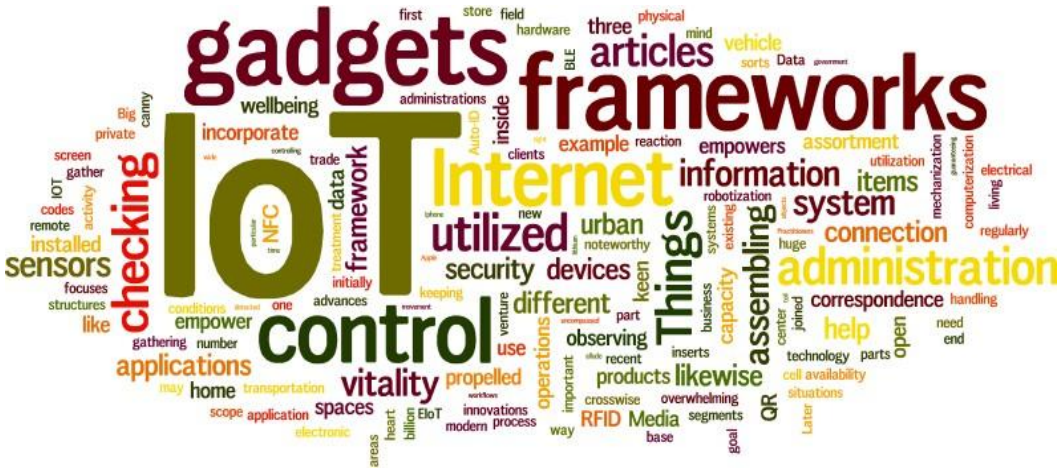
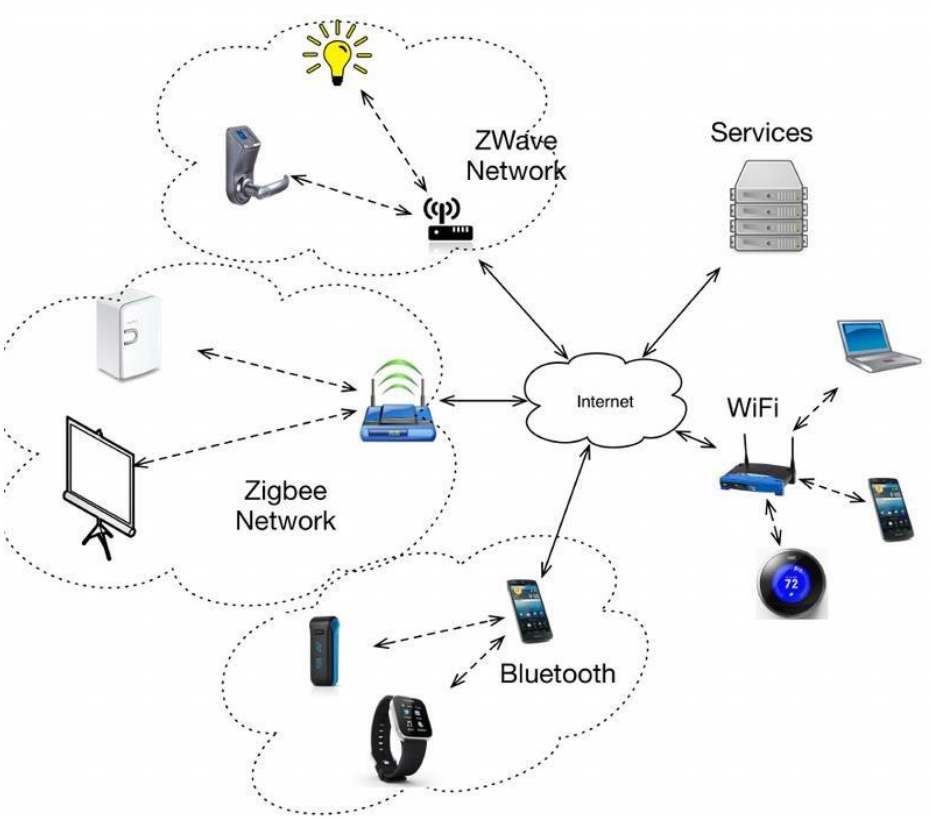
Connecting Smart Objects

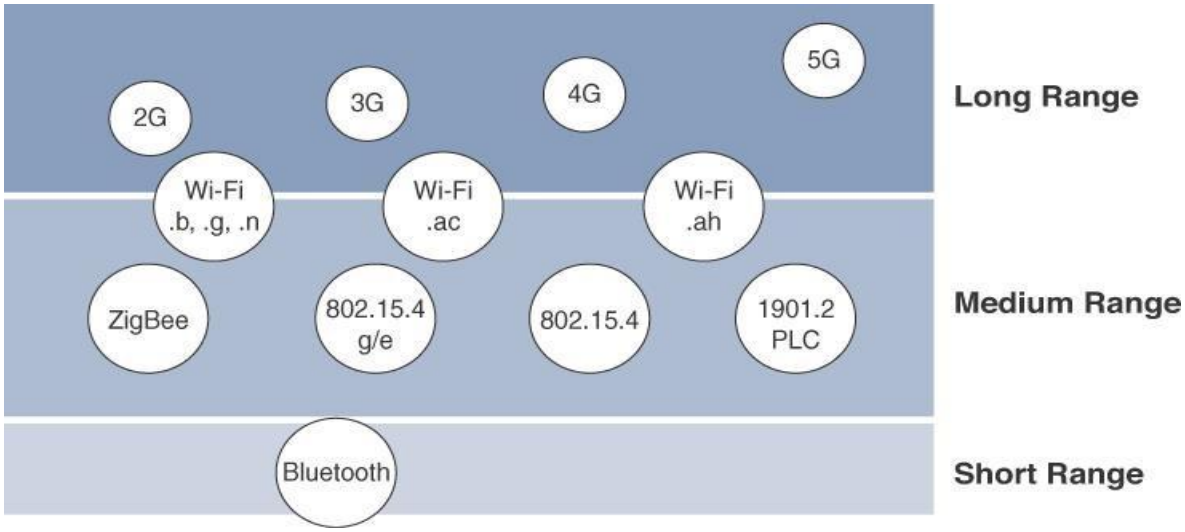


Communications Criteria

- A large number of wired and wireless access technologies are available
- Communication criteria describes the characteristics and attributes of access technologies
- Wireless communication is prevalent for smart object connectivity
  - eases deployment
  - allows smart objects to be mobile without losing connectivity
- Few basic criteria:
  - Range
  - Frequency bands
  - Power consumptions
  - Topology
  - Constrained devices
  - Constrained-node networks



Communication Range

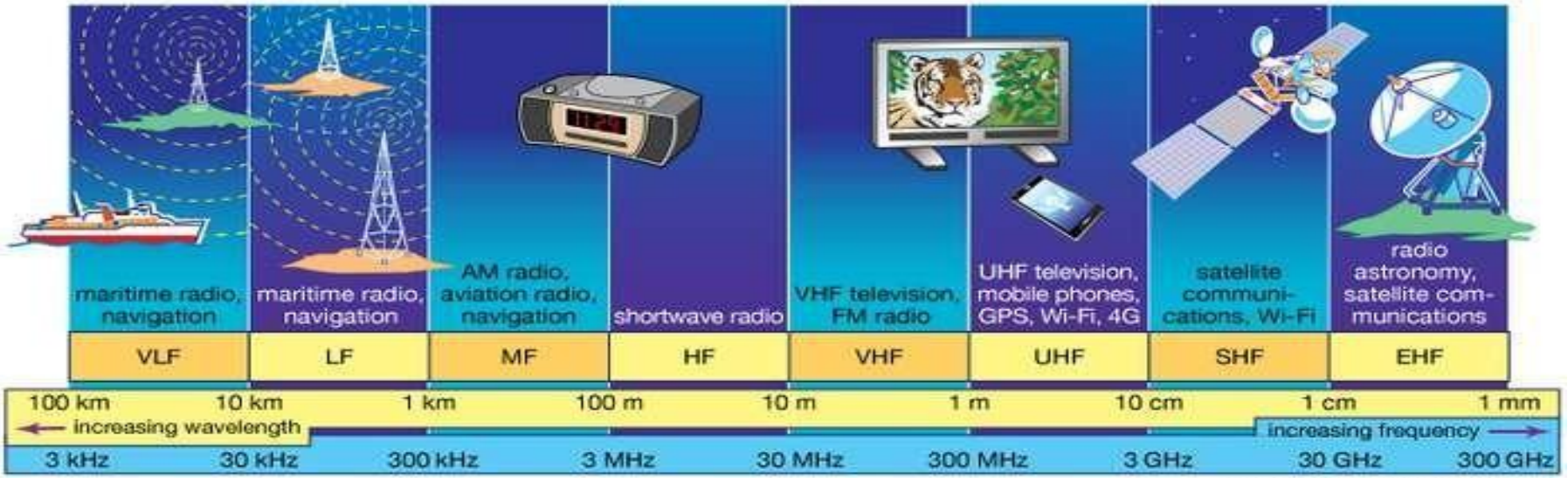


- **Short range**:
  - tens of meters of maximum distance between two devices
  - often considered as an alternative to serial cable
  - IEEE 802.15.1 Bluetooth, IEEE 802.15.7 Visible Light Communications (VLC)
- **Medium range**
  - tens to hundreds of meters between two devices
  - **Wireless** : IEEE 802.11 WiFi, IEEE 802.15.4 Low Rate WPAN, IEEE 802.15.4g Smart Utility Networks (SUN),LORA
  - **Wired** : IEEE 802.3 Ethernet, IEEE 1901.2 Narrowband Power Line Communications (PLC)
- **Long range**
  - greater than 1 mile (1.6 km) between two devices
  - **Wireless** : 2G, 3G, 4G, Outdoor Wi-Fi (IEEE 802.11ah), Low-Power Wide-Area (LPWA) communications
  - **Wired** : IEEE 802.3 ethernet over optical fiber, IEEE 1901.2 Broadband PLC

NB-IoT

- Narrow Band-Internet of Things (NB-IoT) is a standards-based low power wide area (LPWA) technology developed to enable a wide range of new IoT devices and services. It significantly improves the power consumption of user devices, system capacity and spectrum efficiency, especially in deep coverage. Battery life of more than 10 years can be supported for a wide range of use cases.

Frequency Bands



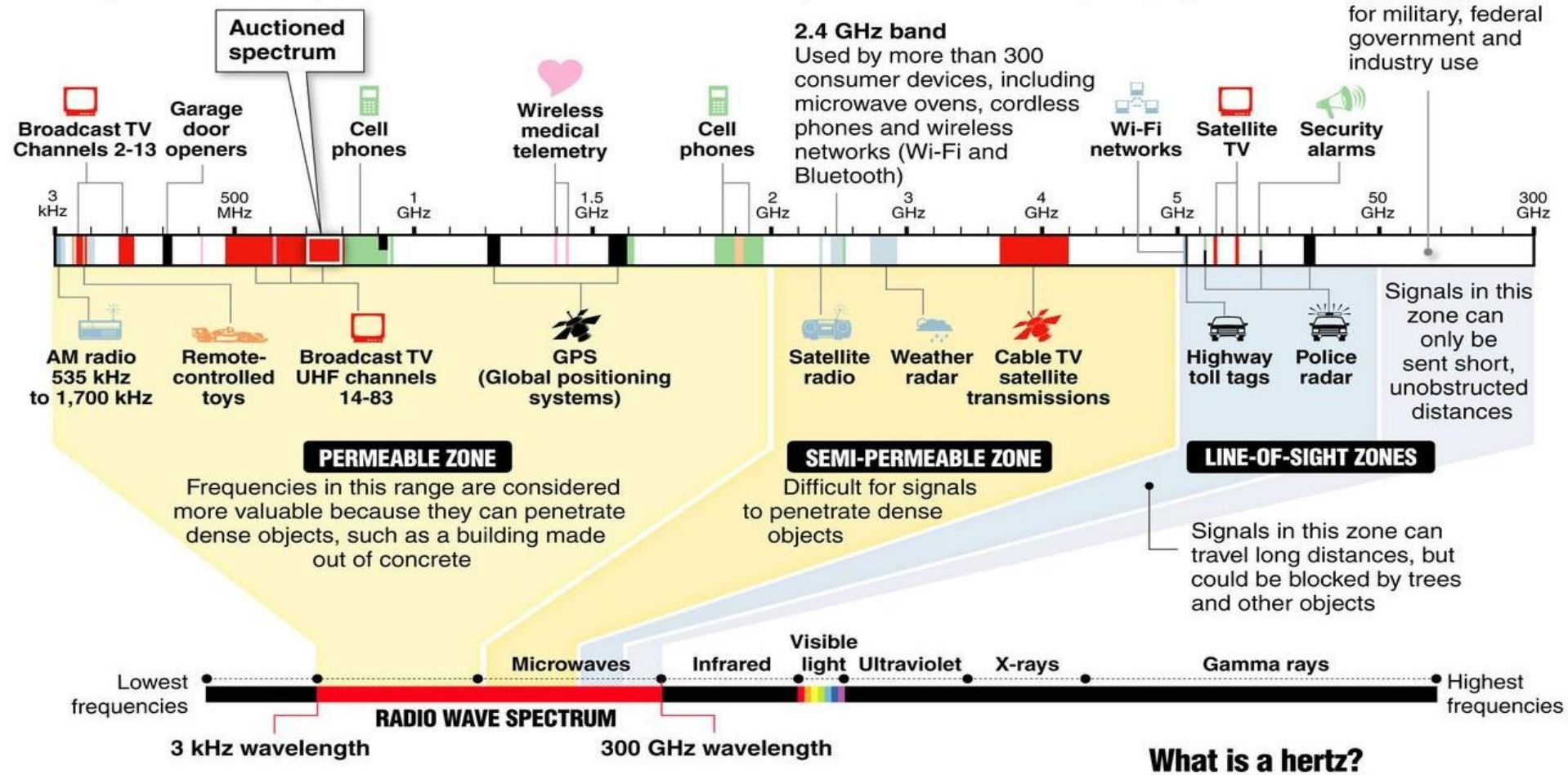
- Radio spectrum is regulated by countries and/or organizations (e.g. International Telecommunication Union (ITU), Federal Communications Commission (FCC))
- frequency bands leveraged by wireless communications are split between licensed and unlicensed bands.

- **Licensed**
  - applicable to long-range access technologies
  - users must subscribe to services
  - common licensed spectrum for IoT : Cellular (900-2100 MHz), NB-IoT (700-900 MHz), WiMax

- **Unlicensed**
  - industrial, scientific, and medical (ISM) portions of the radio bands
  - *Unlicensed* means that no guarantees or interference protections are offered
  - well-known ISM bands for IoT : 2.4 GHz, 5 GHz, 915 MHz for WiFi, BLE, ZigBee; 868 MHz for LoRa

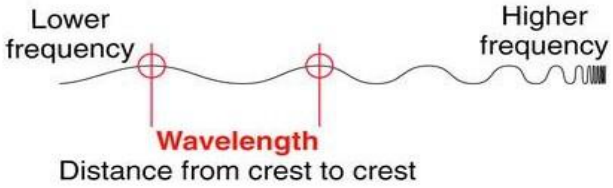
Inside the radio wave spectrum

Almost every wireless technology – from cell phones to garage door openers – uses radio waves to communicate. Some services, such as TV and radio broadcasts, have exclusive use of their frequency within a geographic area. But many devices share frequencies, which can cause interference. Examples of radio waves used by everyday devices:



The electromagnetic spectrum

Radio waves occupy part of the electromagnetic spectrum, a range of electric and magnetic waves of different lengths that travel at the speed of light; other parts of the spectrum include visible light and x-rays; the shortest wavelengths have the highest frequency, measured in hertz



What is a hertz?

One hertz is one cycle per second. For radio waves, a cycle is the distance from wave crest to crest

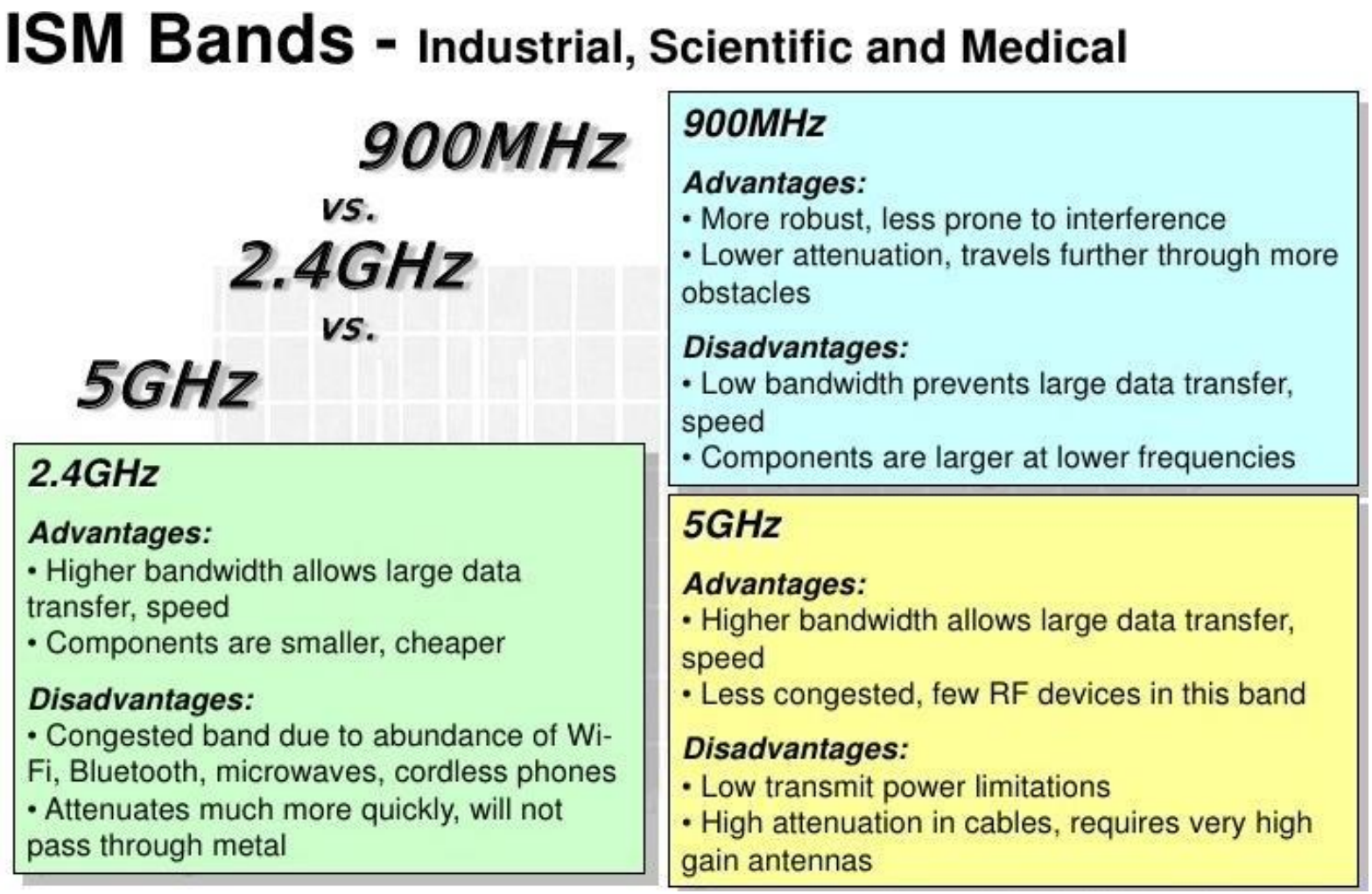
1 kilohertz (kHz) = 1,000 hertz

1 megahertz (MHz) = 1 million hertz

1 gigahertz (GHz) = 1 billion hertz

Source: New America Foundation, MCT, Howstuffworks.com
Graphic: Nathaniel Levine, Sacramento Bee

ISM Bands in India



- **India** also allow 865-867 MHz ISM band

Power Consumption

- Powered node •
  - node has a direct connection to a power source
  - communications are usually not limited by power consumption criteria
  - ease of deployment is limited by the availability of a power source
  - makes mobility more complex

Battery-powered nodes

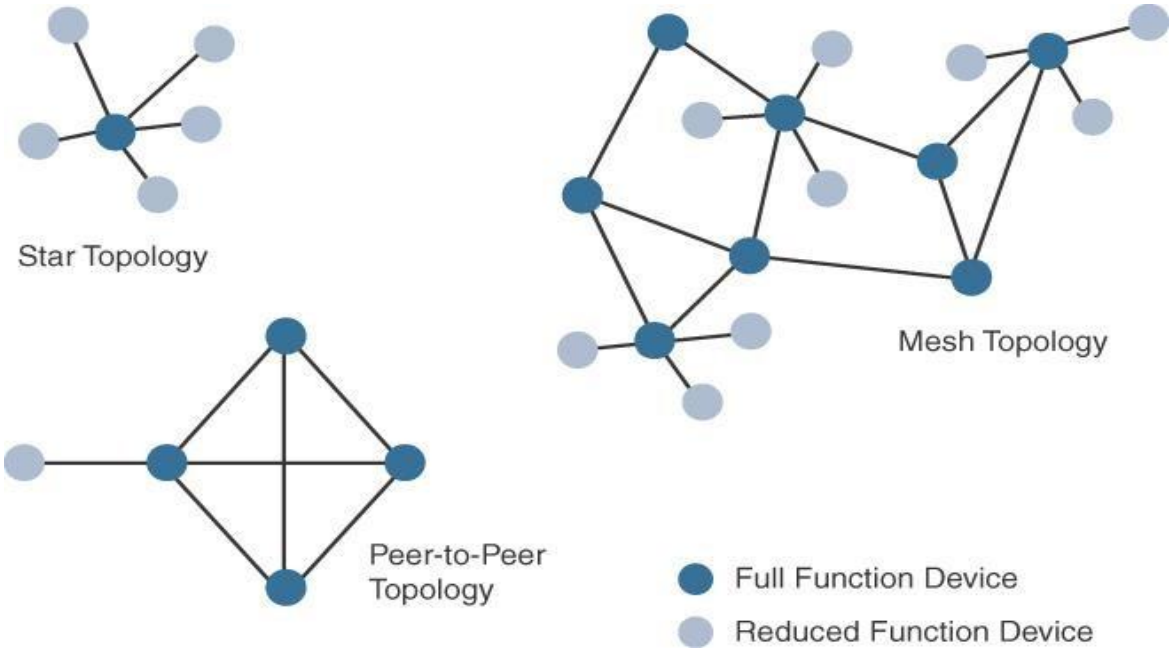
- bring more flexibility to IoT devices
- batteries are small
- batteries can be changed or recharged
- IoT wireless access technologies must address
  - the needs of low power consumption
  - connectivity for battery-powered nodes

	Bluetooth	ZigBee	WiFi	LoRaWAN	NB-IoT
Standard	IEEE 802.15.1	IEEE 802.15.4	IEEE 802.11b	LoRaWAN	3GPP NB-IoT
Sleeping	9 µA	12 µA	30 µA	0.1 µA	3 µA
Awake/Idle	35 mA	50 mA	245 mA	1.4 mA	6 mA
Transmitting	39 mA	52 mA	251 mA	44 mA	220 mA
Receiving	37 mA	54 mA	248 mA	12 mA	46 mA
Power Supply	3.3 V	3.3 V	5 V*	3.3 V	3.6 V

* The ESP8266 module powered by 3.3 V could be used as WiFi module.

Topology

- **Three main topology** schemes are dominant:
  - star, mesh, and peer-to-peer
- For long-range and short-range technologies:
  - star topology is prevalent
- For medium-range technologies:
  - star, peer-to-peer, or mesh topology is common



- IEEE 802.15.4, 802.15.4g, and wired IEEE 1901.2a PLC are generally deployed as a mesh topology.
- Indoor Wi-Fi deployments are mostly star topologies

FFD: A node that implements the full network functions

RFD: The device can implement a subset of protocol functions to perform just a specialized part (communication with the coordinator).

Constrained Devices

- Constrained nodes have limited resources that impact their networking feature set and capabilities.
- RFC 7228 defines three classes for constrained nodes: Class 0, 1, 2

	RAM	Flash Storage	IP stack	Security Scheme	Example
Class 0	< 10 KB	< 100 KB	Not present	No	Push button
Class 1	> 10 KB	> 100 KB	Optimized IP stack	Light	Sensors
Class 2	> 50 KB	> 250 KB	Full IP stack	Yes	Smart meter

Constrained-Node Networks

- Constrained-node networks are often referred to as low-power and lossy networks (LLNs)

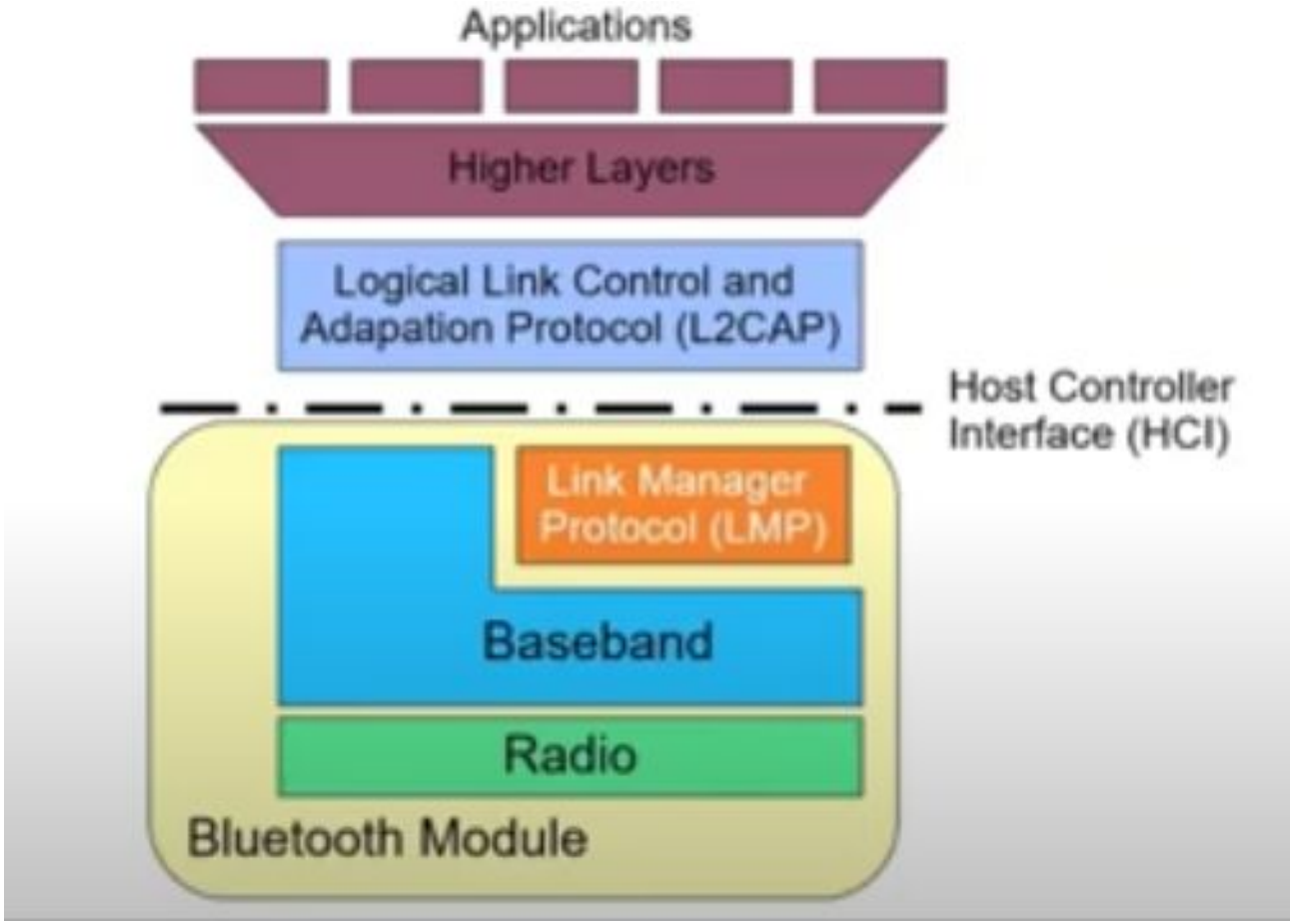
- Layer 1 and Layer 2 protocols must be evaluated in using the following characteristics:
  - data rate and throughput
  - latency and determinism
  - overhead and payload.

- Data rate & throughput:
  - data rates available from 100 bps to tens of megabits per second
  - actual throughput is less, sometimes much less, than the data rate
- Latency & determinism:
  - When latency is a strong concern, emergent access technologies such as Time-Slotted Channel Hopping (TSCH) mode of IEEE 802.15.4e should be considered.
- Overhead & Payload
  - The minimum IPv6 MTU size is expected to be 1280 bytes.
  - the payload size for IEEE 802.15.4 is 127 bytes; payload in LoRaWAN may be from 19 to 250 bytes
  - So, the fragmentation of the IPv6 payload has to be taken into account by the link layer

IoT Access Technologies

- there are many IoT technologies in the market today

Bluetooth


Applications
Higher Layers
Logical Link Control and Adapation Protocol (L2CAP)
Host Controller Interface (HCI)
Link Manager Protocol (LMP)
Baseband
Radio
Bluetooth Module

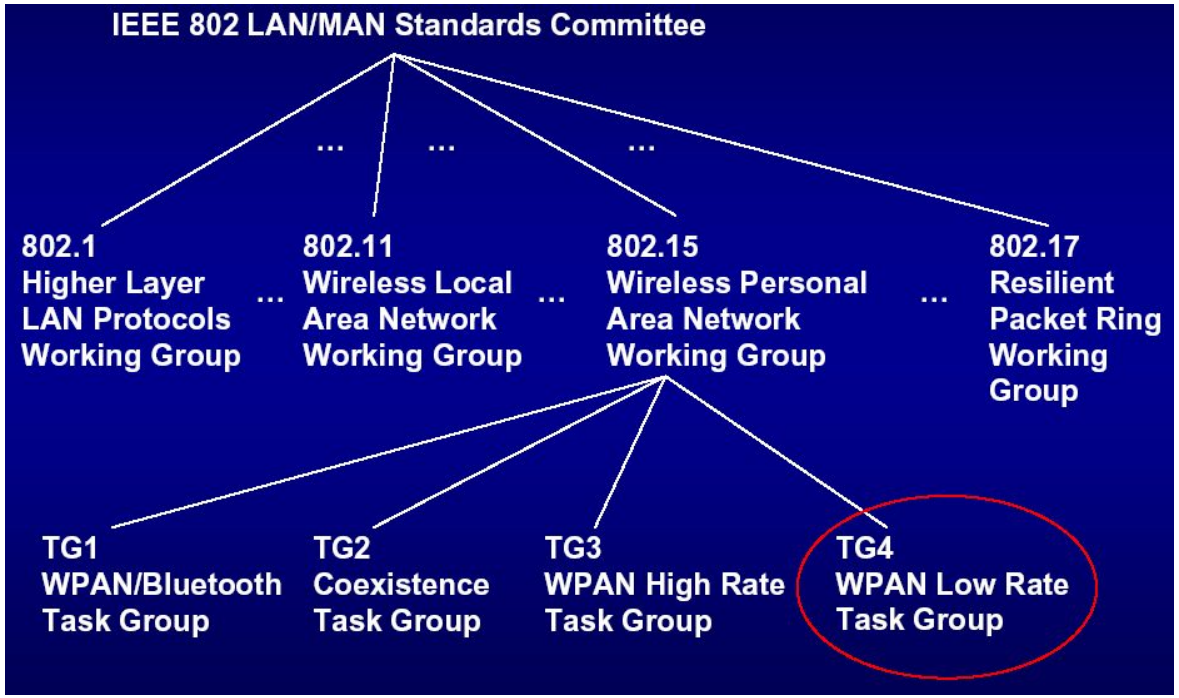
IEEE 802.15.4 PHY and MAC

IEEE 802.15.4 is the IEEE standards for Low Rate Wireless Networks (or Low Rare Wireless Personal Area Networks). Latest version **published in 2015**.

For more details:
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7460875

IEEE 802.15 Task Group 4

- TG4 was formed to define low-data-rate PHY and MAC layer specifications for wireless personal area networks (WPAN)
  - standard has evolved over time:
    - IEEE 802.15.4-2003 ; IEEE 802.15.4-2006
    - IEEE 802.15.4-2011; IEEE 802.15.4-2015



- PAN
  - span a small area (e.g., a private home or an individual workspace)
  - communicate over a short distance
  - low-powered communication
  - primarily uses ad-hoc networking
  - could be wireless or wired (e.g. using USB)

IEEE 802.15.4

- IEEE 802.15.4 is a **wireless access technology** for
  - ✔ low-cost and low-data-rate devices
  - ✔ devices powered by batteries

- It enables easy installation using a compact protocol stack

- Several network communication stacks leverage this technology for many IoT use cases in both the consumer and business markets.

- Few applications:
  - ❖ Home and building automation
  - ❖ Automotive networks
  - ❖ Industrial wireless sensor networks
  - ❖ Interactive toys and remote controls

Cont

. . .

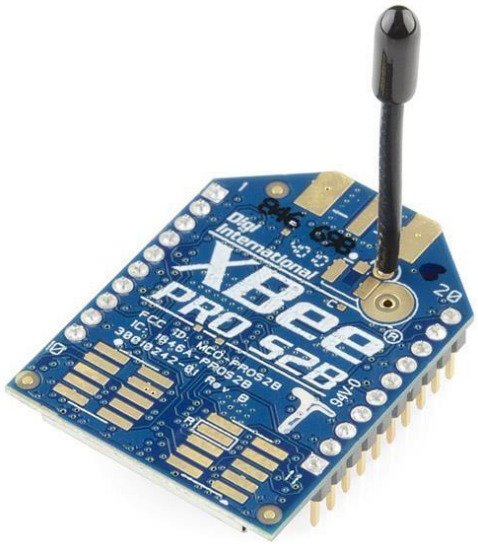
- Few well-known protocol stacks which leverage the IEEE 802.15.4:
  - **ZigBee**
  - **ZigBee IP**
  - **6LoWPAN**
  - WirelessHART
  - Thread
  - ISA100.11a

- **ZigBee** shows how 802.15.4 can be leveraged at the PHY and MAC layers, independent of the protocol layers above.

- Criticisms:
  - MAC reliability
  - unbounded latency
  - susceptibility to interference and multipath fading
  - lacks a frequency-hopping technique

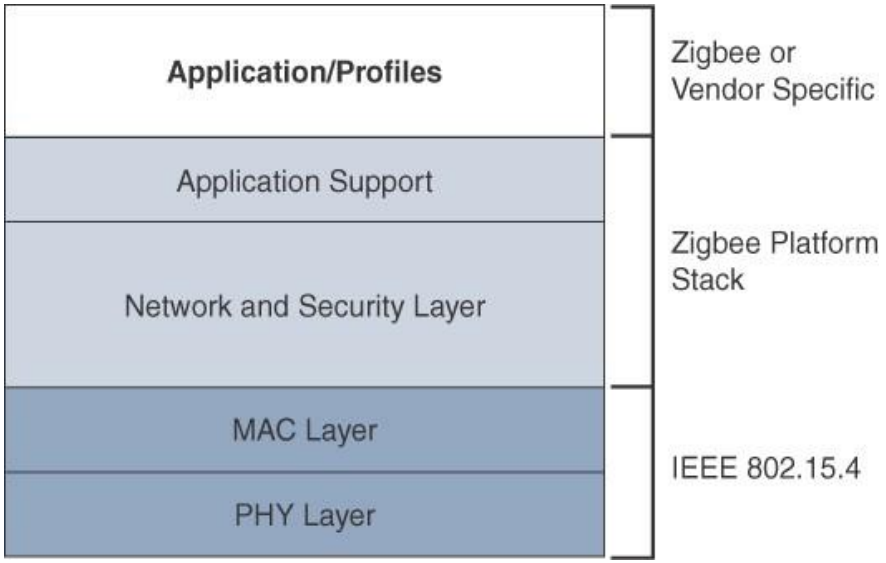
ZigBee

- ZigBee specification was ratified in 2004
- **ZigBee Alliance** is an industry group
  - ✔ certify interoperability between vendors
  - ✔ evolving ZigBee as an IoT solution
- ZigBee solutions are aimed at smart objects and sensors that have low bandwidth and low power needs.
- Well-known application domains:



Industrial and Commercial Automation	Smart Home Applications	Smart Energy
measuring temperature and humidity, and tracking assets	control lighting, thermostats, and security functions	smart meters, that can monitor and control the use and delivery of utilities, such as electricity and water

ZigBee Protocol Stack

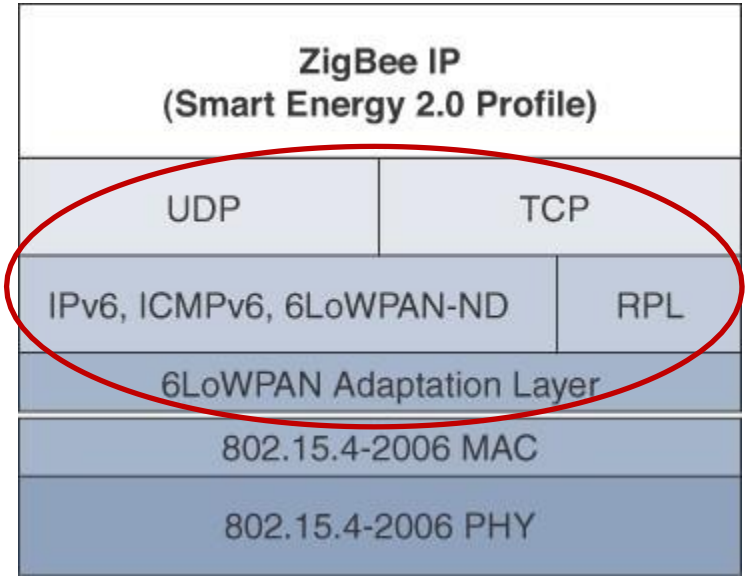


- ZigBee uses AODV routing across a mesh network
- ZigBee utilizes 128-bit AES encryption for security at the MAC layer
- It also provides security at the network and application layers.

- ZigBee predefines many application profiles for certain industries.
- Vendors can optionally create their own custom ones.
- The application support layer interfaces the lower portion of the stack, dealing with the networking of ZigBee devices, with the higher-layer applications
- ZigBee network & security layer provides mechanisms for network startup, configuration, routing, and securing communications.
- ZigBee utilizes the IEEE 802.15.4 standard at the PHY and MAC layers

ZigBee IP

- ZigBee has not provided interoperability with other IoT solutions or open standards
- ZigBee IP was created to embrace the open standards at the network and transport layers
- Open standards designed by IETF's work on LLNs, such as IPv6, 6LoWPAN, and RPL.
- ZigBee IP requires the support of 6LoWPAN's fragmentation and header compression schemes.
- ZigBee IP nodes support
  - IPv6,
  - ICMPv6,
  - 6LoWPAN,
  - Neighbour Discovery (ND), and
  - RPL for the routing of packets.

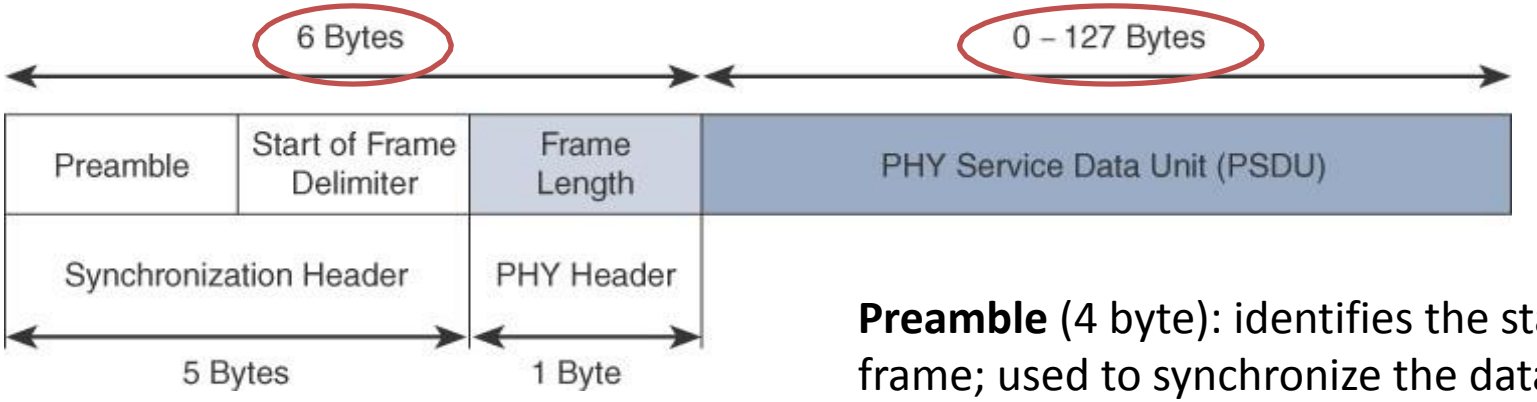


- ZigBee IP is a compelling protocol stack offering because it is based on current IoT standards at every layer under the application layer.

IEEE 802.15.4 PHY layer

- Physical layer transmission options in IEEE 802.15.4-2015
  - **2.4 GHz**, 16 channels, with a data rate of 250 kbps
  - **915 MHz**, 10 channels, with a data rate of 250 kbps
  - **868 MHz**, 3 channel, with a data rate of 100 kbps

- Modulation schemes
  - **OQPSK PHY :** Direct sequence spread spectrum (DSSS) PHY employing offset quadrature phase-shift keying (OQPSK)
  - **BPSK PHY :** DSSS PHY employing binary phase-shift keying (BPSK)
  - **ASK PHY :** parallel sequence spread spectrum (PSSS) PHY employing amplitude shift keying (ASK) and BPSK



IEEE 802.15.4 PHY Frame Format

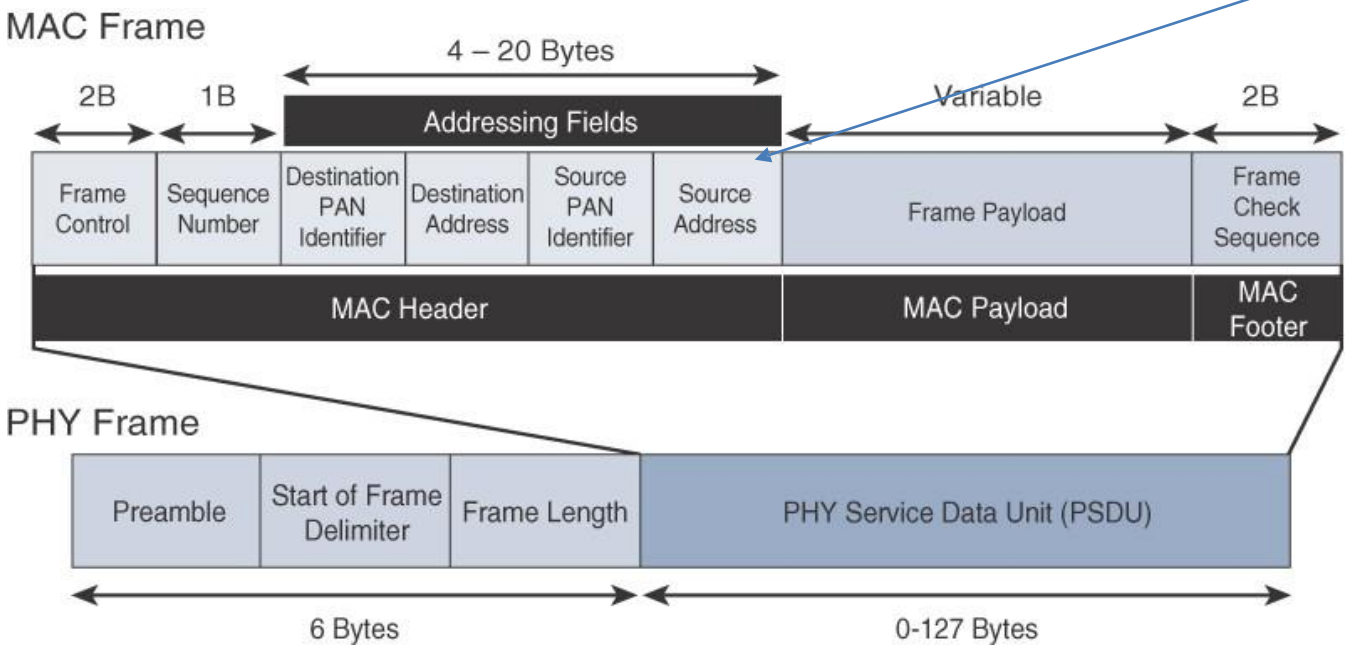
Preamble (4 byte): identifies the start of the frame; used to synchronize the data transmission

SFD (1 byte): informs the receiver about the starting point of frame content

IEEE 802.15.4 MAC layer

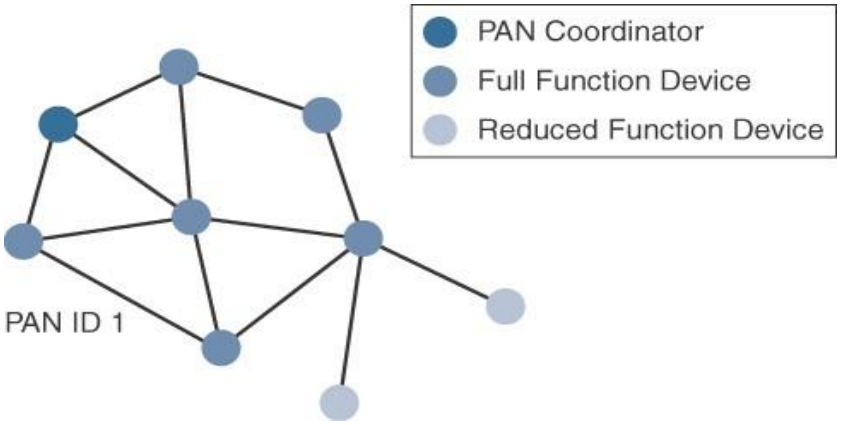
- MAC layer manages access to the PHY channel
  - defines how devices in the same area will share the frequencies allocated.
- Main tasks:
  - Network beaconing for devices acting as coordinators
  - PAN association and disassociation by a device
  - Reliable link communications between two peer MAC entities
  - Device security

16-bit short address
OR
64-bit extended address



- MAC frame types:
  - Data frame
  - Beacon frame
  - ACK frame
  - Command frame

Topology

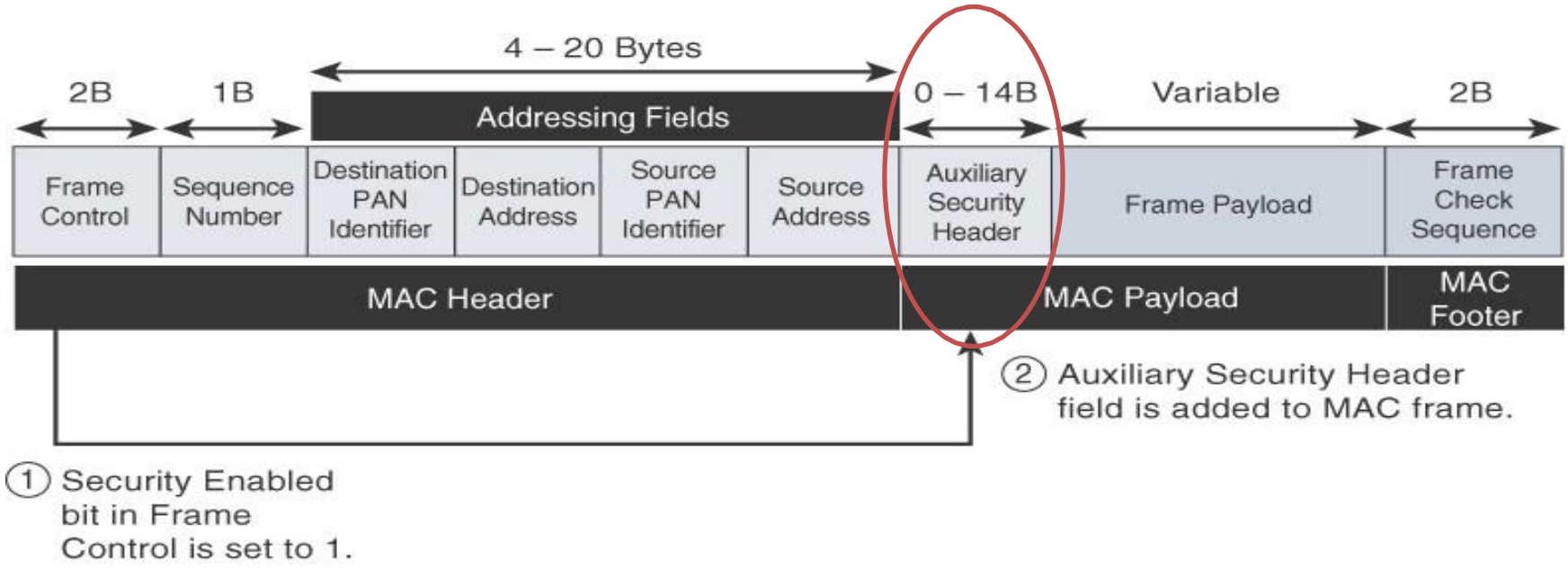


802.15.4 Sample Mesh Network Topology

- Topology for 802.15.4:
  - Star
  - Peer-to-Peer
  - Mesh

- IEEE 802.15.4 does not define a path selection for a mesh topology
  - Mesh-under: Path selection can be done at Layer 2
  - Mesh-over: Path selection can occur at Layer 3 in routing protocol

Security



- IEEE 802.15.4 specification uses Advanced Encryption Standard (AES) with a 128-bit key length as the base encryption algorithm
- Message integrity code (MIC), which is calculated for the entire frame using the same AES key, to validate the data that is sent

IEEE 802.15.4g
IEEE 802.15.4e

IEEE 802.15.4g & **IEEE 802.15.4e** are the PHY and MAC layer amendments of wireless personal area networks (IEEE 802.1.5.4) **published in 2012**.

For more details:
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6185525
https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6471722

IEEE 802.15.4e & 802.15.4g

- **Disadvantages of IEEE 802.1.5.4**
  - MAC reliability
  - unbounded latency
  - multipath fading

- **IEEE 802.15.4e** amendment of 802.15.4-2011 expands the MAC layer feature set

  - to remedy the disadvantages of 802.15.4.
  - to better suitable in factory and process automation, and smart grid

  - Main modifications were:
    - frame format,
    - security,
    - determinism mechanism, and
    - frequency hopping

- **IEEE 802.15.4g** amendment of 802.15.4-2011 expands the PHY layer feature set

  - to optimize large outdoor wireless mesh networks for field area networks (FANs)
  - to better suitable in smart grid or smart utility network (SUN) communication

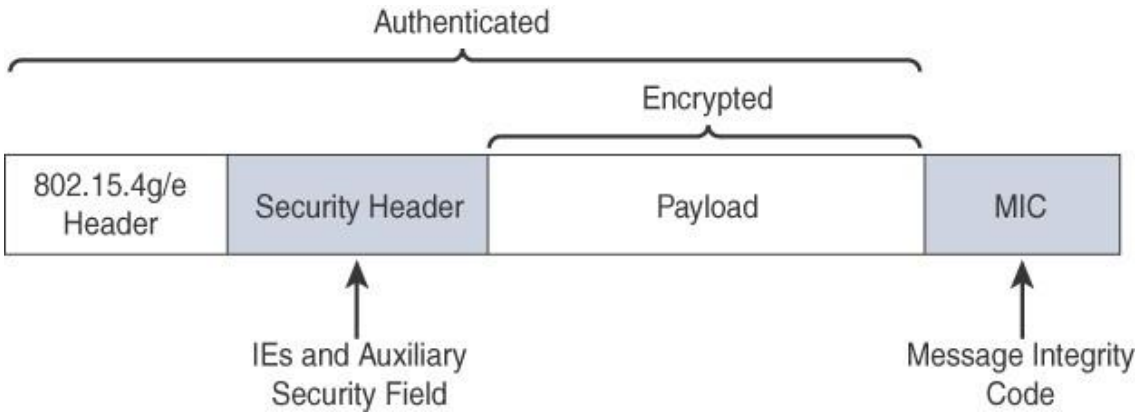
  - Main modifications were:
    - New PHY definitions
    - some MAC modifications were needed to support the new PHY

Wi-SUN PHY layer

- Wireless Smart Utility Network (Wi-SUN) supports multiple data rates and frequency bands to meet different regulatory requirements worldwide. Applications include smart grid and smart cities, with certified products enabling multivendor interoperability.
- 802.15.4g-2012 and 802.15.4e-2012 led to **additional difficulty** in
  - achieving the **interoperability** between devices and mixed vendors
- Wi-SUN Alliance was formed to guarantee interoperability

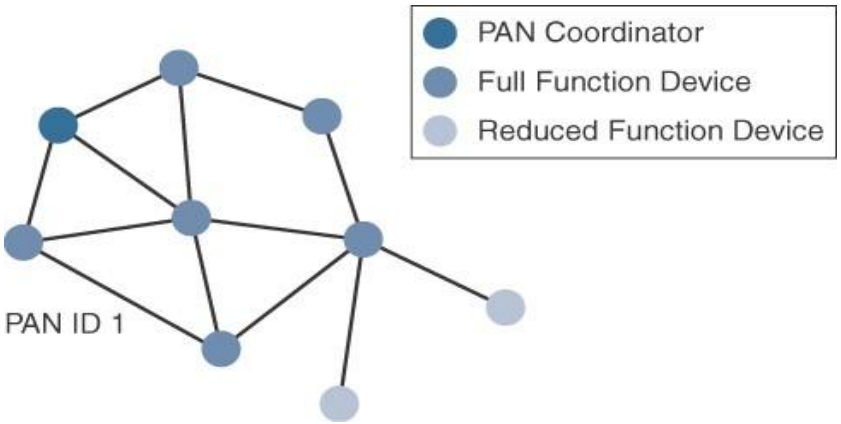
- IEEE 802.15.4 maximum payload size of 127 bytes 2047 bytes for SUN PHY.
  - Fragmentation is no longer necessary at Layer 2 for IPv6 packets
- Error protection was improved in IEEE 802.15.4g by the CRC from 16 to 32 bits.
- SUN PHY supports **multiple data rates** and **more channels** in ISM bands
- Modulation schemes:
  - **MR-FSK** : Multi-Rate and Multi-Regional Frequency Shift Keying
    - good transmit frequency
  - **MR-OFDM** : Multi-Rate and Multi-Regional Orthogonal Frequency Division Multiplexing
    - good data rate
  - **MR-O-QPSK :** Multi-Rate and Multi-Regional Offset Quadrature Phase-Shift Keying
    - cost effective design

Security and Topology



- Encryption is done by AES with a 128-bit key
- Message integrity code (MIC) validates the data that is sent

Mesh Topology



- Battery-powered nodes with a long lifecycle requires
  - optimized Layer 2 forwarding or
  - optimized Layer 3 routing protocol

IEEE 802.11ah

IEEE 802.11ah is a wireless networking protocol **published in 2016**.

For more details: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7920364

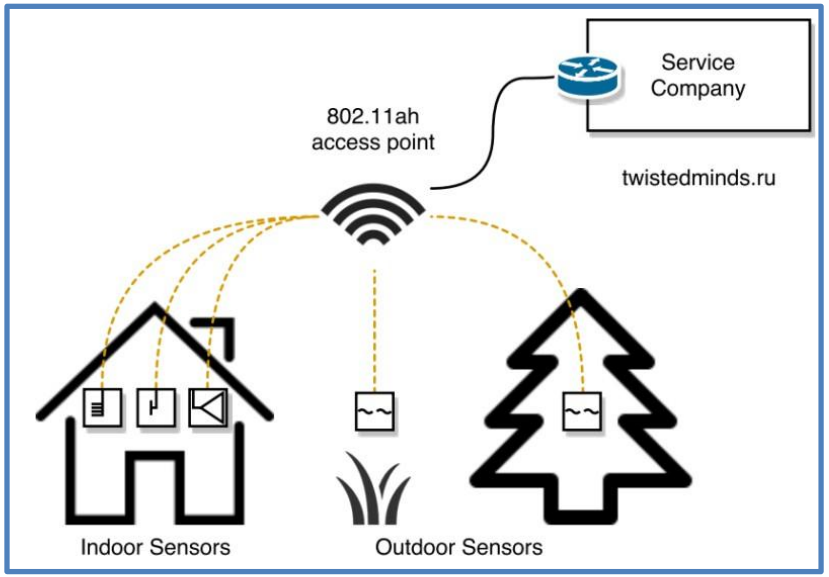
IEEE 802.11ah

- **Advantages** of WiFi
  - Most successful endpoint wireless technology
  - Useful for high data rate devices, for audio-video analytics devices, for deploying WiFi backhaul infrastructure

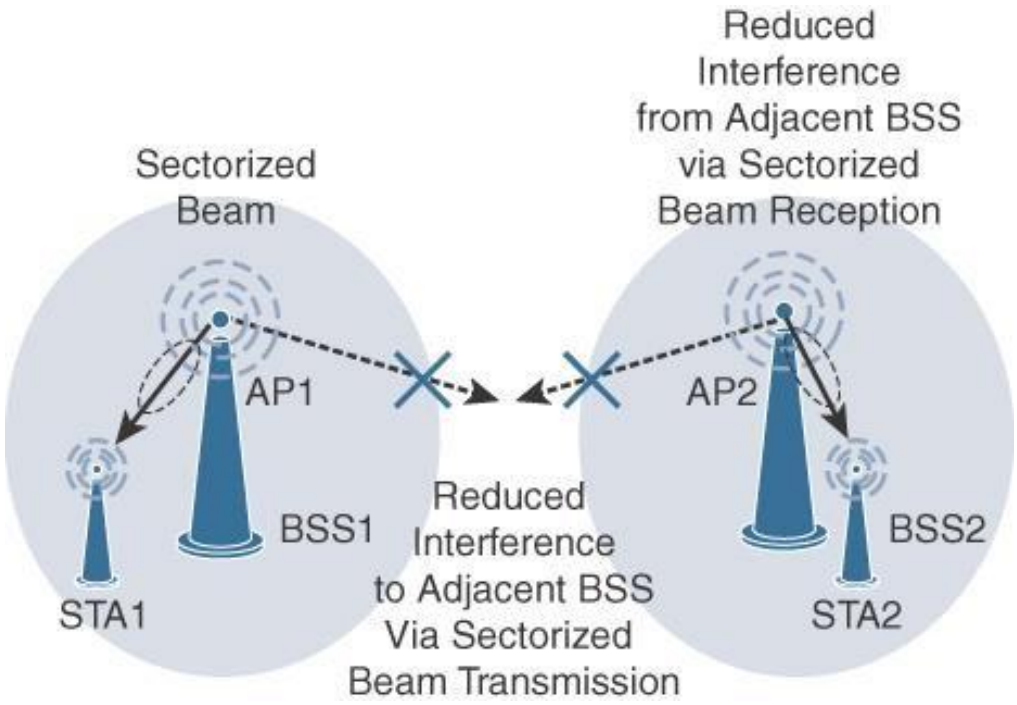
- **Disadvantages** of WiFi
  - Less signal penetration
  - Unsuitable for battery powered nodes
  - Unable to support large number of devices

- Wi-Fi Alliance defined a new technology called Wi-Fi HaLow
  - ah **Ha**
  - Low power network **Low**

- Main use cases for IEEE 802.11ah
  - Sensors and meters covering a smart grid
  - Backhaul aggregation of industrial sensors and meter data
  - Extended range Wi-Fi



802.11ah Topology



- Star topology
- Includes simple hops relay to extend its range
  - Max 2 hops
  - Client handle the relay operation

LoRaWAN

LoRaWAN is a wireless networking protocol **published in 2015**.

For more details: https://lora-alliance.org/sites/default/files/2018-07/lorawan1.0.3.pdf

LPWA Technology

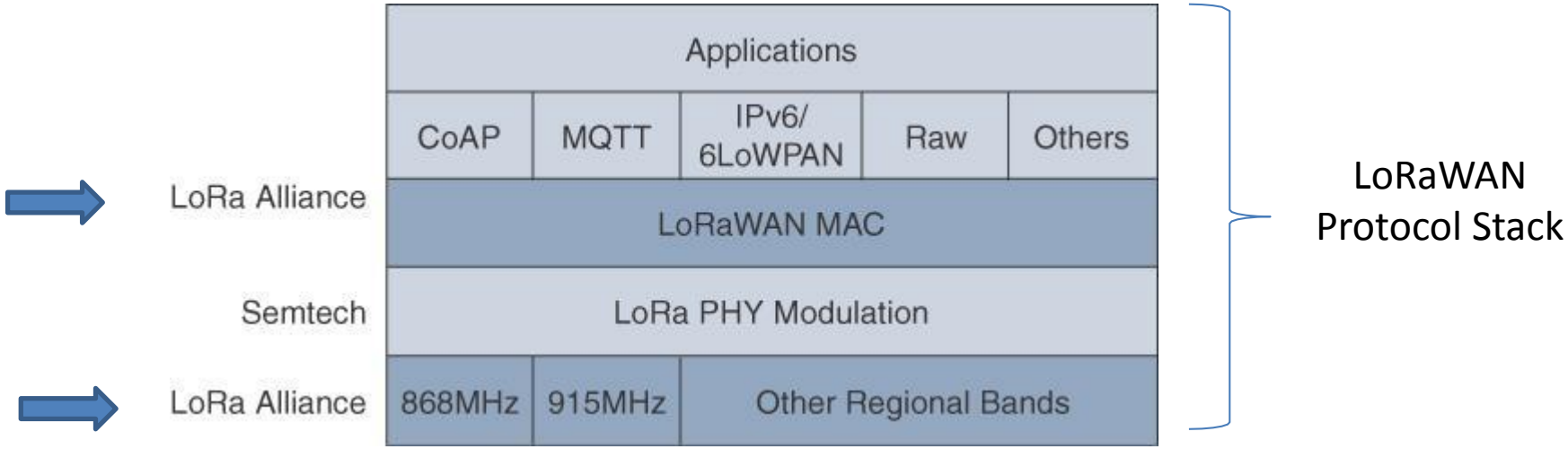
- a new set of wireless technologies has received a lot of attention from the industry, know as
  - **Low-Power Wide-Area** (LPWA) technology

- unlicensed-band LPWA technology
  - LoRaWAN

- licensed-band LPWA technology
  - NB-IoT and Other LTE Variations

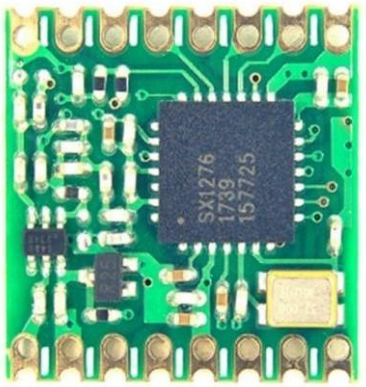
LoRa Alliance

- Initially, **LoRa** was a PHY layer modulation scheme
  - developed by a French company "Cycleo"; Later, Cycleo was acquired by Semtech.
- **Semtech LoRa**: Layer 1 PHY modulation technology available by multiple chipset vendors
- The **LoRa Alliance** is a technology alliance
  - committed to enabling large scale deployment of Low-Power Wide Area Networks (LPWAN) IoT
  - publishing LoRaWAN specifications for LPWAN
- **LoRaWAN** is a premier solution for global LPWAN deployments

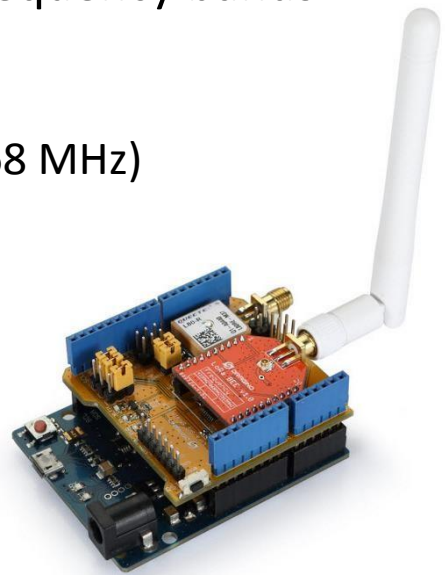


LoRaWAN PHY layer

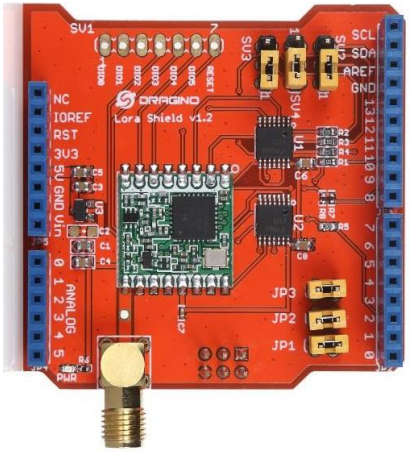
- Semtech LoRa PHY
- Uses **chirp spread spectrum** modulation
  - it allows demodulation below the noise floor, offers robustness to noise and interference
  - manages a single channel occupation by different spreading factors (SFs)
- Main unlicensed sub-GHz frequency bands
  - 433 MHz
  - 779–787 MHz
  - 863–870 MHz (In India: 868 MHz)
  - 902–928 MHz



LoRa Module: **SX1276**
868MHz band



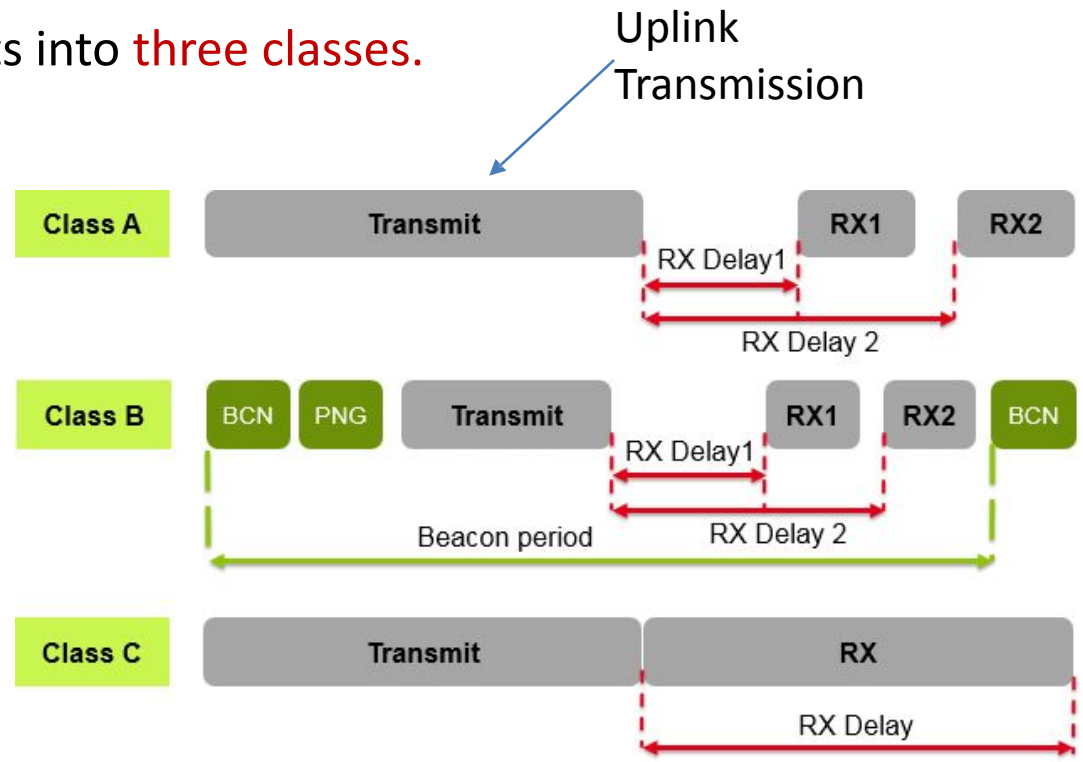
LoRa GPS Shield
with Arduino



LoRa Shield for Arduino

LoRaWAN MAC layer

- Classifies LoRaWAN endpoints into three classes.



Class A:

- this is default implementation
- optimized for battery-powered nodes
- allows bidirectional communications
- two receive windows are available after each transmission

Class B:

- Class B node should get additional receive windows compared to Class A
- gateways must be synchronized through a beaconing process
- "ping slots", can be used by the network infrastructure to initiate a downlink communication

Class C:

- This class is particularly adapted for powered nodes
- enables a node to be continuously listening by keeping its receive window open when not transmitting

LoRaWAN Gateway

- LoRa **gateway** is deployed as the **center hub** of a star network architecture.
- It uses multiple transceivers and channels
- It can demodulate multiple channels at once
- It can also demodulate multiple signals on the same channel simultaneously
- LoRa gateways serve as a transparent bridge relaying data between endpoints
- The endpoints use a single-hop wireless connection to communicate with one or many gateways

Dragino LoRa Gateway

- **Data rate** varies depending on the frequency bands and adaptive data rate (ADR)
- ADR is an algorithm that manages data rate and radio signal for each endpoint.

LoRaWAN Security

- LoRaWAN supports: protect communication and data privacy across the network

- LoRaWAN endpoints must implement **two layers of security**
  - Network security applied in MAC layer
    - authentication of the endpoints
    - protects LoRaWAN packets by performing encryption based on AES

    - Each endpoint implements a network session key (NwkSKey)
    - The NwkSKey ensures data integrity through computing and checking the message integrity code (MIC) of every data message

  - Data privacy applied at the end points (end device and application server)
    - second layer is an application session key (AppSKey)
    - performs encryption & decryption functions between the endpoint and its application server.
    - it computes and checks the application-level MIC

- LoRaWAN service provider does not have access to the application payload if it is not allowed

Protocol details

S.No	Protocol	Description
1.	ZigBee	Promoted through the ZigBee alliance, ZigBee defines upper-layer components (network through application) as well as application profiles. Common profiles include building automation, home automation, and healthcare. ZigBee also defines device object functions such as device role, device discovery, network join and security
2.	6LoWPAN	6LoWPAN is an IPv6 adaptation layer defined by the IETF 6LoWPAN working group that describes how to transport IPv6 packets over IEEE 802.15.4 layers. RFCs document header compression and IPv6 enhancement to cope with the specific details of IEEE 802.15.4
3.	ZigBee IP	An evolution of the ZigBee protocol stack, ZigBee IP adopts the 6LoWPAN adaptation layer , IPv6 network layer, RPL routing protocol. In addition, it offers improvement in IP security.
4.	ISA100.11a	This is developed by the International Society of Automation (ISA) as "Wireless Systems for Industrial automation: Process Control and Related Applications".It is based on IEEE 802.15.4-2006. The network and transport layers are based on IETF 6LoWPAN, IPv6, and UDP standards
5.	Wireless HART	Wireless HART promoted by the HART Communication Foundation, is a protocol stack that offers a time-synchronized, self-organizing, and self healing mesh architecture, leveraging IEEE 802.15.4-2006 over the 2.4GHz frequency band.
6.	Thread	Constructed on top of IETF 6LoWPAN /IPv6, Thread is a protocol stack for a secure and reliable mesh network to connect and control products in the home.

Comparison of Key Attributes

	WiFi	BLE	Thread	Sub-GHz: TI	SigFox	ZigBee	LoRa
Max. Data throughput	72 Mbps	2 Mbps	250 Kbps	200 Kbps	100 bps	250 Kbps	50 Kbps
Range	100 m	750 m	100 m	4 km	25 km	130 m	10 km
Topology	Star	P2P/ Mesh	Mesh/ Star	Star	Star	Mesh/ Star	Star of Star
Frequency	2.4 GHz	2.4 GHz	2.4 GHz	Sub-GHz	Sub-GHz	2.4 GHz	Sub-1GHz
Power consumption	1 Year (AA battery)	Up to years on a coin-cell battery for limited range					Few Years (AA battery)
IP at the device node	Yes	No	Yes	No	No	No	No
Deployed Devices	AP	smart phones	No	No	No	No	No

References/sources:

1. David Hanes *et al.*, “IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things”, 1st Edition, 2018, Pearson India.