Internet of Things

IoT Communications and Networking Technologies and Protocols

Mehdi Rasti
Amirkabir University of Technology

Spring 2020

Physical and Link Layers Protocols- IEEE 802.15.4e/g

- The IEEE frequently makes amendments اصلاحات 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.

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

Physical and Link Layers Protocols- IEEE 802.15.4e/g

- While the IEEE 802.15.4**e**-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.

Physical and Link Layers Protocols- IEEE 802.15.4e/g

- The following are some of the main enhancements to the MAC layer proposed by IEEE 802.15.4**e**-2012:
  - **Time-Slotted Channel Hopping (TSCH):**
    - A MAC operation mode that works to guarantee media access and channel diversity.
    - Channel hopping, also known as frequency hopping, utilizes different channels for transmission at different times.
    - TSCH divides time into fixed time periods, or “time slots,” which offer guaranteed bandwidth and predictable latency.
  - **Information elements (IE):**
    - IEs allow for the exchange of information at the MAC layer in an extensible manner, either as header IEs (standardized) and/or payload IEs (private).
    - Specified in a tag, length, value (TLV) format, the IE field allows frames to carry additional metadata to support MAC layer services, including IEEE 802.15.9 key management.

Physical and Link Layers Protocols- IEEE 802.15.4e/g

- **Enhanced beacons (EBs)**
  - EBs extend the flexibility of IEEE 802.15.4 beacons to allow the construction of application-specific beacon content. This is accomplished by including relevant IEs in EB frames.
  - Some IEs that may be found in EBs include network metrics, frequency hopping broadcast schedule, and PAN information version.
- **Enhanced beacon requests (EBRs)**
  - The IEs in EBRs allow the sender to selectively specify the request of information.
  - Beacon responses are then limited to what was requested in the EBR. For example, a device can query for a PAN that is allowing new devices to join or a PAN that supports a certain set of MAC/PHY capabilities.
- **Enhanced Acknowledgement**
  - The Enhanced Acknowledgement frame allows for the integration of a frame counter for the frame being acknowledged. This feature helps protect against certain attacks that occur when Acknowledgement frames are spoofed.

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 802.15.4**g** is the payload size, with 802.15.4g supporting up to 2047 bytes and 802.15.4 supporting only 127 bytes.

Physical and Link Layers Protocols- IEEE 802.15.4e/g

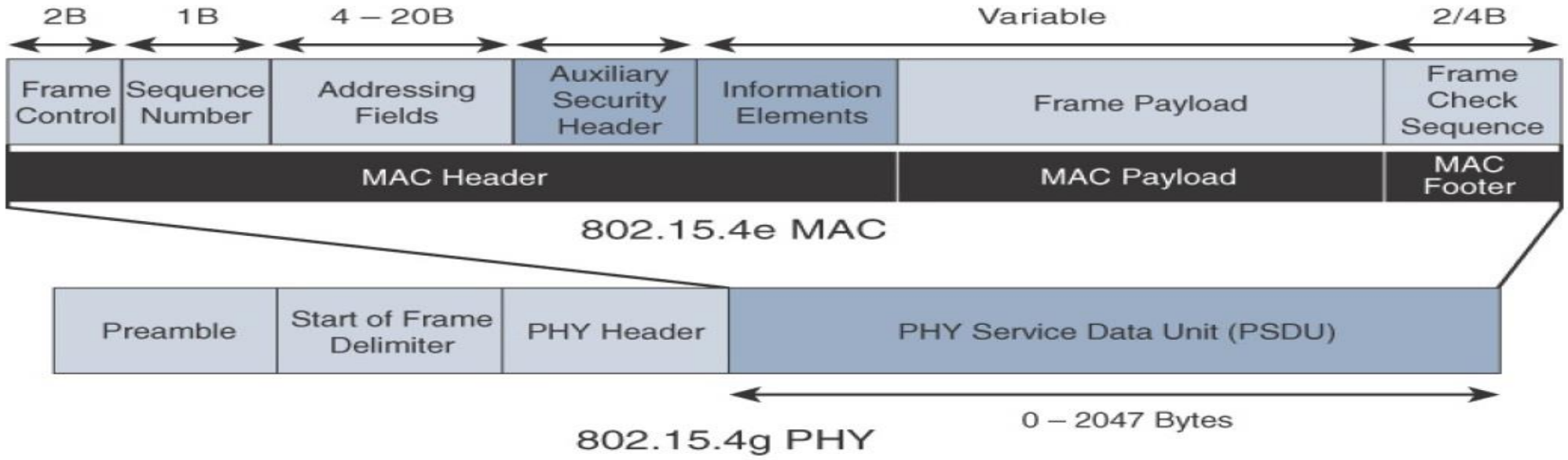
- IEEE 802.15.4e and 802.15.4g- Physical layer
  - In IEEE 802.15.4g-2012, the original IEEE 802.15.4 maximum payload size of 127 bytes was increased to 2047 bytes.
  - Fragmentation is no longer necessary at Layer 2 when IPv6 packets are transmitted over IEEE 802.15.4g MAC frames.
  - The error protection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

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.

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



Physical and Link Layers Protocols- IEEE 802.15.4e/g

- IEEE 802.15.4e and 802.15.4g
  - Topology
    - Mesh

History of BLE 802.15.1

- 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

- 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" on a button cell
- Small size and low cost
- Compatibility with a large installed base of mobile phones, tablets and computers

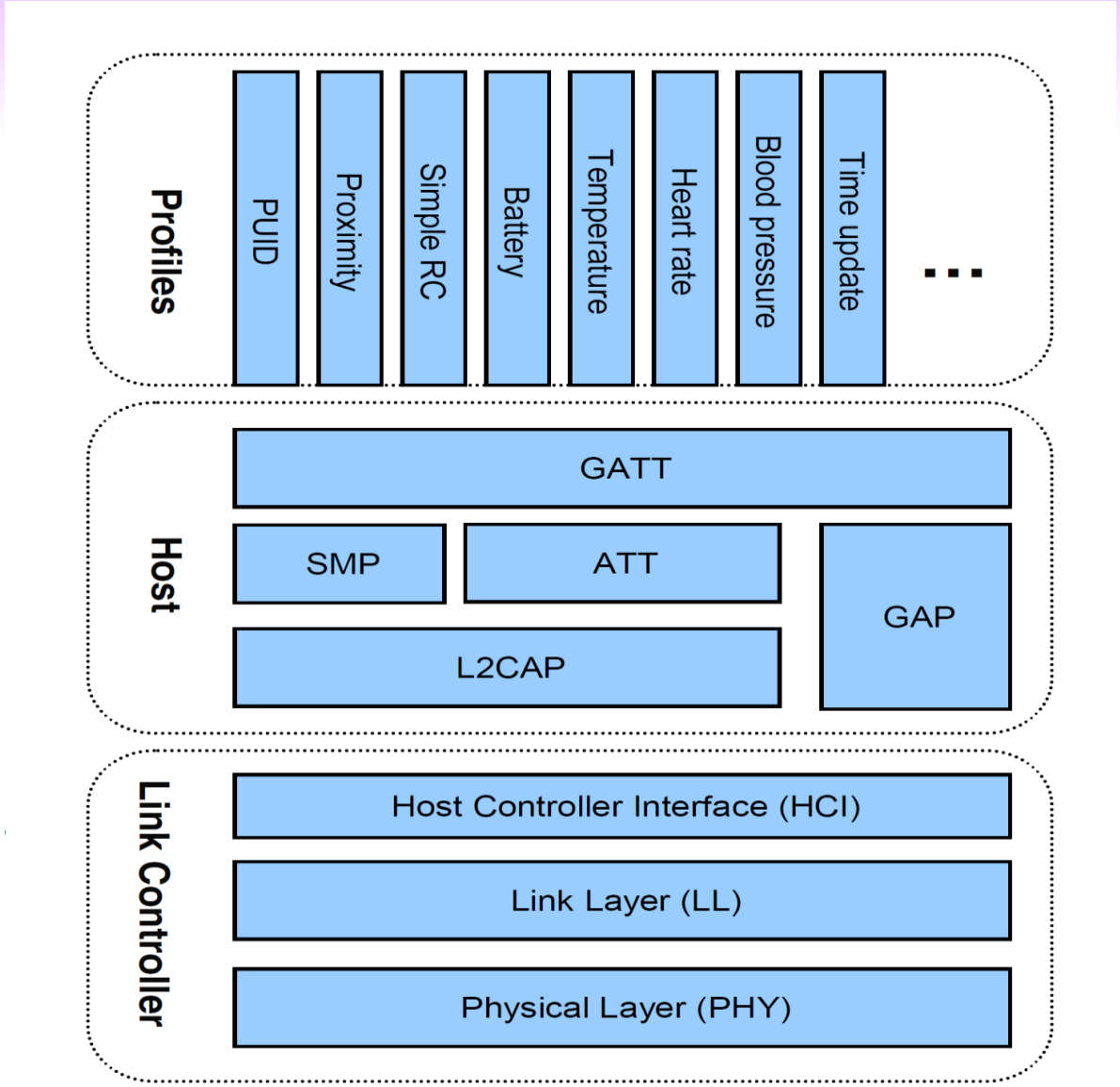
Physical and Link Layers Protocols- BLE

- 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.

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 اپلیکیشن خاصی که یک سری سرویس هایی میخواد(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 System Architecture



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: Star Topology
    - Master Co
      - 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.

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 سیگنال لوگ در مبنای ۲ میگیریم
    - 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.

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 ... و مستر بشه کی شیریت مثال جفت کردن
  - 37 Dynamic Channels:
    - Used to send application data and Adaptively Frequency Hopped

Bluetooth low energy- Link layer- Package Structure

- All packets have same structure
  - Preamble – 01010101 or 10101010
  - Access Address – correlated 32 bit sequence ۱۶ ۱۶ نصف نصف مبداء و مقصد
  - Payload – actual data
  - CRC – 24 bit CRC for robust bit error detection
  - CRC calculated over Payload
    - کلاً مهمه که پی لود و فضای آدرس دهی بلوتوث باید کمتر از مثلاً وای فای باشه
      - اینو باید درک کرد

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

Modulation Technique: Adaptive Frequency Hopping Spread Spectrum

- دو سوال خیلی مهم توی لایه فیزیکی چیه؟
  - یکی این که مودولاسیونش چیه
  - بعدم این که توی چه فرکانسی هستش برا خودش
  - معماریشم حالا مهمه

- Resists Interference تداخل and multi-path effects خلاصه کمک میکنه کانالا منصفانه تقسیم بشه
- 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**

BLE L2CAP

- Advertisement همه پخشی میشه و همه میشنونش
- Scanning
- Connection Establishment

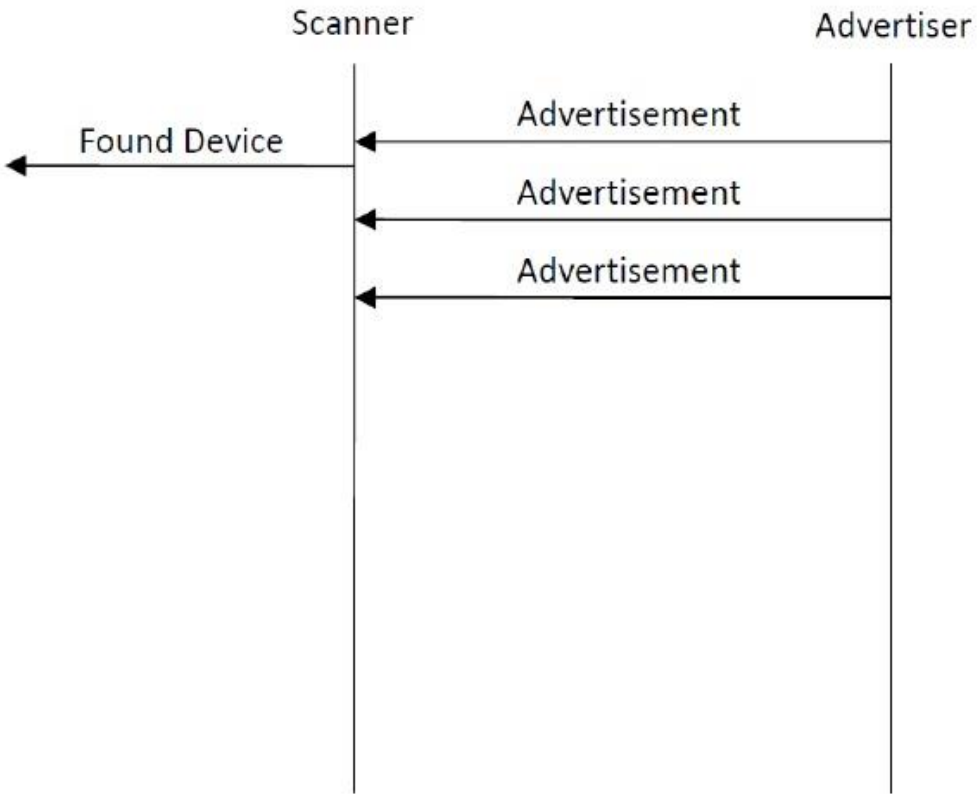
BLE L2CAP - Advertisement

- 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

– باعث میشه فاصله حدودی مشخص بشه

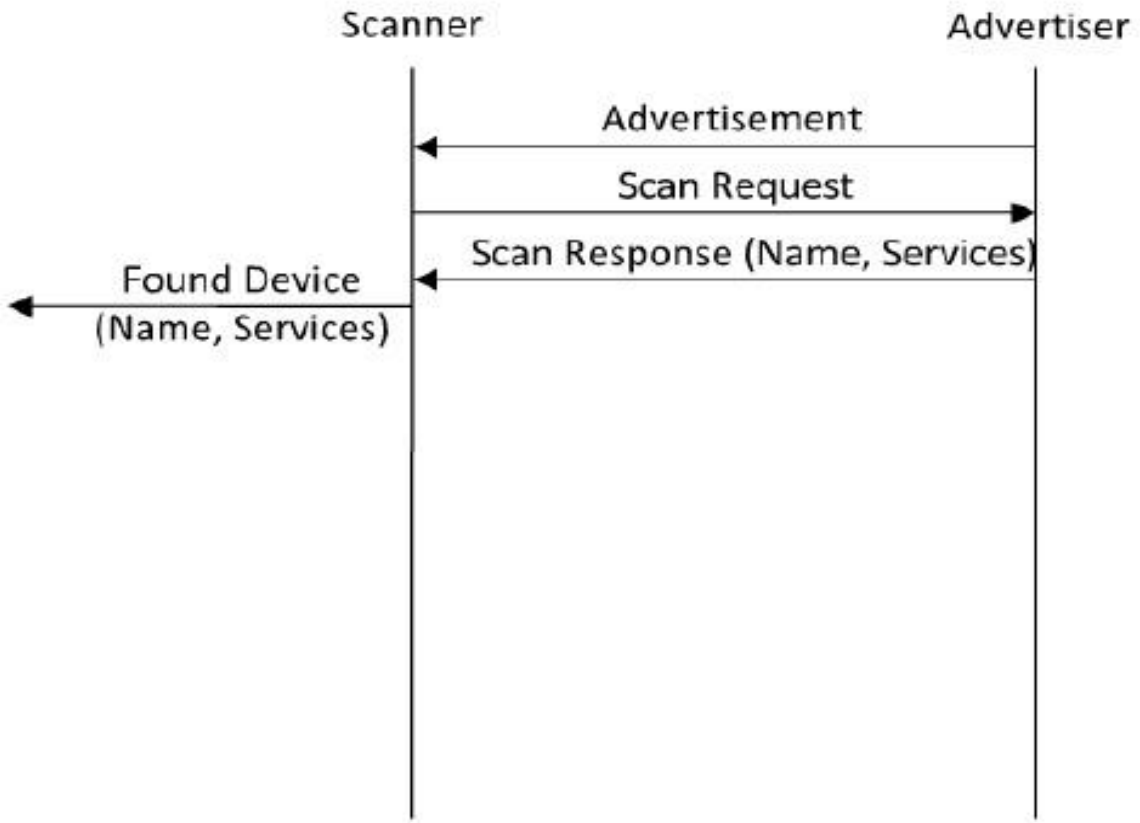
- Device will send advertising broadcast packets to one or multiple advertisement channels, which remote devices will pick up.

BLE L2CAP – Advertisement- Passive Scanning



Bluetooth low energy advertisement

BLE L2CAP – Active Scanning درخواست های بیشتر بدم

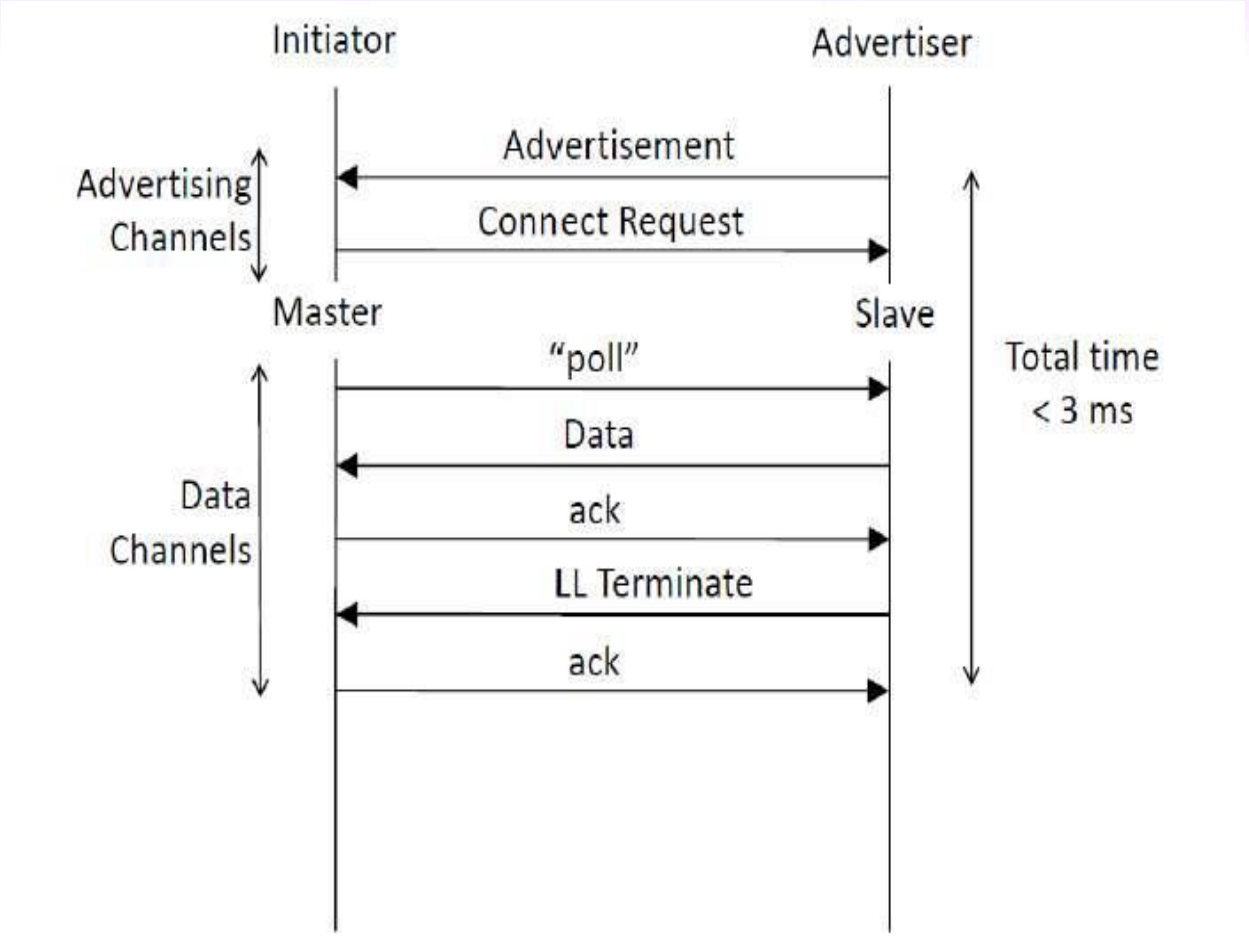


Active scanning

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

BLE L2CAP – Connection

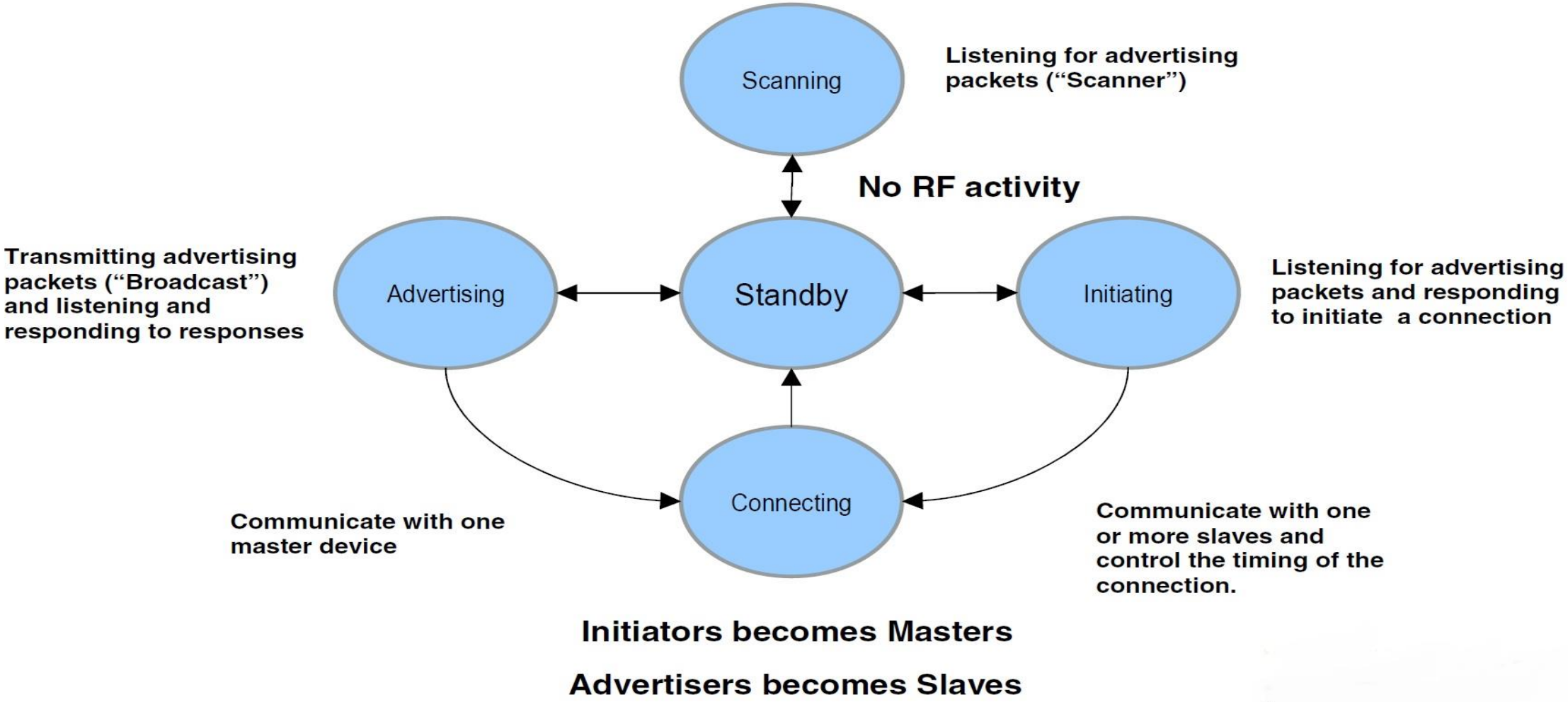


Connection, transmission of packet, and connection termination

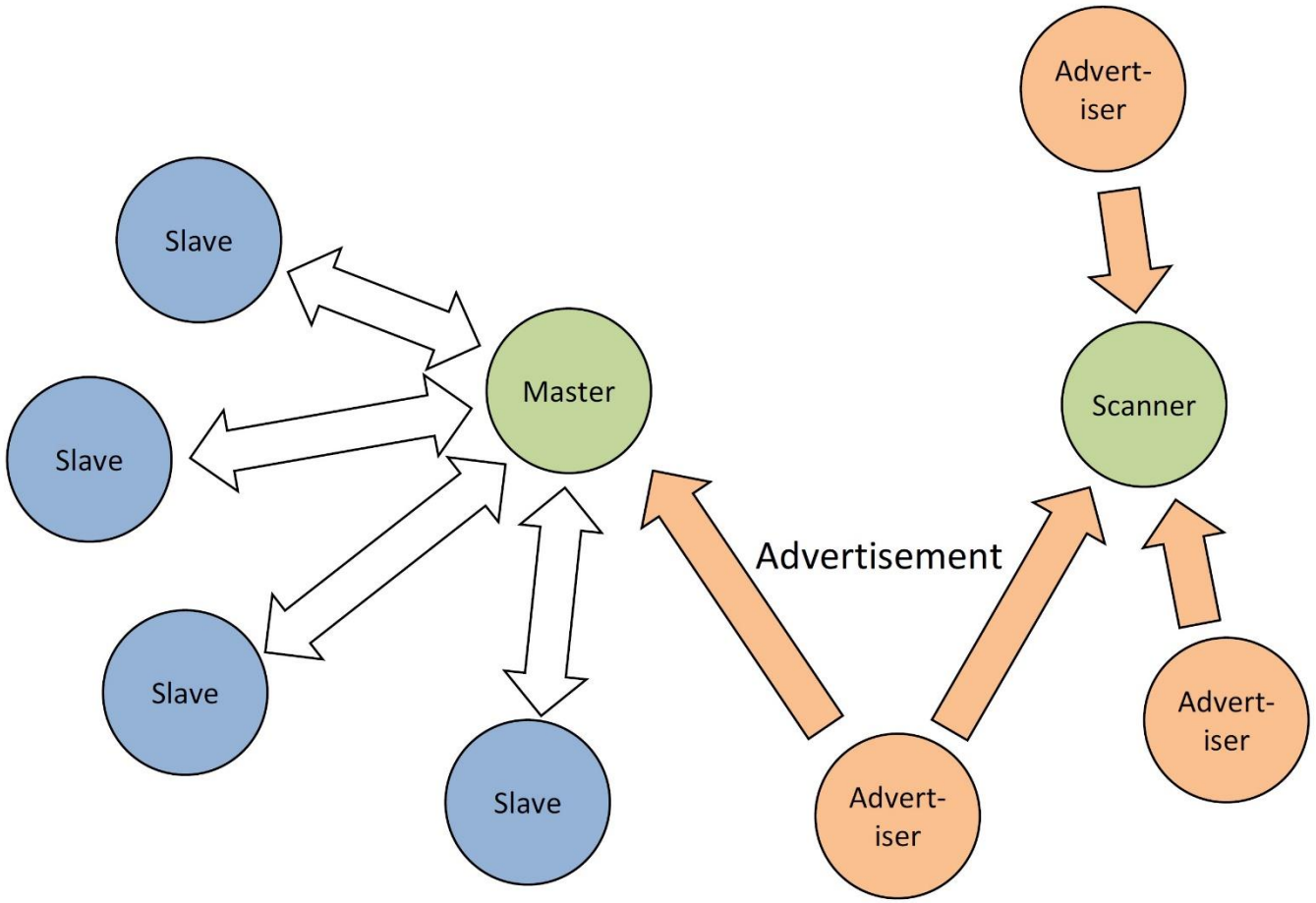
BLE L2CAP – Network Topology

- 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

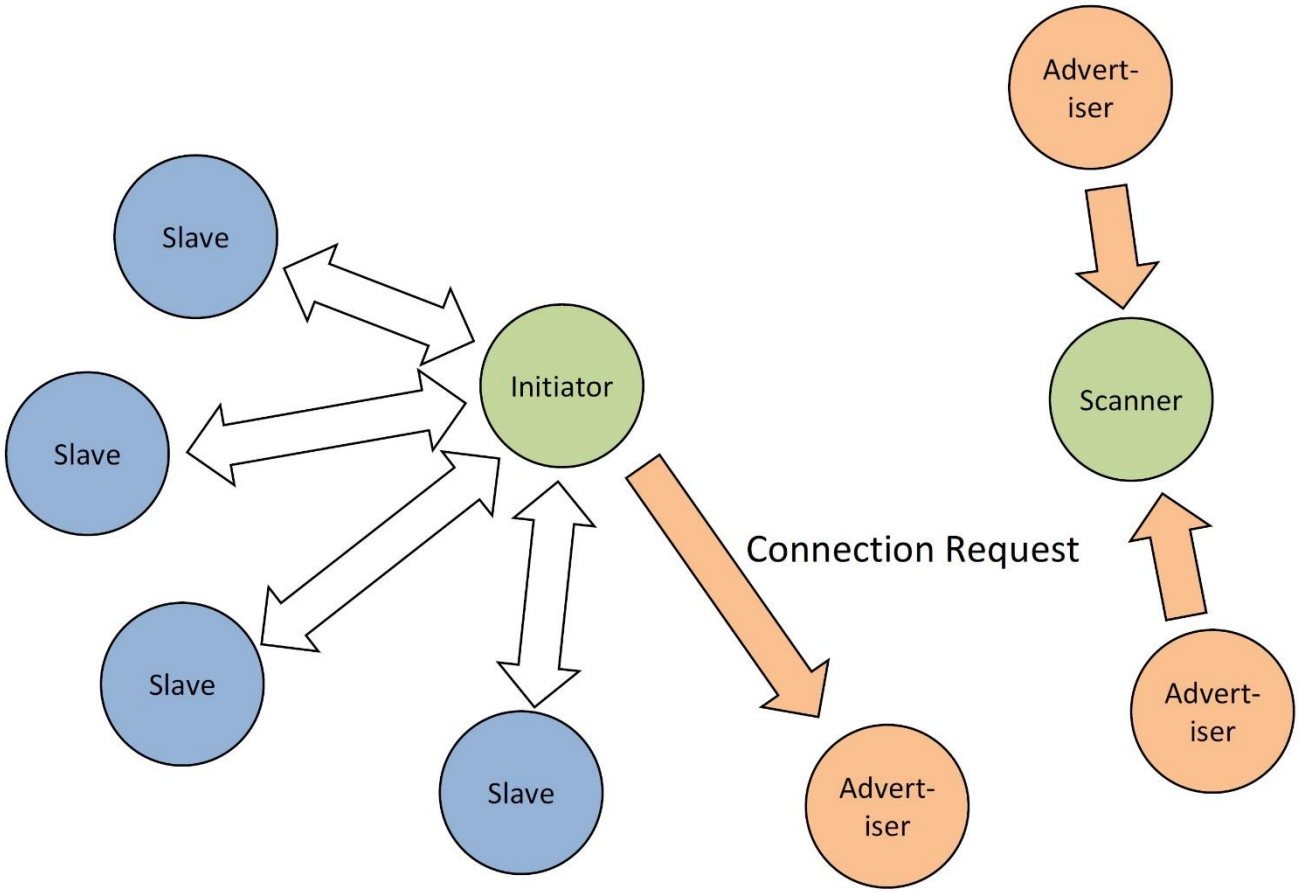
Bluetooth low energy- Link layer- States



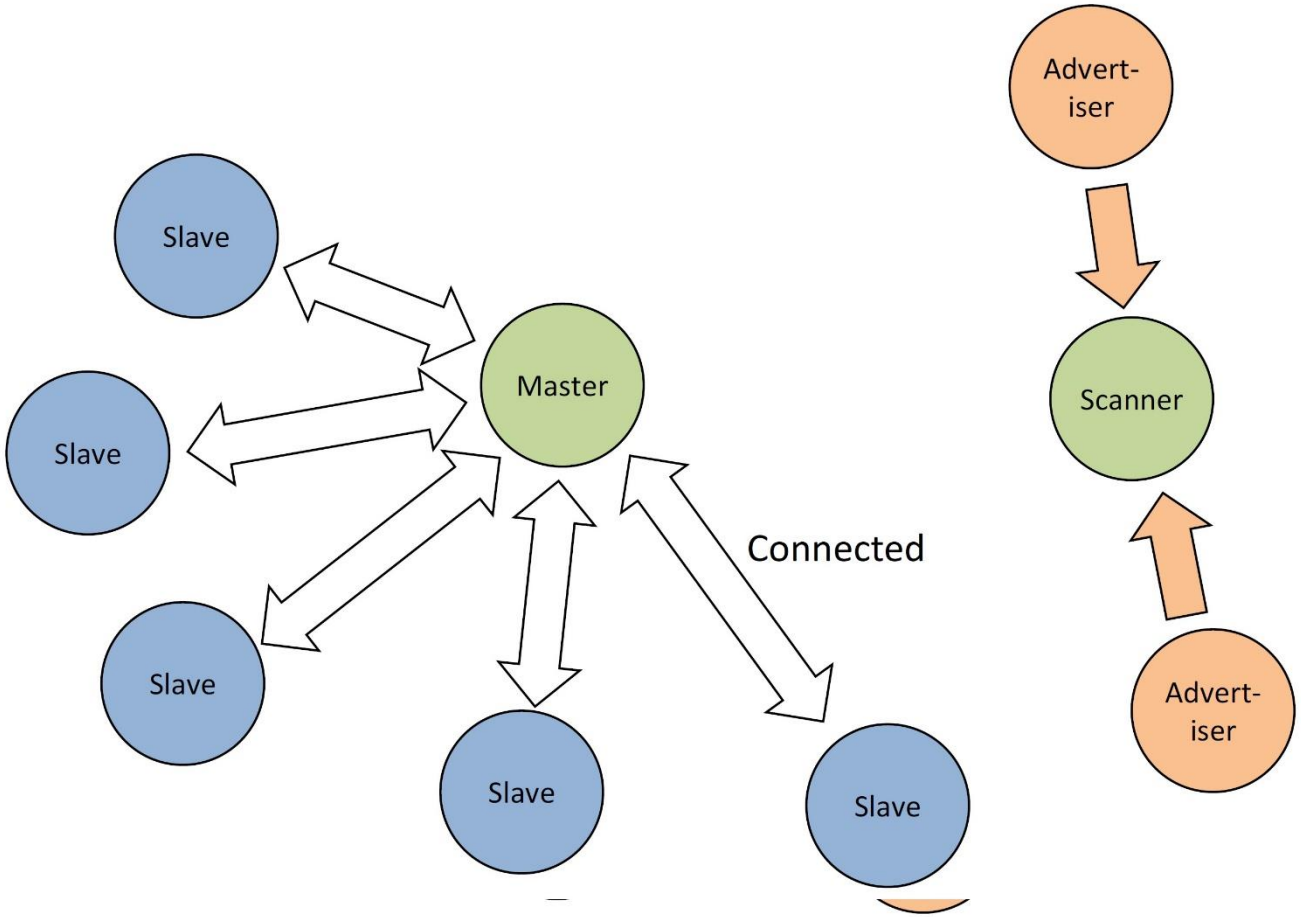
Bluetooth low energy- Link layer- Network Topology 1



Bluetooth low energy- Link layer- Network Topology 2



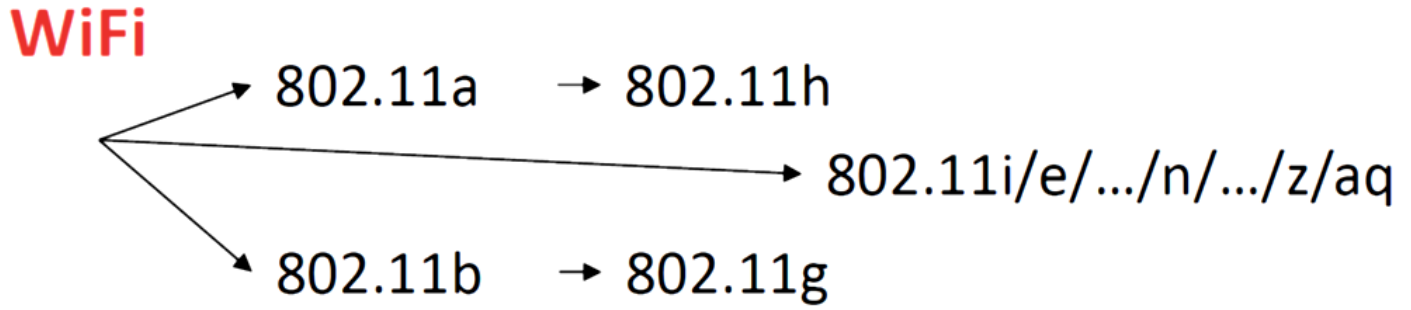
Bluetooth low energy- Link layer- Network Topology 3



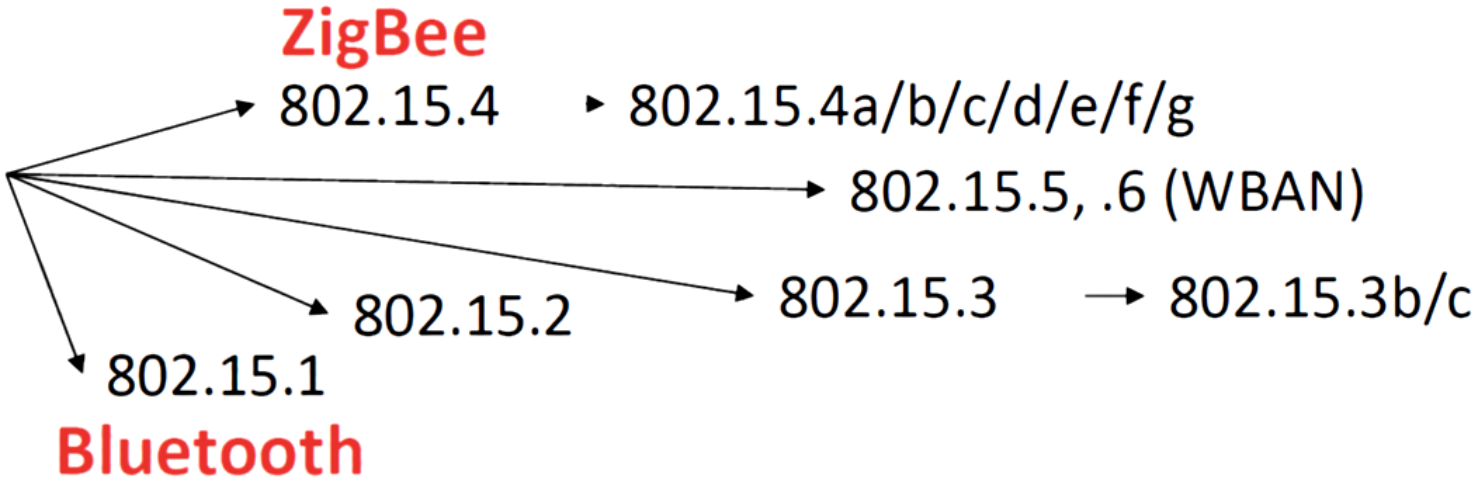
Physical and Link Layers Protocols- LP-WiFi

این دیگه انواع فریم نداره چون سر کانال جدا سازی شده

Local wireless networks
WLAN 802.11



Personal wireless nw
WPAN 802.15



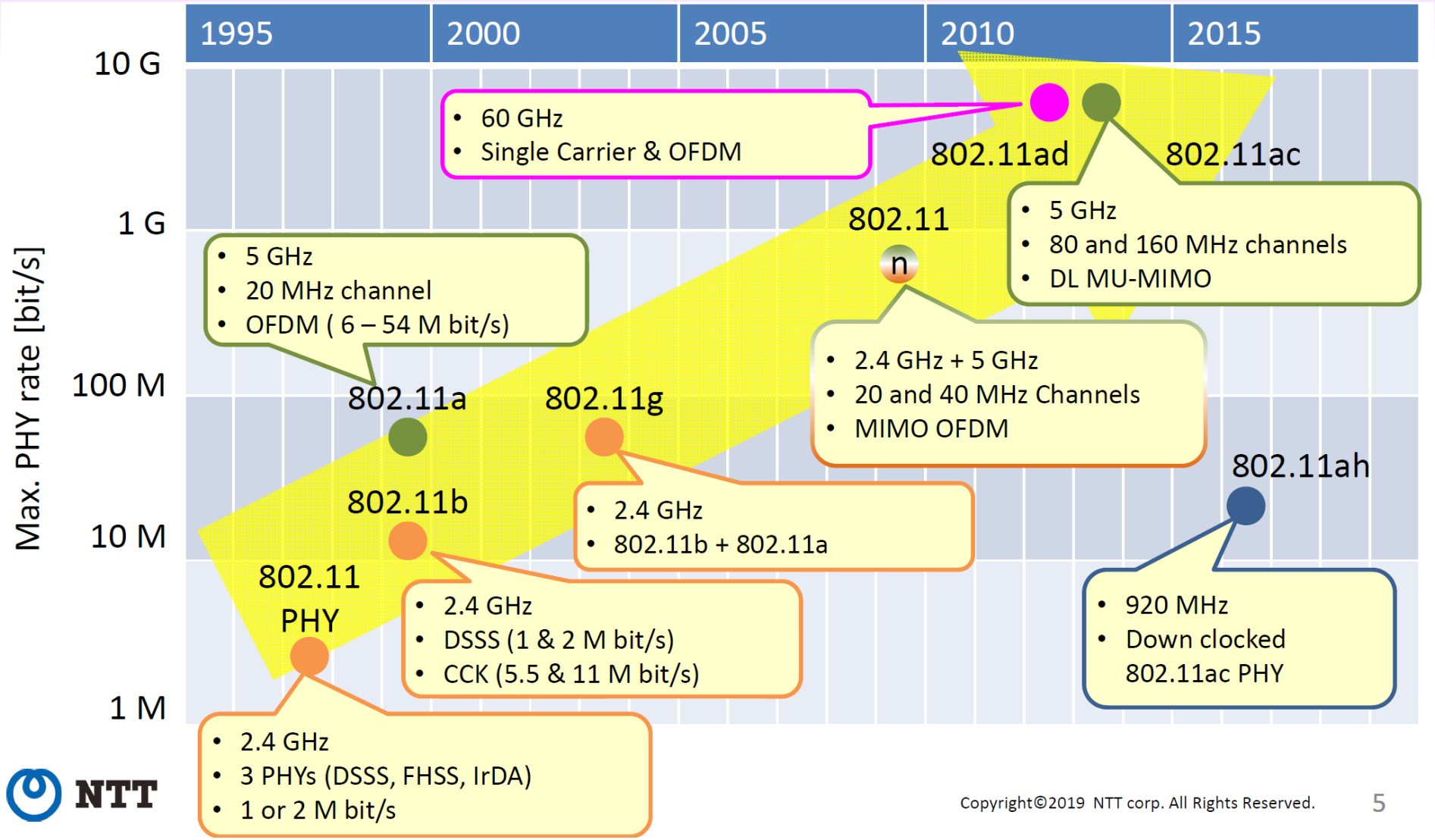
History of IEEE 802.11 Standardization

Standard	Date	Scope
IEEE 802.11	1997	Medium access control (MAC): One common MAC for WLAN applications
		Physical layer: Infrared at 1 and 2 Mbps
		Physical layer: 2.4-GHz FHSS at 1 and 2 Mbps
		Physical layer: 2.4-GHz DSSS at 1 and 2 Mbps
IEEE 802.11a	1999	Physical layer: 5-GHz OFDM at rates from 6 to 54 Mbps
IEEE 802.11b	1999	Physical layer: 2.4-GHz DSSS at 5.5 and 11 Mbps
IEEE 802.11c	2003	Bridge operation at 802.11 MAC layer
IEEE 802.11d	2001	Physical layer: Extend operation of 802.11 WLANs to new regulatory domains (countries)
IEEE 802.11e	2007	MAC: Enhance to improve quality of service and enhance security mechanisms
IEEE 802.11f	2003	Recommended practices for multivendor access point interoperability
IEEE 802.11g	2003	Physical layer: Extend 802.11b to data rates >20 Mbps
IEEE 802.11h	2003	Physical/MAC: Enhance IEEE 802.11a to add indoor and outdoor channel selection and to improve spectrum and transmit power management
IEEE 802.11i	2007	MAC: Enhance security and authentication mechanisms
IEEE 802.11j	2007	Physical: Enhance IEEE 802.11a to conform to Japanese requirements
IEEE 802.11k	2008	Radio Resource Measurement enhancements to provide interface to higher layers for radio and network measurements

History of IEEE 802.11 Standardization

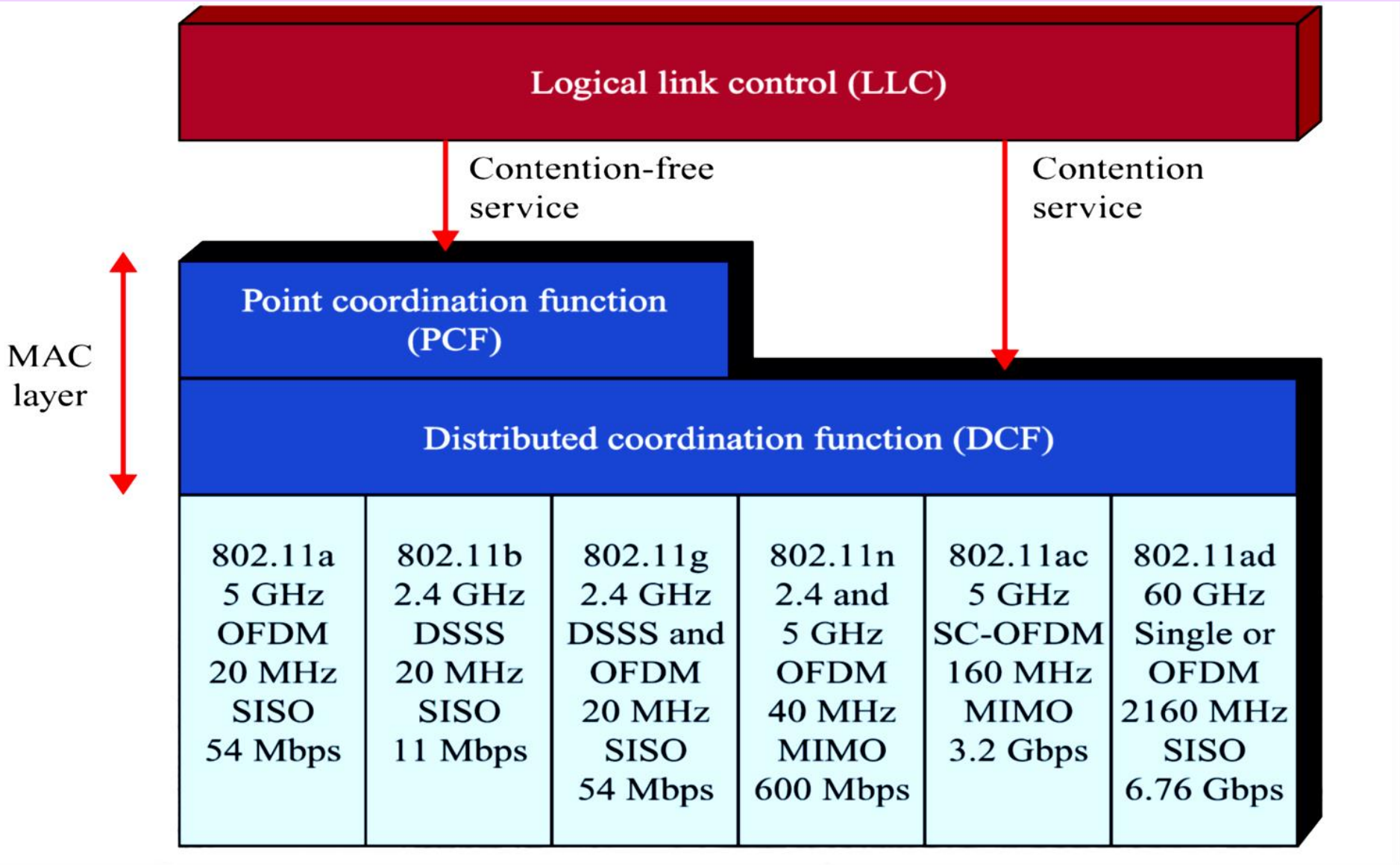
Standard	Date	Scope
IEEE 802.11m	Ongoing	This group provides maintenance of the IEEE 802.11 standard by rolling published amendments into revisions of the 802.11 standard.
IEEE 802.11n	2009	Physical/MAC: Enhancements to enable higher throughput
IEEE 802.11p	2010	Wireless Access in Vehicular Environments (WAVE)
IEEE 802.11r	2008	Fast Roaming/Fast BSS Transition
IEEE 802.11s	2011	Mesh Networking
IEEE 802.11T	Abandoned	Recommended Practice for Evaluation of 802.11 Wireless Performance
IEEE 802.11u	2011	Interworking with External Networks
IEEE 802.11v	2011	Wireless Network Management
IEEE 802.11w	2009	Protected Management Frames
IEEE 802.11y	2008	Contention Based Protocol
IEEE 802.11z	2010	Extensions to Direct Link Setup
IEEE 802.11aa	2012	Video Transport Stream
IEEE 802.11ac	Ongoing	Very High Throughput <6Ghz
IEEE 802.11ad	2012	Very High Throughput in 60 GHz
IEEE 802.11ae	2012	Prioritization of Management Frames
IEEE 802.11af	Ongoing	Wireless LAN in the TV White Space
IEEE 802.11ah	Ongoing	Sub 1GHz
IEEE 802.11ai	Ongoing	Fast Initial Link Set-up
IEEE 802.11aj	Ongoing	China Milli-Meter Wave (CMMW)
IEEE 802.11ak	Ongoing	Enhancements For Transit Links Within Bridged Networks
IEEE 802.11aq	Ongoing	Pre-Association Discovery (PAD)
IEEE 802.11ax	Ongoing	High Efficiency WLAN (HEW)

History of IEEE 802.11 Standardization



NTT

IEEE 802.11 Protocol Architecture



Physical and Link Layers Protocols- 802.11 ah

- The LP-WiFi also known as a new brand called Wi-Fi HaLow consumes lower power than a traditional WiFi device and also has a longer range.
  - This marketing name is based on a play on words between “11ah” in reverse and “low power.”
  - It is similar to the word “hello” but it is pronounced “hay-low.”

- The range of WiFi HaLow is nearly twice that of traditional WiFi.

- Like other WiFi devices, devices supporting WiFi HaLow also support IP connectivity, which is important for IoT applications.

Physical and Link Layers Protocols- IEEE 802.11ah

- In unconstrained networks, IEEE 802.11 Wi-Fi is certainly the most successfully deployed wireless technology.
  - Either for connecting endpoints such as fog computing nodes, high-data-rate sensors, and audio or video analytics devices or for deploying Wi-Fi backhaul infrastructures, such as outdoor Wi-Fi mesh in smart cities, oil and mining, or other environments.
- Wi-Fi lacks sub-GHz support for
  - better signal penetration,
  - low power for battery-powered nodes,
  - the ability to support a large number of devices.
- For these reasons, the IEEE 802.11 working group launched a task group named IEEE 802.11ah to specify a sub-GHz version of Wi-Fi.

Physical and Link Layers Protocols- IEEE 802.11ah

- Three main use cases are identified for IEEE 802.11ah:
  - –Sensors and meters covering a smart grid
    - Meter to pole, environmental/agricultural monitoring, industrial process sensors, indoor healthcare system and fitness sensors, home and building automation sensors
  - –Backhaul aggregation of industrial sensors and meter data
    - Potentially connecting IEEE 802.15.4g subnetworks
  - –Extended range Wi-Fi
    - For outdoor extended-range hotspot or cellular traffic offloading when distances already covered by IEEE 802.11a/b/g/n/ac are not good enough

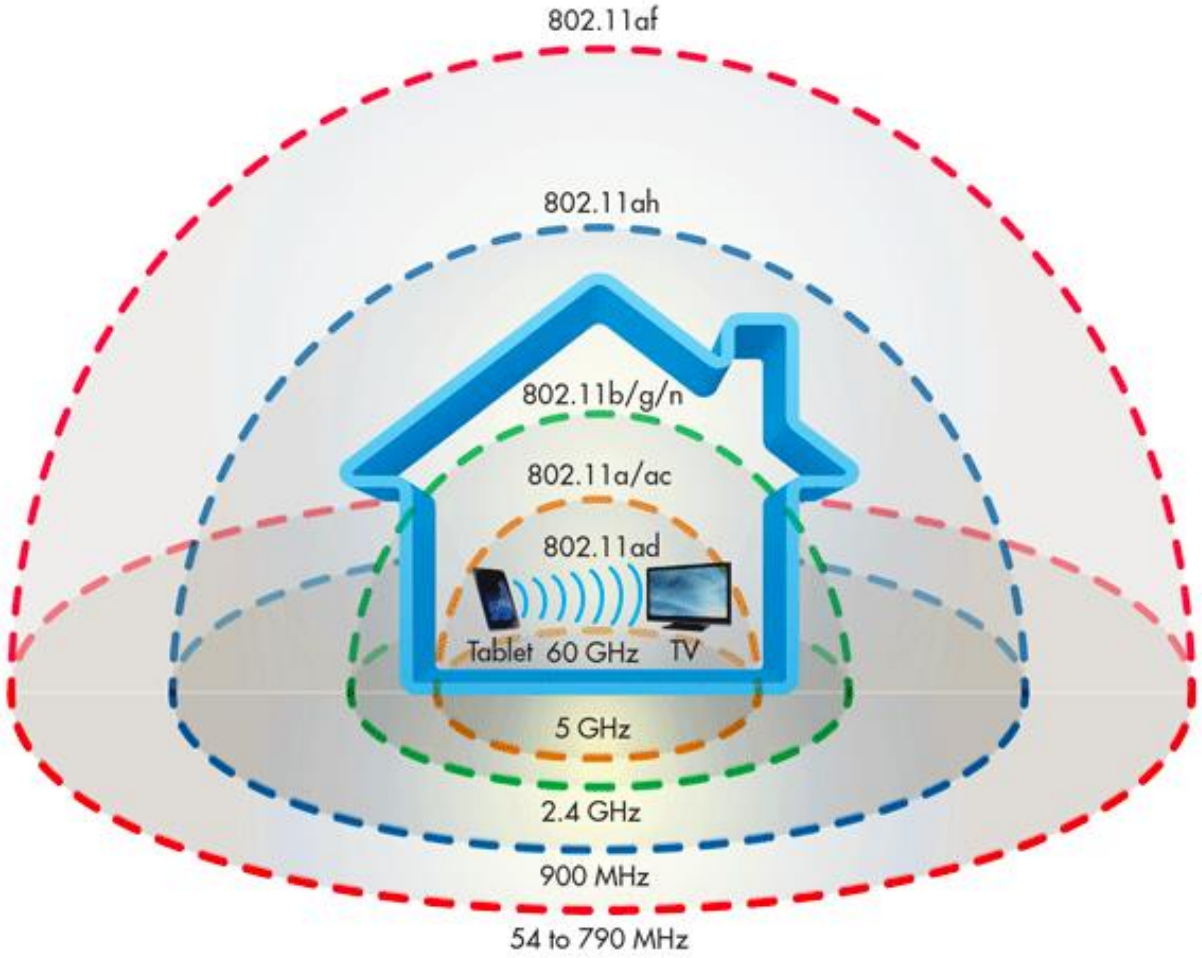
IEEE 802.11ah-Physical Layer

- IEEE 802.11ah essentially provides an additional 802.11 physical layer operating in unlicensed sub-GHz bands.
  - 868–868.6 MHz for EMEAR, 0.6 MHz
  - 902–928 MHz and associated subsets for North America and Asia-Pacific regions
  - 314–316 MHz, 430–434 MHz, 470–510 MHz, and 779–787 MHz for China.

IEEE 802.11ah-Physical Layer

- Based on OFDM modulation, IEEE 802.11ah uses channels of 2, 4, 8, or 16 MHz (and also 1 MHz for low-bandwidth transmission).
  - This is one-tenth of the IEEE 802.11ac channels, resulting in
    - one-tenth of the corresponding data rates of IEEE 802.11ac (The IEEE 802.11ac standard is a high-speed wireless LAN protocol at the 5 GHz band that is capable of speeds up to 1 Gbps)
  - While 802.11ah does not approach this transmission speed (as it uses one tenth of 802.11ac channel width, it reaches one-tenth of 802.11ac speed), it does provide an extended range for its lower speed data.
  - For example, at a data rate of 100 kbps, the outdoor transmission range for IEEE 802.11ah is expected to be 1 km.

Physical and Link Layers Protocols- IEEE 802.11ah



IEEE 802.11ah-MAC Layer

- More efficient to deal with errors at the MAC level than higher layer (such as TCP)

- **Frame exchange protocol**
  - Source station transmits data
  - Destination responds with acknowledgment (ACK)
  - If source doesn‘t receive ACK, it retransmits frame

- **Four frame exchange**
  - Source issues request to send (RTS)
  - Destination responds with clear to send (CTS)
  - Source transmits data
  - Destination responds with ACK

IEEE 802.11ah-MAC Layer

- The 802.11ah MAC layer is focused on
  - power consumption and mechanisms to allow low-power Wi-Fi stations to wake up less often and operate more efficiently.
  - providing low power consumption and the ability to support a larger number of endpoints.
  - This sort of MAC layer is ideal for IoT devices that often produce short, low-bit-rate transmissions.

Physical and Link Layers Protocols- IEEE 802.11ah

- IEEE 802.11ah
  - Topology
    - Star
    - Mesh (relay networks)
  - تموم شدن شرت رنج!