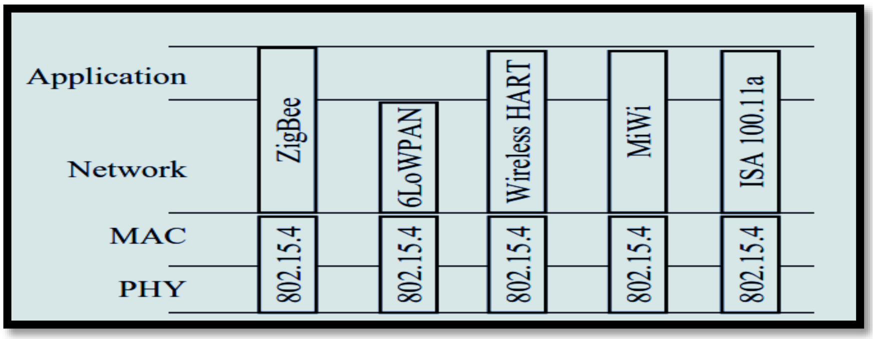
UNIT – 3
Study Material

IEEE 802.15.4 - Low-Rate Wireless Personal Area Networks (LR-WPANs):

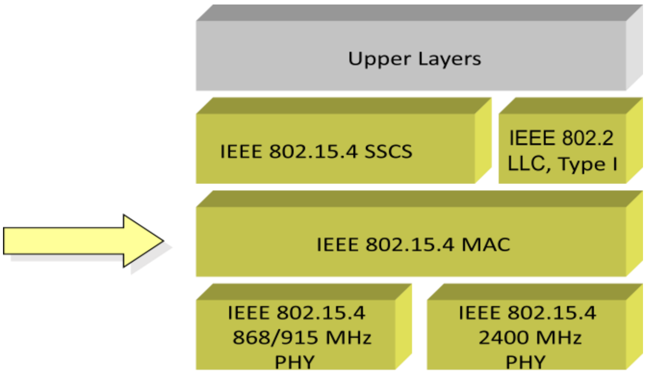
- IEEE 802.15.4 is a standard that was developed to provide a framework and the lower layers in the Open Systems Interconnection (OSI) model for low cost, low power wireless connectivity networks.
- A low-data rate wireless personal area network and is the PHY and MAC layer used by many IoT protocols, such as ZigBee, Wireless HART, 6LoWPAN, Mi-Wi and ISA 100.11a as shown in bellow figure.



- The basic framework conceives a 10-meter communications range with a transfer rate of 250 kbit/s.
- A low data rate solution with multi-month to multi-year battery life and very low complexity. It is operating in an unlicensed, international frequency band ISM.
- Potential applications are Home Automotive, Industrial applications, Games, Metering.

IEEE 802.15.4 Architecture:

The 802.15.4 standard uses only the first two layers plus the logical link control (LLC) and service specific convergence sub-layer (SSCS) additions to communicate with all upper layers as defined by additional standards.

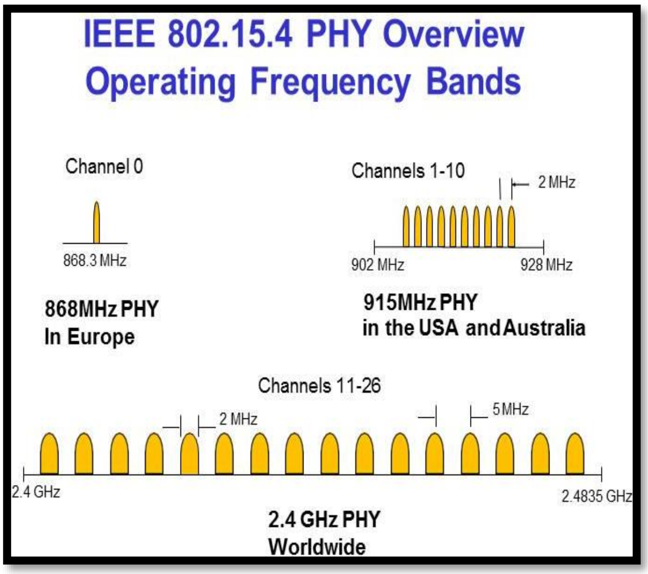


IEEE 802.15.4 Physical Layer:

- Short range, low bit rate, low power consumption.
- It provides different data rates 250 kbps, 40 kbps, 20 kbps at different frequency bands.

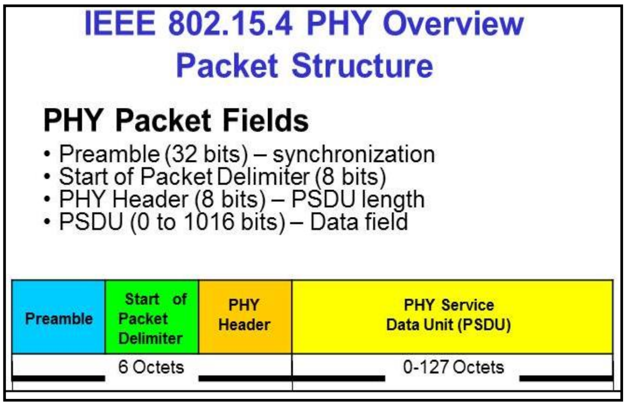
- It Supports multiple network topologies such as point-to-point(star), point-to-multipoint (tree),and mesh networks.
- Modulation: BPSK for 20 and 40 kbps, O-QPSK with DSSS for 250 kbps
- It supports three types of frequency bands with 24 channels. They Are

IEEE 802.15.4 RF CHANNEL DETAILS			
FREQUENCY BAND (MHZ)	CHANNELS AVAILABLE	THROUGHPUT (KBPS)	REGION USE ALLOWABLE
868 - 868.6	1	20	Europe
902 - 928	10 (2003 rel) 30 (2006 rel)	30	USA
2400	16	250	Global



IEEE 802.15.4 PHY Overview
Operating Frequency Bands

pa



IEEE 802.15.4 PHY Overview
Packet Structure

PHY Packet Fields

- Preamble (32 bits) – synchronization
- Start of Packet Delimiter (8 bits)
- PHY Header (8 bits) – PSDU length
- PSDU (0 to 1016 bits) – Data field

Preamble	Start of Packet Delimiter	PHY Header	PHY Service Data Unit (PSDU)
6 Octets			0-127 Octets

IEEE 802.15.4 MAC Overview:

- The purpose of the IEEE 802.15.4 MAC layer is to provide an interface between the PHY or physical layer and the application layer. The as IEEE 802.15.4 does not specify an application layer, this is generally an application system such as Zigbee, RF4CE, MiWi, etc.

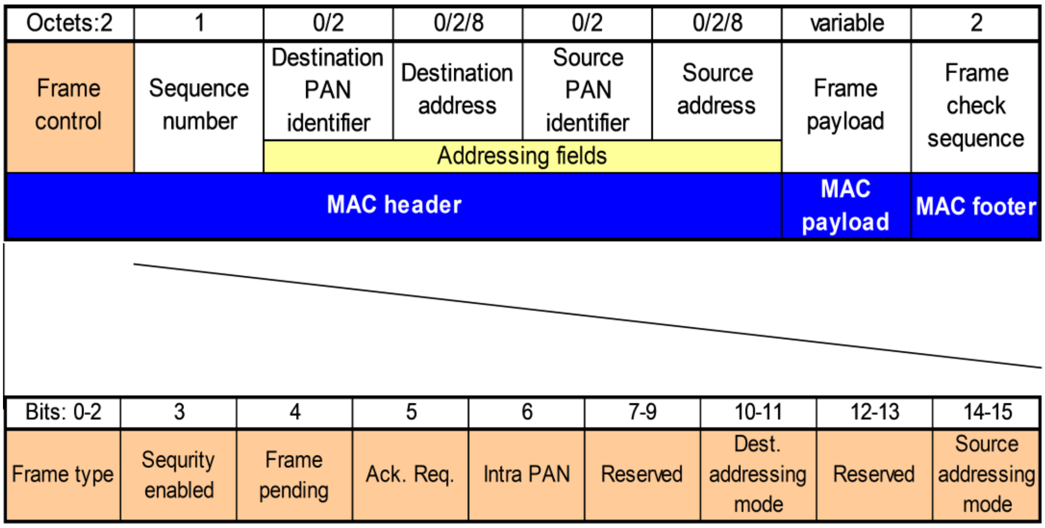
- The IEEE 802.15.4 MAC provides the interface to the application layer using two elements:
- ***MAC Management Service:*** This is called the MAC Layer Management Entity, MLME. It provides the service interfaces through which layer management functions may be called or accessed. The IEEE 802.15.4 MAC MLME is also responsible for controlling a database of objects for the MAC layer. This database is referred to as the MAC layer PAN information base or PIB. The MLME also has access to MCPS services for data transport activities.
- ***MAC Data Service:*** This is called the MAC Common Port Layer, MCPS. This entity within the IEEE 802.15.4 MAC provides data transport services between the peer MACs.

The MAC data service enables the transmission and reception of frames called MAC protocol data units (MPDUs) across the PHY data service.

IEEE 802.15.4 defines four different MAC frame formats/types

- Data Frame
- Beacon Frame
- Acknowledgment Frame
- MAC Command Frame

General MAC Frame Format:



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 address	Frame payload	Frame check sequence
		Addressing fields					
MAC header						MAC payload	MAC footer

Bits: 0-2	3	4	5	6	7-9	10-11	12-13	14-15
Frame type	Sequrity enabled	Frame pending	Ack. Req.	Intra PAN	Reserved	Dest. addressing mode	Reserved	Source addressing mode

It is the basis for all individual frame formats/types. The general IEEE 802.15.4 MAC frame format is shown by the following figure.

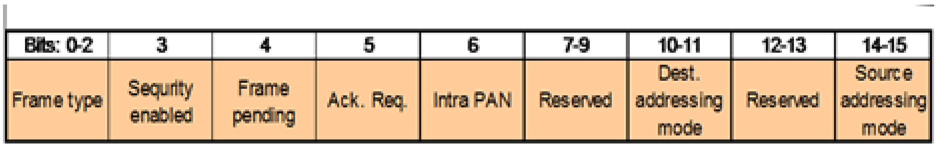
It consists of three main sections: the MAC header (MHR), the MAC payload, MAC footer (MFR).

- All of these sections contain at least one parameter field.
- The frame control field (FCF), the sequence number (SN) and the frame check sequence (FCS) have to be part of every frame whereas the addressing fields, the auxiliary security header and the MAC payload might not be included in a frame (type).

- Fields consisting of more than a single octet (e.g. FCF) are sent to the PHY starting with the octet containing the least significant bits through to the octet containing the most significant bits.

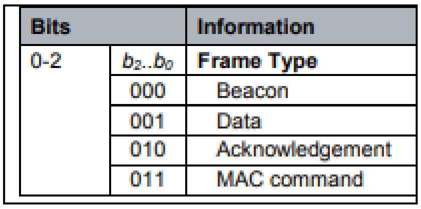
Frame Control Field (FCF):

Its size is 2 0ctates, that means 16 bits.

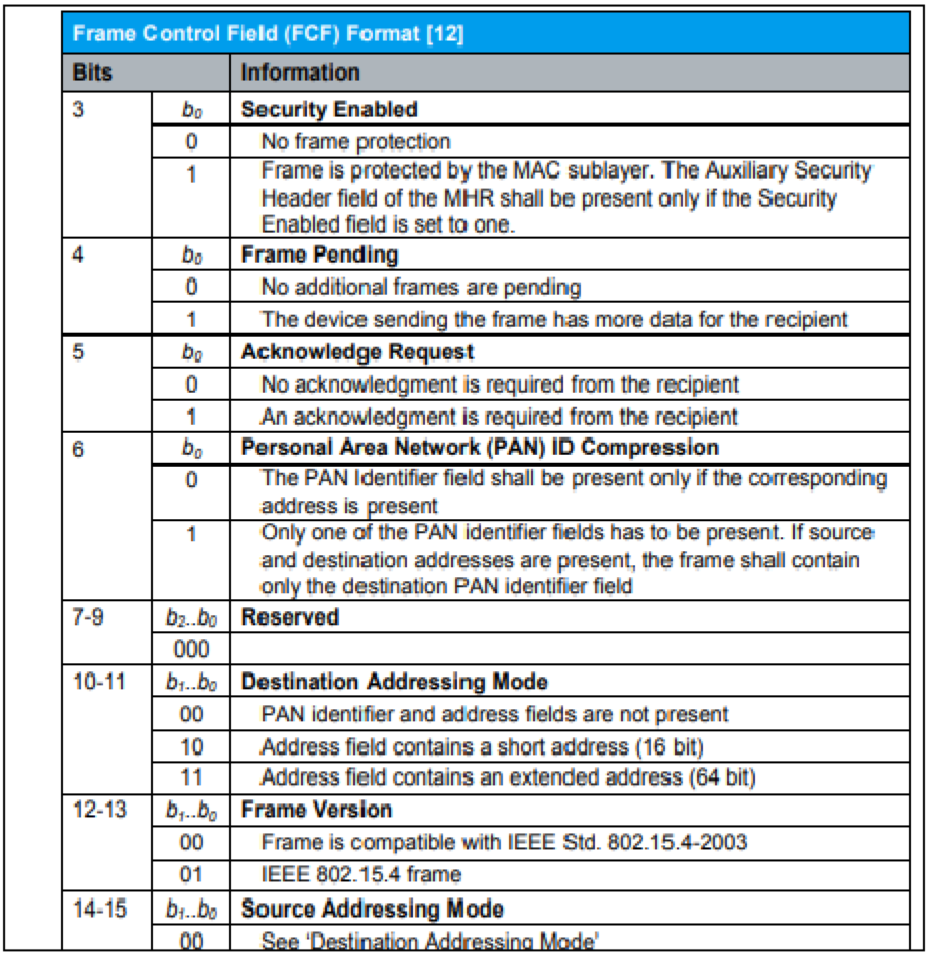


Bits: 0-2	3	4	5	6	7-9	10-11	12-13	14-15
Frame type	Security enabled	Frame pending	Ack. Req.	Intra PAN	Reserved	Dest. addressing mode	Reserved	Source addressing mode

Frame Type:



Bits		Information
0-2	$b_2..b_0$	**Frame Type**
	000	Beacon
	001	Data
	010	Acknowledgement
	011	MAC command



Frame Control Field (FCF) Format [12]

Bits		Information
3	b_0	**Security Enabled**
	0	No frame protection
	1	Frame is protected by the MAC sublayer. The Auxiliary Security Header field of the MHR shall be present only if the Security Enabled field is set to one.
4	b_0	**Frame Pending**
	0	No additional frames are pending
	1	The device sending the frame has more data for the recipient
5	b_0	**Acknowledge Request**
	0	No acknowledgment is required from the recipient
	1	An acknowledgment is required from the recipient
6	b_0	**Personal Area Network (PAN) ID Compression**
	0	The PAN Identifier field shall be present only if the corresponding address is present
	1	Only one of the PAN identifier fields has to be present. If source and destination addresses are present, the frame shall contain only the destination PAN identifier field
7-9	$b_2..b_0$	**Reserved**
	000	
10-11	$b_1..b_0$	**Destination Addressing Mode**
	00	PAN identifier and address fields are not present
	10	Address field contains a short address (16 bit)
	11	Address field contains an extended address (64 bit)
12-13	$b_1..b_0$	**Frame Version**
	00	Frame is compatible with IEEE Std. 802.15.4-2003
	01	IEEE 802.15.4 frame
14-15	$b_1..b_0$	**Source Addressing Mode**
	00	See 'Destination Addressing Mode'

Sequence Number: The sequence number specifies the sequence identifier (e.g. beacon sequence number, BSN; data sequence number, DSN) for the frame. **Destination PAN Identifier:** The destination Personal Area Network (PAN) identifier field, when present, specifies the unique PAN identifier of the intended recipient of the frame.

Destination Address: The destination address field, when present, specifies the address of the intended recipient of the frame.

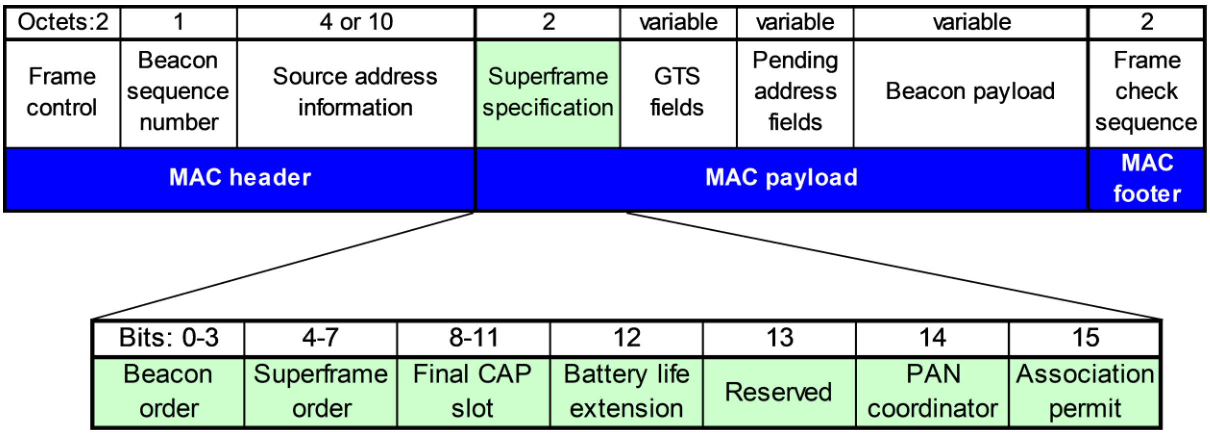
Source PAN Identifier: The source PAN Identifier field, when present, specifies the unique PAN identifier of the originator of the frame. This field shall be included in the MAC frame only if the FCF Source Addressing Mode field is nonzero and the FCF PAN ID compression field is equal to zero.

Source Address: The source address field, when present, specifies the address of the originator of the frame. This field shall be included in the MAC frame only if the FCF source addressing mode field is nonzero.

Auxiliary Security Header: The auxiliary security header field specifies information required for security processing. This field shall be present only if the FCF security enabled field is set to one.

Frame Payload: The frame payload field contains information specific to individual frame types. If the FCF security enabled field is set to one, The 2 byte frame check sequence (FCS) follows the last MAC payload byte. The FCS is calculated over the MPDU. The FCS calculation is based on the International Telecommunications Union (ITU) Cyclic Redundancy Check (CRC)

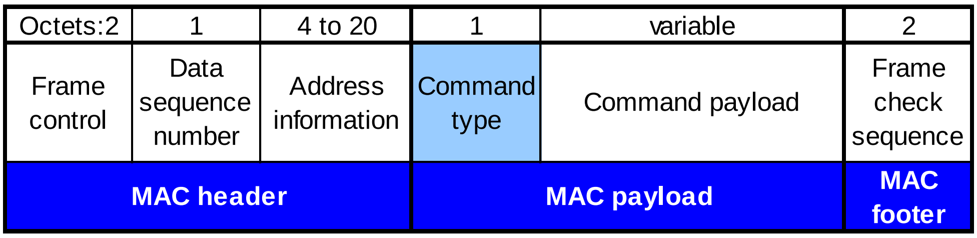
Beacon Frame Format:



Octets:2	1	4 or 10	2	variable	variable	variable	2
Frame control	Beacon sequence number	Source address information	Superframe specification	GTS fields	Pending address fields	Beacon payload	Frame check sequence
MAC header			MAC payload				MAC footer

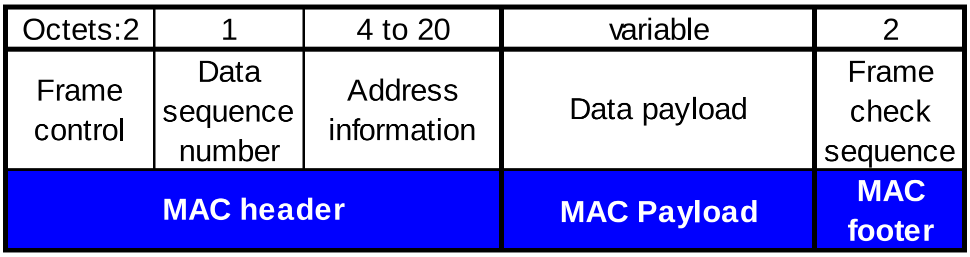
Bits: 0-3	4-7	8-11	12	13	14	15
Beacon order	Superframe order	Final CAP slot	Battery life extension	Reserved	PAN coordinator	Association permit

MAC Command Frame:



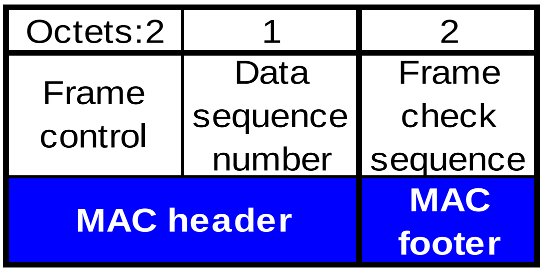
Octets:2	1	4 to 20	1	variable	2
Frame control	Data sequence number	Address information	Command type	Command payload	Frame check sequence
MAC header			MAC payload		MAC footer

Data Frame Format:



Octets:2	1	4 to 20	variable	2
Frame control	Data sequence number	Address information	Data payload	Frame check sequence
MAC header			MAC Payload	MAC footer

Acknowledgement Frame Format:

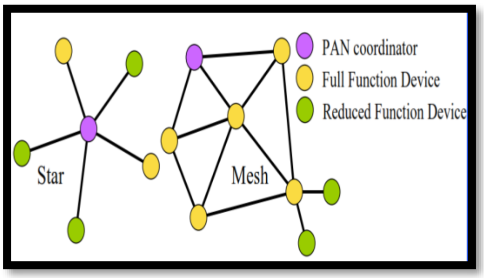


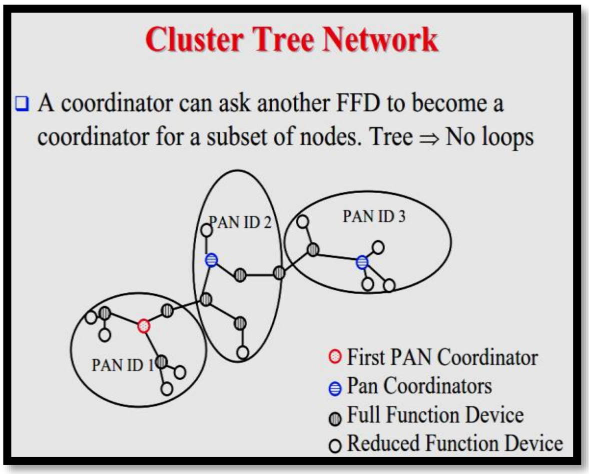
Octets:2	1	2
Frame control	Data sequence number	Frame check sequence
MAC header		MAC footer

802.15.4 CSMA/CA:

- Carrier-sense multiple access with collision avoidance (CSMA/CA) in computer networking, is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by beginning transmission only after the channel is sensed to be "idle". When they do transmit, nodes transmit their packet data in its entirety.
- Wait until the channel is free.
- Wait a random back-off period
- If the channel is still free, transmit.
- If the channel is busy, backoff again.
- Acknowledgement and Beacons are sent without CSMA/CA.

IEEE 802.15.4 supported topologies:





Cluster Tree Network

❑ A coordinator can ask another FFD to become a coordinator for a subset of nodes. Tree ⇒ No loops

IEEE 802.15.4 Device Classes:

- Full function device (FFD)
  - Any topology
  - PAN coordinator capable
  - Talks to any other device
  - Implements complete protocol set
- Reduced function device (RFD)
  - Limited to star topology or end-device in a peer-to-peer network.
  - Cannot become a PAN coordinator
  - Very simple implementation
  - Reduced protocol set

- PAN Coordinator:
  A coordinator that is the principal controller of the PAN. A network has exactly one PAN coordinator.

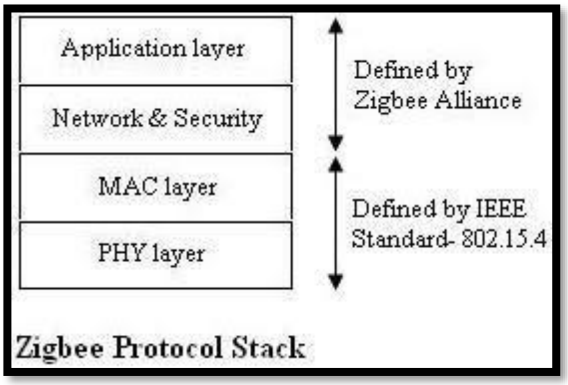
Low-Power Operation:

- Duty-cycle control using superframe structure
  - Beacon order and superframe order
  - Coordinator battery life extension
- Indirect data transmission
- Devices may sleep for extended period over multiple beacons
- Allows control of receiver state by higher layers

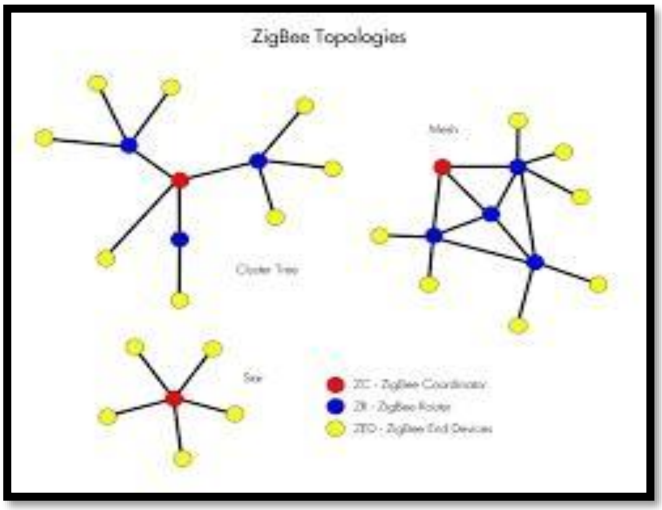
Zigbee Technology:

- Zigbee is a wireless technology developed as an open global standard to address the unique needs of low-cost, low-power wireless IoT networks.
- The Zigbee standard operates on the IEEE 802.15.4 physical radio specification and operates in unlicensed bands including 2.4 GHz, 900 MHz and 868 MHz.

Zigbee Protocal stack:



Zigbee devices:



It Support multiple network topologies such as point-to-point(star), point-to-multipoint (tree), and mesh networks.

ZigBee coordinator (ZC): The most capable device, the coordinator forms the root of the network tree and might bridge to other networks. There is exactly one ZigBee coordinator in each network. It is able to store information about the network, including acting as the repository for security keys.

ZigBee Router (ZR): Routers can act as an intermediate router, passing data from other devices. The router is also a full function device and mostly used in mesh and tree topologies to enhance the network coverage.

ZigBee End Device (ZED): Contains just enough functionality to talk to its parent node (either the coordinator or a router); it cannot relay data from other devices. It requires the least amount of memory, and therefore can be less expensive to manufacture than a ZR or ZC. An end device might be a reduced function device and have the small transmission time. The end device works on the joining of the network and leaving off the network and also aids in transferring the applications.

Zigbee gateway: The ZigBee gateway helps in connecting ZigBee network with another network.

Wi-Fi Technology:

Wi-Fi (Wireless Fidelity) is a family of wireless network protocols, based on the IEEE 802.11 family of standards, which are commonly used for local area networking of devices and Internet access, allowing nearby digital dev6ices to exchange data by radio waves

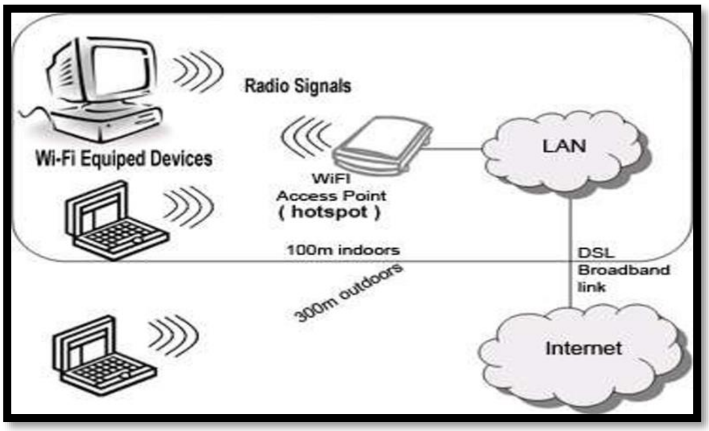
Different wifi IEEE Standard versions are:

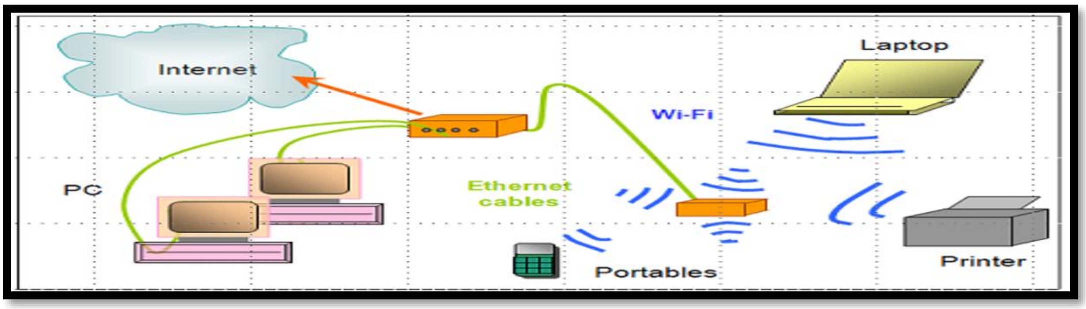
Network standard	**Maximum** **Speed (Mbps)**	**Range (feet)**	**Frequency (GHz)**	**Power drain**	**Cost**
802.11b	**11**	**100-150**	**2.4**	**Moderate**	**Low**
802.11a	**54**	**60-100**	**5**	**High**	**High**
802.11g	**54**	**150-250**	**2.4**	**Moderate**	**Moderate**
802.11n	**200**	**Up to 300 feet**	**2.4 & 5**	**Moderate**	**Moderate**

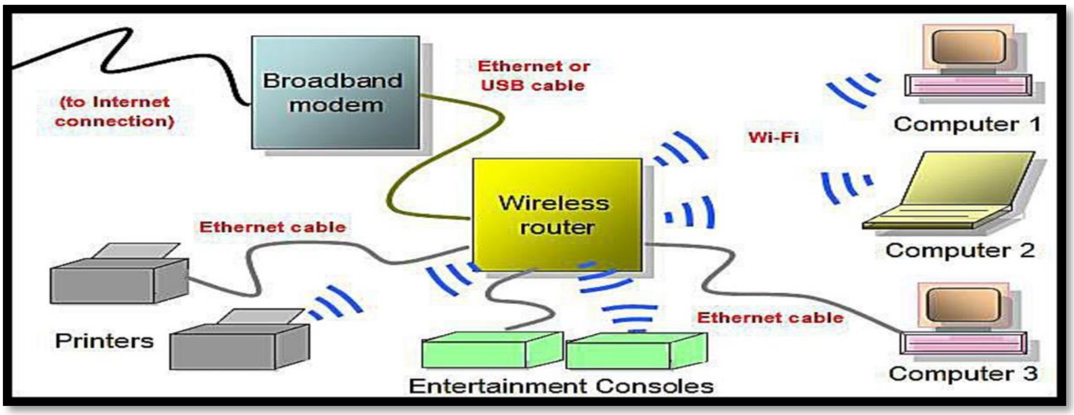
Elements of a Wi-Fi Network:

- **Access Point (AP) -** The AP is a wireless LAN transceiver or "base station" that can connect one or many wireless devices in the same time to the Internet.
- **Safeguards -** Firewalls and anti-virus software protect networks from uninvited users and keep information secure.
- **Wi-Fi cards (Adapters) -** They accept the wireless signal and relay information. They can be internal and external.

How a Wi-Fi Network Works:

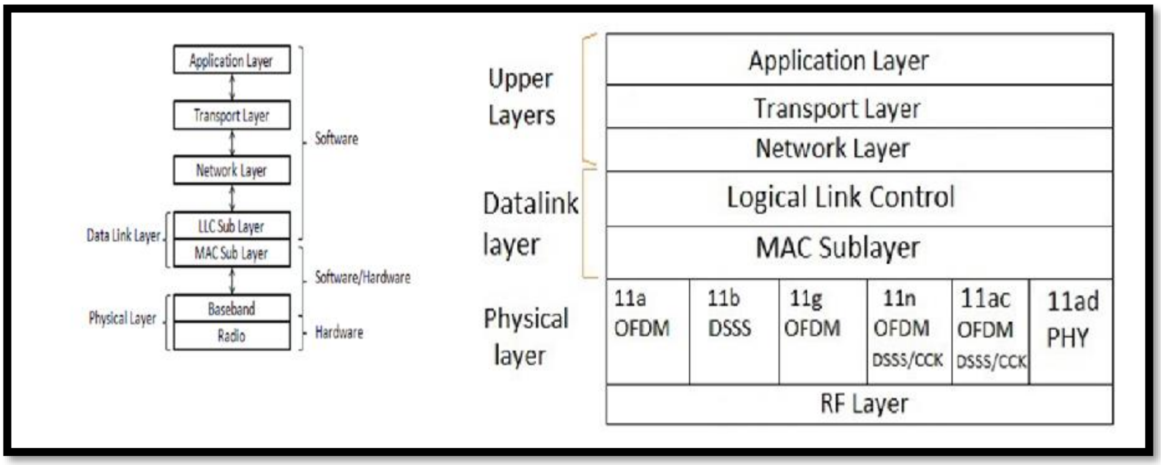






- A Wi-Fi hotspot is created by installing an access point to an internet connection.
- An access point acts as a base station.
- When Wi-Fi enabled device encounters a hotspot the device can then connect to that network wirelessly.
- A single access point can support up to 30 users and can function within a range of 100 – 150 feet indoors and up to 300 feet outdoors.
- Many access points can be connected to each other via Ethernet cables to create a single large network.

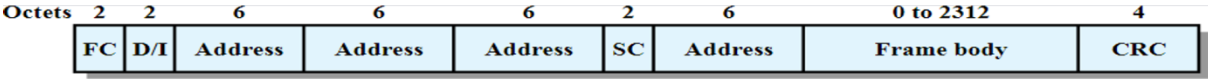
WiFi Protocol stack:



The 802.11 physical layer

- "All 802.11 techniques use short-range radios to transmit signals in either 2.4-GHz or 5-GHz ISM frequency bands". These bands are unlicensed, and so are shared by many other devices such as garage door openers, or microwave ovens.
- Fewer applications tend to use the 5-GHz band, so 5-GHz can be better for some applications despite shorter range due to higher frequency
- All 802.11 transmission methods define multiple rates. Different rates can be used depending on the current conditions. If the signal is weak, a low rate is used. If the signal is clear, the highest rate is used. The process of adjustment is called rate adaption.

802.11 Wireless LAN MAC frame format:



Octets	2	2	6	6	6	2	6	0 to 2312	4
	FC	D/I	Address	Address	Address	SC	Address	Frame body	CRC

- **Frame Control:** Indicates the type of frame (control, management, or data) and provides control information. Control information includes whether the frame is to or from a DS, fragmentation information, and privacy information.
- **Duration/Connection ID:** If used as a duration field, indicates the time (in microseconds) the channel will be allocated for successful transmission of a MAC frame. In some control frames, this field contains an association, or connection, identifier.
- **Addresses:** The number and meaning of the 48-bit address fields depend on context. The transmitter address and receiver address are the MAC addresses of stations joined to the BSS that are transmitting and receiving frames over the wireless LAN. The service set ID (SSID) identifies the wireless LAN over which a frame is transmitted. For an IBSS, the SSID is a random number generated at the time the network is formed. For a wireless LAN that is part of a larger configuration the SSID identifies the BSS over which the frame is transmitted; specifically, the SSID is the MAC-level address of the AP for this BSS. Finally, the source address and destination address are the MAC addresses of stations, wireless or otherwise, that are the ultimate source and destination of this frame. The source address may be identical to the transmitter address and the destination address may be identical to the receiver address.

- **Sequence Control:** Contains a 4-bit fragment number subfield, used for fragmentation and reassembly, and a 12-bit sequence number used to number frames sent between a given transmitter and receiver.
- **Frame Body:** Contains an MSDU or a fragment of an MSDU. The MSDU is a LLC protocol data unit or MAC control information.
- **Frame Check Sequence:** A 32-bit cyclic redundancy check.

WI-FI APPLICATIONS:

- Home
- Small Businesses
- Large Corporations & Campuses
- Health Care
- Wireless ISP (WISP)
- Travellers
- Wi-Fi Camer

Limitations:

- Limited range
- Interference from other devices: such as telephones, microwave ovens'
- High power consumption: making battery life and heat a concern.
- Data security risks: a huge challenge for Wi-FiNetworks

Basic Wi-Fi Security Techniques:

Securing Method	**Encryption Type Used**	**Security Level**	**Notes**
WEP	RC4 encryption algorithm	Low	No longer used; it is can be hacked easily
WPA	TKIP Protocol	High	provides improved encryption security over WEP
WPA2	CCMP Protocol	Very High	An improved version of WPA that uses Advanced Encryption Standard

WEP (Wired Equivalent Privacy): The original encryption technique specified by the IEEE 802.11 standard.

WPA (Wi-Fi Protected Access): A new standard that provides improved encryption security over WEP.

WPA2: is an improved version of WPA that uses Advanced Encryption Standard (AES) technology.

Bluetooth:

Bluetooth is a wireless system that uses radio waves for communication. It has the ability to communicate with many different devices at once without interference on a low-cost, low power, short range radio link

- **It** is an open standard for short-range transmission of digital voice and data that supports point-to-point and multipoint applications.
- When two Bluetooth devices come within 50 meters range of each other, they establish a connection together. It operates at 2.45 GHz which is available globally, although slight variation of location and width of band apply.
- The range is set at 10 to100 meters to optimize for target market of mobile and business user. The range can, however, be increased.

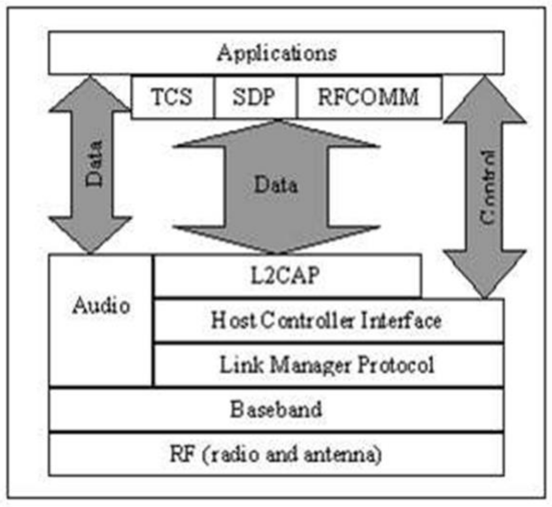
Different Versions of Bluetooth:

1. Bluetooth v1.0 and v1.0B (with mandatory Bluetooth hardware device address)
2. Bluetooth v1.1 (ratified as IEEE standard 802.15.1-2002)
3. Bluetooth v1.2 (faster connection and discovery)
4. Bluetooth v2.0 + EDR (enhanced data rate)
5. Bluetooth v2.1 (secure simple pairing-SSP)
6. Bluetooth v3.0 (high speed data transfer)
7. Bluetooth v4.0 (low energy consumption – recently used in apple i -phone 4S)
8. Bluetooth v4.2 (2014) Designed for the Internet of Things (IoT), BT 4.2 increased the payload size in the Bluetooth packet by 10x, dramatically lowering the overhead to yield 2.5 times more data.
9. Bluetooth v5 (2016) A more robust version with extended battery life, BT 5 increased the outdoor transmission range from 50 to 200 meters.

Maximum Data Rates:

Version	Rate
5.0	3 Mbps (best range 200m)
4.2 + BLE	3 Mbps (IoT)(Payload size more)
4.1	3 Mbps
4.0 + BLE	3 Mbps (low energy)
3.0 + HS	24 Mbps (Wi-Fi) "Bluetooth Classic"
2.1 + EDR	3 Mbps
2.0 + EDR	3 Mbps
1.2	0.7 Mbps
1.0	0.7 Mbps

Bluetooth protocol stack:



Core System Protocols:

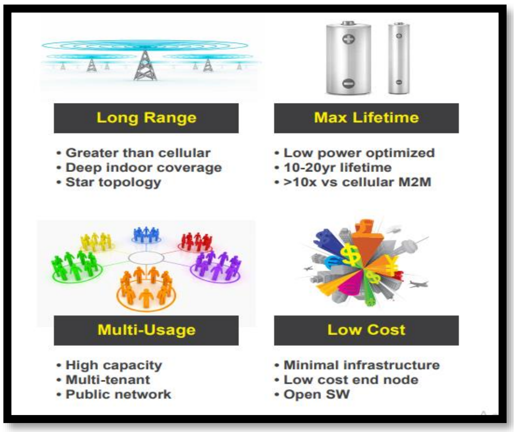
- **Radio (RF) protocol** : Specifies details of the air interface, the use of frequency hopping, modulation scheme, and transmit power.
- **Baseband protocol :** Concerned with connection establishment within a Piconet, addressing, packet format, timing, and power control.
- **Link Manager protocol (LMP) :** Responsible for link setup between Bluetooth devices and ongoing link management.
- **Logical link control and adaptation protocol (L2CAP**):
- L2CAP provides both connectionless and connection-oriented services.
- **Service discovery protocol (SDP) :** Device information, services, and the characteristics of the services can be queried to enable the establishment of a connection between two or more Bluetooth devices
- **RF COMM :** It provides connections to multiple devices by relying on L2CAP to handle multiplexing over single connection
- **Wireless access protocol (WAP):** It supports the limited display size and resolution typically found on mobile devices by providing special formats for Web pages
- **Object exchange protocol (OBEX):** OBEX is a protocol designed to allow a variety of devices to exchange data simply and spontaneously.
- **Telephony control protocol :** Bluetooth's Telephony Control protocol Specification (TCS) defines how telephone calls should be sent across a Bluetooth link
- **Point-to-point protocol (PPP):** The point-to-point protocol is an Internet standard protocol for transporting IP datagram over a point- to-point link

Applications of Bluetooth:

one of the common applications of Bluetooth are −

- In laptops, notebooks and wireless PCs
- In mobile phones and PDAs (personal digital assistant).
- In printers. In wireless headsets.
- In wireless PANs (personal area networks) and even LANs (local area networks)
- To transfer data files, videos, and images and MP3 or MP4.
- In wireless peripheral devices like mouse and keyboards.
- In data logging equipment.
- In the short-range transmission of data from sensors devices to sensor nodes like mobile phones.

LPWAN (Low Power wide area network):



Long Range
- Greater than cellular
- Deep indoor coverage
- Star topology

Max Lifetime
- Low power optimized
- 10-20yr lifetime
- >10x vs cellular M2M

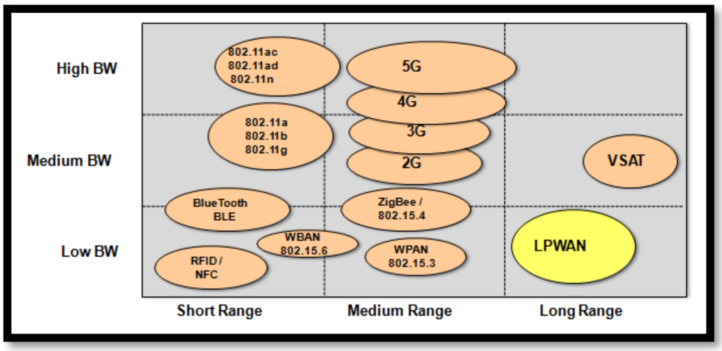
Multi-Usage
- High capacity
- Multi-tenant
- Public network

Low Cost
- Minimal infrastructure
- Low cost end node
- Open SW

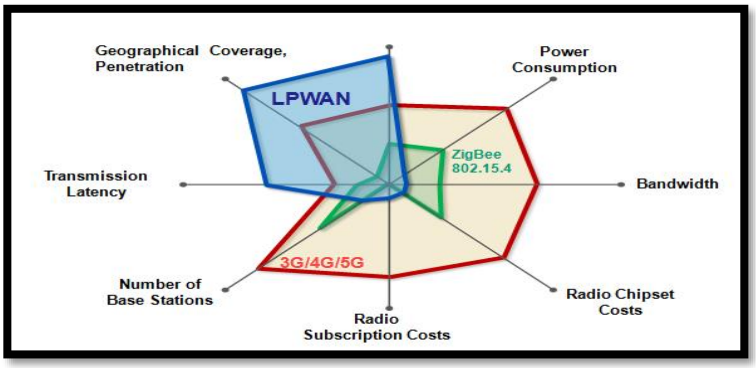
- It is a wireless wide area network technology that interconnects low-bandwidth, battery-powered devices with low bit rates over long ranges.
- It is Created for machine-to-machine (M2M) and internet of things (IoT) networks, LPWANs operate at a lower cost with greater power efficiency than traditional mobile networks. They are also able to support a greater number of connected devices over a larger area.
- LPWANs can accommodate packet sizes from 10 to 1,000 bytes at uplink speeds up to 200 Kbps. LPWAN's long range varies from 2 km to 15 km, depending on the technology.
- Most LPWANs have a star topology where, each endpoint connects directly to common central access points.

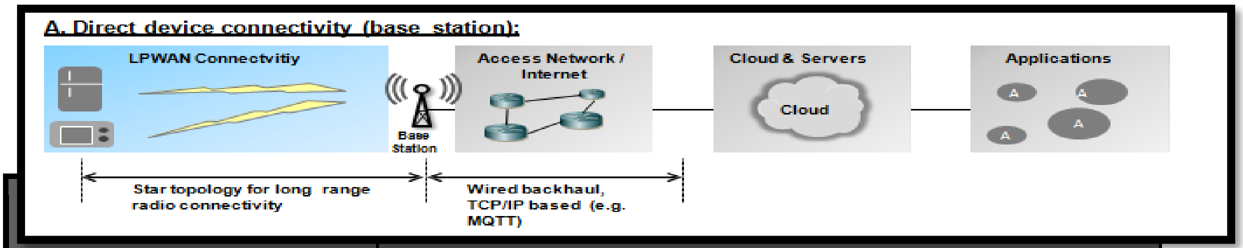
Different communication protocols based on their speed and range:

Different wireless technologies cover different applications with regard to range and bandwidth. Long-range applications with low bandwidth requirements that are typical for IoT and M2M scenarios are not well supported by these existing technologies.



LPWAN requirements and characteristics:



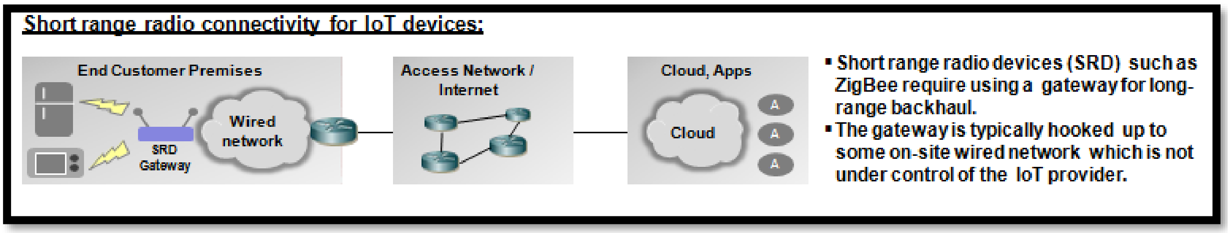

A. Direct device connectivity (base station):
LPWAN Connectvitiy
Base Station
Access Network / Internet
Cloud & Servers
Cloud
Applications
A
A
A
A
Star topology for long range radio connectivity
Wired backhaul, TCP/IP based (e.g. MQTT)

Long range	5 – 40km in the open field
Ultra low power	Battery lifetime of 10 years
Throughput	Depends on the application, but typically a few hundred bit / s or less
Radio chipset costs	$2 or less
Radio subscription costs	$1 per device and year
Transmission latency	Not a primary requirement for LPWAN. IoT applications are typically insensitive to latency.
Required number of base stations for coverage	Very low. LPWAN base stations are able to serve thousands of devices.
Geographic coverage, penetration	Excellent coverage also in remote and rural areas. Good in- building and in-ground penetration (e.g. for reading power meters).

The need for long range wireless connectivity:

- Devices in IoT applications (the "things") are typically installed in the field on residential premises, public places like restaurants or cafés or on industrial plant sites.
- Using short range radio connectivity complicates the IoT setup due to the implications of
- wired on-site connectivity (firewalls, NAT, port and protocol filtering) as shown in bellow figure.

Short range radio connectivity for IoT devices:


Short range radio connectivity for IoT devices:
End Customer Premises
Wired network
SRD Gateway
Access Network / Internet
Cloud, Apps
Cloud
A
A
A

- Short range radio devices (SRD) such as ZigBee require using a gateway for long-range backhaul.
- The gateway is typically hooked up to some on-site wired network which is not under control of the IoT provider.

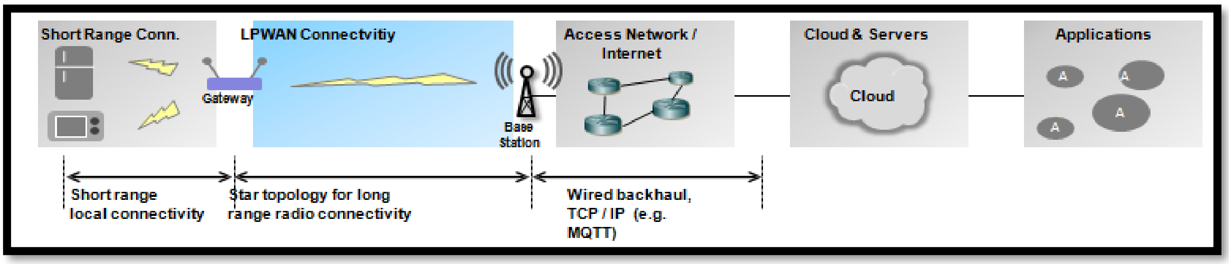
LPWAN network topology:

The wireless portion of LPWAN networks uses a star topology. This obviates the need for complicated wireless mesh routing protocols which would greatly complicate the implementation of end devices and drive up power consumption.

<u>Direct device connectivity (base station):</u>

- A base station provides connectivity to a large number of devices.
- The traffic is backhauled to servers (cloud) through TCP/IP based networks (Internet).
- The base station is responsible for protocol translation from IoT protocols such as MQTT or CoAP to device application protocols.

Indirect device connectivity through a LPWAN gateway:


Short Range Conn.
LPWAN Connectvitiy
Access Network / Internet
Cloud & Servers
Applications
Gateway
Base Station
Cloud
A
A
A
A
Short range local connectivity
Star topology for long range radio connectivity
Wired backhaul, TCP / IP (e.g. MQTT)

- In setups where devices cannot be directly reached through LPWAN, a local gateway bridges LPWAN connectivity to some short-range radio (SRD) technology (e.g., ZigBee, BLE).
- The gateway typically runs on mains power since it serves a larger number of devices and must convert between LPWAN and SRD radio technologies and protocols.
- Gateways may help to improve security since more powerful security algorithms can be implemented on the gateway than is possible on the constrained devices.

Technologies for LPWAN:

LPWAN Technology	Standard / Specification	Range	Spectrum
ETSI LTN	ETSI GS LTN 001 - 003	40 km in open field	Any unlicensed spectrum such as ISM (433MHz, 868MHz, 2.4GHz)
LoRaWAN	LoRa Alliance LoRaWAN	2-5km in urban areas <15km in suburban areas	Any unlicensed spectrum 868MHz (Eu) 915MHz (US) 433MHz (Asia)
Weightless-N	Weightless SIG	<5km in urban areas 20-30km in rural areas	800MHz – 1GHz (ISM)
RPMA	Proprietary (On-Ramp Wireless), planned to become an IEEE standard	<65km line of sight <20km non line of sight	2.4GHz

LoRaWAN (Long range wide area network):

- LoRa is an RF modulation technology for low-power, wide area networks (LPWANs).
- The name, LoRa, is a reference to the extremely long-range data links that this technology enables. Created by Semtech to standardize LPWANs,
- LoRa provides for long-range communications: up to three miles (five kilometers) in urban areas, and up to 10 miles (15 kilometers) or more in rural areas (line of sight).

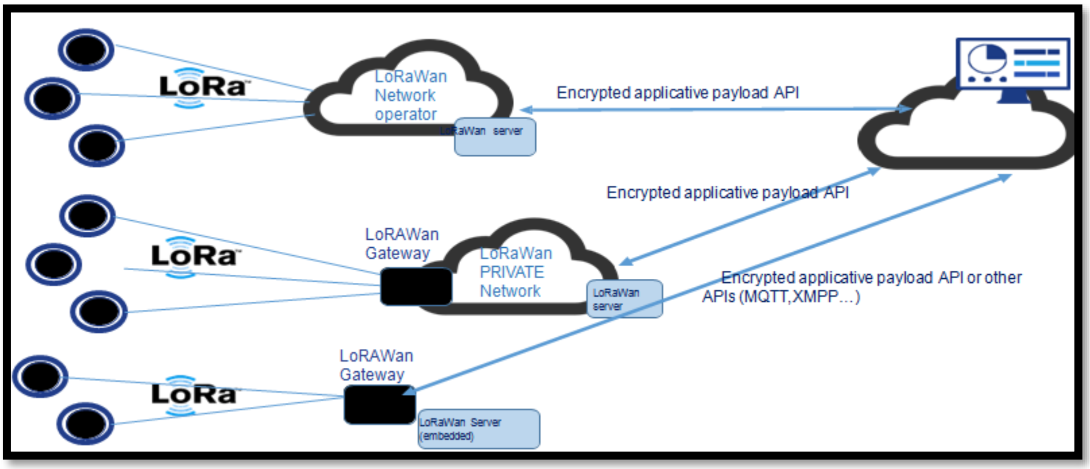
- A key characteristic of the LoRa-based solutions is ultra-low power requirements, which allows for the creation of battery-operated devices that can last for up to 10 years.
- Deployed in a star topology, a network based on the open LoRaWAN protocol is perfect for applications that require long-range or deep in-building communication among a large number of devices that have low power requirements and that collect small amounts of data.
- LoRaWAN is a media access control (MAC) protocol for wide area networks.
- It is designed to allow low-powered devices to communicate with Internet-connected applications over long range wireless connections.
- LoRaWAN can be mapped to the second and third layer of the OSI model. It is implemented on top of LoRa or FSK modulation in industrial, scientific and medical (ISM) radio bands.
- The LoRaWAN protocols are defined by the LoRa Alliance and formalized in the LoRaWAN Specification.
- Datarate of 0.3 to 50 Kb/s
- Encryption AES128 device – server & end-node – user app
- Stars of stars architecture
- 3 classes of devices (bidirectionnal communication)
- A Class
- B Class (beacon)
- C Class (continuous)
- **Uplink messages format**

Preamble	PHDR	PHDR_CRC	PHYPayload	CRC

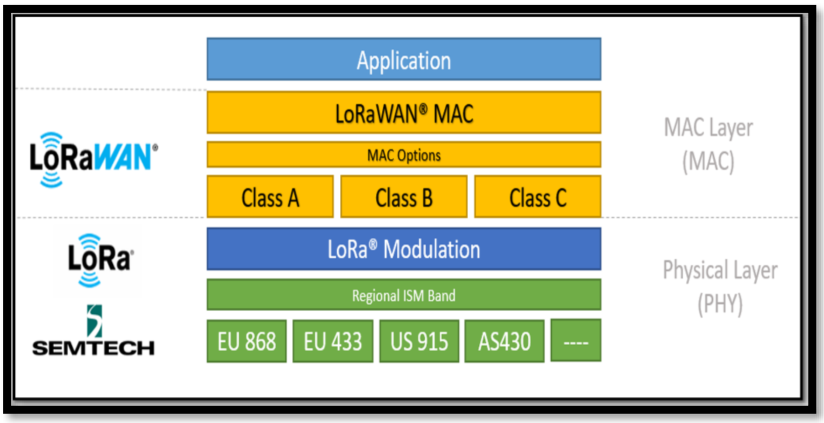
- **Downlink messages format :**

Preamble	PHDR	PHDR_CRC	PHYPayload

Lora Architecture Principles:

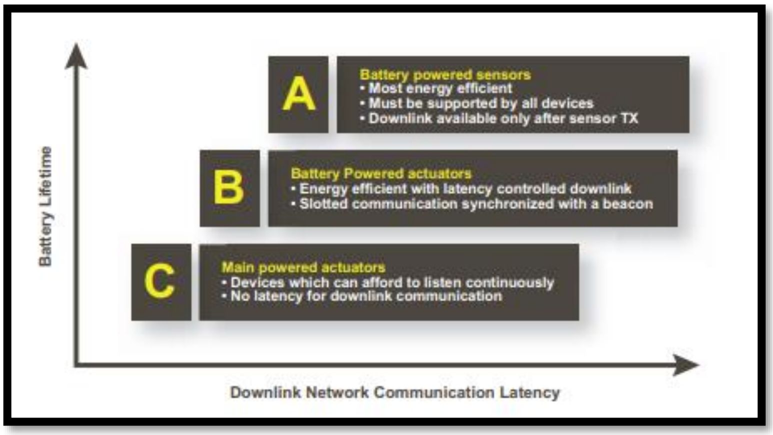

LoRa
LoRaWan Network operator
LoRaWan server
Encrypted applicative payload API
LoRa
LoRAWan Gateway
LoRaWan PRIVATE Network
LoRaWan server
Encrypted applicative payload API
Encrypted applicative payload API or other APIs (MQTT,XMPP…)
LoRa
LoRAWan Gateway
LoRaWan Server (embedded)

LoRaWAN Stack & Architecture:



Device Classes –

End-devices serve different applications and have different requirements. In order to optimize a variety of end application profiles, LoRaWAN™ utilizes different device classes. The device classes trade off network downlink communication latency versus battery lifetime. In a control or actuator-type application, the downlink communication latency is an important factor.


A
Battery powered sensors
• Most energy efficient
• Must be supported by all devices
• Downlink available only after sensor TX
B
Battery Powered actuators
• Energy efficient with latency controlled downlink
• Slotted communication synchronized with a beacon
C
Main powered actuators
• Devices which can afford to listen continuously
• No latency for downlink communication
Battery Lifetime
Downlink Network Communication Latency

Bi-directional end-devices (Class A):

End-devices of Class A allow for bi-directional communications whereby each end-device's uplink transmission is followed by two short downlink receive windows. The transmission slot scheduled by the end-device is based on its own communication needs with a small variation based on a random time basis (ALOHA-type of protocol).

Bi-directional end-devices with scheduled receive slots (Class B):

In addition to the Class A random receive windows, Class B devices open extra receive windows at scheduled times. In order for the end-device to open its receive window at the scheduled time, it receives a time-synchronized beacon from the gateway. This allows the server to know when the end-device is listening. Bi-directional end-devices with maximal receive slots (Class C): End-devices of Class C have almost continuously open receive windows, only closed when transmitting.

5G Technology:

- 5G is the 5th generation mobile network. It is a new global wireless standard after 1G, 2G, 3G, and 4G networks.
- 5G enables a new kind of network that is designed to connect virtually everyone and everything together including machines, objects, and devices.
- 5G wireless technology is meant to deliver higher multi-Gbps peak data speeds, ultra-low latency, more reliability, massive network capacity, increased availability, and a more uniform user experience to more users.
- Higher performance and improved efficiency empower new user experiences and connects new industries.

5G Frequency bands:

5G networks operate on up to three frequency bands – low, medium, and high.

- Low-band 5G uses a similar frequency range to 4G cell phones, 600–850 MHz, giving download speeds a little higher than 4G: 30–250 megabits per second (Mbit/s). Low-band cell towers have a range and coverage area similar to 4G towers.
- Mid-band 5G uses microwaves of 2.5–3.7 GHz, allowing speeds of 100–900 Mbit/s, with each cell tower providing service up to several kilometres in radius.
- High-band 5G uses frequencies of 25–39 GHz, near the bottom of the millimetre wave band, although higher frequencies may be used in the future. It often achieves download speeds in the gigabit per second (Gbit/s) range.
- The frequency bands for 5G networks come in two sets. Frequency range 1 (FR1) is from 450 MHz to 6 GHz, which includes the LTE frequency range. Frequency range 2 (FR2) is from 24.25 GHz to 52.6 GHz.
- The sub-6 GHz range is the name for FR1 and the millimetre wave (mm Wave) spectrum is the name for FR2.
- 5G is based on OFDM (Orthogonal frequency-division multiplexing), a method of modulating a digital signal across several different channels to reduce interference.

Application areas:

The ITU-R has defined three main application areas for the enhanced capabilities of 5G. They are

1. Enhanced Mobile Broadband (eMBB)
2. Ultra Reliable Low Latency Communications (URLLC)
3. Massive Machine Type Communications (mMTC)

Enhanced Mobile Broadband (eMBB):

eMBB aims to meet the people's demand for an increasingly digital lifestyle, and focuses on services that have high requirements for bandwidth, such as high definition (HD) videos, virtual reality (VR), and augmented reality (AR).

It uses 5G as a progression from 4G LTE mobile broadband services, with faster connections, higher throughput, and more capacity. This will benefit areas of higher traffic such as stadiums, cities, and concert venues.

Ultra-Reliable Low-Latency Communications (URLLC):

uRLLC aims to meet expectations for the demanding digital industry and focuses on latency-sensitive services, such as assisted and automated driving, and remote management.

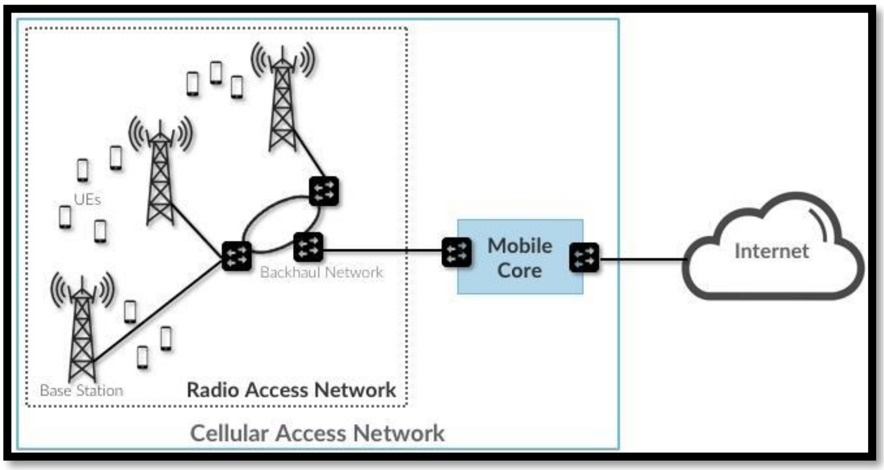
It refer to using the network for mission critical applications that require uninterrupted and robust data exchange.

Massive Machine-Type Communications (mMTC):

mMTC aims to meet demands for a further developed digital society and focuses on services that include high requirements for connection density, such as smart city and smart agriculture.

It is used to connect to a large number of devices. 5G technology will connect some of the 50 billion connected IoT devices. Most will use the less expensive Wi-Fi. Drones, transmitting via 4G or 5G, will aid in disaster recovery efforts, providing real-time data for emergency responders**.**

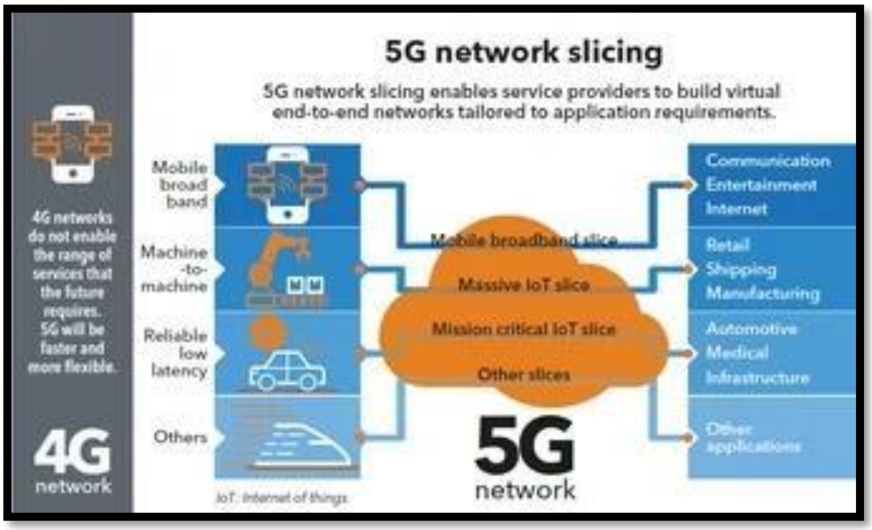
Basic 5G Architechture:



Above figure the cellular network consists of two main subsystems: the Radio Access Network (RAN) and the Mobile Core.

- The cellular network provides wireless connectivity to devices that are on the move. These devices, which are known as User Equipment (UE), have traditionally corresponded to smartphones and tablets, but will increasingly include cars, drones, industrial and agricultural machines, robots, home appliances, medical devices, and so on.
- The **RAN** manages the radio spectrum, making sure it is used efficiently and meets the quality-of-service requirements of every user. It corresponds to a distributed collection of base stations. As noted above, in 4G these are (somewhat cryptically)named eNodeB (or eNB), which is short for evolved Node B. In 5G they are known as gNB. (The g stands for "next Generation".).
- The **Mobile Core** is a bundle of functionality (as opposed to a device) that serves several purposes.
  1. Provides Internet (IP) connectivity for both data and voice services.
  2. Ensures this connectivity fulfills the promised QoS requirements.
  3. Tracks user mobility to ensure uninterrupted service.
  4. Tracks subscriber usage for billing and charging.

5G Network Slicing:


5G network slicing
5G network slicing enables service providers to build virtual end-to-end networks tailored to application requirements.
4G networks do not enable the range of services that the future requires. 5G will be faster and more flexible.
4G network
Mobile broad band
Machine -to- machine
Reliable low latency
Others
IoT: Internet of things
Mobile broadband slice
Massive IoT slice
Mission critical IoT slice
Other slices
5G network
Communication Entertainment Internet
Retail Shipping Manufacturing
Automotive Medical Infrastructure
Other applications

- 5G network slicing is the use of network virtualization to divide single network connections into multiple distinct virtual connections that provide different amounts of resources to different types of traffic.
- The basic idea of network slicing is to "slice" the original network architecture in multiple logical and independent networks that are configured to effectively meet the various services requirements.

5G Based IoT Applications:

- **Smart Cities** – Cities with wide variety of devices such as, home appliances, surveillance cameras, monitoring sensors, actuators, displays, vehicles, and so on, can be fostered under one network of connected devices.
- **Self-driving Cars** – Google’s subsidiary self-driving cars currently average about 20,000+autonomous miles every week.
- **Smartwatches** – becoming a part of everyday life. By 2020, a quarter of a billion vehicles will be connected to the Internet, providing passengers new possibilities for in vehicle services.
- **Patients Surveillance -** Monitor the condition of patients inside hospitals and at home.
- **Structural Health -** Monitor vibrations and material conditions in buildings, bridges, and historical monuments.
- **Earthquake Early Detection -** Better systems for detecting tremors.
- **M2M Applications -** Machine auto-diagnosis and assets control.
- **Hydroponics** – Exercise precise environmental control for plants grown in hydroponic systems to produce efficient crops.