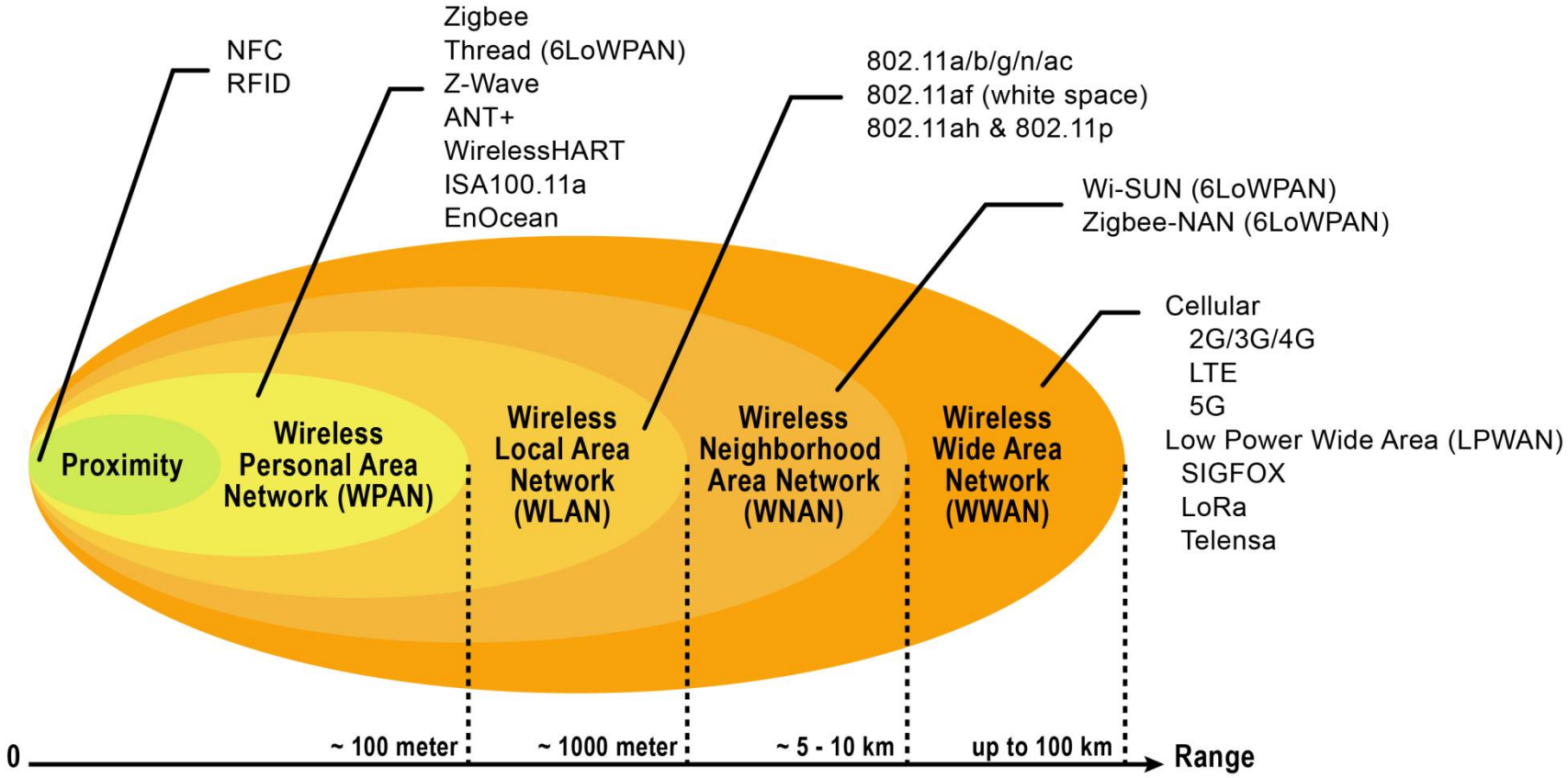
Introduction Zigbee

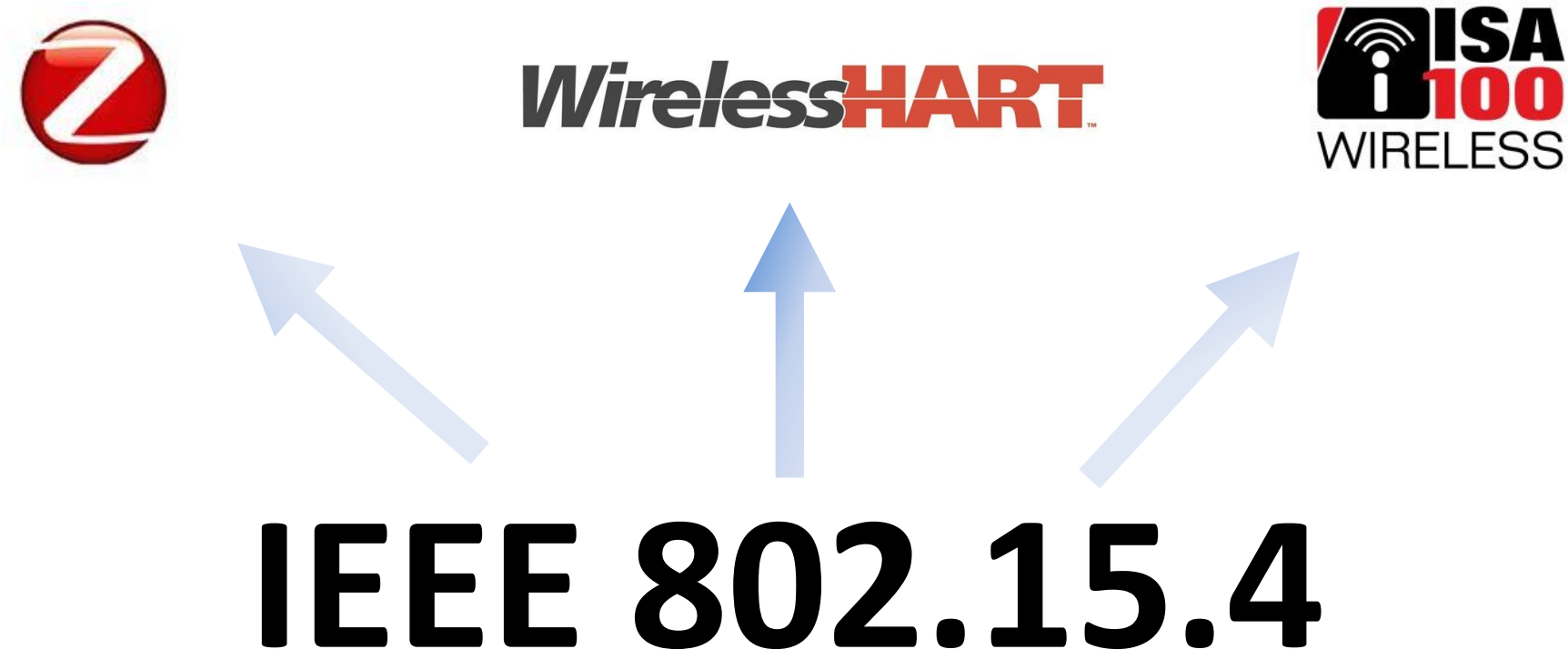
I am security researcher

- Specialize in ICS security of embedded devices
- Dedicate a lot of time to programming industrial controllers for ICS
- Took part in smart home development projects

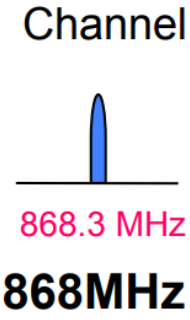
Introduciton to Zigbee

6LoWPAN

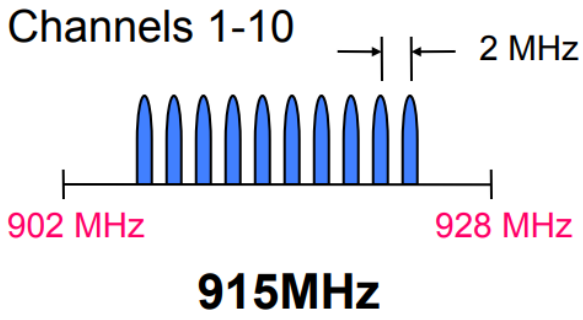

NFC
RFID
Zigbee
Thread (6LoWPAN)
Z-Wave
ANT+
WirelessHART
ISA100.11a
EnOcean
802.11a/b/g/n/ac
802.11af (white space)
802.11ah & 802.11p
Wi-SUN (6LoWPAN)
Zigbee-NAN (6LoWPAN)
Cellular
2G/3G/4G
LTE
5G
Low Power Wide Area (LPWAN)
SIGFOX
LoRa
Telensa
Proximity
Wireless Personal Area Network (WPAN)
Wireless Local Area Network (WLAN)
Wireless Neighborhood Area Network (WNAN)
Wireless Wide Area Network (WWAN)
0
~ 100 meter
~ 1000 meter
~ 5 - 10 km
up to 100 km
Range


WirelessHART
ISA 100 WIRELESS
IEEE 802.15.4

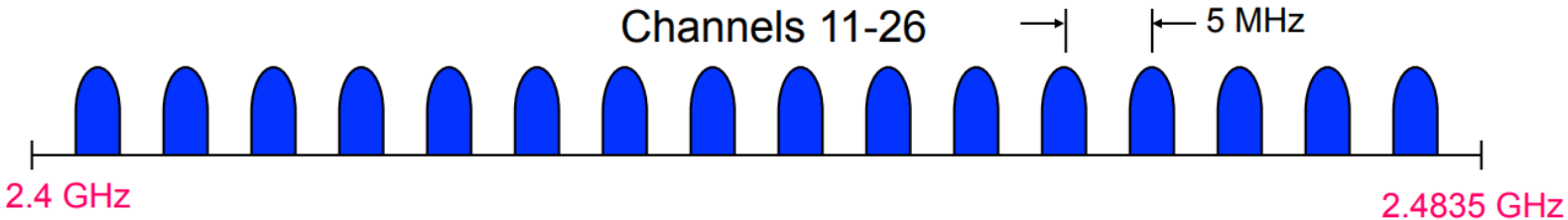
Range			Speed	Channels	Modulation
2,4 GHz	ISM	All world	250 Kbit/s	16	O-QPSK
915 MHz	ISM	USA	40 Kbit/s	10	BPSK
868 MHz	ISM	Europe	20 Kbit/s	1	BPSK



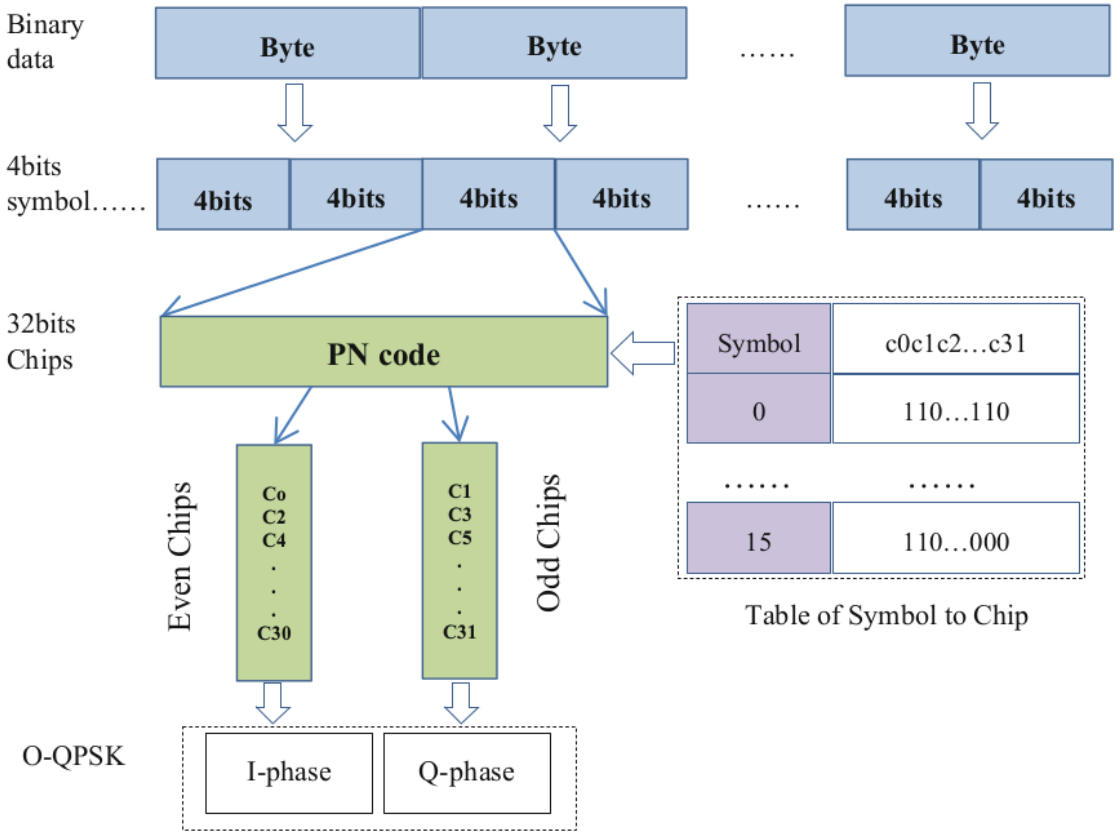
868MHz

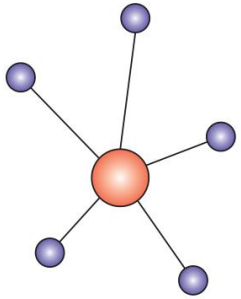


915MHz

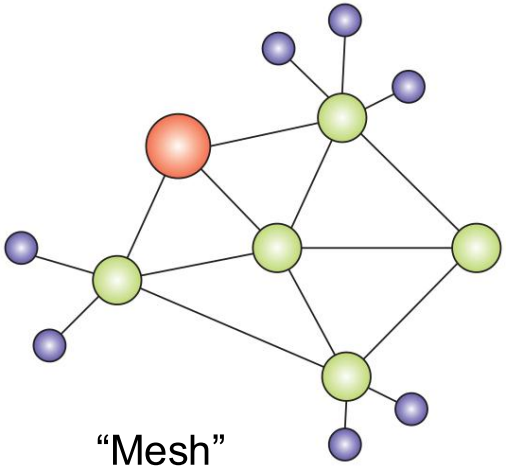


2.4 GHz


Binary data
Byte
Byte
……
Byte
4bits symbol……
4bits
4bits
4bits
4bits
……
4bits
4bits
32bits Chips
PN code
Symbol
c0c1c2…c31
0
110…110
……
……
15
110…000
Table of Symbol to Chip
Even Chips
Co C2 C4 . . . C30
C1 C3 C5 . . . C31
Odd Chips
O-QPSK
I-phase
Q-phase

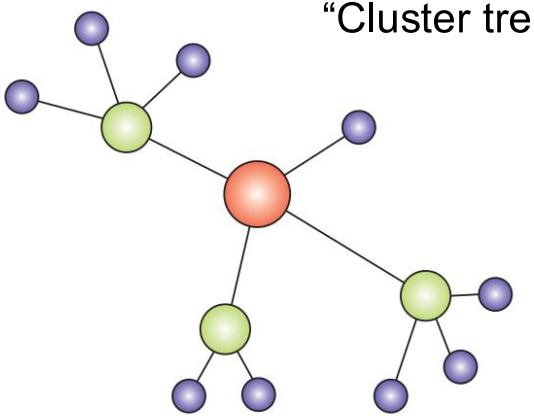


"Star"



"Mesh"

"Cluster tree"



Coordinator

Router

End-node

Coordinator

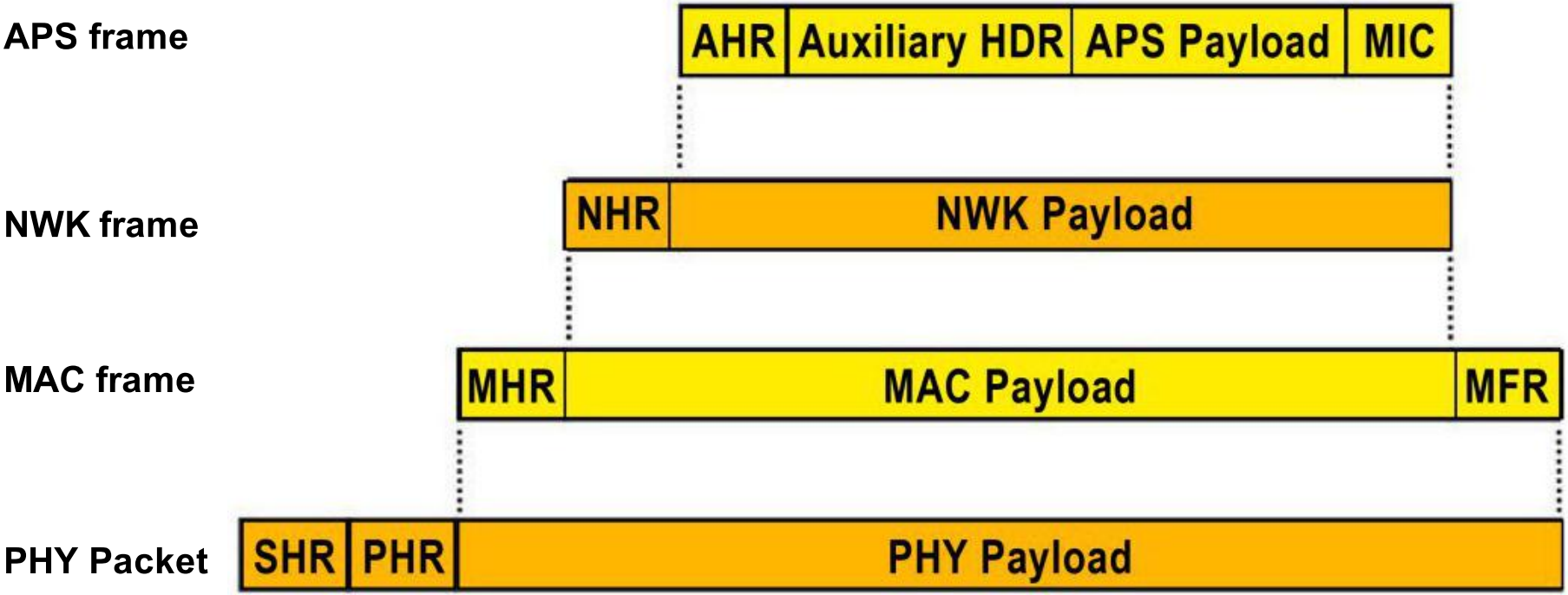
- selecting the network encryption key
- creating the network
- usually act as a trust center
- cannot be put to sleep and cannot be battery

Router

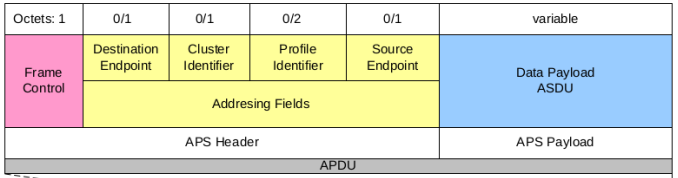
- the intermediates nodes and route the information sent by end devices to the
- cannot be put to sleep and cannot be battery

End-node

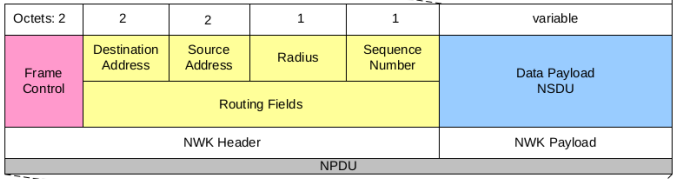
- usually the sensor nodes that collect environment data
- can optionally be battery powered and put to sleep


APS frame
AHR
Auxiliary HDR
APS Payload
MIC
NWK frame
NHR
NWK Payload
MAC frame
MHR
MAC Payload
MFR
PHY Packet
SHR
PHR
PHY Payload

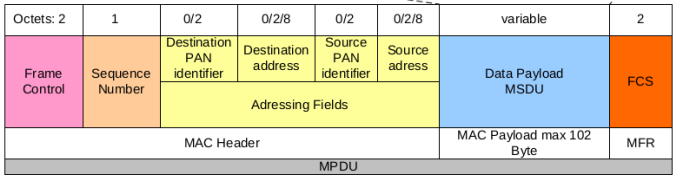
APS



NWK

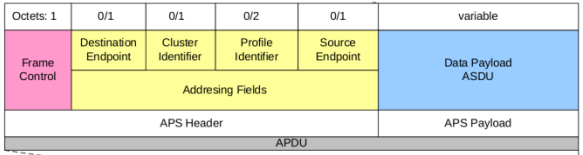


MAC

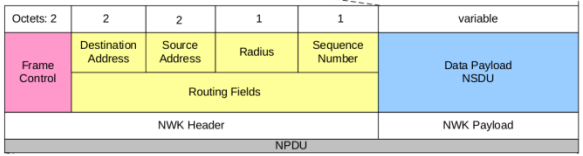


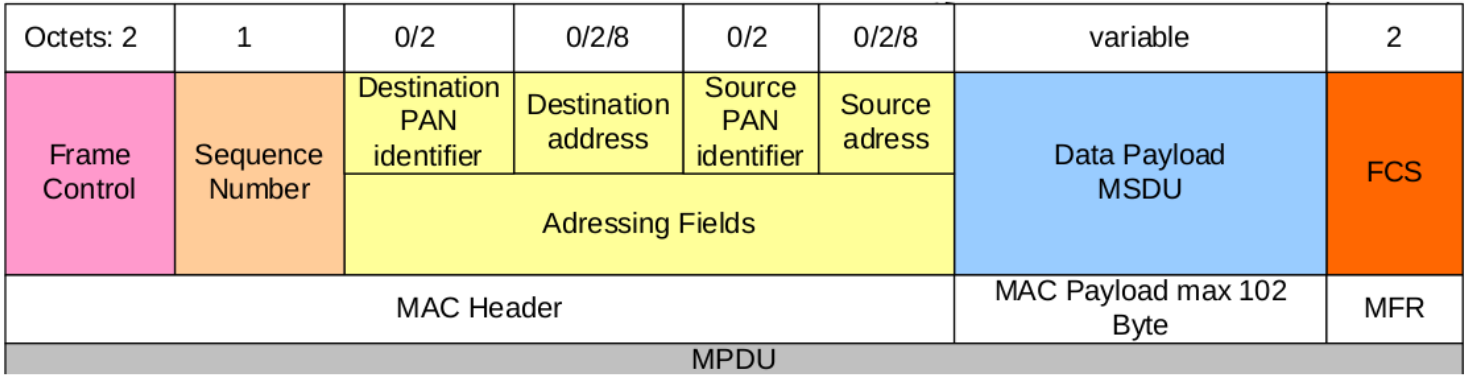
Octets: 4	1	1		variable
Preamble	SFD	Frame length (7 bits)	Reserved (1 bit)	Data Payload PSDU
Synchronization Header		PHY Header		PHY payload max 127 Byte
PPDU				

APS

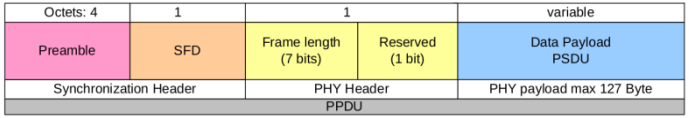

Octets: 1
0/1
0/1
0/2
0/1
variable
Frame Control
Destination Endpoint
Cluster Identifier
Profile Identifier
Source Endpoint
Data Payload ASDU
Addresing Fields
APS Header
APS Payload
APDU

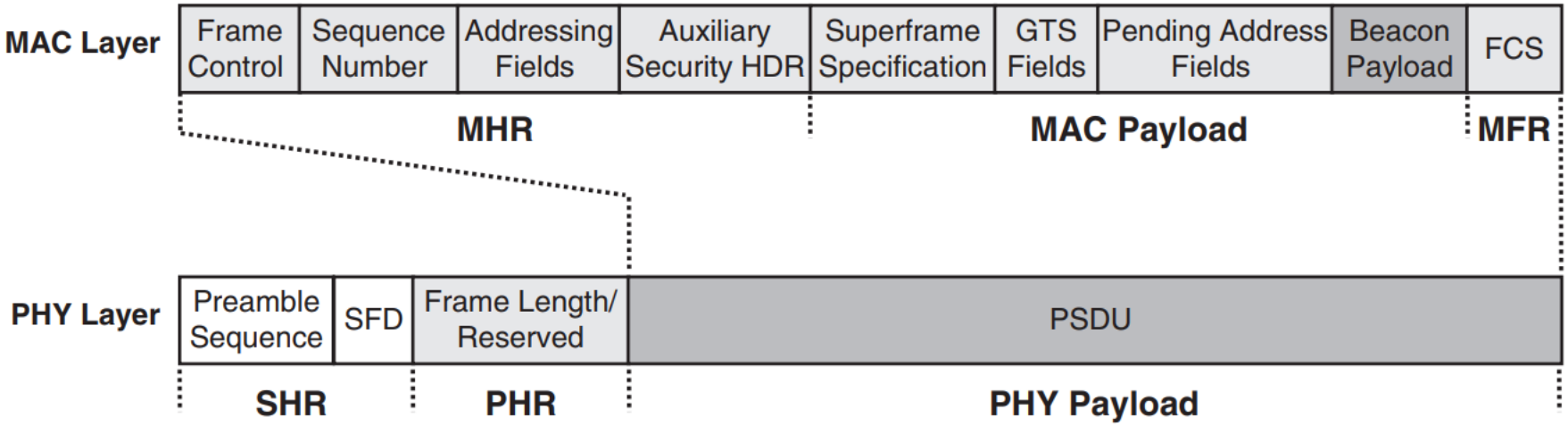
NWK


Octets: 2
2
2
1
1
variable
Frame Control
Destination Address
Source Address
Radius
Sequence Number
Data Payload NSDU
Routing Fields
NWK Header
NWK Payload
NPDU

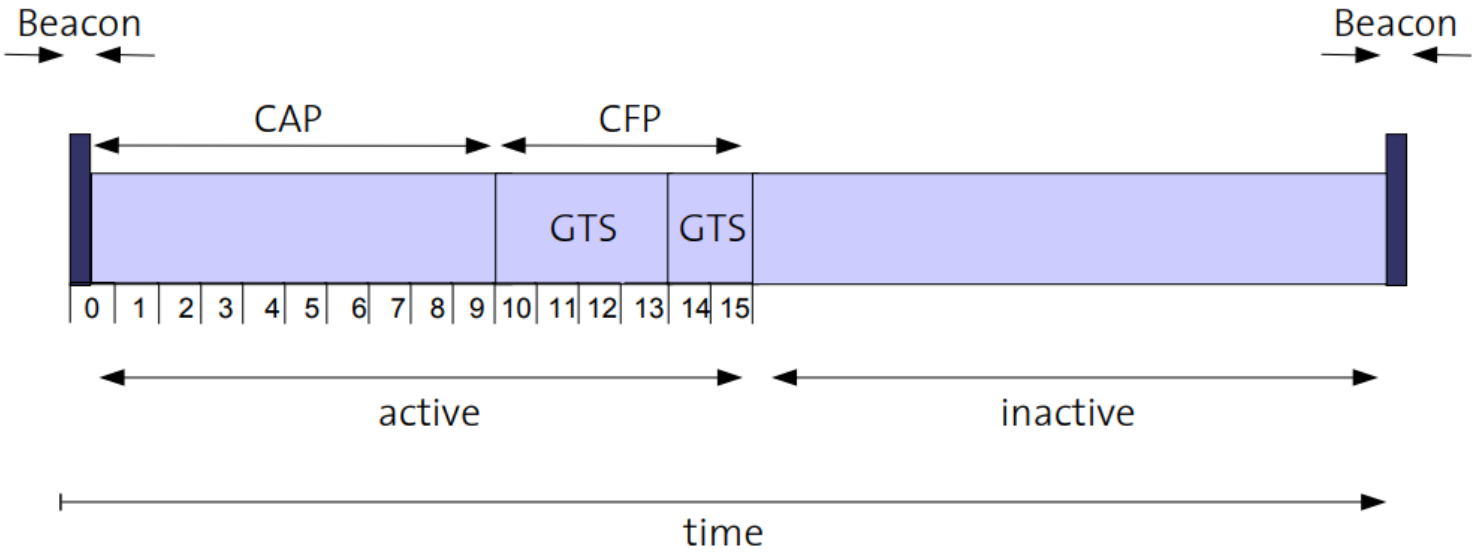

Octets: 2
1
0/2
0/2/8
0/2
0/2/8
variable
2
Frame Control
Sequence Number
Destination PAN identifier
Destination address
Source PAN identifier
Source adress
Data Payload MSDU
FCS
Adressing Fields
MAC Header
MAC Payload max 102 Byte
MFR
MPDU

PHY


Octets: 4
1
1
variable
Preamble
SFD
Frame length (7 bits)
Reserved (1 bit)
Data Payload PSDU
Synchronization Header
PHY Header
PHY payload max 127 Byte
PPDU


MAC Layer
Frame Control
Sequence Number
Addressing Fields
Auxiliary Security HDR
Superframe Specification
GTS Fields
Pending Address Fields
Beacon Payload
FCS
MHR
MAC Payload
MFR
PHY Layer
Preamble Sequence
SFD
Frame Length/ Reserved
PSDU
SHR
PHR
PHY Payload

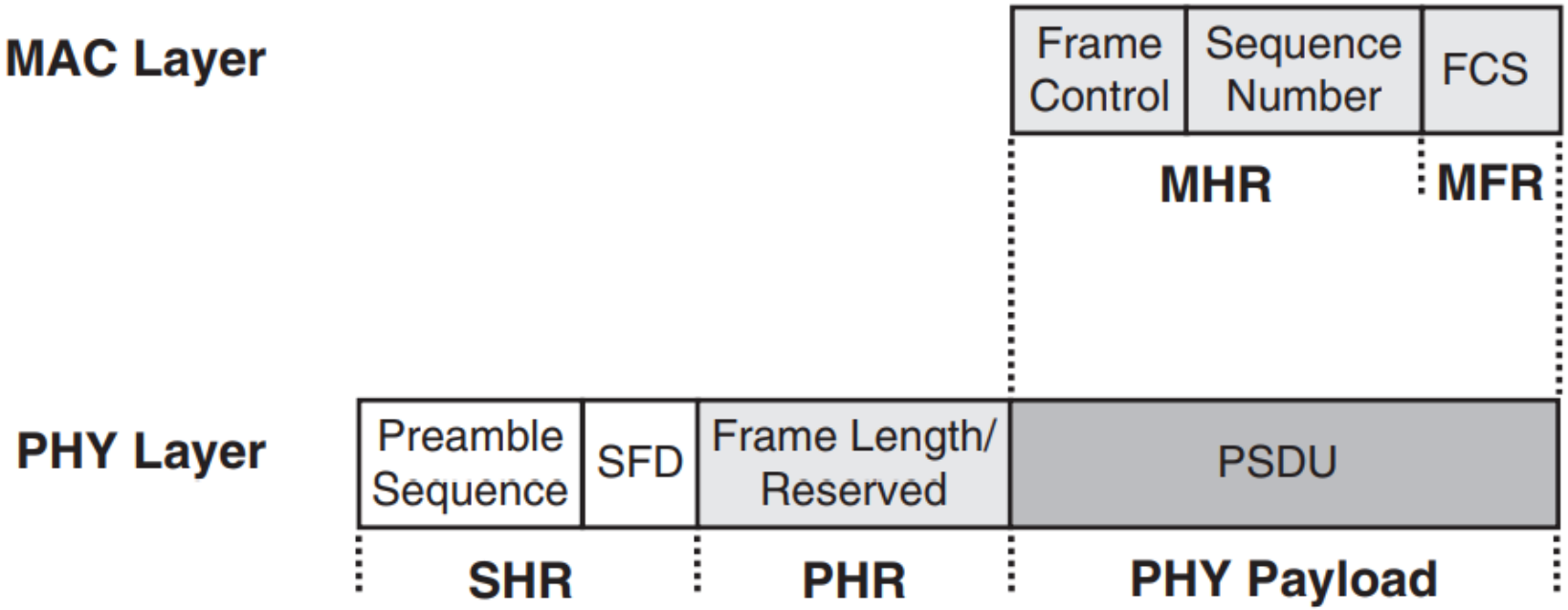
Beacon mode

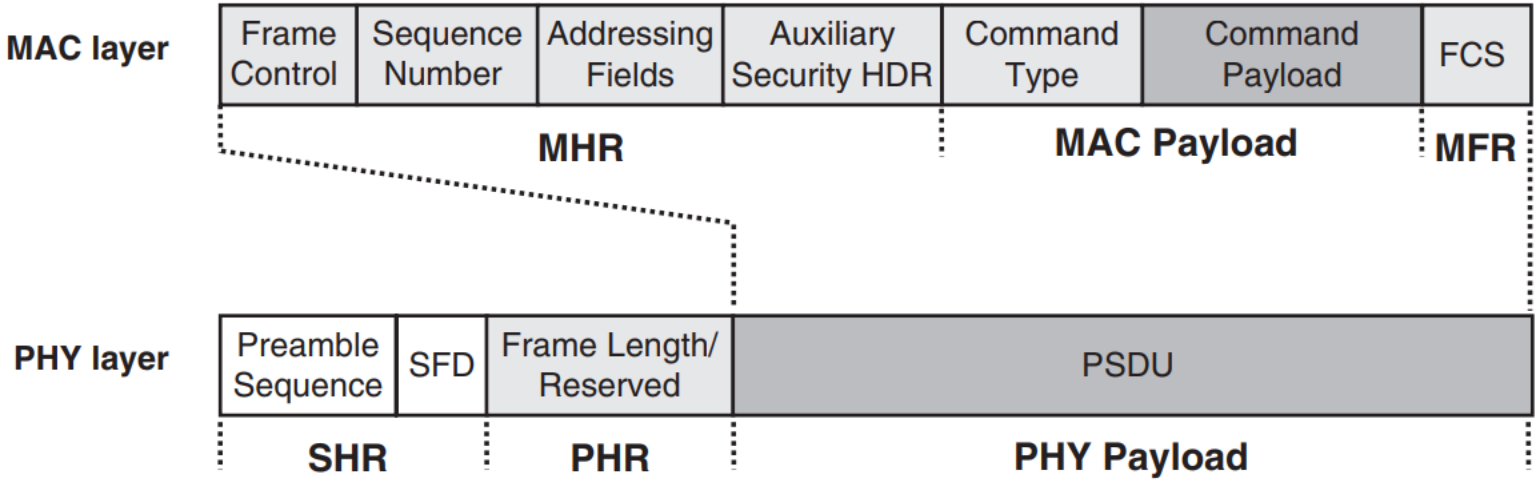


CAP = Contention Access Period

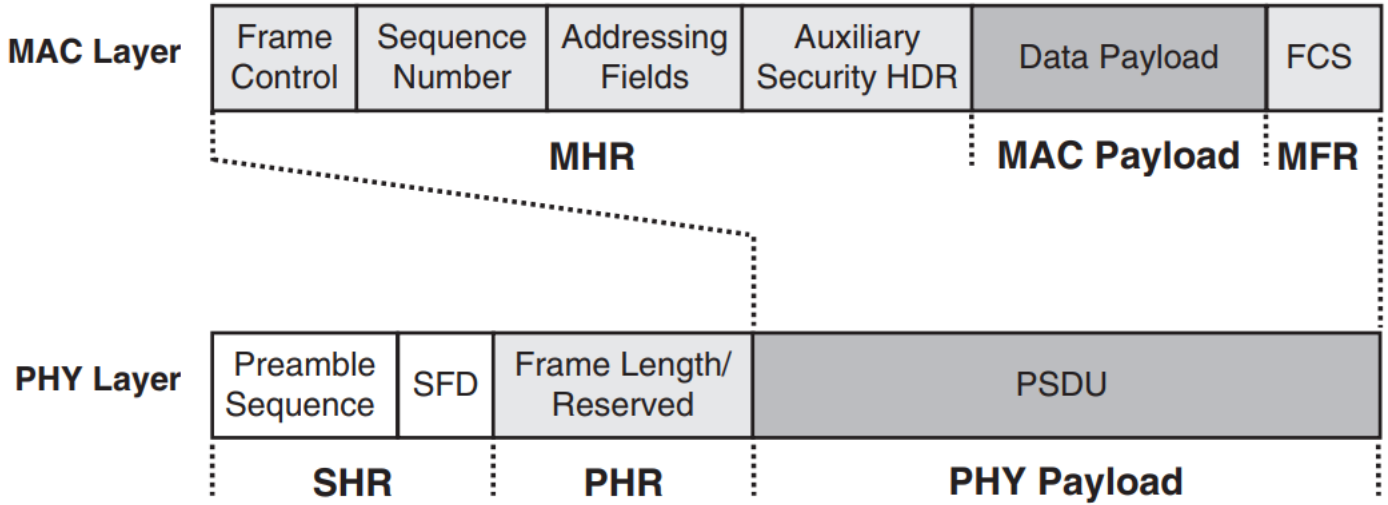
CFP = Contention Free Period

GTS = Guaranteed Time Slot

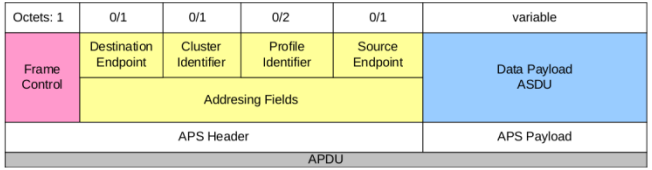

MAC Layer
Frame Control
Sequence Number
FCS
MHR
MFR
PHY Layer
Preamble Sequence
SFD
Frame Length/ Reserved
PSDU
SHR
PHR
PHY Payload

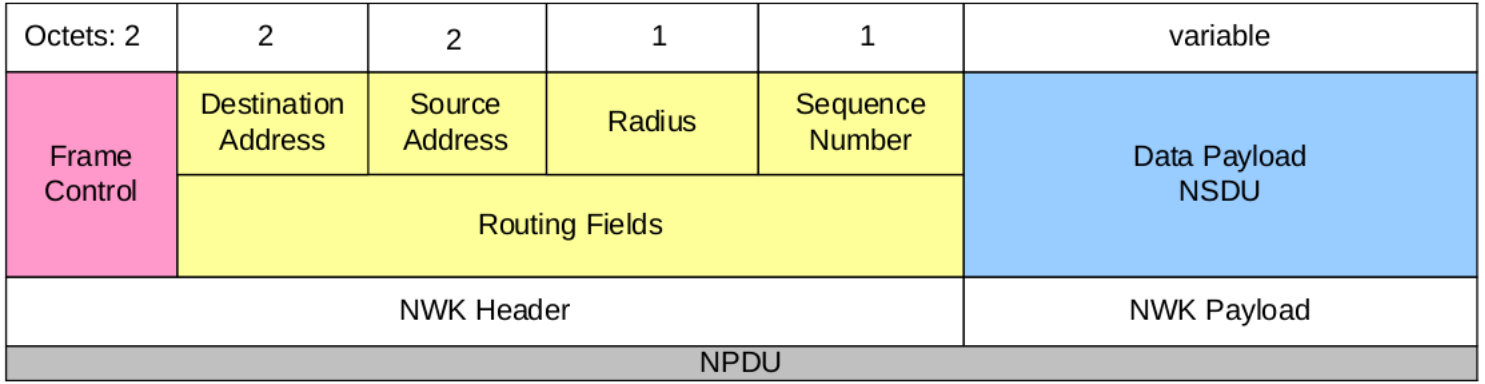

MAC layer
Frame Control
Sequence Number
Addressing Fields
Auxiliary Security HDR
Command Type
Command Payload
FCS
MHR
MAC Payload
MFR
PHY layer
Preamble Sequence
SFD
Frame Length/ Reserved
PSDU
SHR
PHR
PHY Payload

Command frame identifier	Command name	RFD	
		Tx	Rx
0 x 01	Association request	X	
0 x 02	Association response		X
0 x 03	Disassociation notification	X	X
0 x 04	Data request	X	
0 x 05	PAN ID conflict notification	X	
0 x 06	Orphan notification	X	
0 x 07	Beacon request		
0 x 08	Coordinator realignment		X
0 x 09	GTS request		
0 x 0a—0 x ff	Reserved		


MAC Layer
Frame Control
Sequence Number
Addressing Fields
Auxiliary Security HDR
Data Payload
FCS
MHR
MAC Payload
MFR
PHY Layer
Preamble Sequence
SFD
Frame Length/ Reserved
PSDU
SHR
PHR
PHY Payload

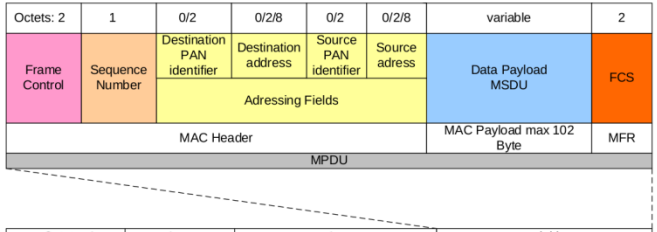
APS



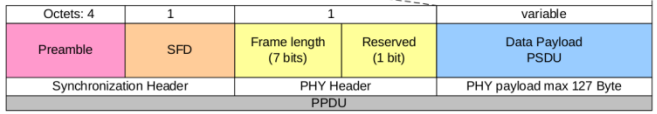


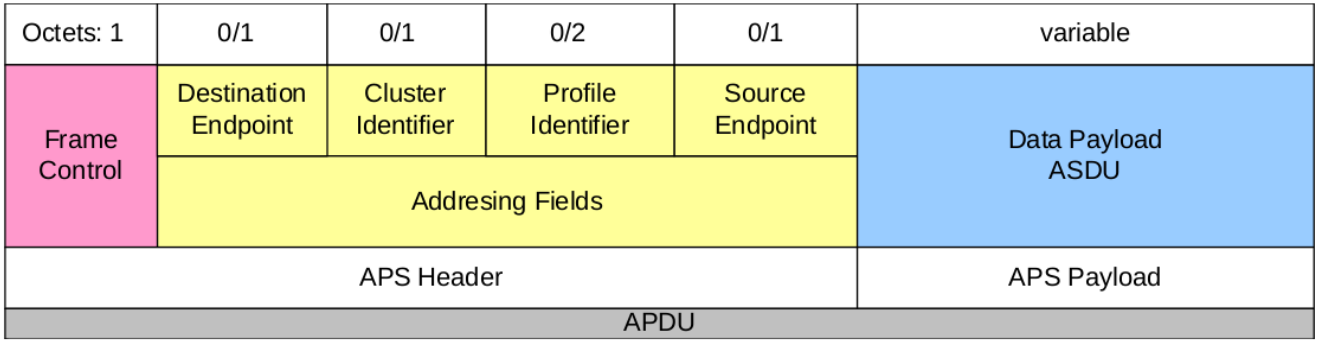
- **Topology models**
- **Packet Routing**
- **Security**

MAC

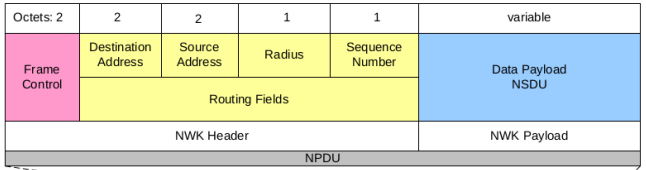


PHY

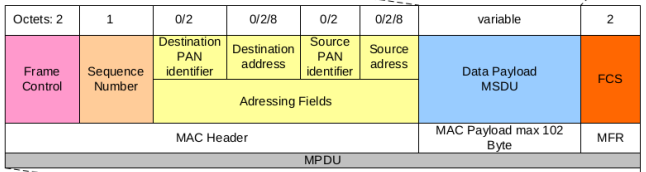



Octets: 1
0/1
0/1
0/2
0/1
variable
Frame Control
Destination Endpoint
Cluster Identifier
Profile Identifier
Source Endpoint
Data Payload ASDU
Addresing Fields
APS Header
APS Payload
APDU

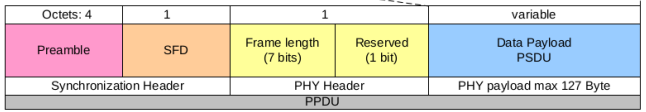
NWK


Octets: 2
2
2
1
1
variable
Frame Control
Destination Address
Source Address
Radius
Sequence Number
Data Payload NSDU
Routing Fields
NWK Header
NWK Payload
NPDU

MAC


Octets: 2
1
0/2
0/2/8
0/2
0/2/8
variable
2
Frame Control
Sequence Number
Destination PAN identifier
Destination address
Source PAN identifier
Source adress
Data Payload MSDU
FCS
Adressing Fields
MAC Header
MAC Payload max 102 Byte
MFR
MPDU

PHY


Octets: 4
1
1
variable
Preamble
SFD
Frame length (7 bits)
Reserved (1 bit)
Data Payload PSDU
Synchronization Header
PHY Header
PHY payload max 127 Byte
PPDU

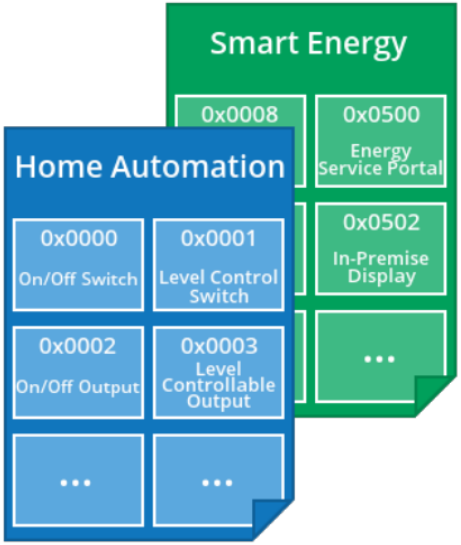
Application profile

- Public profile
- Private profile

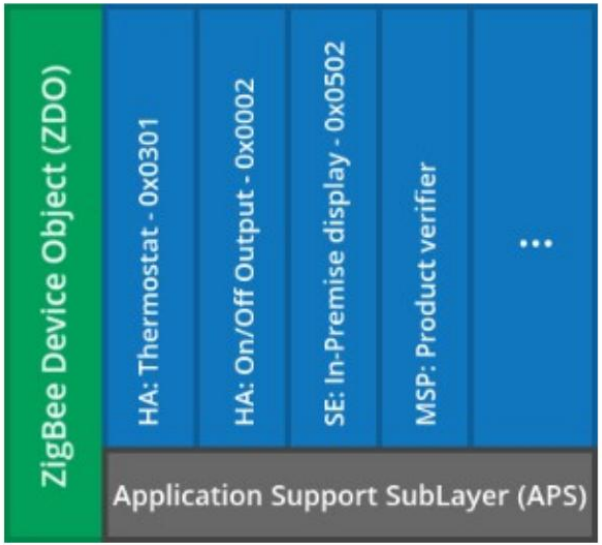
16 bit "***profile ID***"

- 0101 Industrial Plant Monitoring (IPM)
- 0104 Home Automation (HA)
- 0105 Commercial Building Automation (CBA)
- 0107 Telecom Applications (TA)
- 0108 Personal Home & Hospital Care (PHHC)
- 0109 Advanced Metering Initiative (AMI)

Device description



Each device description is identified by a unique 16-bit “***device ID***”



Clusters

"*cluster ID*" **-** 16-bit

0x0000 … 0x7FFF : Zigbee standard cluster

0x8000 … 0xFBFF : reserved for future

0xFC00 … 0xFFFF : Manufacturer specific

Domain	Zigbee Cluster IDs	Description
Generic	0x0000	Basic
	0x0001	Power configuration
	0x0002	Device temperature configuration
	0x0003	Indentify
	0x0004	Groups
	0x0005	Scenes
	0x0006	ON/OFF
	0x0007	ON/OFF Switch configuration
	0x0008	Level Control
	0x0009	Alarms
	0x000A	Time
	0x000B	RSSI Location

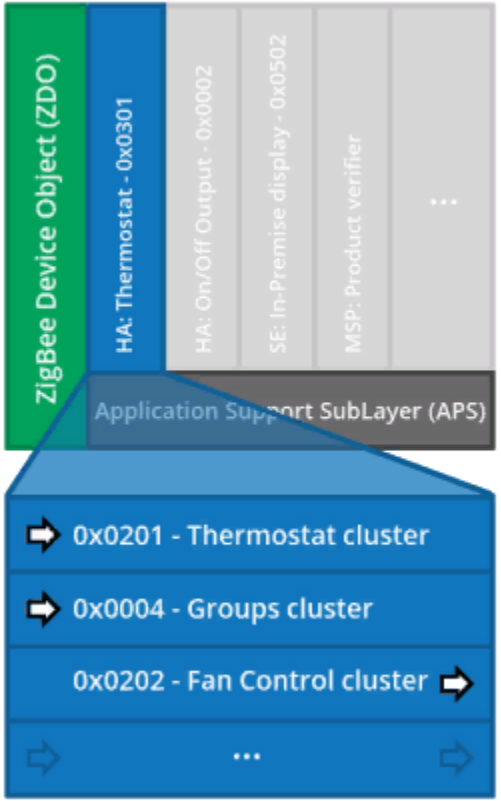
Example HA thermostat

Mandatory cluster

- Thermostat cluster (cluster ID: 0x0201)

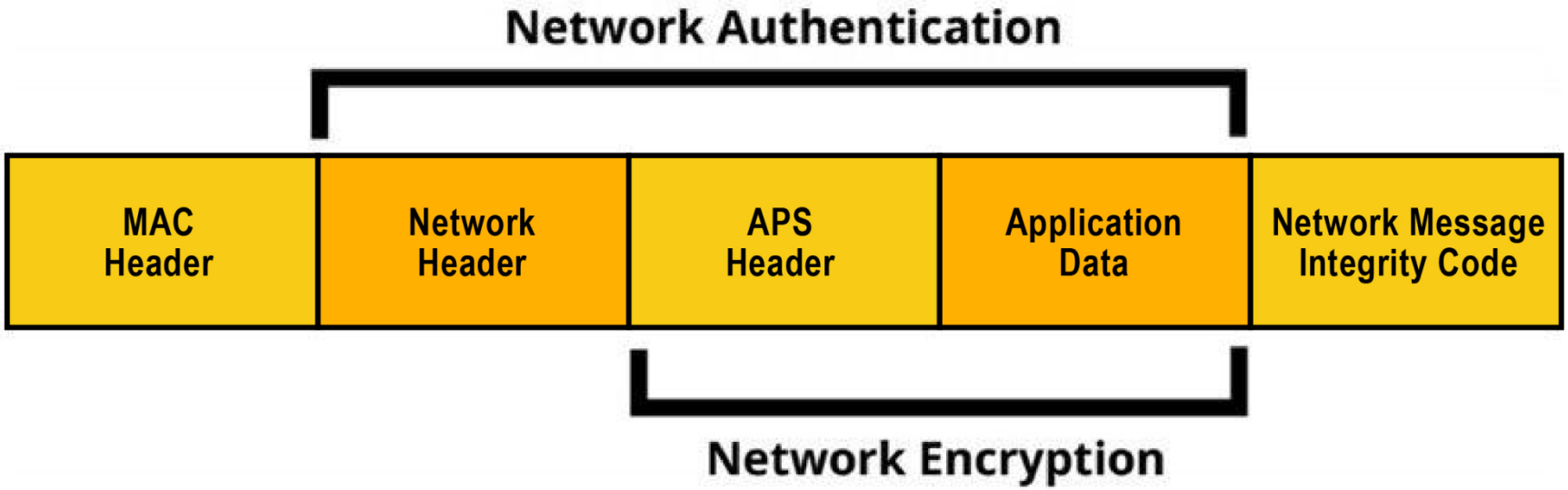
Optional clusters

- Groups (0x0004) for group addressing;
- Fan Control (0x0202) to control the speed of a fan;
- Temperature Measurement (0x0402) to receive temperature reports

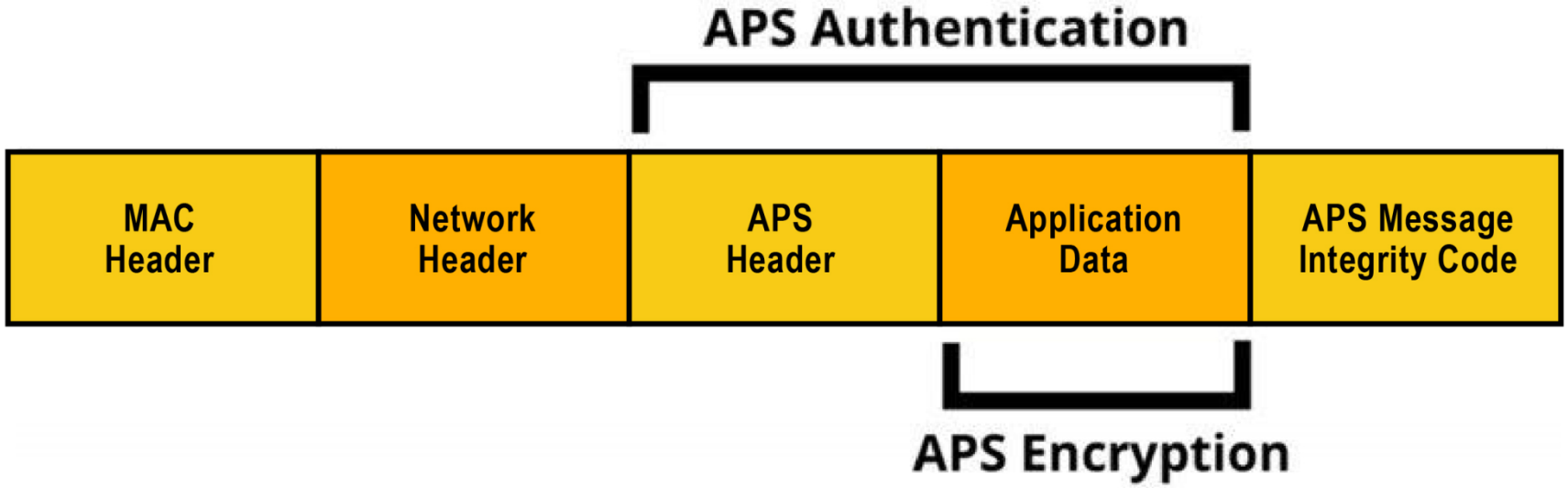


Zigbee Security

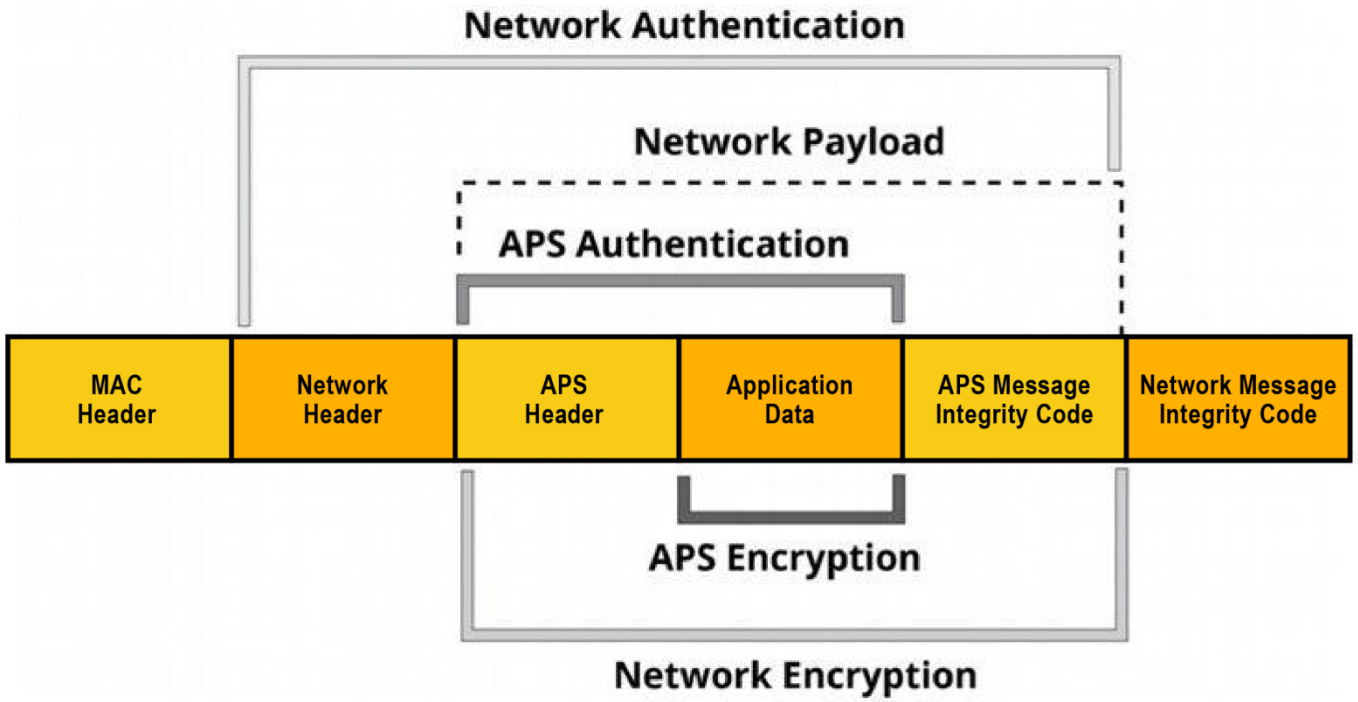
NWK layer security



APS layer security



NWK + APS layer security



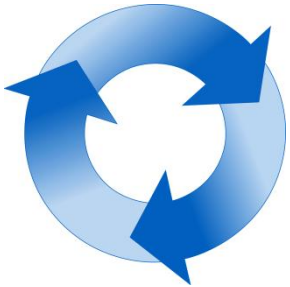
Possible attack vectors

Default link key

“ZigbeeAlliance09”

5A 69 67 42 65 65 41 6C 6C 69 61 6E 63 65 30 39

Replay attack

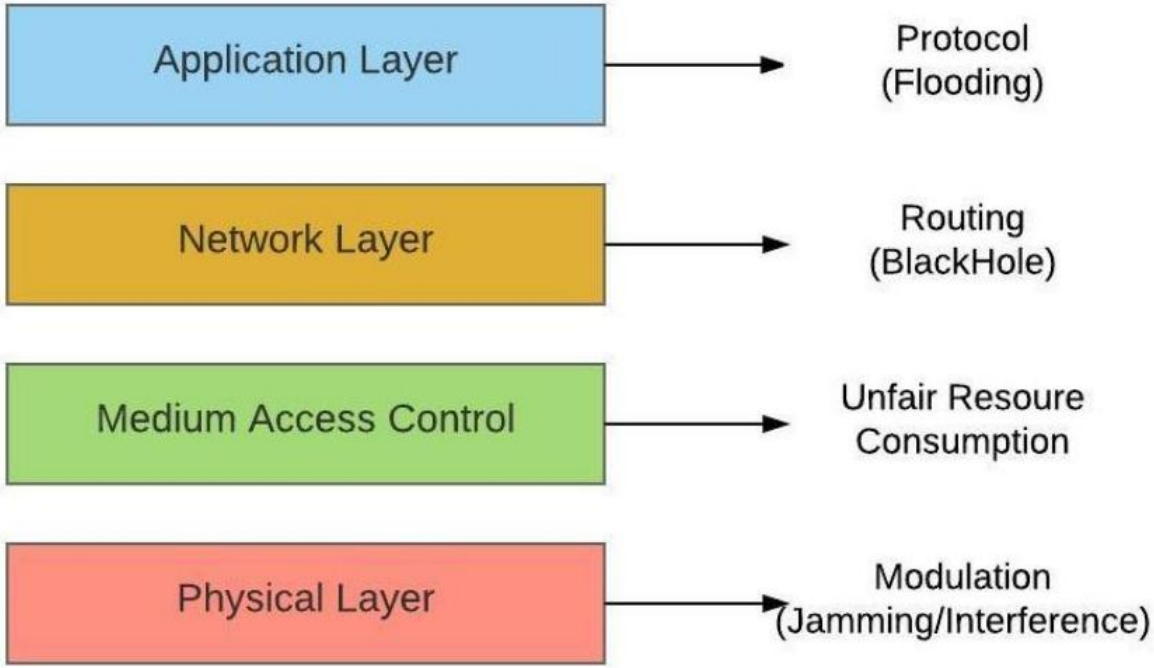


mechanism to avoid replay attacks

but implementation…

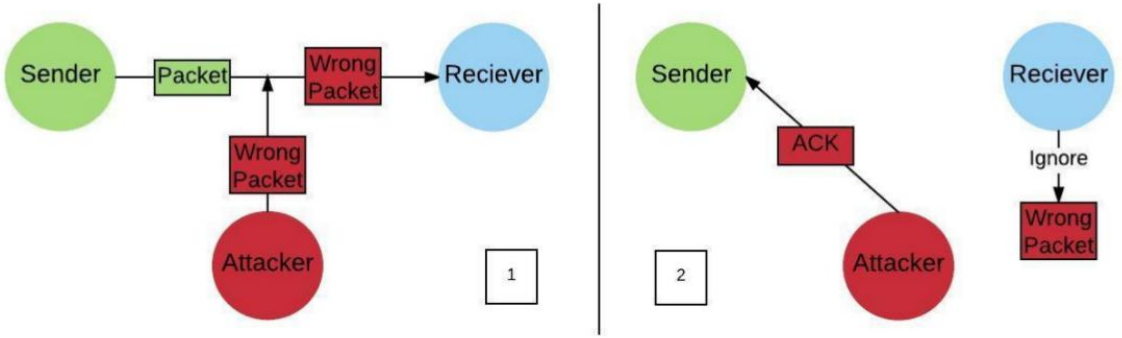
DoS Attacks


DDoS


Application Layer
Protocol
(Flooding)
Network Layer
Routing
(BlackHole)
Medium Access Control
Unfair Resoure
Consumption
Physical Layer
Modulation
(Jamming/Interference)

DoS Attacks

Spoof ACK packets



Tools and Devices

Tools to pentest Zigbee network

KillerBee

https://github.com/riverloopsec/killerbee

Attify

Zigbee Framework

https://github.com/attify/Attify-Zigbee-Framework

+

Xbee Mesh kit

XCTU

Next Generation Configuration Platform for XBee/RF Solution

Out from box

+ **Rx Zigbee**

+ **Tx Zigbee**

CC2531

USB dongle

\+ ccsniffpiper +

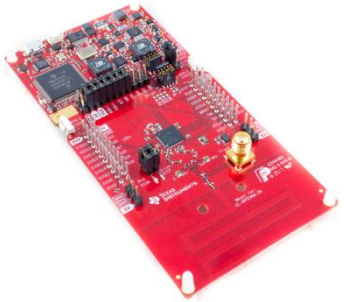
https://github.com/andrewdodd/ccsniffpiper

Wireshark

Out from box

\+ Rx Zigbee

\- Tx Zigbee



CC1352

LaunchPad

+

IDE

Code Composer Studio

SmartRF Studio

SDK SimpleLink

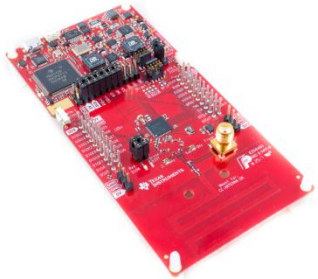
Out from box

+ Rx

+ Tx

http://dev.ti.com/tirex/content/simplelink_academy_cc13x0sdk_1_15_03_10/modules/prop_01_basic/prop_01_basic.html

Why CC1352 ?



Sub-1GHz

2.4 GHz

Support

M-Bus wireless

ZigBee

KNX RF

THREAD

Bluetooth 5

Why CC1352 ?

Feature	Main 2-(G)FSK Mode	High Data Rates	Low Data Rates	SimpleLink™ Long Range
Programmable preamble, sync word and CRC	Yes	Yes	Yes	No
Programmable receive bandwidth	Yes	Yes	Yes (down to 4 kHz)	Yes
Data / Symbol rate(1)	20 to 1000 kbps	≤ 2 Msps	≤ 100 ksps	≤ 20 ksps
Modulation format	2-(G)FSK	2-(G)FSK 4-(G)FSK	2-(G)FSK 4-(G)FSK	2-(G)FSK
Dual Sync Word	Yes	Yes	No	No
Carrier Sense(2)(3)	Yes	No	No	No
Preamble Detection(3)	Yes	Yes	Yes	No
Data Whitening	Yes	Yes	Yes	Yes
Digital RSSI	Yes	Yes	Yes	Yes
CRC filtering	Yes	Yes	Yes	Yes
Direct-sequence spread	No	No	No	1:2 1:4 1:8
	No	No	No	Yes
	Yes	Yes	Yes	Yes

25.10.1 Packet Formats

For compatibility with existing TI parts, the packet format given in Figure 25-9 can be used in most cases. This packet format is supported through the use of the commands CMD_PROP_TX and CMD_PROP_RX.

Figure 25-9. Standard Packet Format

1 bit to 32 bytes	8 to 32 bits	0 or 1 byte	0 or 1 byte	0 to 255 bytes	0 or 16 bits (0 to 32 bits)
Preamble	Sync word	Length field	Address	Payload	CRC

A more flexible packet format is also possible, as defined in Figure 25-10. This format is supported by the commands CMD_PROP_RX_ADV and CMD_PROP_TX_ADV. The format in Figure 25-9 is an example of this format.

Figure 25-10. Advanced Packet Format

1 bit to 32 bytes or repetition	8 to 32 bits	0 to 32 bits	0 to 8 bytes	Arbitrary	0 or 16 bits (0 to 32 bits)
Preamble	Sync word	Header	Address	Payload	CRC

Proprietary radio command

egor21@gmail.com