Comparison of ZigBee and other IoT Protocols

Focus of this document: Physical Layer Comparison.

IEEE 802.15.4 Physical Layer (used by Zigbee)

* Supports three frequency bands: 2450 MHz band (with 16 channels), 915 MHz band (with 10 channels) and 868 MHz band (1 channel).
* All bands use the DSSS (Direct Sequence Spread Spectrum) Access Mode.
* 2450 MHz band coincides with what is used by Wifi.

PHY Protocol Data Units

The PHY Protocol Data Unit (PPDU) – The protocol data unit that encloses the MAC Frames sent to the PHY as a PHY Service Data Unit (PSDU).

Each PPDU consists of the SHR, PHR and PSDU.

SHR – Synchronization Header.

Allows the receiving device to synchronize and lock into the bit stream.

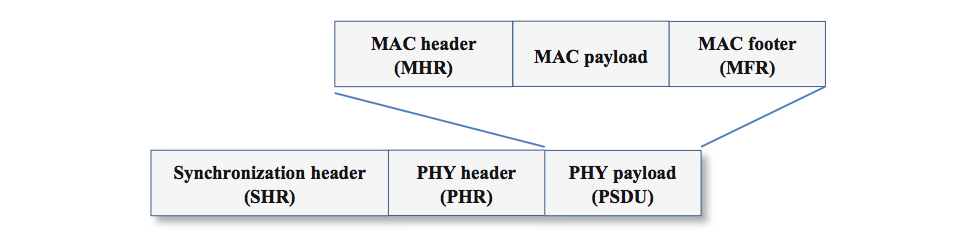
PHR – Physical Header

Contains the Frame Length information.

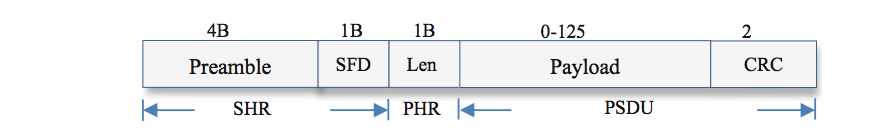
PSDU - PHY Service Data Unit

A variable length payload which carries the MAC sub-layer frame.

Schematic view of a PPDU



PPDU Frame Structure



The Synchronization Header consists of two parts: the Preamble and SFD (Start of Frame Delimiter).

* The Preamble:
  + sequence consists of 32 zeroes, all 4 bytes as 0x00.
  + It is used for chip and symbol synchronization at the receiver part of the transceiver.
* The SFD (Start of Frame Delimiter Field):
  + follows the Preamble and is 8-bits/ 1 byte in size.
  + The SFD indicates the end of the SHR and beginning of the packet data.
  + SFD is set to 0x7A.
  + At the receiver side, an 802.15.4 radio synchronizes to incoming zero symbols, and searches for the SFD sequence to receive incoming packets.
* The PHR (Physical Header Field):
  + It includes a 1-byte length field that describes the number of bytes in the packet’s payload, including the 2-byte CRC
  + The payload is the frame sent by the MAC sub-layer.
* The PSDU (PHY service data unit) Field:
  + This field consists of two parts: the payload and the CRC.
  + The PSDU consists of the PHY packet but the payload is transferred from the MAC sub-layer. The payload is of variable length.
  + The length of the payload can be anything from 0-125 bytes and the CRC field is of 2-bytes in size.
  + CRC stands for Cyclic Redundancy Check and is used for detecting accidental changes to raw data.
  + Hence, the maximum size of the PSDU field is 127 bytes.

Adding the lengths of all of the above fields, headers and payload we see that the maximum size of the PPDU (PHY Protocol Data unit) is 133 bytes.

The IEEE 802.15.4 standard mandates the size of the preamble to be 4 bytes, but some radios like the CC2420 allow the preamble to be up to 17 bytes.

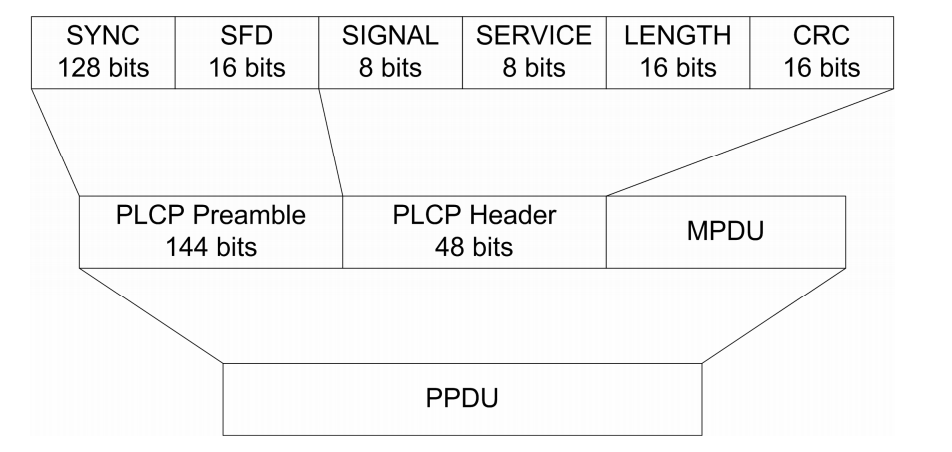
Source: <http://www.springer.com/cda/content/document/cda_downloaddocument/9783319478050-c2.pdf?SGWID=0-0-45-1593332-p180328094>

802.11 Standard (Wi-Fi) Physical Layer

DSSS PHY (Direct Sequence Spread Spectrum Physical Layer)

This layer delvers frames at 1, 2, 5.5 and 11 Mbps rates in the 2.4 GHz band.

DSSS PLCP Protocol Data Unit (PPDU) Structure

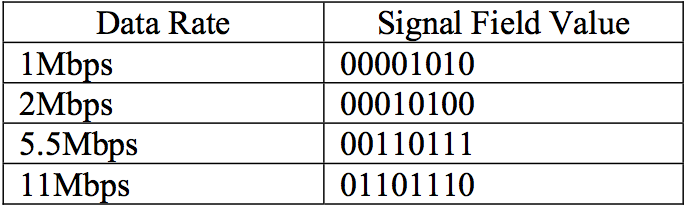
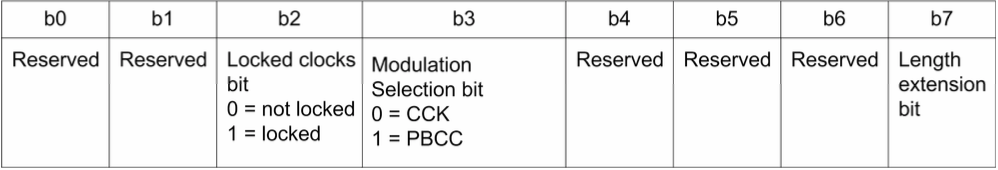


* The above structure shows the Long Preamble format where 144 bits are used for the preamble.
* The MPDU is the equivalent of the PSDU - PHY Service Data Unit (seen in the standard 802.15.4 above). This is the payload which encloses the MAC Frame.
* The Preamble enables the receiver to synchronize to the incoming signal properly before the actual content of the frame arrives.
* The Header provides information about the frame.
* MPDU (MAC Protocol Data Unit) transmitted by the station consists of the actual frame sent by the MAC layer to the PHY layer.

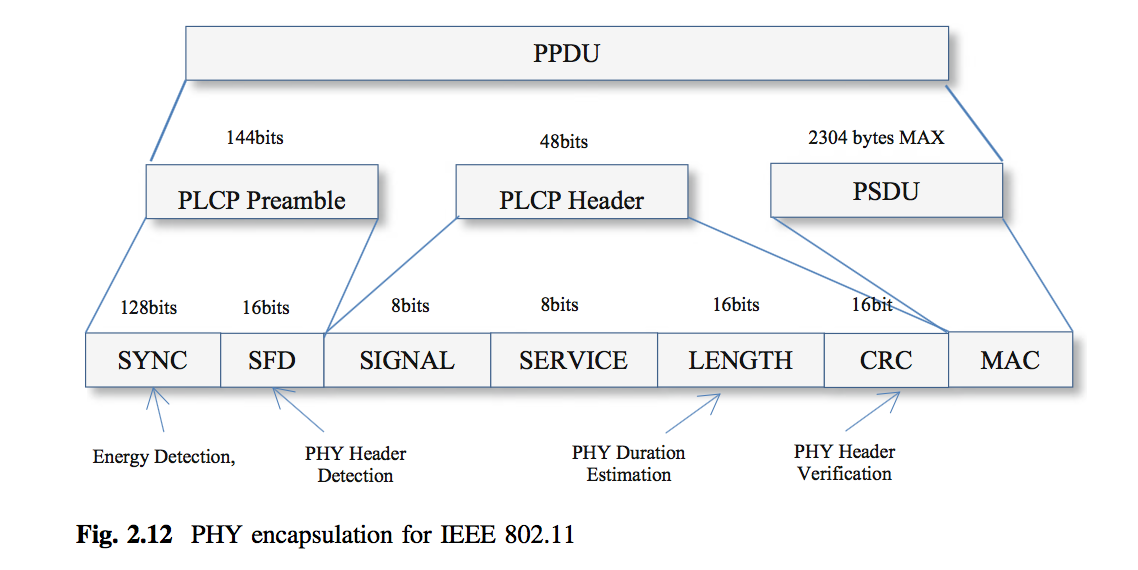
The Preamble

* Consists of two parts: The Synchronization (Sync) field and Start Frame Delimiter (SFD) field.
* The Sync Field: alerts the receiver that there is an incoming receivable signal. The receiver then sync to this signal. Even if the receiver does not receive the entire sync field but just a few bits of the pattern, it is okay. All the receiver needs to do is to sync with the signal before the SFD field arrives.
* SFD (Start Frame Delimiter): Defines the beginning of a frame. Pattern of this field is always 1111001110100000 when using long preambles and reversed when using short preambles. Patterns unique to DSSS PLCP.

The Header (48 bits):

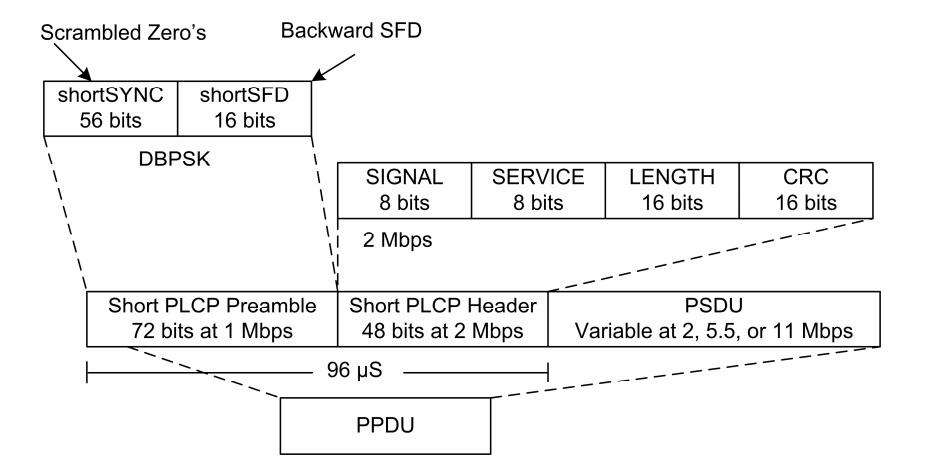
* Signal Field (8 bits):
  + Identifies the type of modulation that the receiver must use to demodulate the signal.
  + Value of the field = Data Rate/ 100 kbps
  + 
* Service Field (8 bits):
  + 802.11 (original standard) reserved the Service Field for future use.
  + 00000000 means 802.11 compliance.
  + The 802.11b standard made use of the Service Field as below:
  + 
* Length field (16 bits):
  + Depending on the modulation technique, this field may signify different things.
  + OFDM: Length field = No. of octets to transfer between the MAC and the PLCP layer.
  + DSSS: No. of microseconds required to transmit the payload.
* CRC field (16 bits):
  + CRC: Cyclic Redundancy Check
  + Used to verify if the message is corrupted.
  + Mechanism: divide a binary message by a fixed binary number. Remainder is the checksum or more commonly the CRC.

Another great high level view:



802.11b, DSSS PLCP Protocol Data Unit (PPDU) Structure, Short Preamble

The 802.11b introduced the option a short preamble. It also enabled transmission at higher speeds of 5.5 Mbps and 11 Mbps.



5G: Layer 1 specifications may not have been decided yet.

<https://www.theregister.co.uk/2017/02/24/the_final_5g_technical_performance_specs_have_been_set/>

WirelessHART Physical Layer

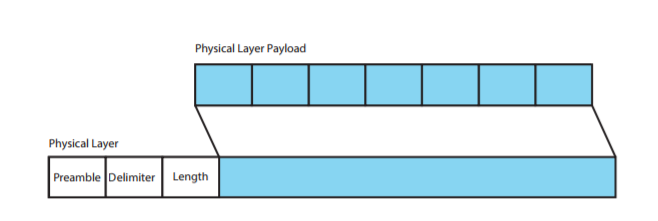


Fig: Physical Layer PDU

The physical Layer defines the electrical and physical level relationship between a node and a physical medium. It defines characteristics such as antenna, air medium, power level, timing of voltage changes, physical data rates, maximum transmission distances, etc. The WirelessHART standard is based on the IEEE 802.15.4 standard. WirelessHART physical layer is a much simplified subset of that defined in the IEEE 802.15.4 standard.

WirelessHART supports RF frequency band of 2400-2483.5 MHz license-free ISM band with a data rate of up to 250 kbits/s. The channels supported here are from 11 to 26, with a 5MHz gap between two adjacent channels.

The various fields in the WirelessHart Physical Layer Header are:

1. Preamble - The preamble consists of a 56-bit (seven-byte) pattern of alternating 1 and 0 bits, allowing devices on the network to easily synchronize their receiver clocks, providing bit-level synchronization. It is followed by the SFD to provide byte-level synchronization and to mark a new incoming frame.
2. Delimiter – The Start of the Frame Delimiter (SFD) is a eight-bit (one-byte) value that marks the end of the preamble and indicates the beginning of the frame. The SFD is designed to break the bit pattern of the preamble and signal the start of the actual frame
3. Length – Indicates the length of the PayLoad.
4. PayLoad - IEEE compliant Physical Layer PDU, Maximum payload 127 bytes.

For any WirelessHART device:

• There are only one or two IEEE 802.15.4 messages per 10ms timeslot (broadcast messages are not acknowledged).

• The closest time between two messages is between the two messages within a timeslot, 1ms from the end of the message to the start of the acknowledgement message.

• All WirelessHART messages are IEEE 802.15.4 messages of data type.

• Only the 2.4GHz frequency band is defined for WirelessHART.

• Channels 11-25 can be used with the WirelessHART standard. Channel 26, which is not legal in many locales, is not supported.

In summary, the WirelessHART physical layer limits itself to transmitting and receiving IEEE 802.15.4 data messages. The noticeable items in WirelessHART physical layer are:

• Channel hopping. In WirelessHART physical channel is changed each transmission.

• Transmit power. The IEEE 802.15.4 standard is defined for personal area network with personal operating space of 10 meters. WirelessHART mesh covers a relatively larger area. All devices must provide a nominal EIRP of +10dBm (10mW) ±3dB. The transmit power is programmable from -10dBm to +10dBm.

• Data Rate : 250KBPS (62.5 KBAUD)  
• Operating Frequency : 2400-2483.5 MHz  
• Modulation : O-QPSK; Direct Sequence Spread Spectrum (DSSS)  
• Transmit Power : about 10dBm adjustable in discrete steps (e.g., 0dBM and others).

The maximum outdoor line of sight transmission distance could be 100 meters.

LoRa and ZigBee:

Frequency Bands:

LoRa -> The LoRa wireless system makes use of the unlicensed frequencies that are available worldwide. The most widely used frequencies / bands are:

* 868 MHz for Europe
* 915 MHz for North America
* 433 MHz band for Asia

Using lower frequencies than those of the 2.4 or 5.8 GHz ISM bands enables much better coverage to be achieved especially when the nodes are within buildings.

Although the sub-1GHz ISM bands are normally used, the technology is essentially frequency agnostic and can be used on most frequencies without fundamental adjustment.

ZigBee -> Supports three frequency bands: 2450 MHz band (with 16 channels), 915 MHz band (with 10 channels) and 868 MHz band (1 channel).

Coverage Distance:

LoRa -> 2-5 Km (urban areas), 15 Km (suburban areas)

ZigBee -> 10 to 100 meters

Modulation Technique:

LoRa -> LoRa modulation (CSS modulation) , FSK or GFSK

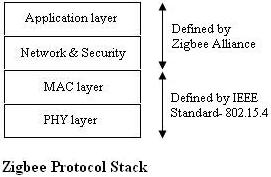
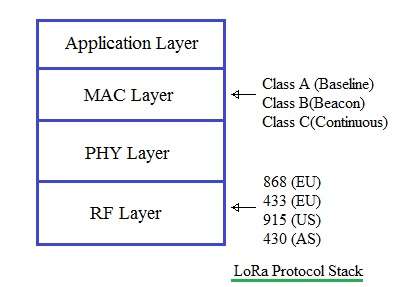
ZigBee -> BPSK, OQPSK modulation. Also uses DSSS technique to convert bits to chips.

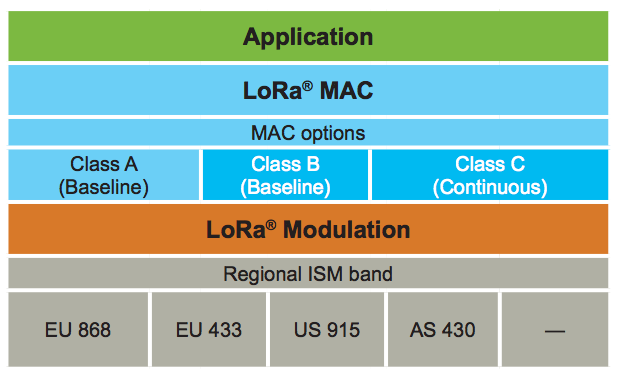
Data Rate:

LoRa -> Adaptive Link (0.3 to 22 Kbps (LoRa modulation) and 100 Kbps (using GFSK))

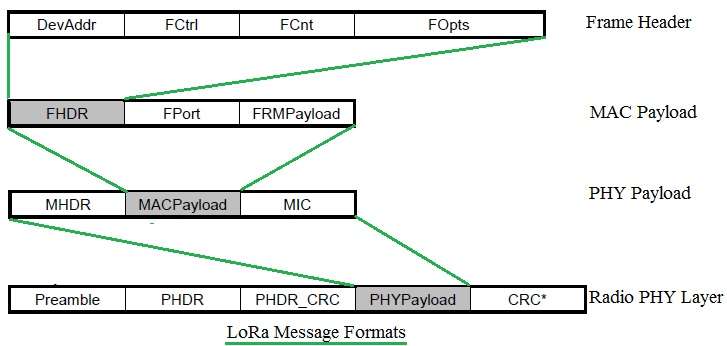
The fact that only low data rates are used, and low levels of overall data transfer means that low bandwidths are required. A variety of bandwidths are available: 7.8 kHz; 10.4 kHz; 15.6 kHz; 20.8 kHz; 31.2 kHz; 41.7 kHz; 62.5 kHz; 125 kHz; 250 kHz; 500 kHz. The required bandwidth can be selected according to the data requirements as well as the link conditions.

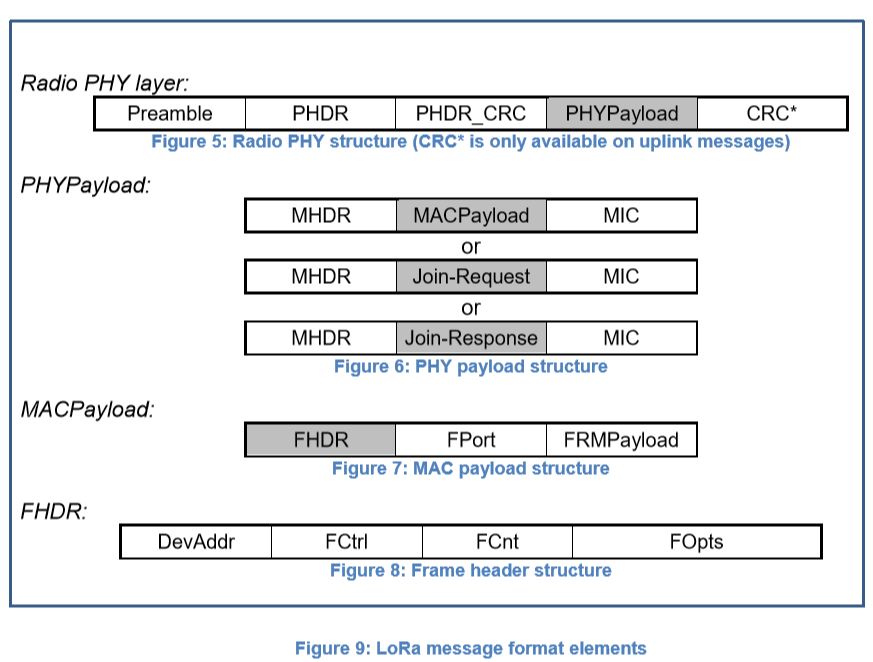
ZigBee -> 20 kbps (868 MHz band) , 40Kbps (915 MHz band ) , 250 kbps (2450 MHz band)

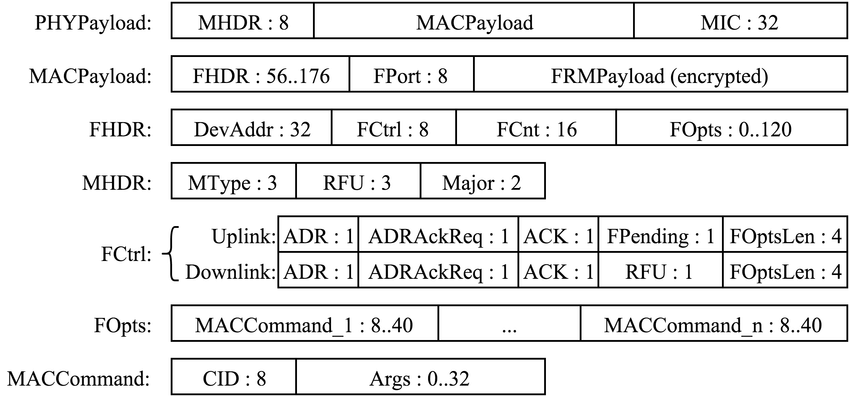
 

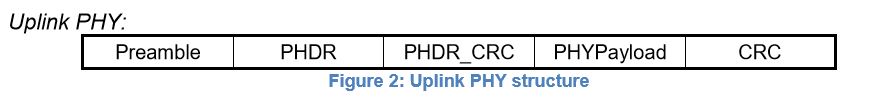


RF Layer PHY Layer MAC Layer









* Uplink messages are sent by end-devices to the network server relayed by one or many

gateways.

* Uplink messages use the LoRa radio packet explicit mode in which the LoRa physical

header (PHDR) plus a header CRC (PHDR\_CRC) are included. The integrity of the payload

is protected by a CRC.

* The PHDR, PHDR\_CRC and payload CRC fields are inserted by the radio transceiver.

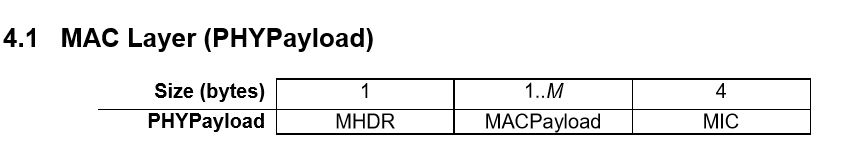


* Each downlink message is sent by the network server to only one end-device and is

relayed by a single gateway.

* Downlink messages use the radio packet explicit mode in which the LoRa physical header

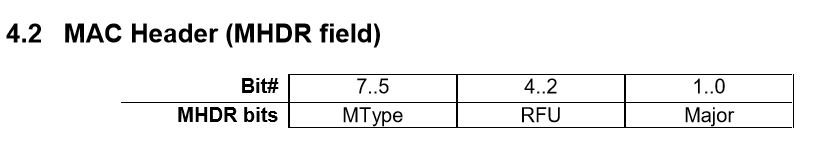
(PHDR) and a header CRC (PHDR\_CRC) are included.

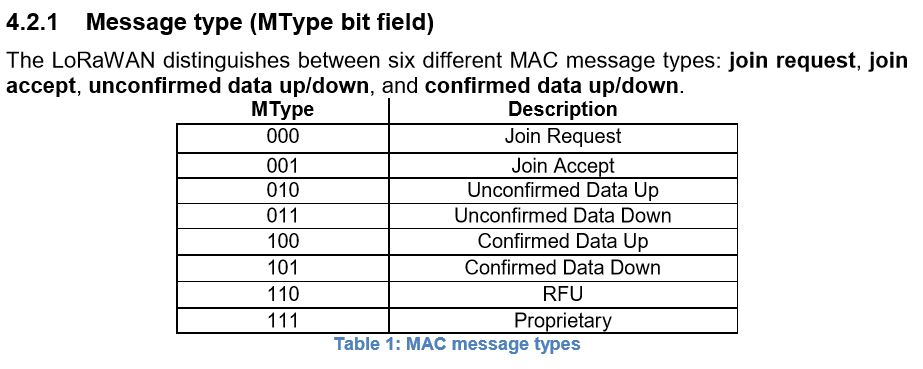


MHDR = MAC Header -> 8 bits

MIC = Message Integrity Code -> 32 bits

The maximum length (M) of the MACPayload field is region specific

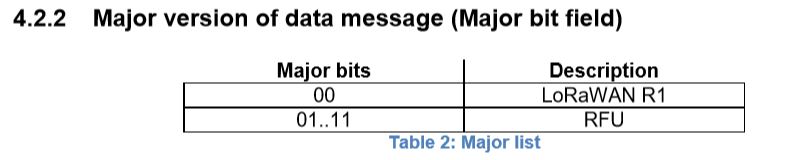




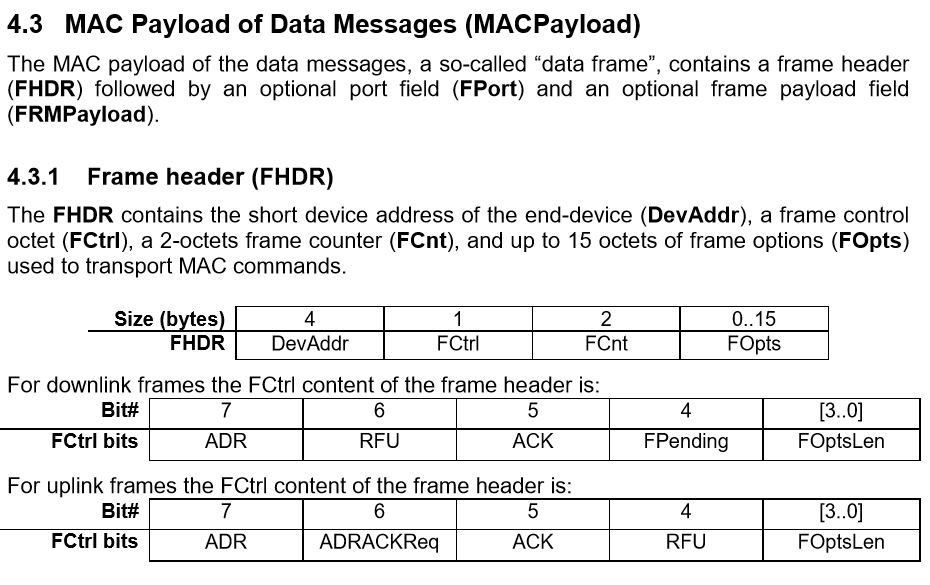
**Proprietary** **messages** can be used to implement non-standard message formats that are not interoperable with standard messages but must only be used among devices that have a common understanding of the proprietary extensions.

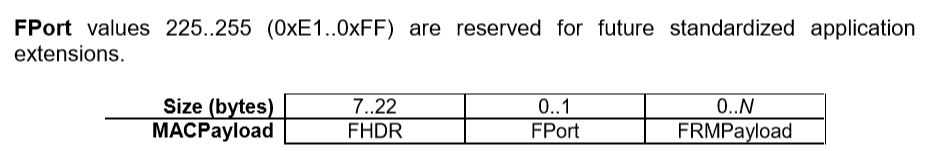
RFU = Reserved for Future Use

Message integrity is ensured in different ways for different message types.



The Major version specifies the format of the messages exchanged in the join procedure and the first four bytes of the MAC Payload. For each major version, end-devices may implement different minor versions of the frame format. The minor version used by an end-device must be made known to the network server beforehand using out of band messages.



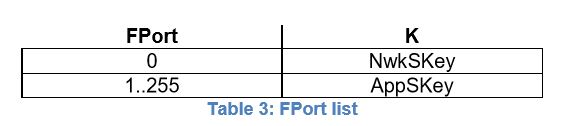


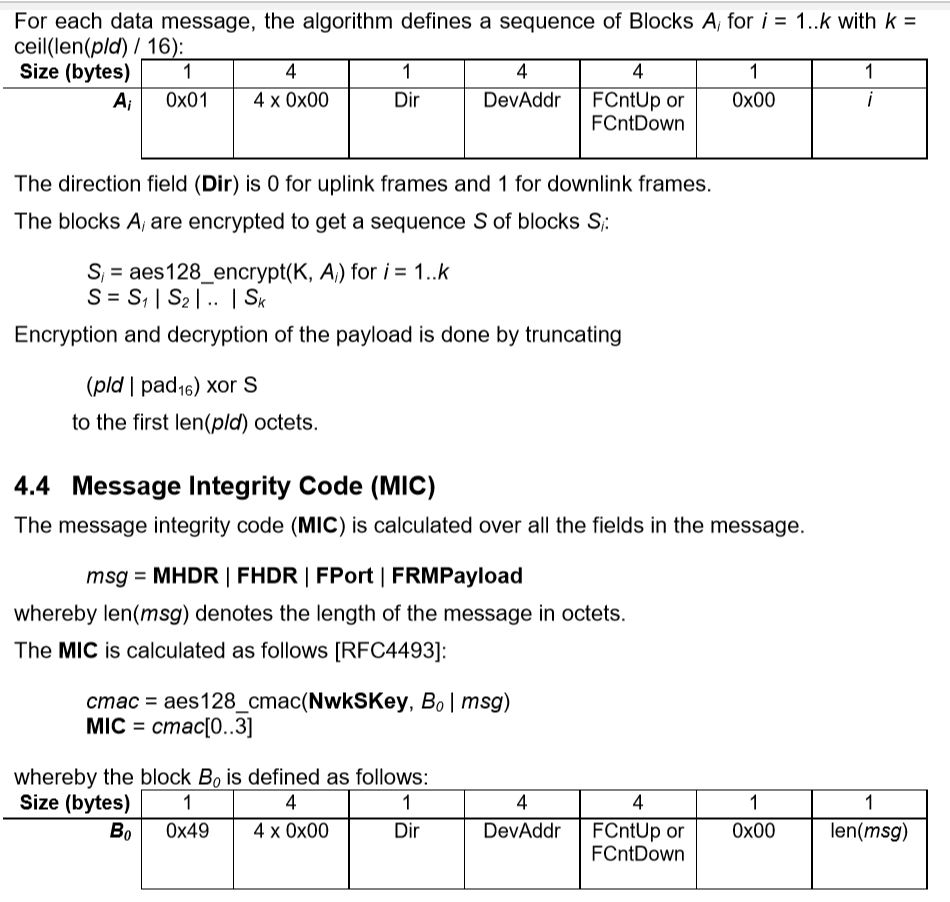
N is the number of octets of the application payload. The valid range for N is region specific and is defined in the LoRaWAN Regional Parameters document.

If a data frame carries a payload, FRMPayload must be encrypted before the message integrity code (MIC) is calculated.

The encryption scheme used is based on the generic algorithm described in IEEE 802.15.4/2006 Annex B [IEEE802154] using AES with a key length of 128 bits.

The key K used depends on the FPort of the data message:





The direction field (Dir) is 0 for uplink frames and 1 for downlink frames.

**MAC Commands**

For network administration, a set of MAC commands may be exchanged exclusively between the network server and the MAC layer on an end-device. MAC layer commands are never visible to the application or the application server or the application running on the end-device.

A single data frame can contain any sequence of MAC commands, either piggybacked in the **FOpts** field or, when sent as a separate data frame, in the **FRMPayload** field with the **FPort** field being set to 0. Piggybacked MAC commands are always sent without encryption and must not exceed 15 octets.

MAC commands sent as FRMPayload are always encrypted and must not exceed the maximum FRMPayload length.

**Note:** MAC commands whose content shall not be disclosed to an eavesdropper must be sent in the FRMPayload of a separate data message.

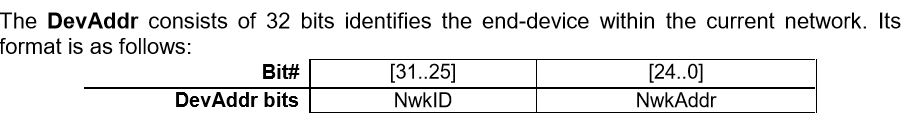
A MAC command consists of a command identifier (CID) of 1 octet followed by a possibly empty command-specific sequence of octets.

**Activation of end-devices:**

**Data Stored in the End-device after Activation:**

After activation, the following information is stored in the end-device: a device address (**DevAddr**), an application identifier (**AppEUI**), a network session key (**NwkSKey**), and an application session key (**AppSKey**).

**6.1.1 End-device address (DevAddr)**



* The most significant 7 bits are used as network identifier (**NwkID**) to separate addresses of territorially overlapping networks of different network operators and to remedy roaming issues.
* The least significant 25 bits, the network address (**NwkAddr**) of the end-device, can be arbitrarily assigned by the network manager.

**6.1.2 Application identifier (AppEUI)**

* The AppEUI is a global application ID in IEEE EUI64 address space that uniquely identifies the entity able to process the **JoinReq** frame.
* The AppEUI is stored in the end-device before the activation procedure is executed.

**6.1.3 Network session key (NwkSKey)**

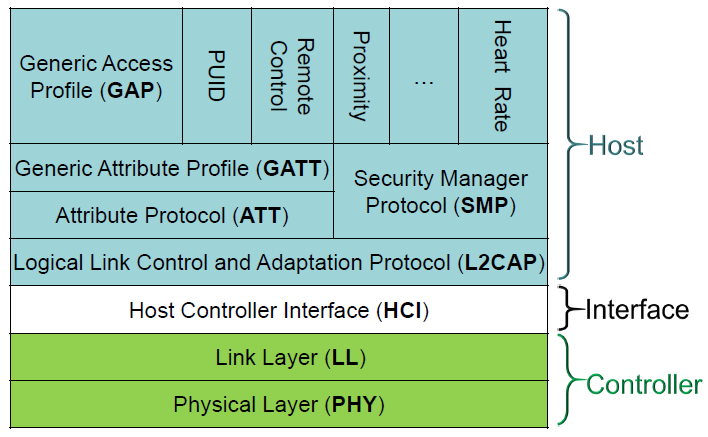
* The NwkSKey is a network session key specific for the end-device. It is used by both the network server and the end-device to calculate and verify the MIC (message integrity code) of all data messages to ensure data integrity.
* It is further used to encrypt and decrypt the payload field of a MAC-only data messages.

**6.1.4 Application session key (AppSKey)**

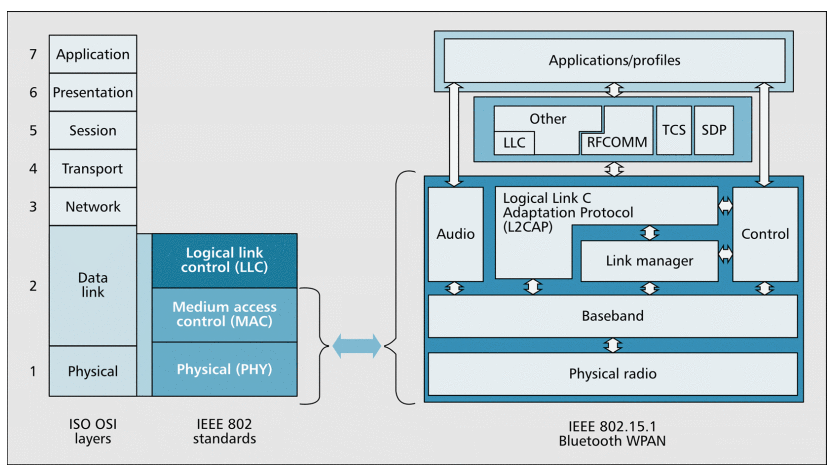
* The AppSKey is an application session key specific for the end-device.
* It is used by both the application server and the end-device to encrypt and decrypt the payload field of application-specific data messages.
* Application payloads are end-to-end encrypted between the end-device and the application server, but they are not integrity protected.

BLUETOOTH LOW ENERGY

BLE Protocol Stack



Bluetooth Protocol Stack in comparison with OSI layers



Controller:

Physical Layer (PHY):

It contains the analog communications circuitry used for modulating and demodulating analog signals and transforming them into digital symbols.

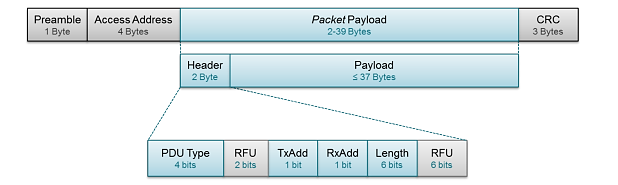
BLE can communicate over 40 channels from 2.4000 GHz to 2.4835 GHz.

Channels 0-36 - They are used for connection data

Channels 37, 38, and 39 - They are used as advertising channels to set up connections and send broadcast data.

**Frequency Hopping Spread Spectrum (FHSS)** - In this technique the radio hops between channels on each connection event. The value of the hop is communicated when the connection is established, so it is different for every new established connection based on the range of the receiver device. Therefore, FHSS minimizes the effect of any radio interference.

BLE Data Packet



* Preamble – It is a 1 byte value used for synchronization and timing estimation at the receiver. It will always be 0xAA for broadcasted packets.
* Access Address - It is also fixed for broadcasted packets, set to 0x8E89BED6.
* Packet payload - It consists of a header and payload.
* Header - It describes the packet type.
* PDU Type - It defines the purpose of the device.

For broadcasting applications, there are three different PDU Types, as shown in the table below,

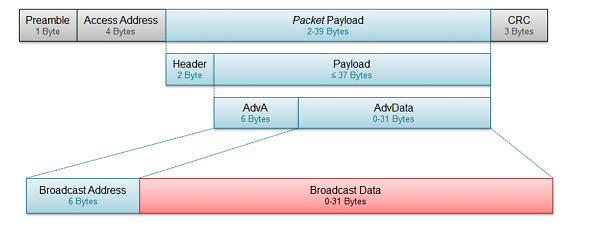
ADV\_IND and ADV\_NONCONN\_IND have been described previously (as connectable and non-connectable).

ADV\_SCAN\_IND is simply a non-connectable broadcaster that can provide additional information by scan responses.

|  |  |  |
| --- | --- | --- |
| PDU Type | Packet Name | Description |
| 0000 | ADV\_IND | Connectable undirected advertising event |
| 0010 | ADV\_NONCONN\_IND | Non-connectable undirected advertising event |
| 0110 | ADV\_SCAN\_IND | Scannable undirected advertising event |

* TxAdd bit - It indicates whether the advertiser's address (contained in the Payload) is public (TxAdd = 0) or random (TxAdd = 1).
* RxAdd - It is reserved for other types of packets not covered in this application note, as they do not apply to beacons.
* Radio Frequency Unit (RFU) - It a 6 bit field to define the radio frequency.
* Cyclic Redundancy Check (CRC) - It is an error-detecting code used to validate the packet for unwanted alterations. It ensures data integrity for all transmitted packets over the air.

BLE Broadcast Data Packet

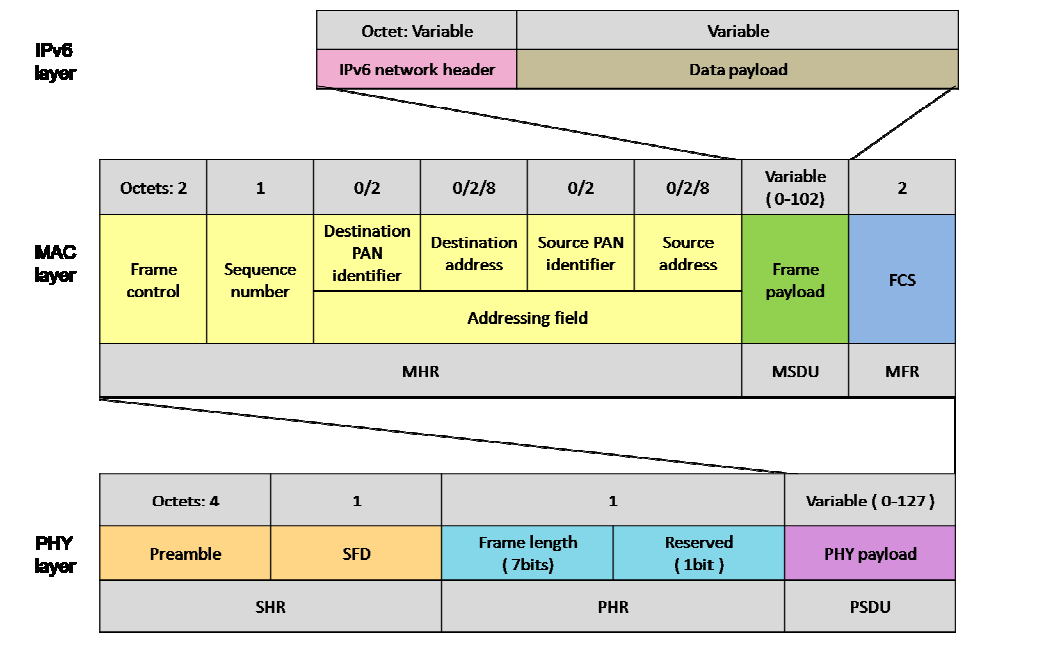


| Standard | Zig Bee | Bluetooth |
| --- | --- | --- |
| IEEE specification | 802.15.4 | 802.15.1 |
| Frequency band | 868/915MHz; 2.4 GHz | 2.4 GHz |
| Max signal rate | 250Kb/s | 1Mb/s |
| Nominal range | 10–100 m | 10m |
| Transmission power | 20 dBm | 0–10 dBm |
| Number of RF channels | 1/10;16 | 79 |
| Channel bandwidth | 0.3/0.6MHz; 2 MHz | 1 MHz |
| Modulation type | BPSK (+ ASK), O-QPSK | GFSK |
| Spreading | DSSS | FHSS |
| Coexistence mechanism | Dynamic freq. selection | Adaptive freq. hopping |
| Basic cell | Star | Piconet |
| Extension of the basic cell | Cluster tree, Mesh | Scatternet |
| Max number of cell nodes | >65000 | 8 |
| Encryption | AES block cipher(CTR, counter mode) | EO stream cipher |
| Authentication | CBC-MAC (ext. of CCM) | Shared secret |
| Data protection | 16-bit CRC | 16-bit CRC |

6LowPAN Physical layer

6LoWPAN is an open standard defined in RFC 6282 by the Internet Engineering Task Force (IETF), the standards body that defines many of the open standards used on the Internet such as UDP, TCP and HTTP to name a few. A powerful feature of 6LoWPAN is that while originally conceived to support IEEE 802.15.4 low-power wireless networks in the 2.4-GHz band, it is now being adapted and used over a variety of other networking media including Sub-1 GHz low-power RF, Bluetooth® Smart, power line control (PLC) and low-power Wi-Fi®.

The physical layer converts data bits into signals that are transmitted and received over the air. In the 6LoWPAN example, IEEE 802.15.4 is used. In addition to the well-rounded 2006 version of the standard, two important amendments exist: e and g. IEEE 802.15.4e is a MAC amendment and provides enhancements such as time slotted channel hopping (TSCH) and coordinated sampled listening (CSL). Both enhancements aim to further lower the power consumption and make the interface more robust. The IEEE 802.15.4g is a PHY (or physical layer) amendment and aims to provide an additional range of radio frequency bands to enable worldwide use even in the Sub-1 GHz frequency bands.



* MSDU- MAC service data unit
* MHR - MAC header
* MFR – MAC footer
* FCS – frame check sequence
* PSDU – physical service data unit
* SHR – synchronization header
* PHR – physical header – frame length info.
* SFD- start of frame delimiter

The pervasive nature of IP networks allows use of existing infrastructure. IP-based technologies already exist, are well-known, and proven to be working. Open and freely available specifications vs. closed proprietary solutions. Tools for diagnostics, management, and commissioning of IP networks already exist. IP-based devices can be connected readily to other IP-based networks, without the need for intermediate entities like translation gateways or proxies.

How Signal Modulation Affects Bandwidth?

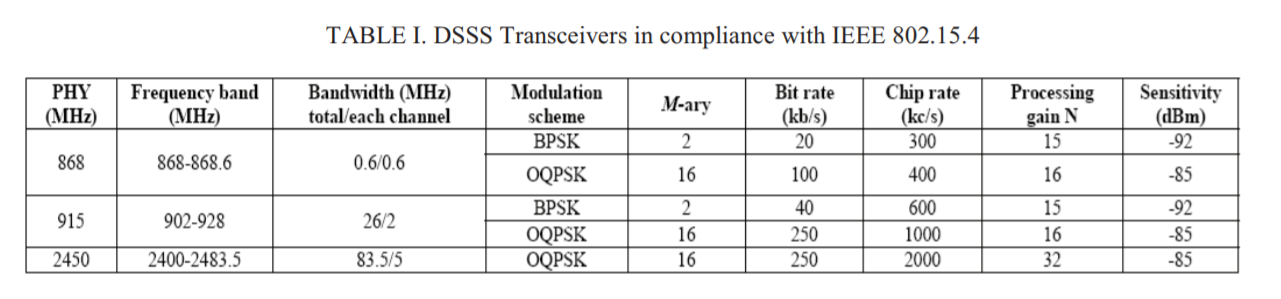
# How Signal Modulation affects Data Rate?

The WirelessHART Physical Layer (PHY) is based on the IEEE 802.15.4 PHY. Unlike IEEE 802.15.4, WirelessHART only defines operation in the 2.4 GHz band, employing **Direct Sequence Spread Spectrum (DSSS) and Offset-Quadrature Phase Shift Keying (OQPSK)** modulation.

**This allows for a bit rate of 250 Kbit/s.**

Similarly, ZigBee uses BPSK or OQPSK modulation and uses DSSS technique to convert bits to chips. Hence, **ZigBee also has a maximum data rate of 250 Kbits/sec**.

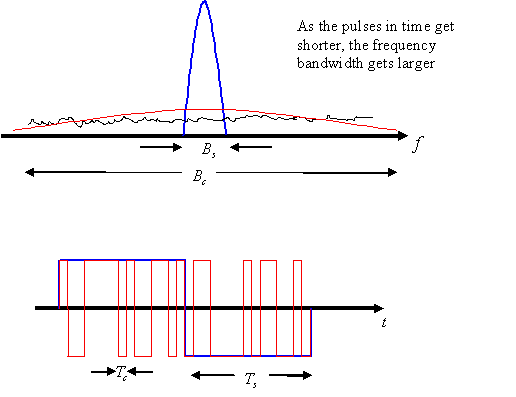
WirelessHART uses only 15 of the 16 channels defined by the IEEE 802.15.4; which is channel number 11 to 25. Channel 26 is not included in the WirelessHART specification since it, due to national regulations, is not legal to use in some countries. The WirelessHART channels each utilize a bandwidth of 3 MHz and they are uniformly distributed 5 MHz apart throughout the frequency band to ensure nonoverlapping communication.



**Source:** <http://ieeexplore.ieee.org.libproxy.utdallas.edu/document/5686062/?reload=true>

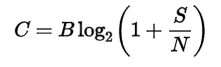
### Direct Sequence Spread Spectrum (DSSS)

Direct sequence spread spectrum (DSSS) introduces rapid phase transition to the data making it larger in bandwidth. As the period T of a signal gets shorter in time (or rate R increases), the bandwidth B of the signal increases: R = 1/T = 2B (Nyquist Rate)  
The following figures explain it

  
***Figure 3: Rate and period are related to bandwidth by when pulse shaping is used.***

Shannon’s Theorem:

The Shannon–Hartley theorem states the channel capacity C, meaning the theoretical tightest upper bound on the information rate of data that can be communicated at an arbitrarily low error rate using an average received signal power S through an analog communication channel subject to additive white Gaussian noise of power N:



Where:

C is the **channel capacity** in bits per second, a theoretical upper bound on the net bit rate (information rate, sometimes denoted I) excluding error-correction codes;

B is the **bandwidth** of the channel in hertz (passband bandwidth in case of a bandpass signal);

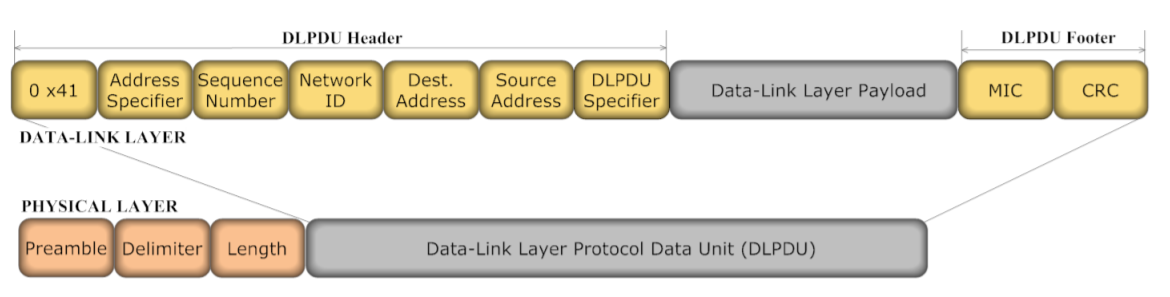
S is the average received signal power over the bandwidth (in case of a carrier-modulated passband transmission, often denoted C), measured in watts (or volts squared);

N is the average power of the **noise** and interference over the bandwidth, measured in watts (or volts squared); and

S/N is **the signal-to-noise ratio** (SNR) or the carrier-to-noise ratio (CNR) of the communication signal to the noise and interference at the receiver (expressed as a linear power ratio, not as logarithmic decibels).

# LAYER 2

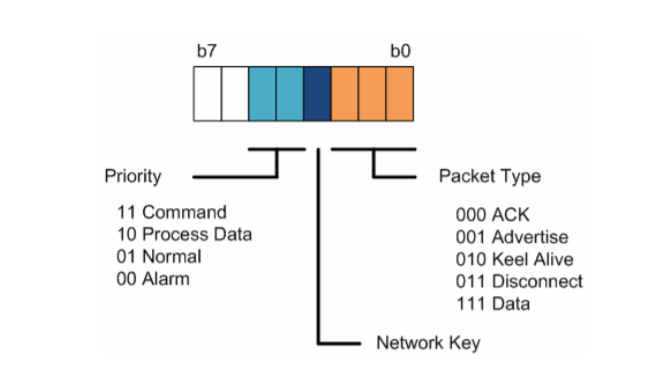
**WIRELESSHART PROTOCOL:**

****

* Each Data-Link packet (DLPDU) consists of the following fields:
* A single byte set to 0x41
* A 1-byte address specifier
* 1-byte Sequence Number
* 2 byte Network ID
* Destination and Source Addresses either of which can be 2 or 8-bytes long
* A 1-byte DLPDU Specifier
* The DLL payload
* A 4-byte keyed Message Integrity Code (MIC)
* A 2-byte CRC16

1. **0x41** - Since security is an essential part of the WirelessHART protocol, bit four of the first byte is set to indicate that an IEEE 802.15.4-2006 security is enabled
2. **Address Specifier**: One Byte Field. The first byte alongside with an Address Specifier field is an IEEE 802.15.4 Frame Control Field.
3. **Sequence Number**: Each frame is assigned a unique consecutive sequence number, and the receiver uses the numbers to place received frames in the correct order. Length is one byte.
4. **Dest Address:** MAC Address of the destination node.
5. **Src Address:** MAC address of the source node.
6. **MIC** - A keyed Message Integrity Code (MIC) is used for link-layer authentication of DLPDU. Devices shall reply only to unicast, non-acknowledgement DLPDUs that have been successfully authenticated.

**DLPDU Frame Types**



The TDMA Data Link Layer Specification defines five WirelessHART frame types:

1. **Acknowledgment DLPDU** - ACK DLPDUs are the immediate link level response to receipt of the source device’s transmission DLPDU

2. **Advertise DLPDU** - Advertise DLPDUs provide information to neighboring devices wishing to join the network

3. **Keep-Alive DLPDU** - Keep-Alive DLPDUs facilitate connection maintenance between neighboring devices.

4. **Disconnect DLPDU** - Disconnect DLPDUs are used to advise neighboring devices that the device is leaving the network

5. **Data DLPDU** - Data DLPDUs contain network and device data in transit to their final destination device

**BLUETOOTH LOW ENERGY**

**(BLE)**

**Link Layer:**

The Link Layer is the part that directly interfaces with the physical layer, and it is usually implemented as a combination of custom hardware and software. The Link Layer defines following roles for it’s devices, based on logical groups:

**Advertiser** – A device sending advertising packets

**Scanner** – A device scanning for advertising packets.

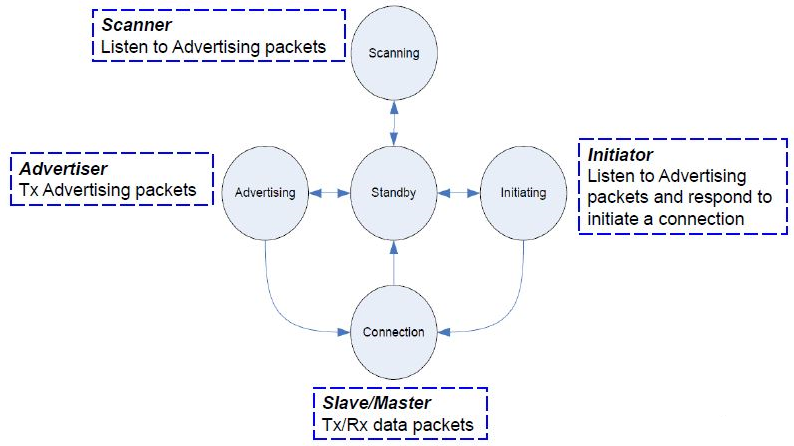
**Master** – A device that initiates a connection and manages it later.

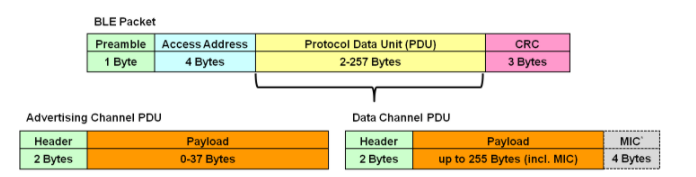
**Slave** – A device that accepts a connection request and follows the master’s timing.

**Bluetooth Device Address – It is a 48-bit number which uniquely identifies a device among peers.**

The Link Layer is also in charge of establishing **connections;**it filters out advertising packets depending on the Bluetooth address or based on the data itself. It also manages the **connection interval ie, time between the beginning of two consecutive connection events.**

The link layer can also configure **Encryption**, which is highly desirable in case of a lot of devices present in the same range.

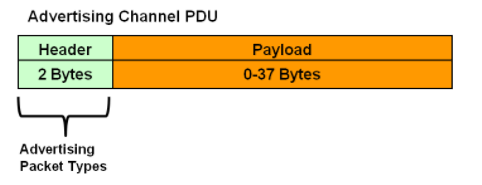




**1. Advertising channel PDU:**

It serves two purposes:

* Broadcast data for applications that do not require a full connection
* Discover slaves in the network and connect to them



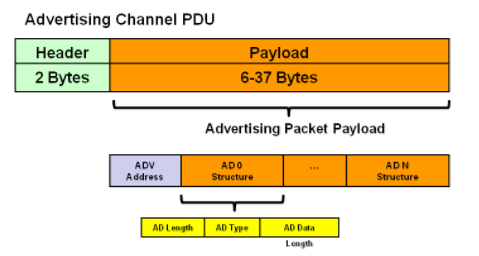
There are seven advertising channel PDU types with a different payload format and function:

* **Advertising PDUs -** ADV\_IND, ADV\_DIRECT\_IND, ADV\_NONCONN\_IND, ADV\_SCAN\_IND
* **Scanning PDUs -** SCAN\_REQ, SCAN\_RSP
* **Initiating PDUs -** CONNECT\_REQ

|  |  |
| --- | --- |
| **Packet Name** | **Description** |
| ADV\_IND | Connectable undirected advertising event |
| ADV\_DIRECT\_IND | Connectable Directed Advertising |
| ADV\_NONCONN\_IND | Non-connectable undirected advertising event |
| ADV\_SCAN\_IND | Scannable undirected advertising event |

**Description of Packets -**

**ADV\_IND Packet -** This packet type supports connectable and undirected advertising. It is used when a slave device is powered up for the first time and has never connected with a master. It is looking to connect with any node. This represents a factory default state.



The payload consists of:

* **Advertiser**[**device address**](http://microchipdeveloper.com/wireless:ble-link-layer-address) – It is a length of 6 bytes.
* Advertisement Data Structures have the following format:

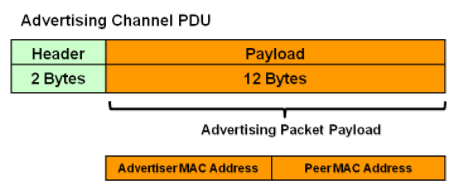
1. **AD Length** – It has a length of 1 byte.

2. **AD Type** - It has a length of 1 byte

3. **AD Data** - It has a maximum length of 29 bytes

ADV\_IND packets contain the Complete Local Name (Type id 0x09) and 128-bit Service UUID (Type id 0x07).

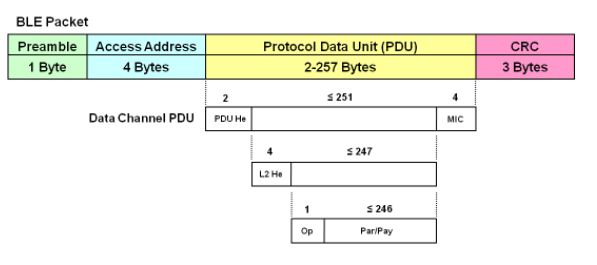
### **ADV\_DIRECT\_IND Packet** - This packet type supports connectable and directed advertising. It would typically be used after a slave device has connected with a master. It is not looking to be discovered, rather, it already has the device address of its peer and wishes to re-connect quickly to a specific master device.



The payload consists of:

* **Advertiser**[**device address**](http://microchipdeveloper.com/wireless:ble-link-layer-address) – It has a length of 6 bytes.
* **Scanner**[**device address**](http://microchipdeveloper.com/wireless:ble-link-layer-address) - It has a length of 6 bytes.

**2. Data Channel PDU**



**PDU He -** It is called as the Data PDU Header. It has length of 2 bytes.

**MIC -** It is called as Message Integrity Check. It has length of 4 bytes. It is included as a part of the payload for security.

**L2 He –** It is called as the L2CAP (Logical Link Control and Adaptation Protocol) Header. It has length of 4 bytes.

**Op -** It is called as the ATT Operation Code. It has length of 1 byte.

**Par/Pay** – It is called as ATT Parameters and Payload. In BLE v4.0 and BLE v4.1 the size of parameters and payload is 22 bytes.