

# Communications & Controls in IoT

## IEEE 802.15.4 and WLAN

**Instructor: Sachin Chaudhari**

**Feb. 09, 2023**



INTERNATIONAL INSTITUTE OF  
INFORMATION TECHNOLOGY

---

H Y D E R A B A D

---

**Recap:** *Communication Techniques for IoT*

# Polling Protocol

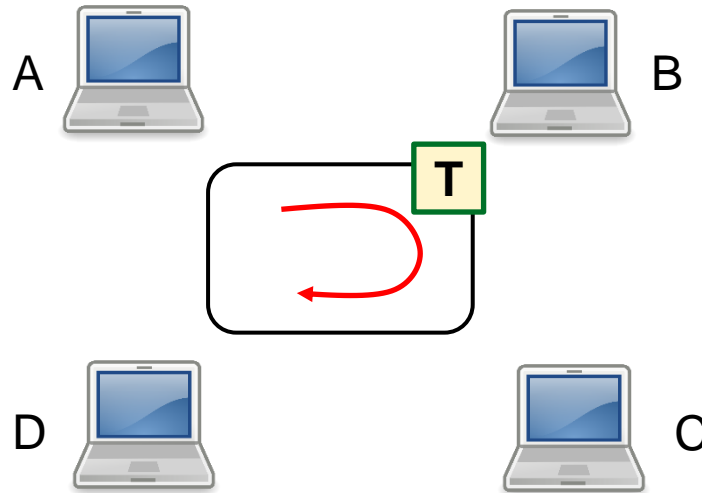
---

- One of the nodes becomes master node
- Master node polls each node in round-robin fashion
- Node polled can transmit up to maximum number of frames
- Eliminates the collisions that plague random access protocols and empty slots in channel partitioning protocols
- Issue of single point failure, delay in polling and instructing to send
- Example: used in Bluetooth and 802.15 protocols

# Token Passing (or Token Ring)

---

- A token is circulating in the ring and whichever node grabs that token will have right to transmit the data.
- This protocol provides fairness and eliminates collision
- Advantages: Decentralized and highly efficient
- Disadvantages: Node failure and node not releasing token
- Used in networks prior to Ethernet



# Simplex and Duplexing Communications

---

- Simplex communication system: one device transmits, other listens
  - TV, FM, Surveillance monitors, wireless microphones
- Duplex communication system: both devices can transmit and receive
  - Most of the communication systems including cellphone, laptops, tablets

# Types of Duplexing

---

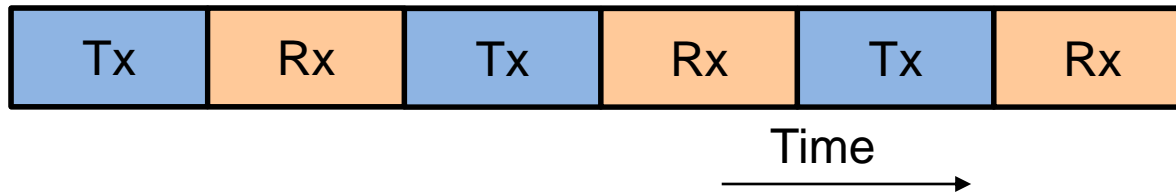
- Half Duplex
  - Both parties cannot communicate simultaneously
  - Walkie-talkie (Push to talk button)
- Full Duplex
  - Both parties can talk simultaneously
  - Most of the communication devices

# Duplexing Methods

- Methods used for dividing forward and reverse communication channels, they are called as duplexing methods such as

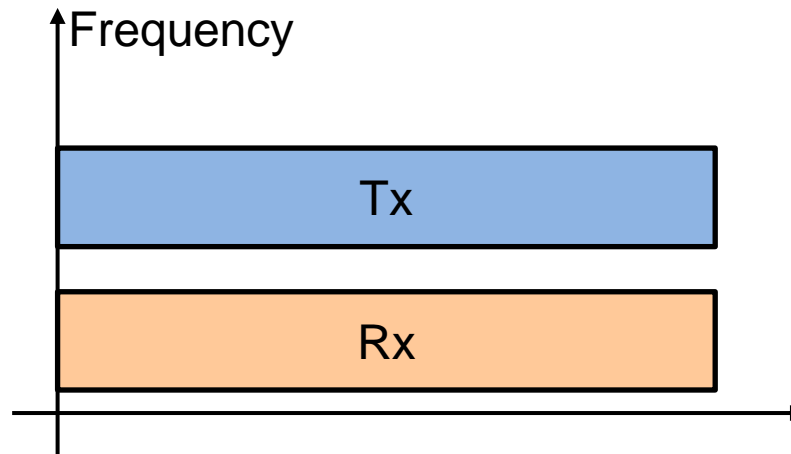
- Time division duplexing (TDD)

- Half Duplex

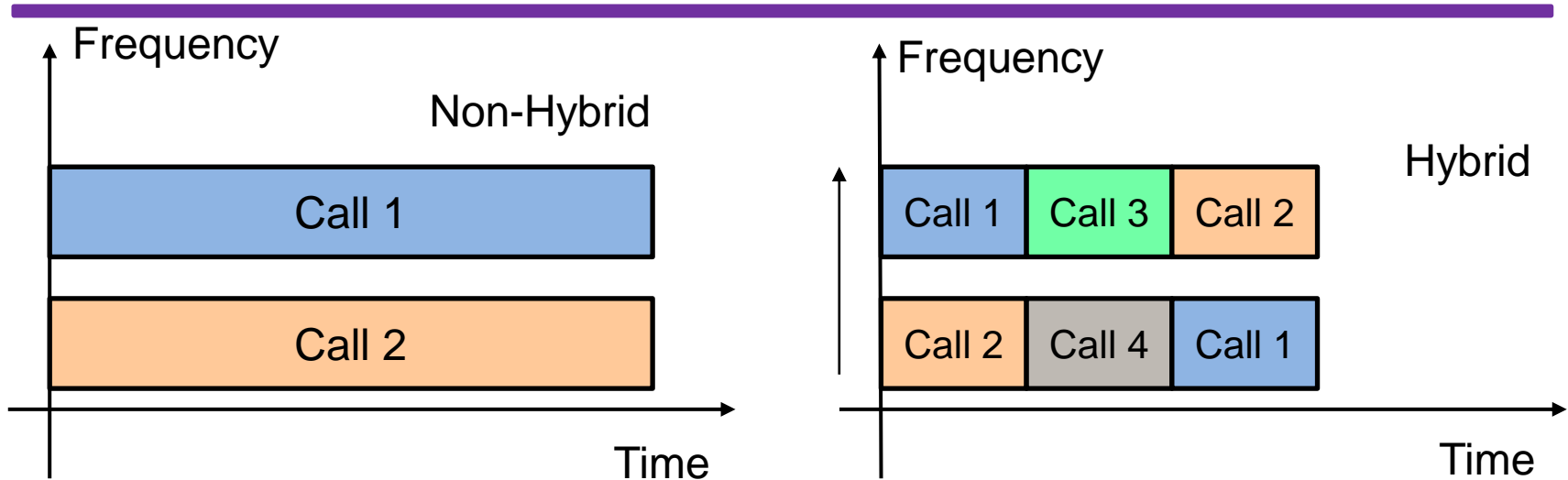


- Frequency division duplexing (FDD)

- Full Duplex



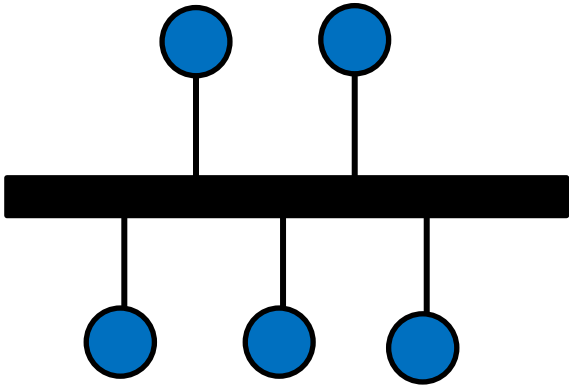
# Hybrid Channel Access



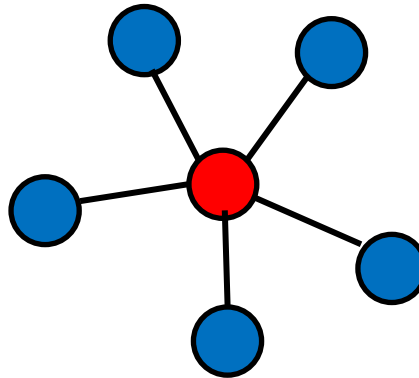
- The GSM cellular system combines the use of FDD to prevent interference between outward and return signals with FDMA and TDMA to allow multiple handsets in a single cell.
- Bluetooth packet mode communication combines frequency hopping for shared channel access among several private area networks in the same room with CSMA/CA for shared channel access inside a medium
- IEEE 802.11b WLAN are based on FDMA and DS-CDMA for avoiding interference among adjacent WLAN cells or access points



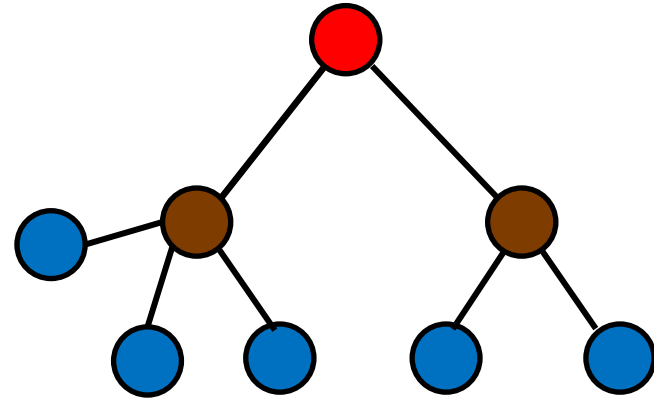
# Network Topologies



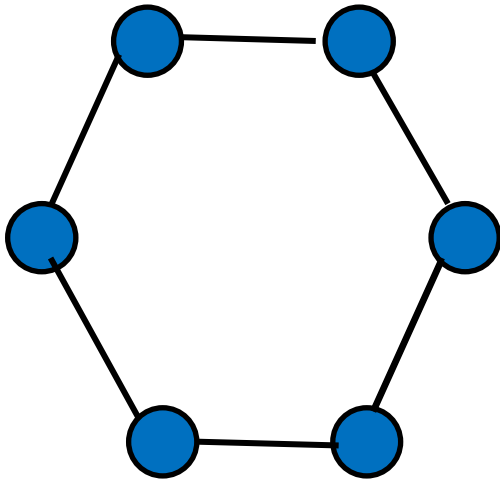
**Bus**



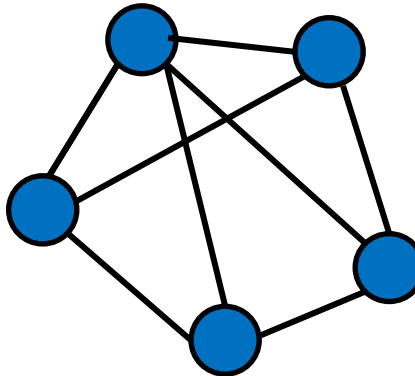
**Star**



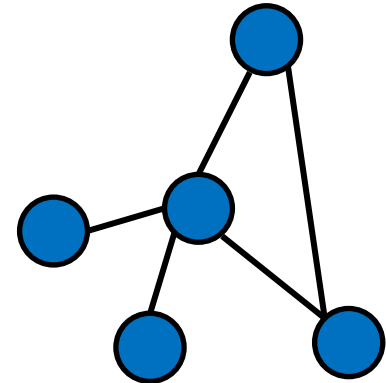
**Tree**



**Ring**



**Mesh**



**Hybrid**

# Issues in IoT from Communication Perspective

---

[Not an exhaustive list!]

- Low power consumption
- Support large number of devices with low data rates
- Coverage
- Quality of service
- Low cost
  - Network/Private (DIY)
  - Licensed/Unlicensed
- Privacy and security
- Standardization for interoperability between different vendors

# Factors contributing to energy waste/expense

---

- Energy consumption in transmission
  - Longer distances
  - Higher frequencies
  - More bandwidth
- Energy waste
  - Excessive overhead
  - Idle listening
  - Overhearing
  - Packet collisions and retransmissions

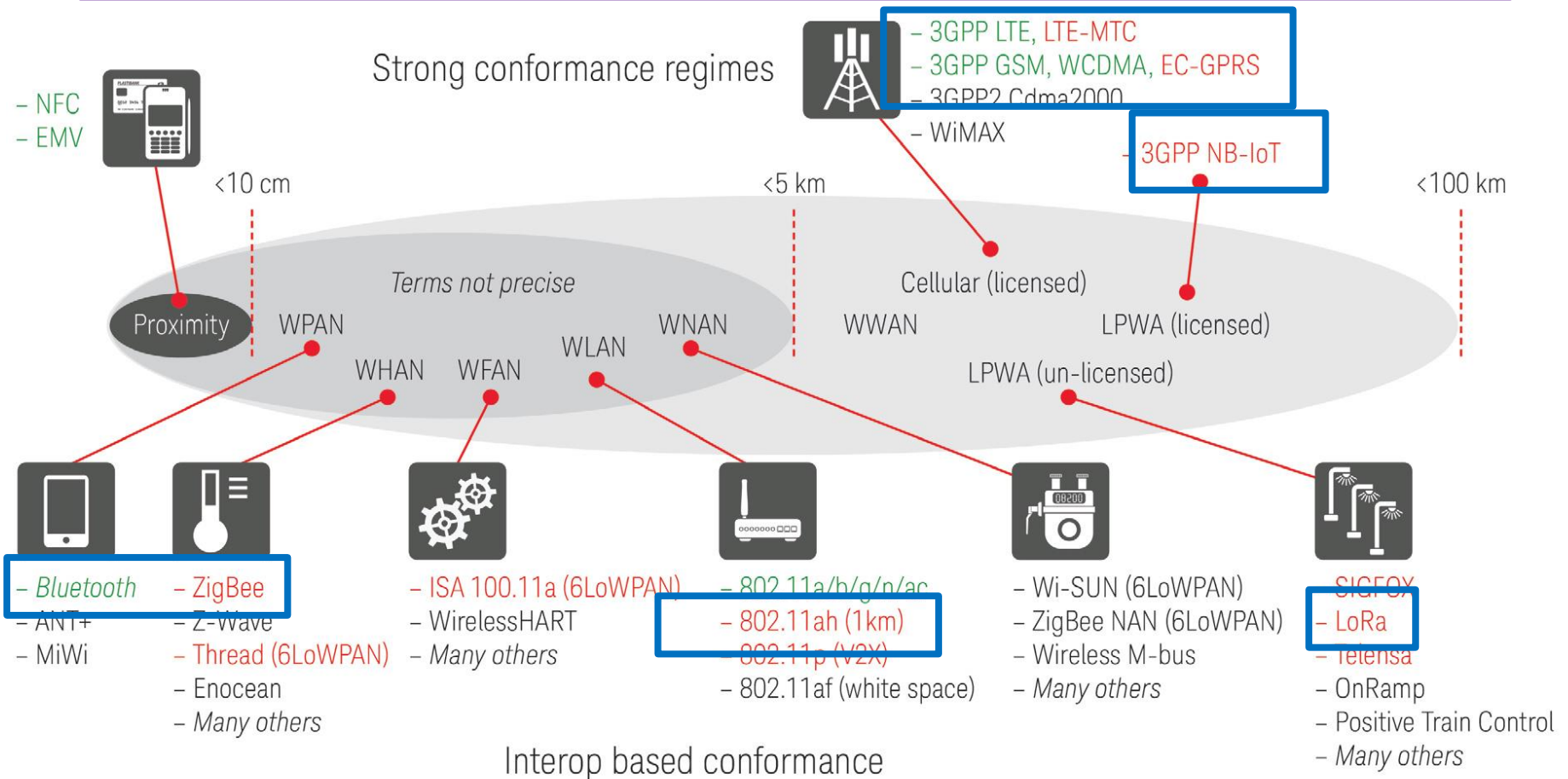
[Not exhaustive!]

# Ways to Reduce Energy Waste/Consumption

---

- Reduced frequency/data rate/ bandwidth/ coverage
- Sleep
  - Low duty cycle
- Energy saving protocols
  - Schedule based (reduction in over-hearing and idle-listening)
    - Licensed spectrum; BLE
  - Contention based (less overhead and no need of synchronization)
    - Zigbee, WiFi
- Multihop and aggregation of data
- Signal processing
  - censoring, predictive filters
- Reduced overhead

# Communication Techniques for IoT



---

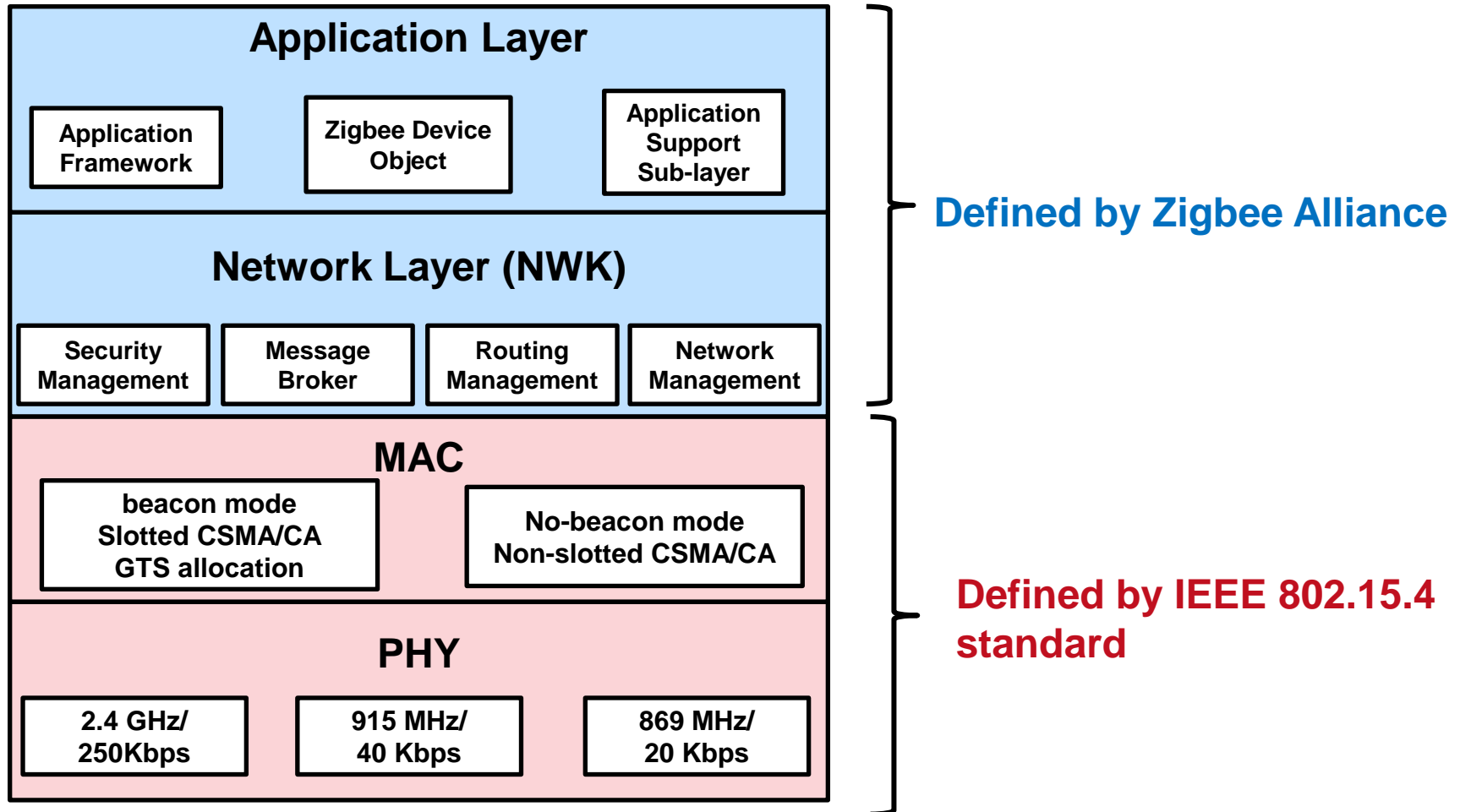
# Today's Class

---

# IEEE 802.15.4

Ref: K. Sohraby, D. Minoli, T. Znati, *Wireless Sensor Networks*, Wiley, 2007

# IEEE 802.15.4/Zigbee Protocol Stack

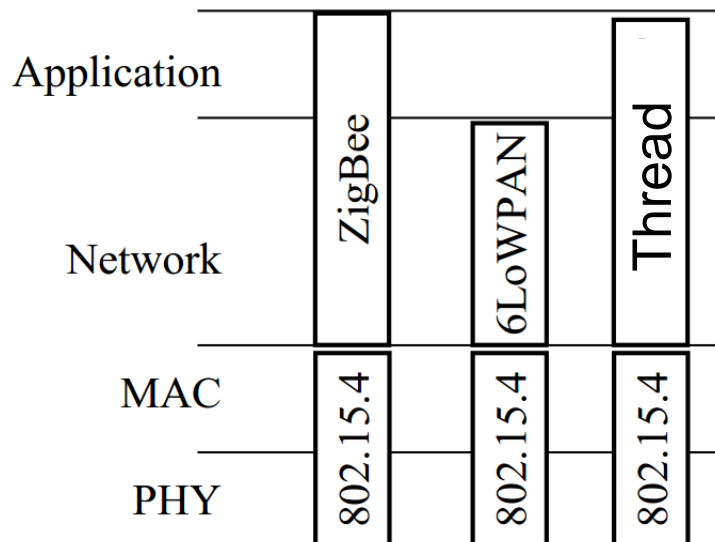


- Full protocol stack for low power, low rate and low cost wireless communications. Also applicable to Low rate WPAN – LR-WPAN.



# IEEE 802.15.4

- IEEE 802.15.4 defines the operation of low-rate wireless personal area networks (LR-WPANs)
- Widely used in wireless sensor-network (WSN) applications
  - Vast number of industrial, home and medical applications
- It specifies the physical layer (PHY) and media access control (MAC) for LR-WPANs
- Does not have IP address
- Used by several “Internet of Things” protocols:
  - ZigBee, 6LoWPAN, Thread, WiSuN etc.

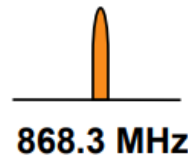


# Physical Layer (PHY): *Operating Frequency Bands*

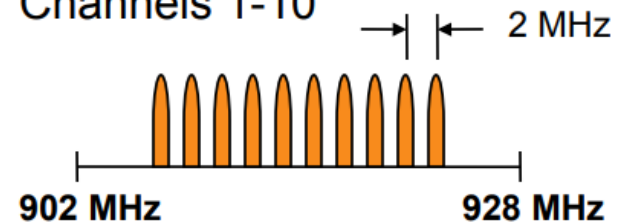
---

**868MHz/915MHz  
PHY**

Channel 0

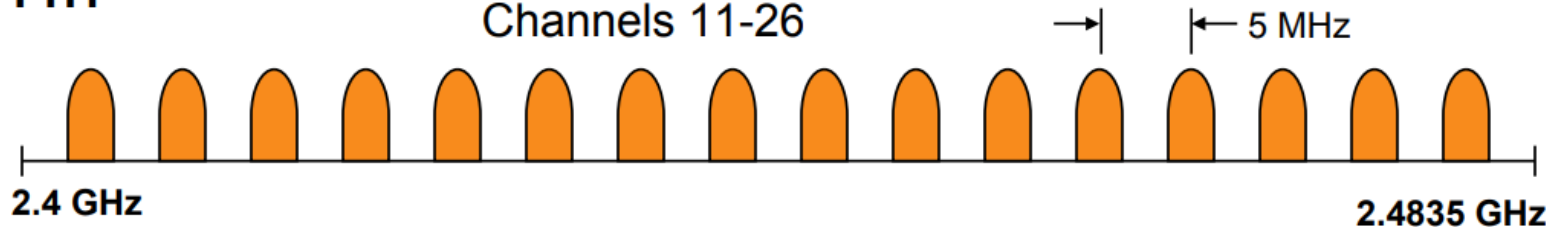


Channels 1-10






**2.4 GHz  
PHY**

Channels 11-26



# PHY: *Frequency Bands Worldwide*

	Channel	Center Frequency (MHz)	Availability
868 MHz Band	0	868.3	 Europe
915 MHz Band	1	906	 Americas
	2	908	
	3	910	
	4	912	
	5	914	
	6	916	
	7	918	
	8	920	
	9	922	
	10	924	
2.4 GHz Band	11	2405	 World Wide
	12	2410	
	13	2415	
	14	2420	
	15	2425	
	16	2430	
	17	2435	
	18	2440	
	19	2445	
	20	2450	
	21	2455	
	22	2460	
	23	2465	
	24	2470	
	25	2475	
	26	2480	

# PHY: *Modulation Parameters*

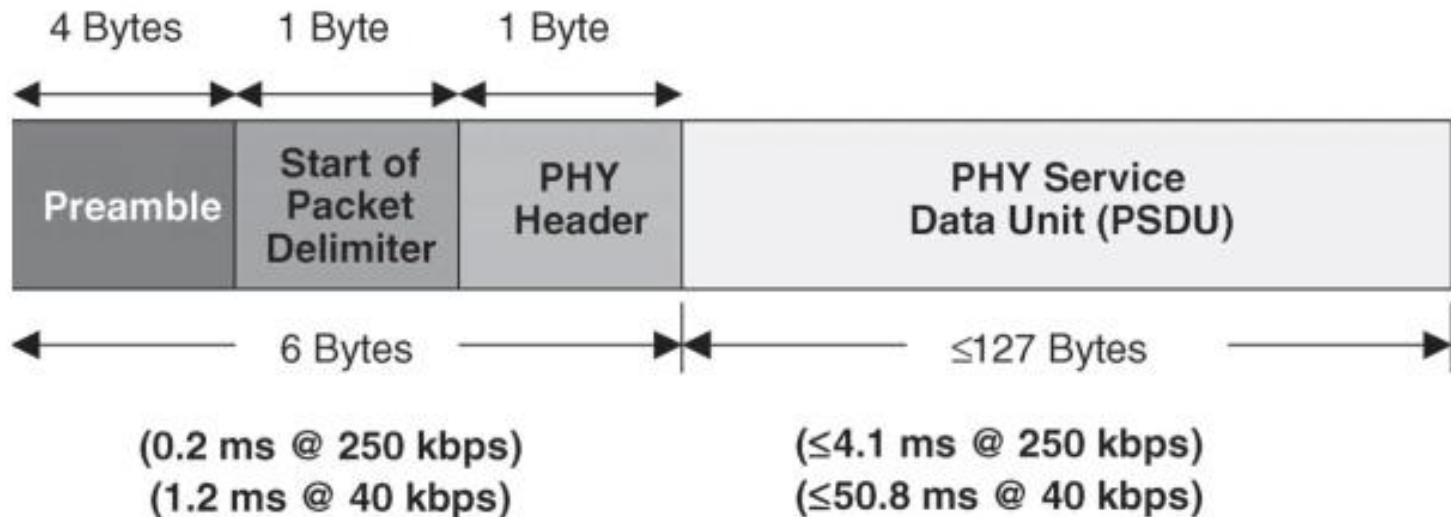
---

Freq. band (MHz)	Spreading Parameters		Data Parameters		
	Chip rate (kchip/s)	Modulation	Bit rate (kbps)	Symbol rate (ksymbol/s)	Symbols
868	300	BPSK	20	20	Binary
915	600	BPSK	40	40	Binary
2400	2000	O-QPSK	250	62.5	16-ary

[Koubaa2007]

All bands are based on Direct sequence spread spectrum (DSSS),  
a form of CDMA

# PHY-layer packet structure



- Preamble -> Symbol synchronization
- Packet delimiter -> Frame synchronization
- PHY header: length of the PSDU
- PSDU can carry upto 127 bytes

# Additional Tasks of PHY of IEEE 802.15.4

---

- **Activation and deactivation of the radio transreceiver**
  - Three states: Transmitting, receiving and sleeping
- **Receiver energy detection**
  - No decoding or signal identification
  - Required to understand if the channel is busy or idle
- **Link quality indication**
  - Using energy or SNR estimation or both
- **Clear channel assessment**
  - Energy detection or carrier sense or both
- **Channel frequency selection**
  - 27 channels

# MAC Layer features

---

- Designed to support vast number of industrial and home applications for control and monitoring
- Enabling deployment of large number of devices with low cost and complexity
- Several features for flexible network configuration and low-power operation
  - Different topologies and network devices
  - Optional superframe structure with duty-cycle control
  - Both contention and scheduled based MAC protocols
  - Synchronized and non-synchronized operation
  - Efficient energy management
    - Adaptive sleep
    - Extended sleeping time
  - Flexible addressing scheme for large number of nodes

# MAC Layer: *Device Types*

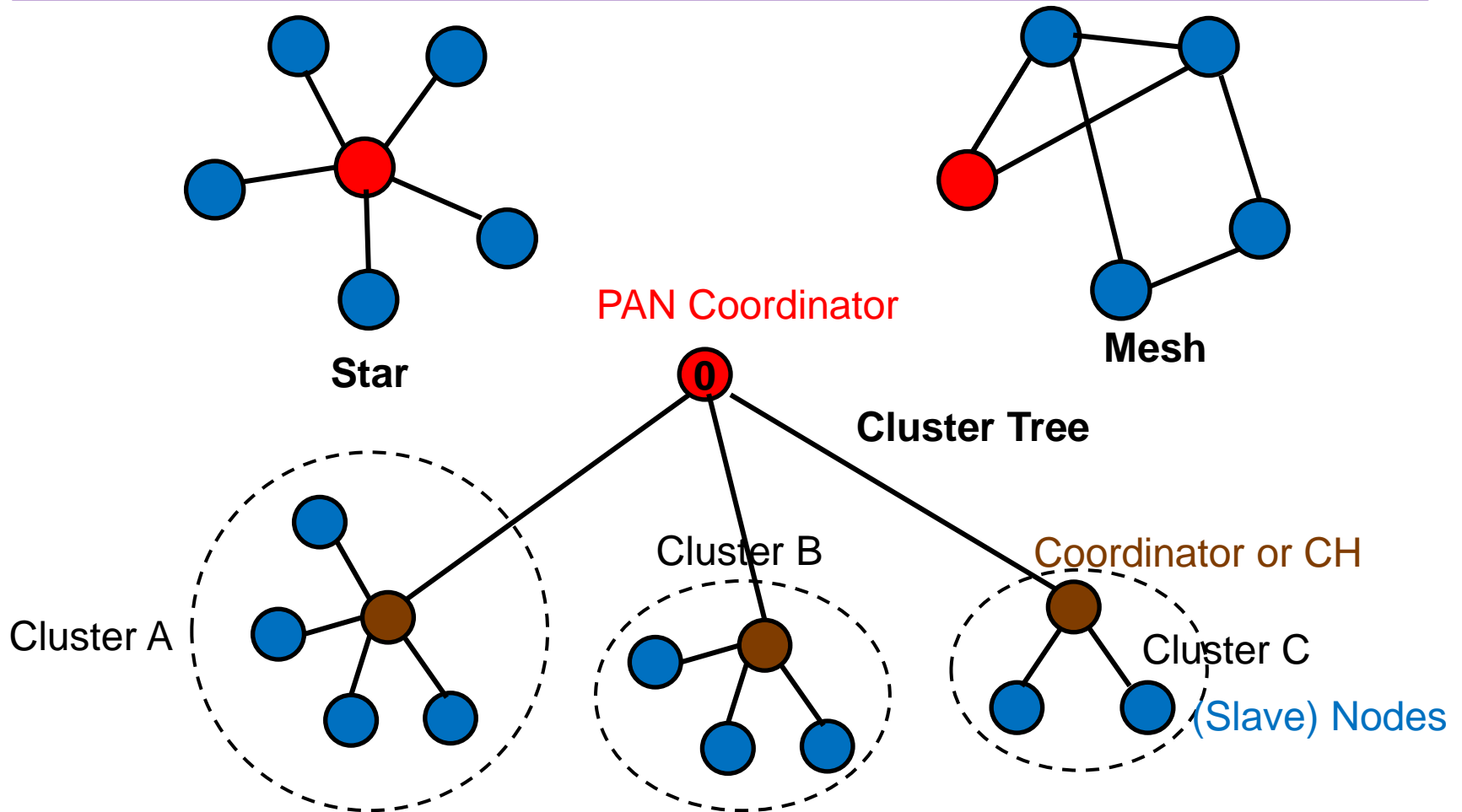
---

Two kind of devices in IEEE 802.15.4 based on complexity and capability

- Fully functional devices (FFD)
  - More resources
  - Multiple network responsibilities
- Reduced functionality devices (RFD)
  - Simple and low-cost device
  - Can only communicate with one FFD



# Topologies: Zigbee (Network Layer)



- 16 bit addresses support 65536 devices in a PAN. For clusters, 255 clusters with 254 nodes each
- Self recovering ability

# Zigbee Node Types

---

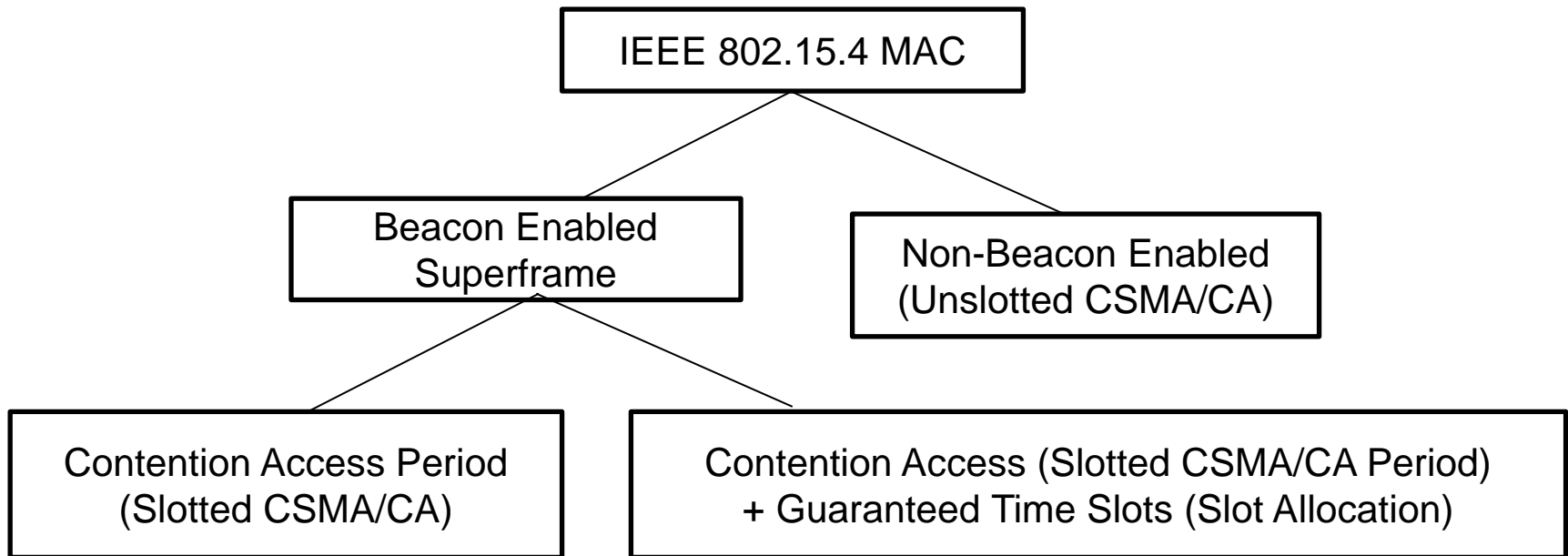
Zigbee defines three kinds of logical devices

- **PAN coordinator or Master**
  - Principal controller of network
  - Managing list of all network devices or nodes
  - Identifies PAN and nodes associated with it
  - Provides global synchronization by transmitting beacon frames containing relevant information
- **Coordinator or cluster head (CH)**
  - Same functionalities as PAN coordinator locally in cluster
  - Managing association and disassociation of other nodes to PAN
  - Does not create its PAN
- **Simple (Slave) Nodes**
  - No coordination functionalities
- PAN Coordinator and CH are **FFD** while slave nodes are **RFD**

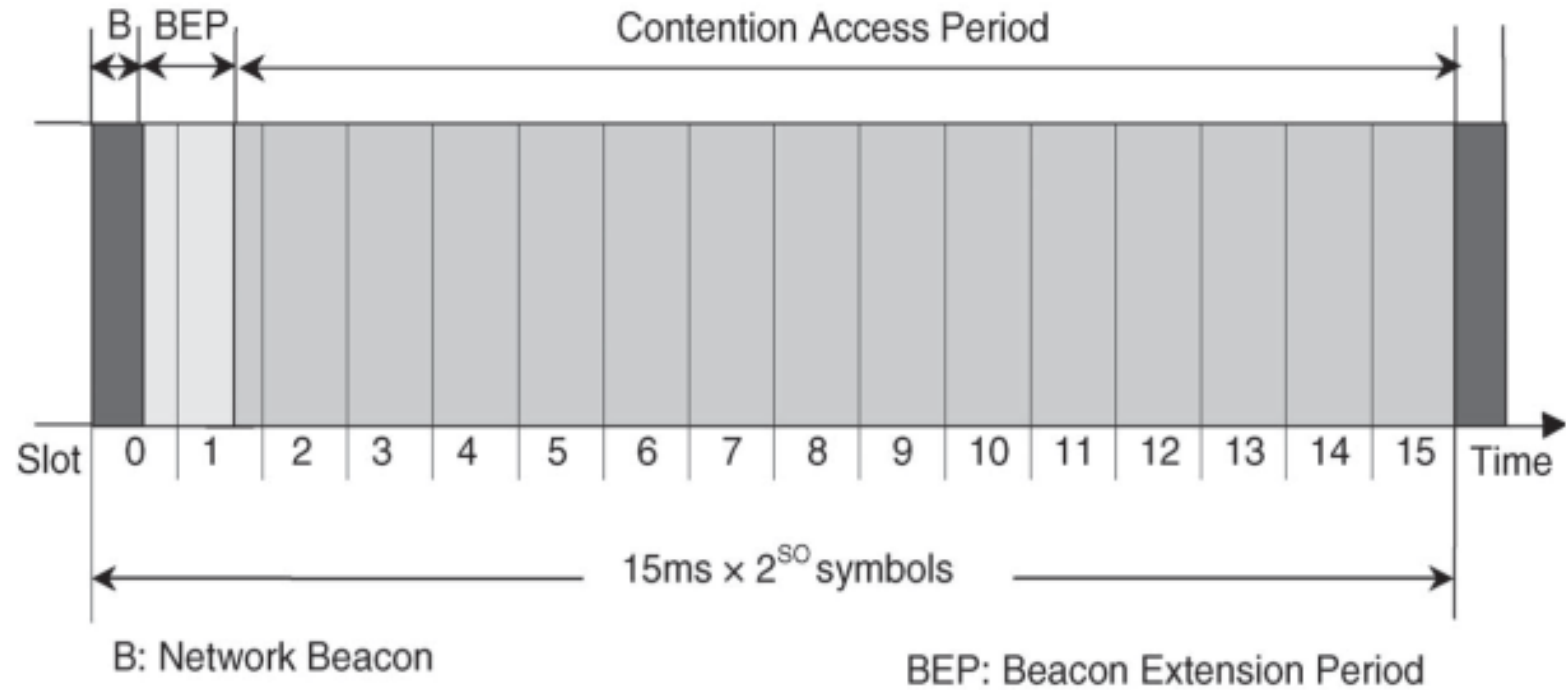
# MAC layer functions

---

- Network association and disassociation
- Two modes of operation
  - Beaconsing
  - Non-beaconsing

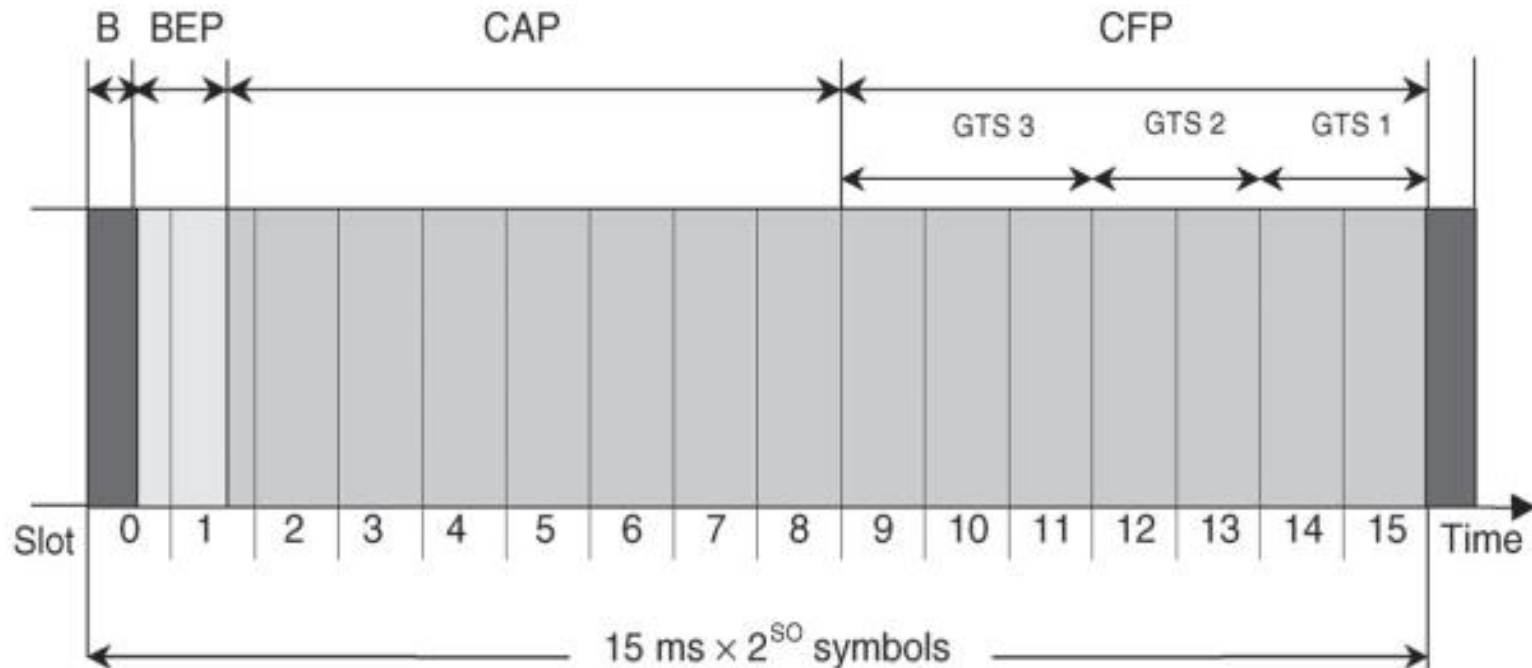


# MAC: Superframe Structure



[Sohraby2007]

# MAC: QoS Superframe Structure



CAP: Contention Access Period

GTS: Guaranteed Time Slot

SO: Superframe Order

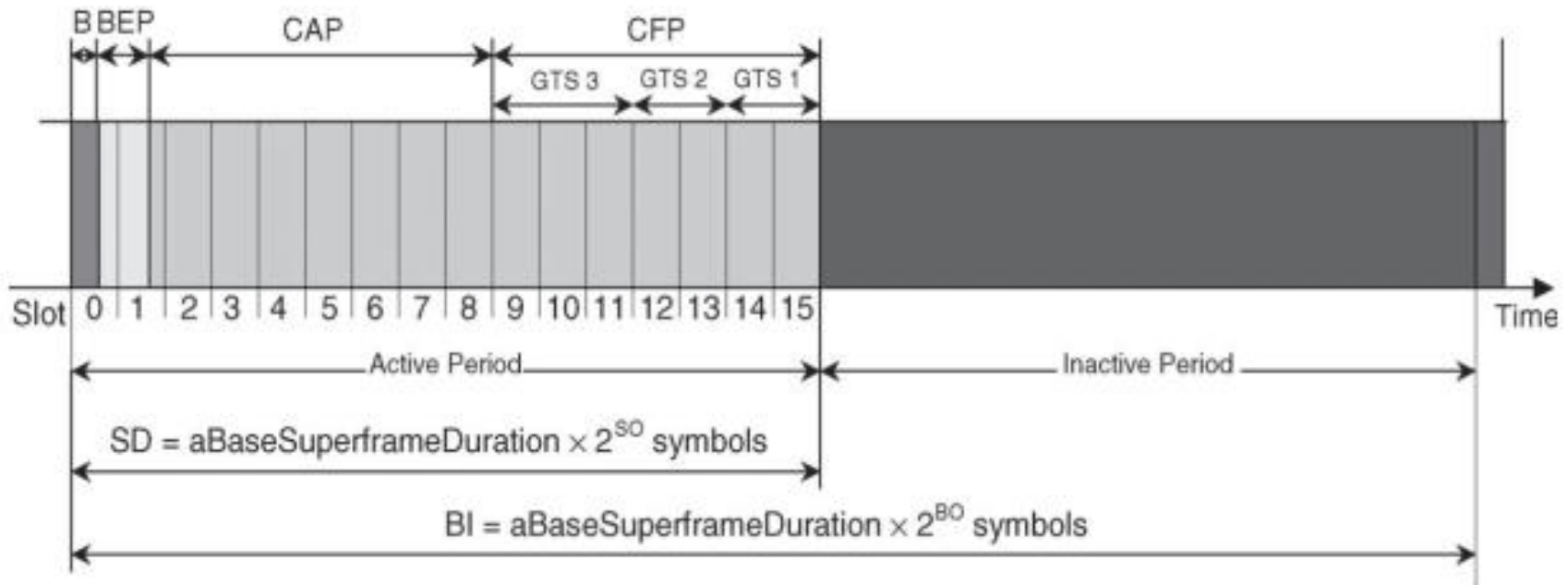
B: Network Beacon

BEP: Beacon Extension Period

CFP: Contention Free Period

[Sohraby2007]

# MAC: Superframe Structure with Energy Saving



CAP: Contention Access Period  
CFP: Contention Free Period  
GTS: Guaranteed Time Slot

BO: Beacon Order  
BI: Beacon Interval  
SO: Superframe Order

B: Network Beacon  
BEP: Beacon Extension Period  
SD: Superframe Duration

SO and BO are MAC attributes,  $0 \leq SO \leq BO \leq 14$ .

[Sohraby2007]

# General MAC frame format

Octets:	1	0/	0/2/	0/	0/2/	Variabl	2
Frame Control	Sequence number	Destination n PAN	Destination n	Source PAN Identifier	Source Address	Frame Payload	Frame Check Sequence
	Addressing						
	MAC					MAC Payload	MAC Footer

Bits: 0-	3	4	5	6	7-	10-	12-	14-
Frame Type	Security Enabled	Frame Pending	Ack Request	Intra PAN	Reserved	Destination Addressing Mode	Reserve	Source Addressing Mode

Frame Type Value b <sub>0</sub> b <sub>1</sub> b <sub>2</sub>	Description
0 0 0	Beacon
0 0 1	Data
0 1 0	Acknowledgement
0 1 1	MAC Command
1 0 0 - 1 1 1	Reserved

[Sohraby2007]

# Frame Types

---

- Beacon
  - Transmitted periodically by PAN coordinator
  - Several purposes such as identifying the network and its structure, wake-up devices, synchronizing network operations
- Data
  - Payload up to 104 octets
  - Use of sequence number and frame sequence number field
- Acknowledgement
  - Receiver acknowledges reception of data
  - Successful or not
- Command
  - Control and configure devices remotely
  - Negotiation and communication with other nodes
    - Device association and disassociation, data request, beacon request, GTS requests



# MAC: *Types of traffic supported*

---

- Periodic
  - temperature
- Intermittent
  - External impulse: pollution level exceeded
- Repetitive low-latency
  - Mouse, Security

# IEEE 802.15.4 Versions

---

- Since the first version in 2003, new amendments are constantly being introduced.
- Modifications
  - New country specific (frequencies, regulation)
  - New application and network specific:
    - SUN: Smart utility meter monitoring
    - LECIM: Low Energy Critical Infrastructure Monitoring
    - RFID: Radio Frequency Identification
    - RCC: Railway Communications and Control
    - TVWS: TV White Space
    - Medical
  - New PHY specific
    - OFDM, ASK, FSK, QAM, GMSK, MSK, OOK
  - New Protocols
    - TSCH, Aloha, PCA

# IEEE 802.15.4 Versions

Not in Syllabus for Exam

Classification	PHY	MAC	Revision
Versions			IEEE 802.15.4-2006
	IEEE 802.15.4a-2007	IEEE 802.15.4a-2007	
	IEEE 802.15.4c-2009		
	IEEE 802.15.4d-2009	IEEE 802.15.4d-2009	
			IEEE 802.15.4-2011
		IEEE 802.15.4e-2012	
	IEEE 802.15.4f-2012		
	IEEE 802.15.4g-2012	IEEE 802.15.4g-2012	
	IEEE 802.15.4j-2013		
		IEEE 802.15.4k-2013	
	IEEE 802.15.4m-2014	IEEE 802.15.4m-2014	
	IEEE 802.15.4p-2014	IEEE 802.15.4p-2014	
			IEEE 802.15.4-2015
	IEEE 802.15.4n-2016		
	IEEE 802.15.4q-2016		
	IEEE 802.15.4u-2016		
	IEEE 802.15.4t-2017		
	IEEE 802.15.4v-2017	IEEE 802.15.4v-2017	
	IEEE 802.15.4s-2018	IEEE 802.15.4s-2018	
	IEEE 802.15.4x-2019		

# IEEE 802.15.4 Versions

Not in Syllabus for Exam

Versions	Date	Type of network	Max Data rate kb/s	Modulation Encoding	protocole used	Features
802.15.4	2003	LR-WPAN	250	BPSK O-QPSK O-QPSK	CSMA/CA	Ultra-low power consumption Low data rate, usage of security suite Very low-cost
802.15.4	2006	LR-WPAN	250	ASK O-QPSK BPSK	CSMA/CA	Improves usage of security suite Allowing synchronization of broadcast messages
802.15.4a	2007	LR-WPAN	1000	DQPSK DQPSK BPM-BPSK DQPSK	ALOHA	Using the same frequency channel simultaneously Precision ranging Support of long-range links
802.15.4c	2009	CWPAN	250	MPSK O-QPSK	–	–
802.15.4d	2009	LR-WPAN	100	BPSK GFSK GFSK	CSMA/CA	Coexistence of listen before talk Coexistence of transmission control Coexistence of duty cycle
802.15.4	2011	LR-WPAN	1000	See Sect. 4.5	CSMA/CA ALOHA	Editorial changes and not technical

# IEEE 802.15.4 Versions

Not in Syllabus for Exam

Versions	Date	Type of network	Max Data rate kb/s	Modulation Encoding	protocole used	Features
802.15.4e	2012	Industrial LR-WPAN	–	–	DSME LLDN TSCH	QoS, Security Minimizing collisions Deterministic yet flexible bandwidth Interference avoidance Multi-channel, multi-superframe High reliability of the system
802.15.4f	2012	RFID	250	MSK OOK PPM	ALOHA	Multi-year battery life Reliable communications Precision location
802.15.4g	2012	SUN	800	FSK BPSK QPSK QAM O-QPSK	CCA	Interference avoidance Security
802.15.4j	2013	MBAN	250	O-QPSK	– –	Keeping a channelization scheme flexible
802.15.4k	2013	LECIM	–	BPSK O-QPSK FSK GFSK P-FSK P-GFSK	CSMA/CA PCA ALOHA PCA	Reduction of collision probability Good transmit power efficiency Higher sensitivity Priority Forward error correction QoS, security

# IEEE 802.15.4 Versions

Not in Syllabus for Exam

Versions	Date	Type of network	Max Data rate kb/s	Modulation Encoding	protocole used	Features
802.15.4m	2014	TVWS	1638	FSK BPSK QPSK 16-QAM	–	Low energy mechanism Ranging performance enhancement
802.15.4p	2014	RCCN	36	64-QAM GMSK C4FM QPSK $\frac{\pi}{4}$ DQPSK DPSK BPSK	CSMA/CA CSMA/CA PCA	Supporting fixed-to-fixed, fixed-to-mobile, and mobile-to-mobile communications
802.15.4	2015	SUN, TVWS MBAN RFID LECIM, RCC	1000	See Sect. 4.14	TSCH CCA TSCH CSMA CSMA/CA PCA ALOHA PCA	Editorial changes and not technical
802.15.4n	2016	CMB	500	O-QPSK GFSK	–	Medical information transmission

# IEEE 802.15.4 Versions

Not in Syllabus for Exam

Versions	Date	Type of network	Max Data rate kb/s	Modulation Encoding	protocole used	Features
802.15.4q	2016	–	Up to 1000	GFSK ASK	–	Reduction in energy consumption Higher data rates Further reduction in peak power Tradeoff between receiver complexity and performance
802.15.4u	2016	SUN	150	2-FSK	–	Used for broader unlicensed of power levels up to 4 W
802.15.4t	2017		2000	GMSK	–	High data-rate
802.15.4v	2017	SUN LECIM TVWS	300	O-QPSK FSK OFDM	–	Enabling the regional sub-GHz bands
802.15.4s	2018			–	–	Selection of the best available PAN
802.15.4x	2019	TVWS	Up to 2400	FSK O-QPSK OFDM	–	Efficient radio spectrum High data-rate

# IEEE 802.15.4u-2016: *India specific*

---

PHY (MHz)	Frequency band (MHz)	Modulation	Data-rate (kb/s)	Number of channels
866	865-867	2-FSK mode 1	50	19
		2-FSK mode 2	100	10
		2-FSK mode 3	150	10

- Needed for M2M/IoT use cases in sub 1 GHz band in India
- Approved in Sept. 2016 as a third amendment to IEEE 802.15.4-2015
  - IEEE 802.15.4n-2016
  - IEEE 802.15.4q-2016
- Defines a new alternate SUN FSK PHY extension in the 866 MHz band



# Zigbee Versions

---

- 2005 – Zigbee 2004 released
- 2006 – Zigbee 2006 released
- 2007 – Zigbee 2007 released (also known as Zigbee Pro)
- 2015 – Zigbee 3.0 version (with IP)
- 2019 – Zigbee Alliance merges into **Connectivity Standards Alliance**
  - Amazon, Apple, Google and Zigbee Alliance
  - Develop a new open standard for smart home device connectivity
  - Connected home over IP (CHIP) project
  - **Matter as home connectivity technology**
    - **In addition to IEEE 802.15.4, Matter also supports Ethernet and WiFi**

# Zigbee Green Power

---

- Integrating battery-less (energy harvesting-based) or life-long battery-operated devices into the Zigbee network



Sensors, open/close detectors, emergency buttons, industrial switches, ...



- (Light) switch: flipping the switch generates the energy for data-communication

# Zigbee Use Case: *Smart Lighting (Philips Hue)*

---

- Benefits of Smart Lighting
  - Controlling lights automatically or remotely via app
  - Easily Dimmable
  - Energy efficient using LED bulbs
  - Can connect bulb to other devices in home such as camera, audio equipment, thermostat or home assistant
  - Configure the lights to mimic your presence when you are away
  - Mood lighting



# Zigbee Use Cases

---



Amazon Echo Plus (2nd Gen+)



Samsung SmartThings



Philips Hue by Signify



IKEA



Xfinity by Comcast



Wink



Tuya



Lumi

# Key IoT Features

---

## Advantages

- Low power
  - Zigbee (20 mJ per hour)
  - Zigbee Pro (Green Power: 20 microJ per hour)
- Large coverage of 1Km in Sub-GHz band
  - Even more for boosted modules (3.2 km for Xbee)
- Easy to install and maintain (mesh, self-healing, self-organization)
- Reliable (mesh, multiple channels, demonstrated interference tolerance, automated retransmissions)
- Supports thousands of nodes
- Low cost (many suppliers)
- Long battery life (years on AA battery)
- Secure (AES 128 bit)

**Source: Zigbee 3.0**

## Issues

- No mobility support, Scalability
- Less coverage area in 2.4 GHz band

---

**Questions?**

---

**WiFi: IEEE 802.11 family**

# WiFi: What's in a name?

---

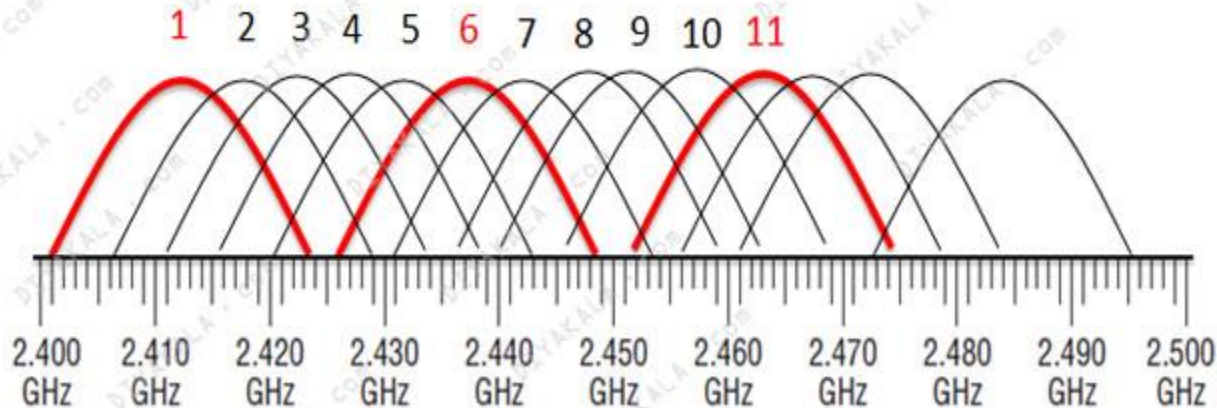
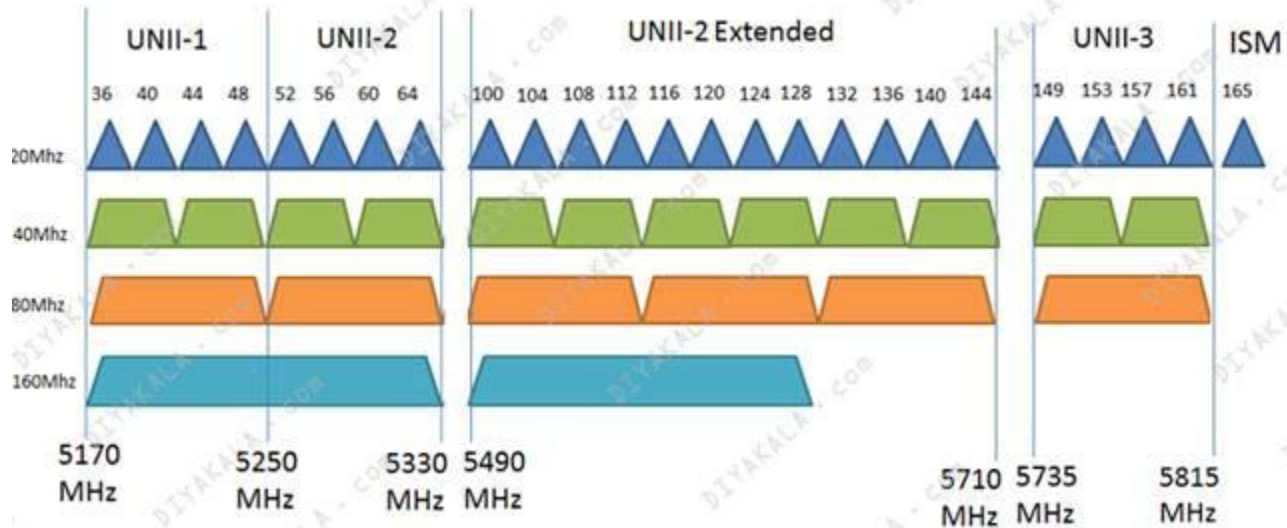
- WiFi is a short name for Wireless Fidelity
- On the lines of *Hi-Fi* (high fidelity), a term for high-quality audio technology
- *Fidelity is defined as the degree of exactness with which something is copied or reproduced.*
- This is also called Wireless Local Area Network (WLAN)



# WLAN Standards

	1G	2/3G	4G	5G	6G	
	2000	2004	2008	2012	2016	2020
Standard	11b	11a/g	11n	11ac (wave1)	11ac (wave2)	11ax
MCS	Spread Spectrum	OFDM				OFDM (OFDMA)
Freq	2.4GHz	2.4GHz 5GHz				Same Freq (<7GHz)
Bandwidth	20MHz	20MHz	+40MHz	+80MHz	+160MHz	Same BW (+320M)
Multiple Antenna			MIMO Beamforming		MU-MIMO (DL)	MU-MIMO (UL)
PHY Rate	11Mbps	54Mbps	600Mbps (40M,4SS)	1.7Gbps (80M,4SS)	6.7Gbps (160M,8SS)	9.6Gbps (160M,8SS)
MAC	CSMA/CA in DCF	Security QoS	Aggregation			BSS Management

# WLAN Bandwidths



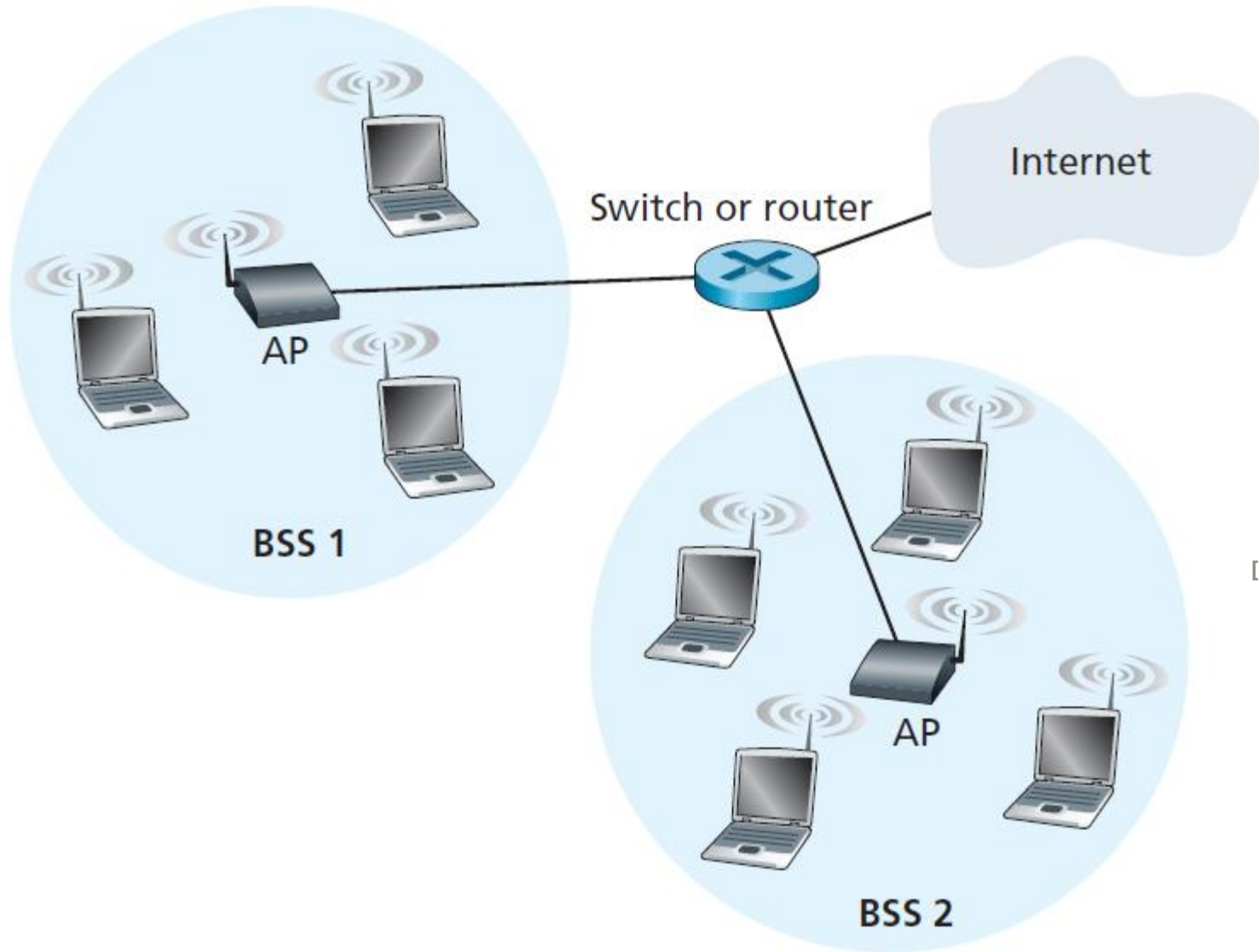
# IEEE 802.11 Network Topologies

---

Nodes as **stations** and cluster head as **access point**

- Basic service set (BSS) or Star
- Extended service set (ESS) or cluster tree
- Independent basic service set (IBSS)
  - Ad-hoc = Mesh without access point
- Mesh basic service set (MBSS)
  - (wired or wireless) Mesh of cluster heads (Hybrid)

# WLAN architecture: *Infrastructure mode*

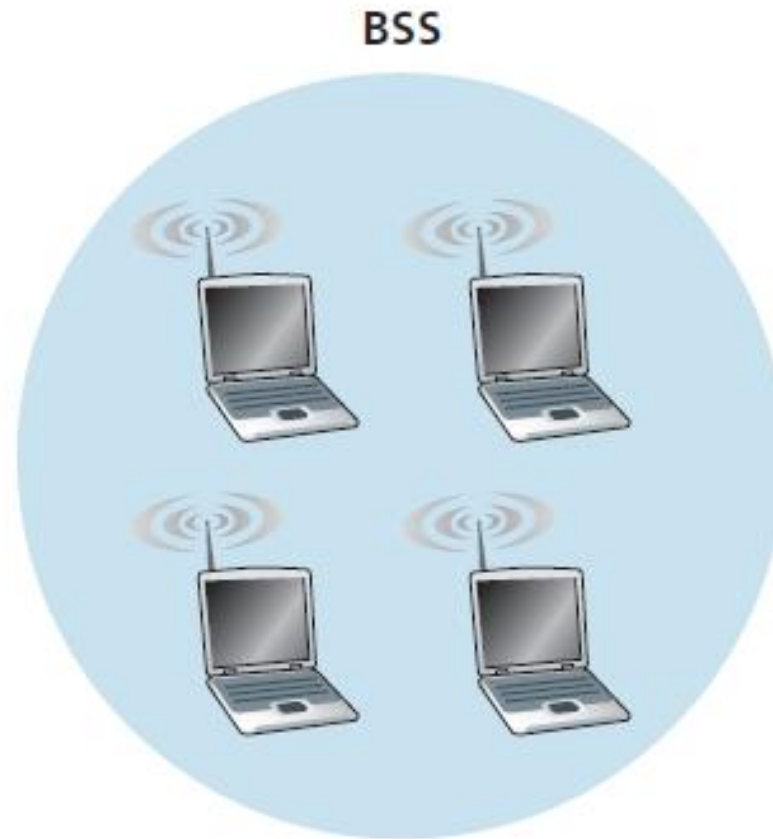


[Kurose2012]

# WLAN: *Adhoc mode*

---

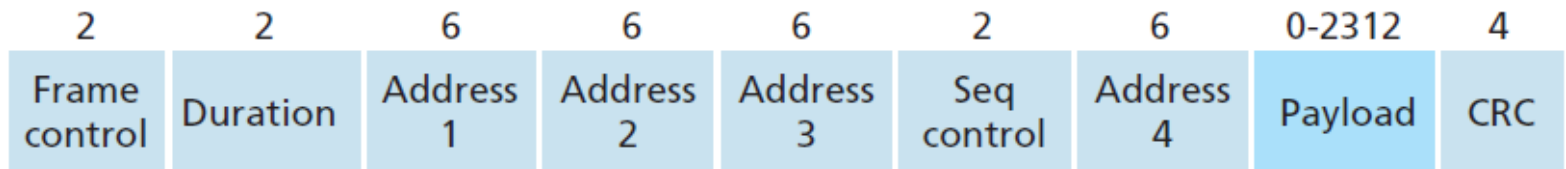
- Also called WiFi Direct



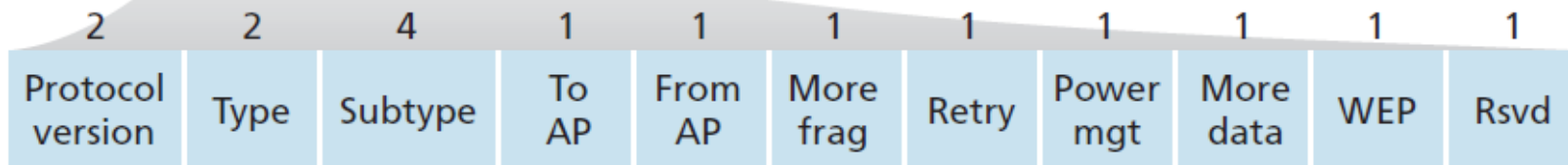
# MAC Frame Format

---

Frame (numbers indicate field length in bytes):



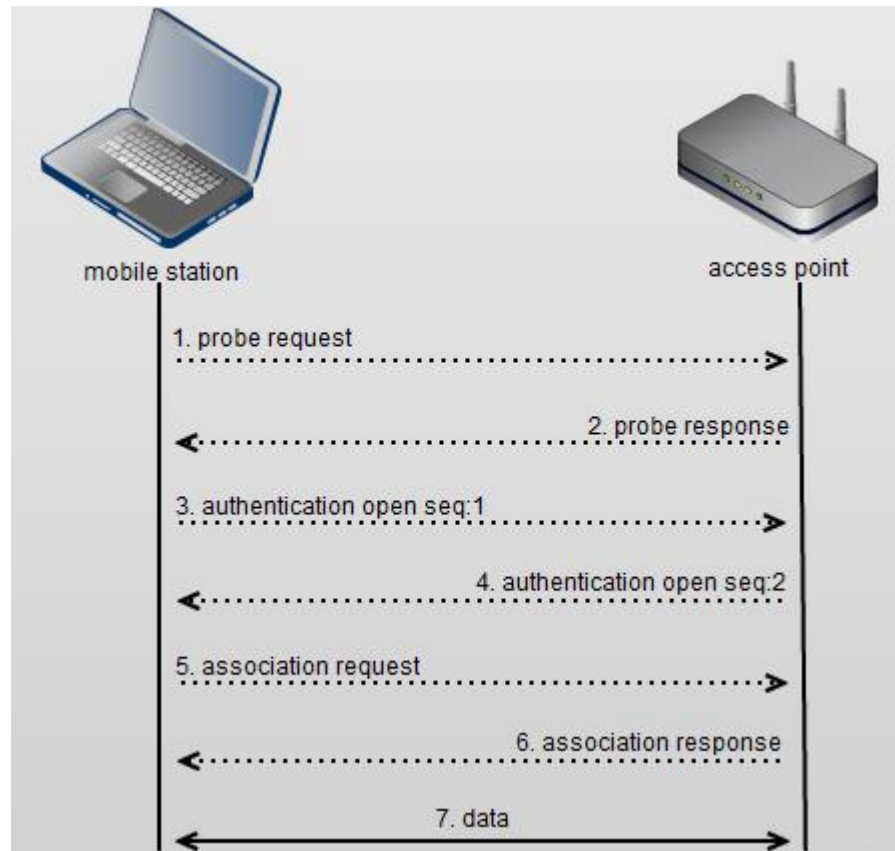
Frame control field expanded (numbers indicate field length in bits):



- CRC: 32-bit Cyclic Redundancy Check
- WEP: Wired Equivalent Privacy

# Association Process

- Three states
  - Not authenticated or associated
  - Authenticated but not associated
  - Authenticated and associated



---

**How IEEE 802.11 adopted for IoT?**



# 802.11ac (5G of WiFi) and 802.11ah (WiFi-Halow)

---

	802.11ac	802.11ah
Operating Bands	2.4 and 5 GHz	Sub 1-GHz
Spectrum available	100 + 150 MHz	26 MHz
Use Cases	Broadband wireless	Sensors and Meters Extended WiFi
Data Rate Requirement	20 Mbps - 3 Gbps	100 Kbps
Single Frame Size	Large (e.g., 1500 bytes)	Small (e.g., 100 bytes)
Traffic type	Video Streaming/ Large file transfer	Periodic packet transmission every few to tens minutes
Distance between devices	Up to 60 m	Up to 1 Km
Number of stations	3-20	8191
Location	Mostly indoor	Indoor and outdoor
Backward compatibility	Yes	No

[Park2015, Gonzalvez2016]

# PHY parameters for 802.11ah

- Use of orthogonal frequency division multiplexing (OFDM)
- Basically adapted a scaled-down version of 802.11ac
  - Bandwidths of 20-160 MHz to 2-16 MHz
  - Same number of subcarrier
  - Increased symbol duration

[Park2015]

Parameters	Supported Values
Channel Bandwidths	2, 4, 8, and 16 MHz
Modulation Schemes	BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
Code Rates	1/2 with 2 times repetition 1/2 , 2/3, 3/4 and 5/6 Convolution or low-density parity check (LDPC)
MIMO	Support up to 4 by 4
Data Rates	150 Kbps (1 MHz bandwidth, 1 spatial stream, BPSK, 1/2 coding rate, repetition) to 347 Mbps (16 MHz bandwidth, 4 spatial streams, 256 QAM, 5/6 coding rate )

# Link Budget Comparison

---

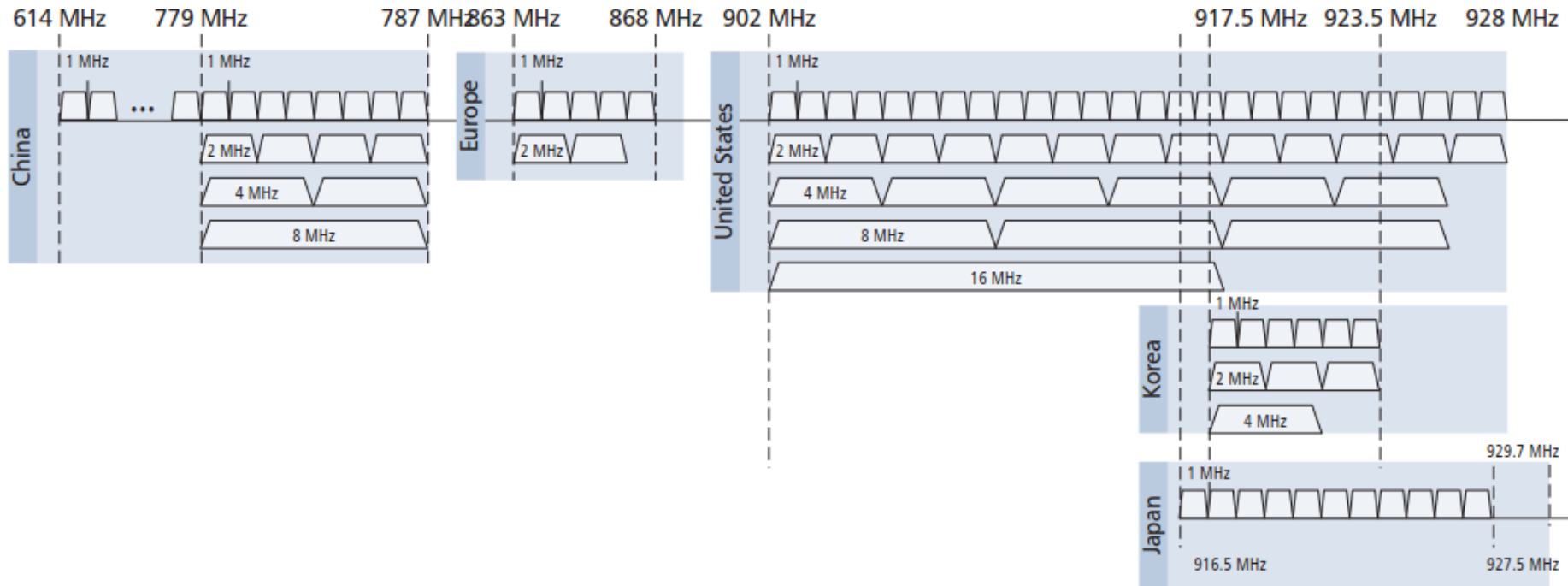
Parameters	Link budget enhancements of 900 MHz 802.11ah over 2.4 GHz 802.11n
Free space path loss	+8.5 dB
Noise bandwidth	+10 dB
Sub-total link budget gain	+18.5 dB
1 MHz channel width	+3 dB
Repetition coding	+3 dB
Total link budget gain	+24.5 dB

[Park2015]

## **Low Power and Low Cost Support for Indoor Sensors:**

This can reduce the transmit energy consumption and also lower the cost of an 802.11ah radio of a small sensor device.

# Frequency Bands in Different Countries



[Park2015]

# 802.11ah MAC features

---

- Hierarchical association identifier
- Access scheme: Hybrid Coordination Function (HCF)
- Optional Restricted Access Window (RAW)
- Increased sleep time
- Target wake-up time
- Bidirectional transmission opportunity
- Short MAC frame
- Null data packet for ACK
- Synchronization frame operation
- And few more!

# Hybrid Coordination Function (HCF)

---

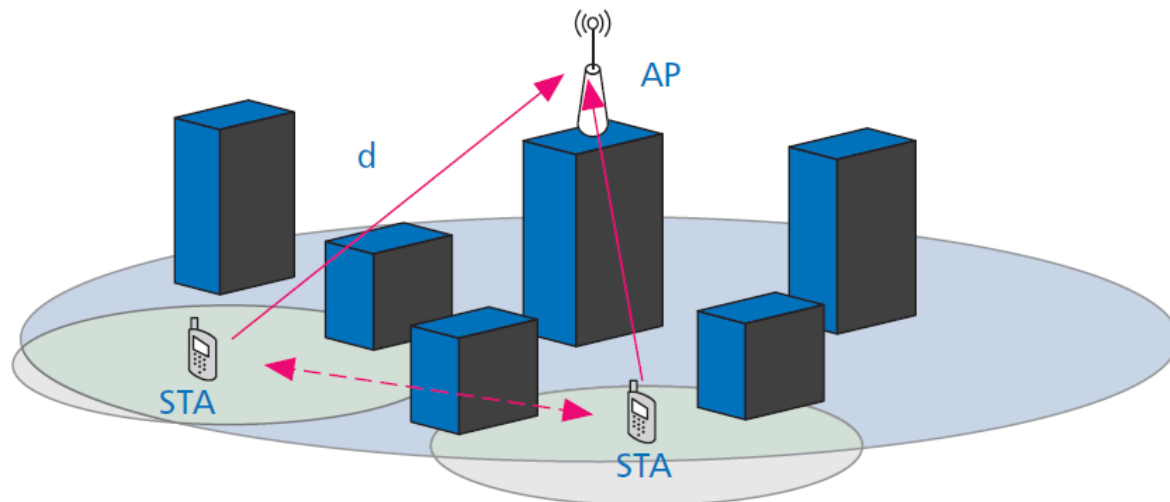
- 802.11
  - CSMA/CA
- 802.11ah
  - HCF controlled channel access
    - Polling based for infrastructure based networks
    - Guarantees Quality of Service
  - Enhanced distributed channel access (EDCA)
    - EDCA is extension of CSMA/CA that tries to implement service differentiation by classifying the traffic into different categories with different priorities

[Gonzalez2016]

# Restricted Access Window (RAW)

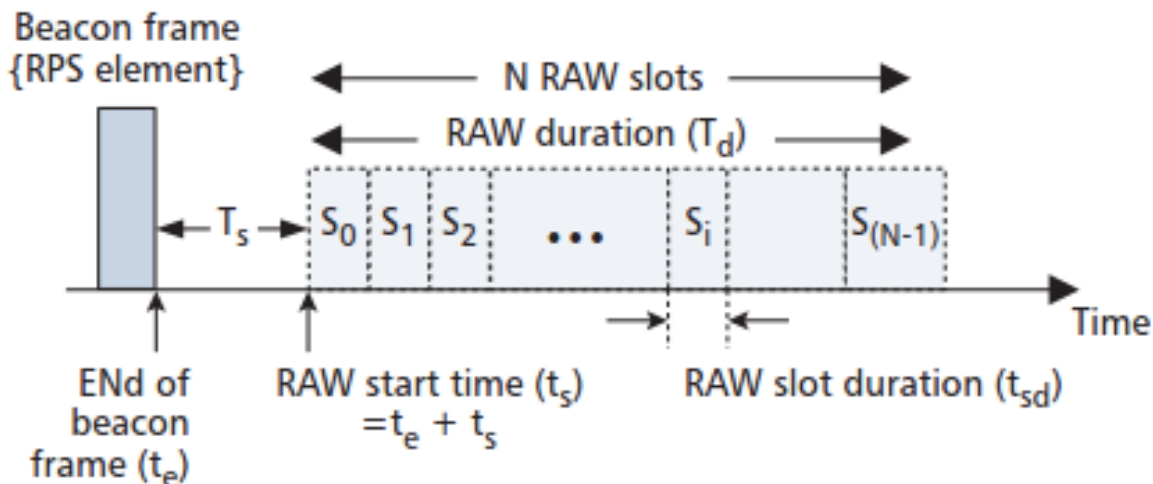
---

- Issue with supporting 1 Km range outdoors
  - Access point for outdoor applications are installed on top while users are near grounds
    - High path loss and Shadowing
  - Severe hidden node problem between several APs supporting thousands of nodes
    - Several collisions and subsequent retransmissions cause energy consumption
- RAW minimizes the issue



# Restricted Access Window (RAW)

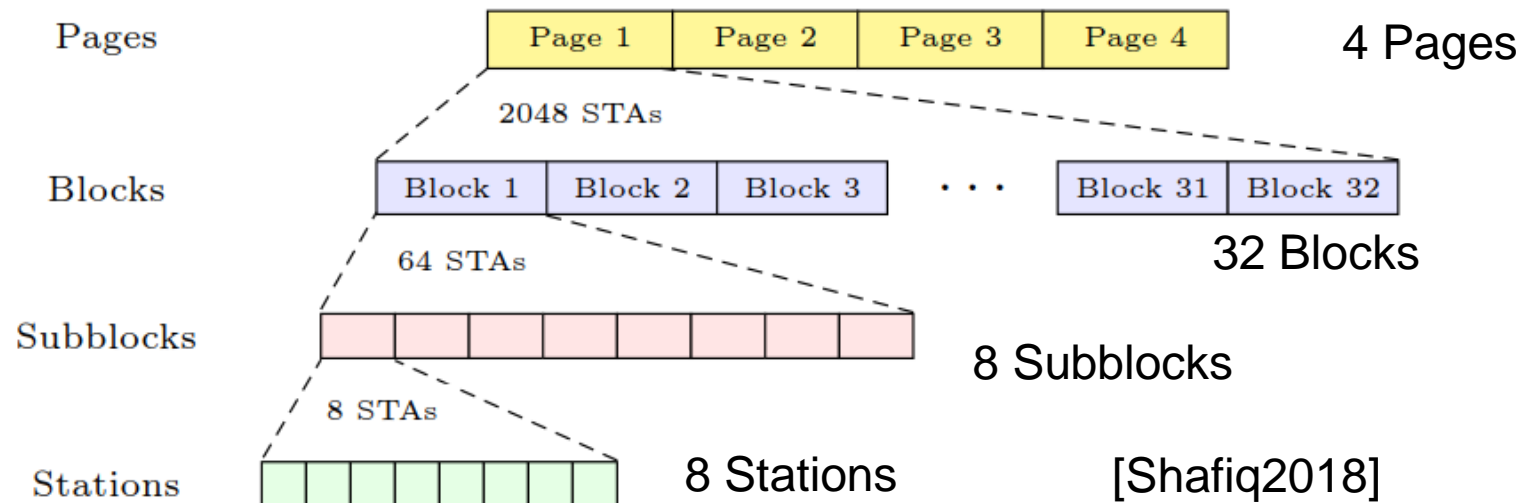
- Station or node grouping mechanism
- New optional contention channel access scheme
  - Combination of TDMA and CSMA/CA
- In the time window frame is divided into RAW slots
  - maximum of 64 slots
- Nodes are divided into groups and only members of a particular group have access to that time slot
- Reduces collisions, improve channel efficiency, and allows an increasing number of users





# Hierarchical Association Identifier (AID)

- Legacy 802.11 supports 2007 nodes (or associated stations) per access point
- 802.11ah uses a novel hierarchical AID
  - New AID consists of 13 bits and can support 8191 nodes
  - Four levels: Page, block, sub-block, and station-index in sub-block
  - This structure can be used to group stations based on similar characteristics such as traffic, pattern, location, battery levels, etc.



# Increased Sleep Time

---

- In 802.11, the max sleep time is 18 hours without getting disassociated with the AP
- For 802.11ah, the max sleep time is redefined such that the station can sleep for approximately 5.2 years

# Target Wakeup Time (TWT)

---

- 802.11
  - An AP buffers data destined for a station while the station is in sleep state
  - The station periodically wakes up at beacon transmission times and receives a beacon to see if there is any buffered data at the AP based on the information in traffic indication map (TIM)
  - If TIM indicates that there is data buffered at AP, it sends a PS-Poll frame to the AP to indicate the station is awake and is ready to receive the buffered data
  - The AP needs time to find the buffered data and has to contend for the medium: this indefinite latency makes the station consume energy waiting for the buffered data
- 802.11ah
  - Uses target wake-up time between an AP and a station so that the AP knows when the station will be awake
  - Removes the processing time and medium access latency

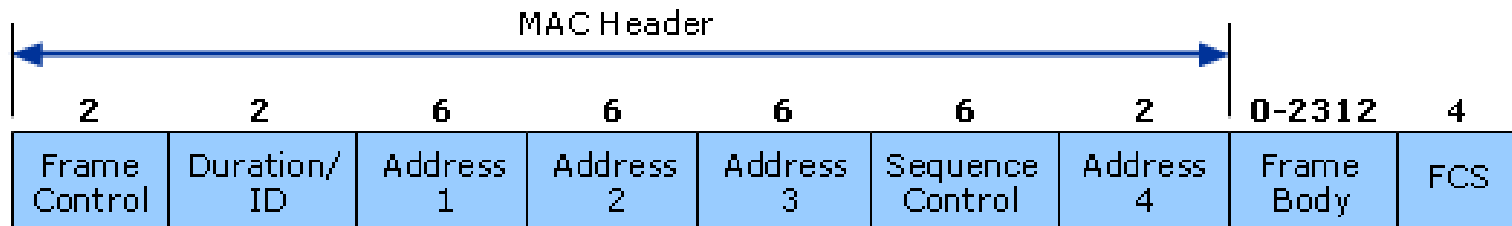
# Bidirectional Transmission Opportunity

---

- Bidirectional transmission (BDT) allows an AP and a station to exchange one or more uplink and downlink packets in one TXOP.
- Packets are separated by short inter frame space (SIFS)
- In the BDT procedure, a station uses the More Data bit in the SIGNAL field of PHY preamble of a packet to indicate whether the station has more data to transmit following the current packet transmission.
- This reduces the number of contention-based channel accesses, improves channel efficiency by minimizing the number of frame exchanges required for uplink and downlink data frames, and enables stations to extend battery lifetime by keeping Awake-times short.

# Short MAC Frame

- In 802.11n, the MAC header can be 30 bytes long



[https://technet.microsoft.com/en-us/library/cc757419\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc757419(v=ws.10).aspx)

- For IoT application transmitting only 50 bytes of data infrequently, this is big overhead
- In 802.11ah, the length of header is reduced to 12 bytes

# 802.11ax (6G of WiFi)

---

- ❑ Convergence of high data rates and IoT applications
- ❑ Smarter access points for improved outdoor coverage with longer guard intervals
- ❑ Target Wake-up Time
- ❑ BSS coloring to reduce interference
- ❑ Only on 5 GHz
- ❑ Comparison with 802.11ac
  - 6 times speed, 7 times battery life with TWT, 4 times range
  - Support much more than 7 devices
- ❑ OFDMA instead of OFDM
- ❑ MU-MIMO
- ❑ 1024 QAM and 160 MHz bandwidth to give multi-giga bit data rates

# Key IoT Features (802.11ah)

---

- High data rates
  - Can handle diverse range of applications including camera
- Longer range than traditional WiFi
- Scalable to thousands of nodes
- Widely used

## Issues

- Most of the world is using 2.4 GHz
  - Problem for 802.11ah
- 802.11ah available, but products are hardly there
  - Mostly using 802.11b/g/n
- Security
- High power consumption
- Roaming

# WiFi Halow products

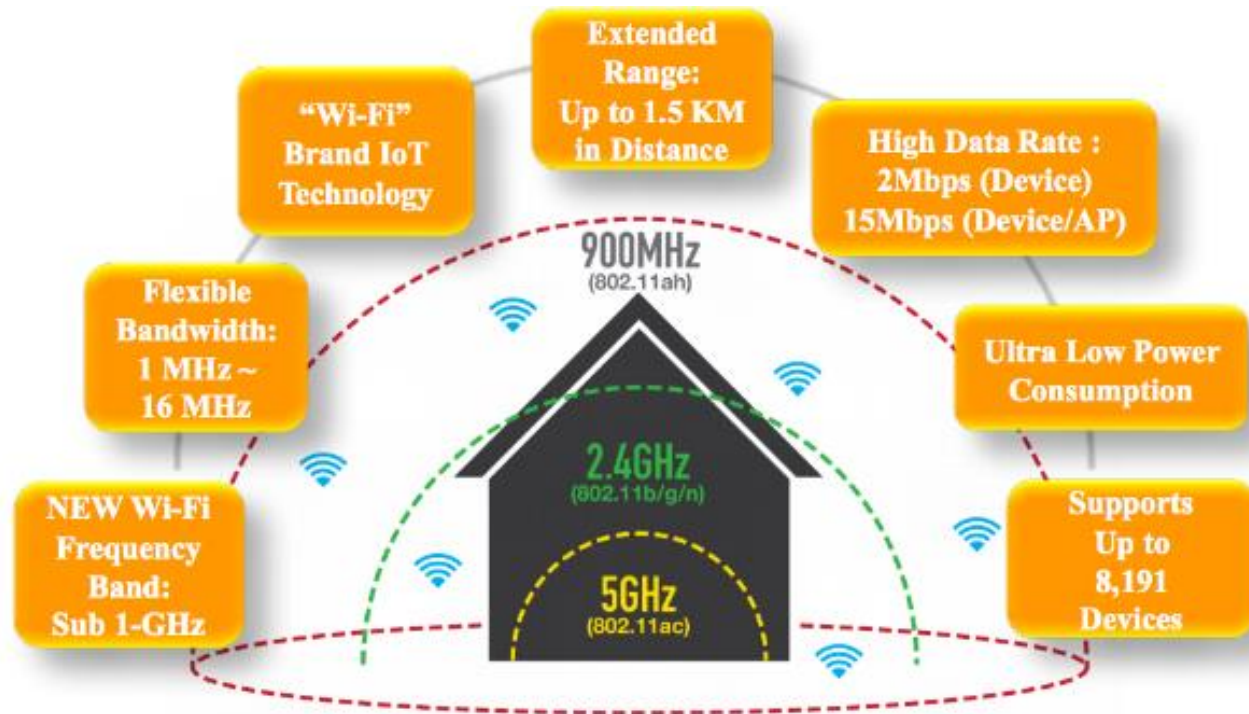
---

- [Adapt-IP](#)
- [Alfa wireless](#)
- [Methods2Business](#)
- [Newratek](#) / [Newracom](#)
- [Palma Ceia SemiDesign](#)
- [Huge-IC](#)
- [Silex Technology's SX-NEWAH](#)

Links embedded



# Example of SX-NEWAH



**NEWRACOM** © 2017 NEWRACOM INC.

<https://www.silextechnology.com/connectivity-solutions/embedded-wireless/sx-newah>

---

**Questions?**

# References

---

- Perry Lea, *Internet of Things for Architect*, Packt Publication, 2018
- [Gonzalez]
- [Kurose2012] J. Kurose and K. Ross, *Computer Networking*, Pearson, 2012
- [Park 2015] M. Park, “IEEE 802.11ah: Sub 1-GHz License Exempt Operation for the Internet of Things,” *IEEE Communications Magazine*, September 2015
- [Tian2021] L. Tian et al., “WiFi HaloW for the Internet of Things: An up-to-date survey on IEEE 802.11ah research,” *Journal of Network and Computer Applications*, 2021

---

**That's all for today!**  
**Thank You!**