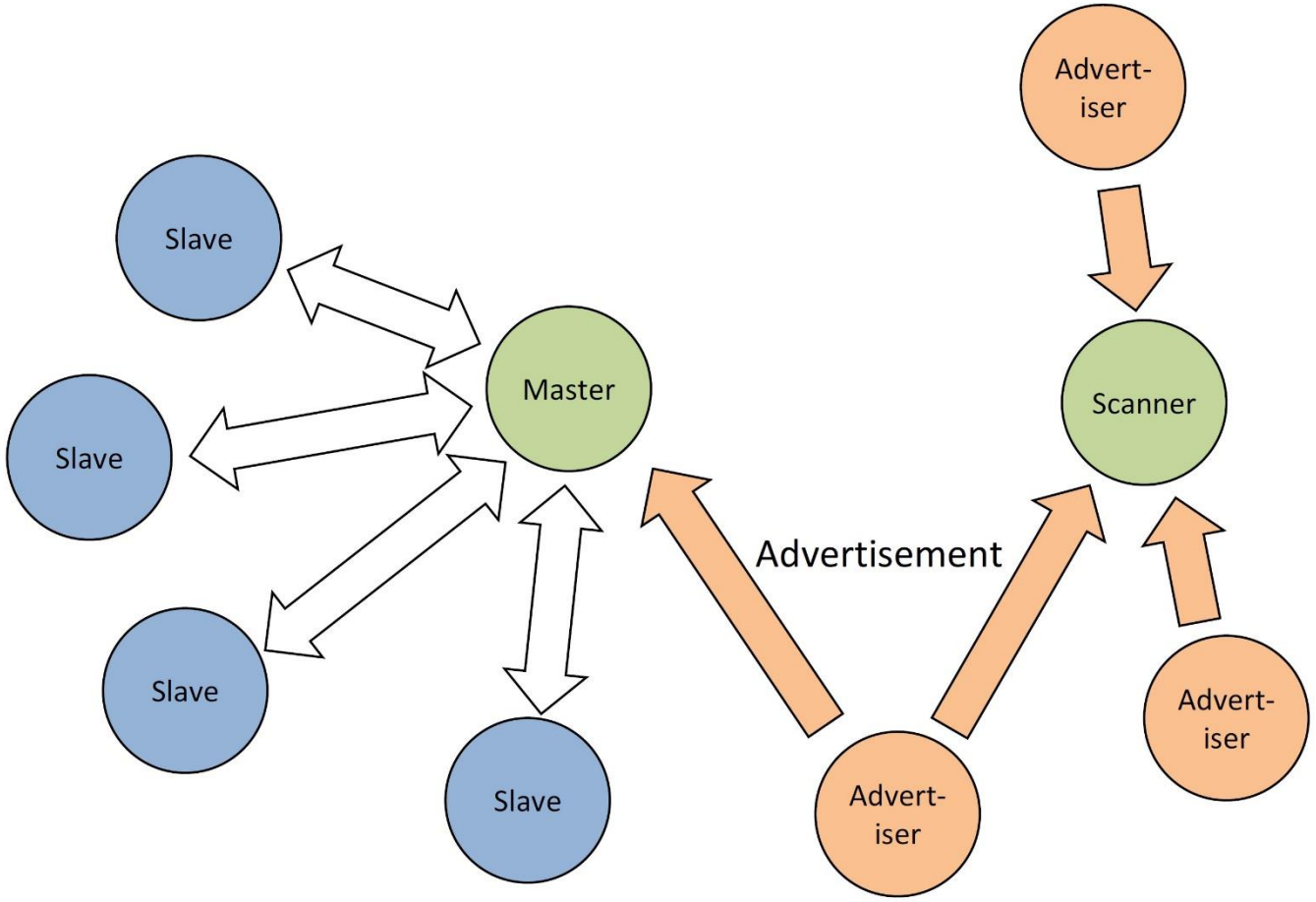
* "Bluetooth Low Energy: An insight", Robert Bosch Centre for Cyber-Physical Systems

Bluetooth low energy- Link layer- States



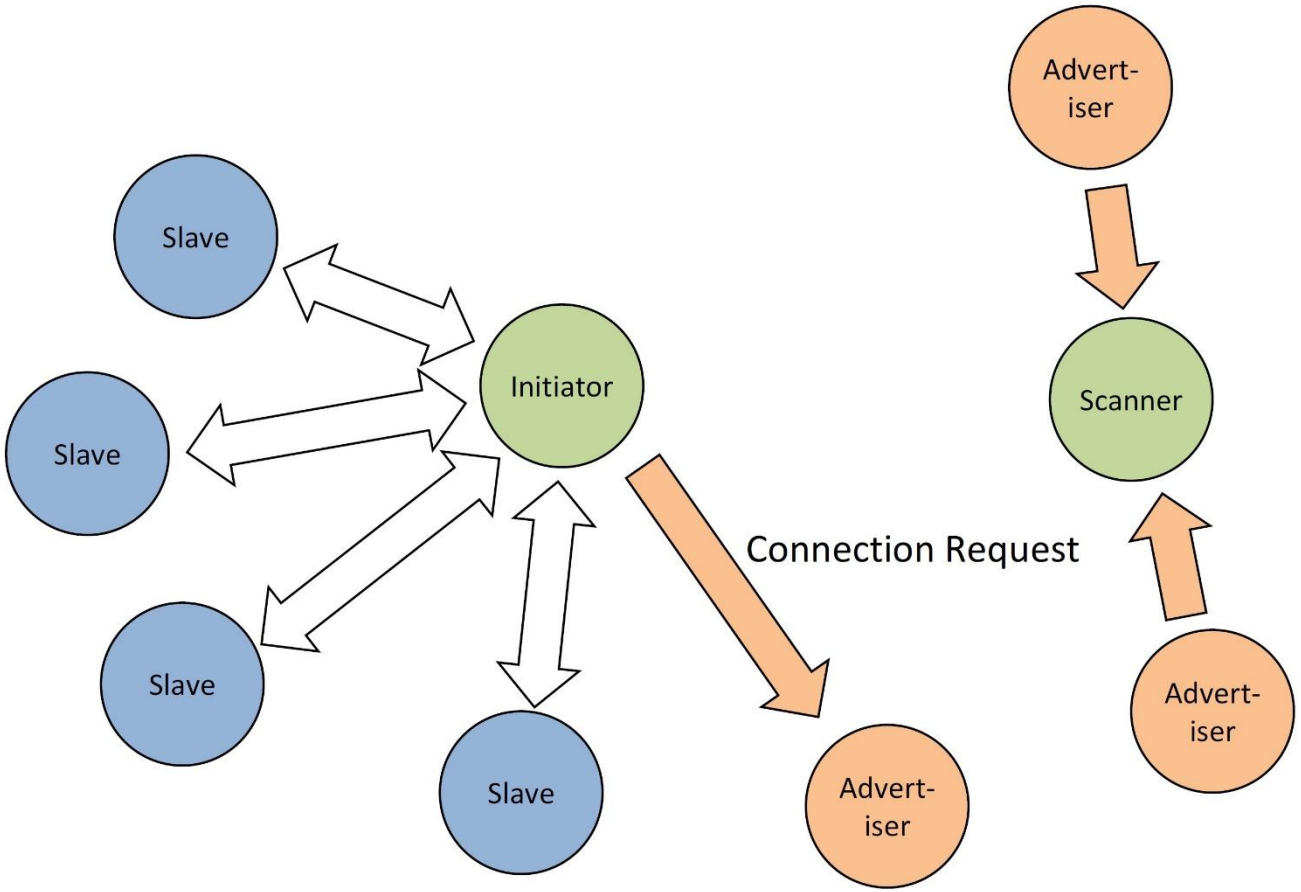
* Bluetooth low energy, Nordic semiconductor, 2010

Bluetooth low energy- Link layer- Network Topology 1



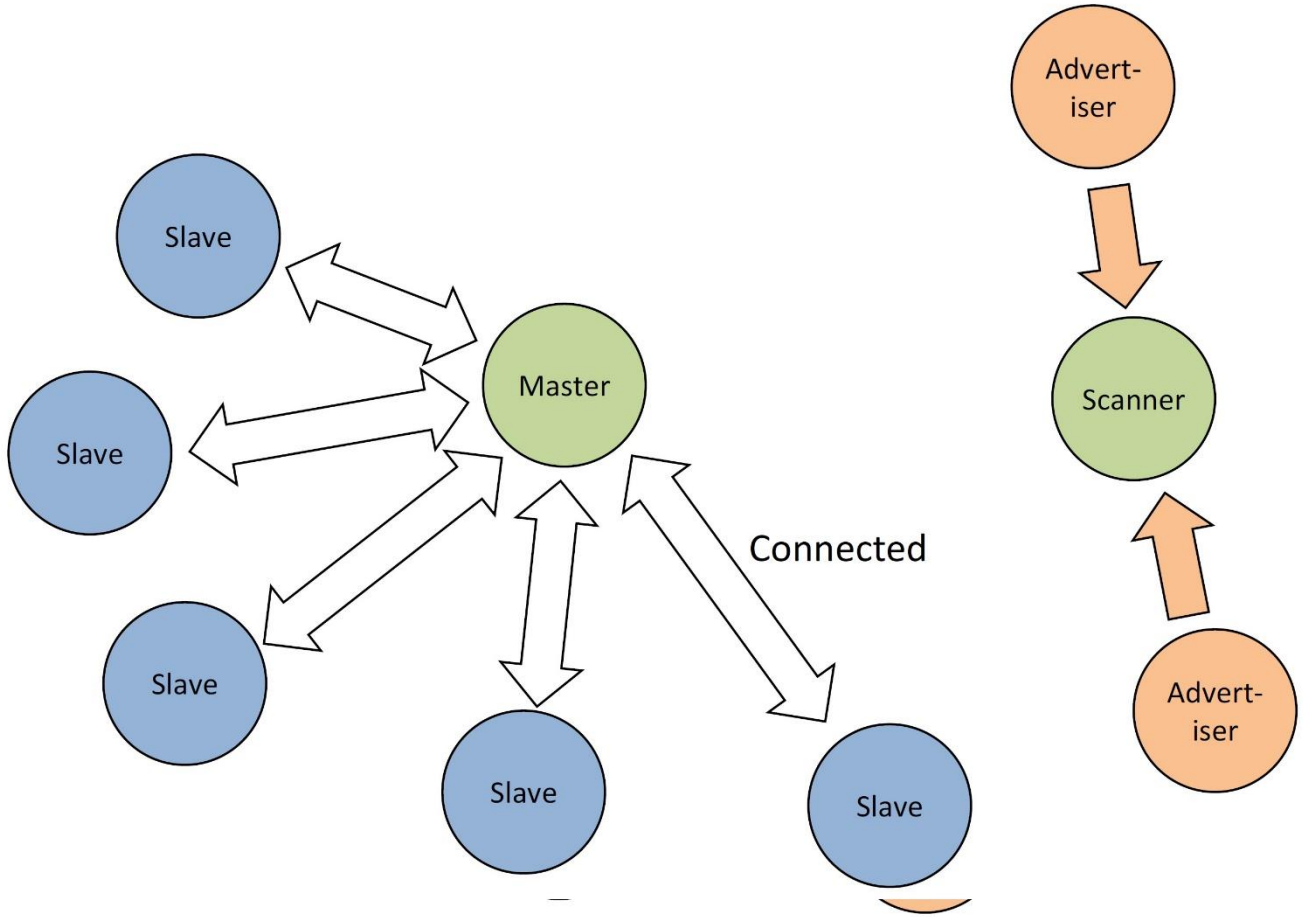
* Bluetooth low energy, Nordic semiconductor, 2010

Bluetooth low energy- Link layer- Network Topology 2



* Bluetooth low energy, Nordic semiconductor, 2010

Bluetooth low energy- Link layer- Network Topology 3



* Bluetooth low energy, Nordic semiconductor, 2010