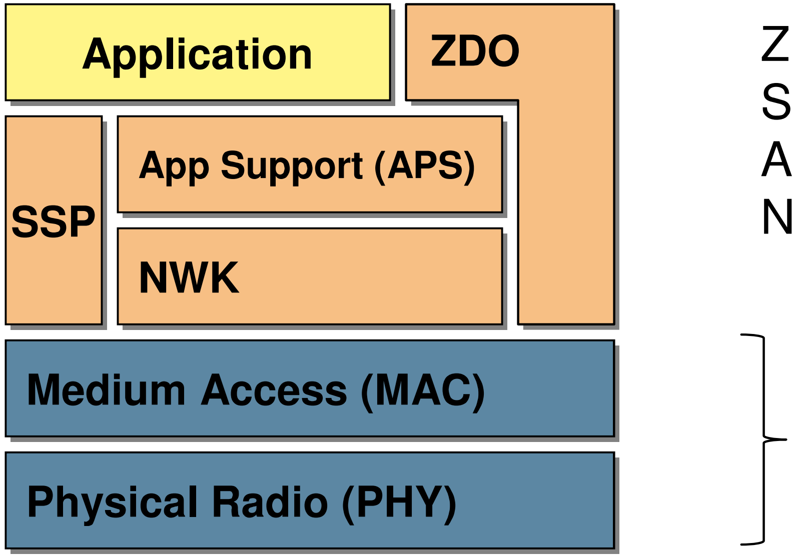
ZigBee

Evangéline BENEVENT

Università Mediterranea di Reggio Calabria
DIMET

ZigBee

- ZigBee Architecture
  - Following the standard Open Systems Interconnection (OSI) reference model, ZigBee's protocol stack is structured in layers. The first two layers, physical (PHY) and media access (MAC) are defined by the IEEE 802.15.4 standard. The layers above them are defined by the ZigBee Alliance.

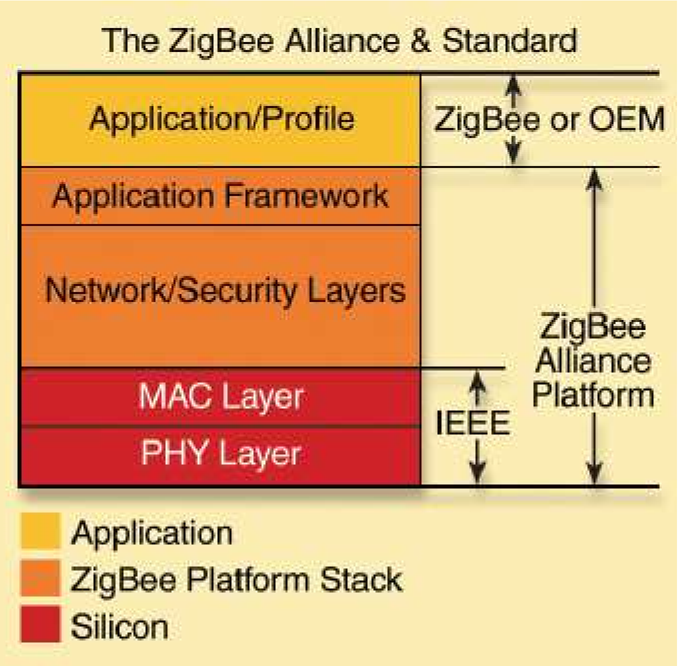


IEEE 802.15.4 standard

ZDO: ZigBee Device Object
SSP: Security Service Provider
APS: Application Support sub-layer
NWK: Network layer

ZigBee

- ZigBee Architecture
  - Three areas of architectural responsibility are in a ZigBee engineering effort:
    - 1. the physical radio,
    - 2. the logical network,
    - 3. the application layer.



ZigBee firmware model

ZigBee

- ZigBee Architecture

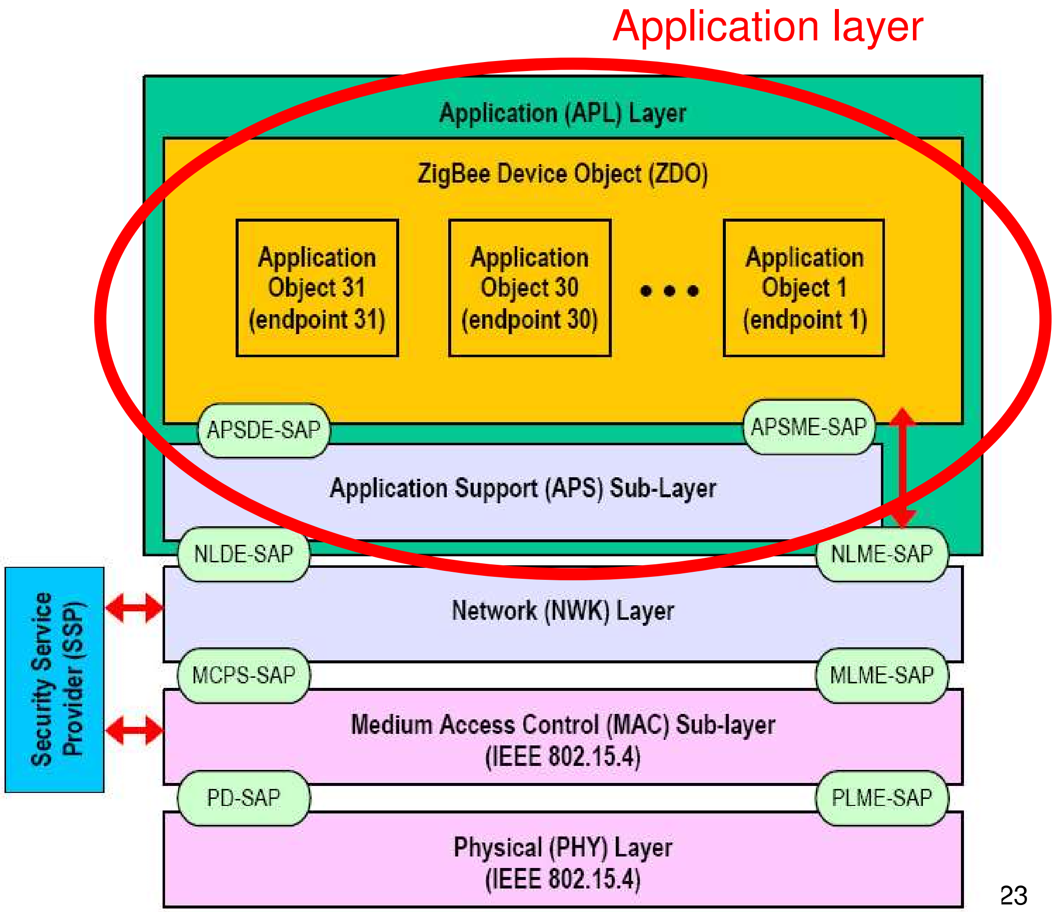
  - 1. The physical and MAC layers take full advantage of the **physical radio** specified by the IEEE 802.15.4. The 802.15.4 specification describes a peer-to-peer radio, the data rates, channels, and modulation techniques to be employed.

  - 2. The ZigBee Alliance specifies the **logical network**, security and application software which are implemented in a firmware stack. It's the ZigBee networking stack that creates the mesh networking capabilities. Each microcontroller / RF chip combination requires its own ZigBee stack due to the differences in microcontrollers and RF chips.

  - 3. The **application layer** is defined by profiles, of which there are two types: *public* profiles are those certified by the ZigBee Alliance for interoperability purposes, and *private* profiles are for use in closed systems. For public profiles, ZigBee Logo Certification is available. Private profiles are not intended to interoperate and, therefore, cannot be certified.

ZigBee

- ZigBee Application Layer
  - The ZigBee application layer consists of the Application Support (APS) sublayer, the ZigBee Device Object (ZDO), and the manufacturer-defined application objects.


Application layer
Application (APL) Layer
ZigBee Device Object (ZDO)
Application Object 31 (endpoint 31)
Application Object 30 (endpoint 30)
• • •
Application Object 1 (endpoint 1)
APSDE-SAP
APSME-SAP
Application Support (APS) Sub-Layer
NLDE-SAP
NLME-SAP
Security Service Provider (SSP)
Network (NWK) Layer
MCPS-SAP
MLME-SAP
Medium Access Control (MAC) Sub-layer (IEEE 802.15.4)
PD-SAP
PLME-SAP
Physical (PHY) Layer (IEEE 802.15.4)

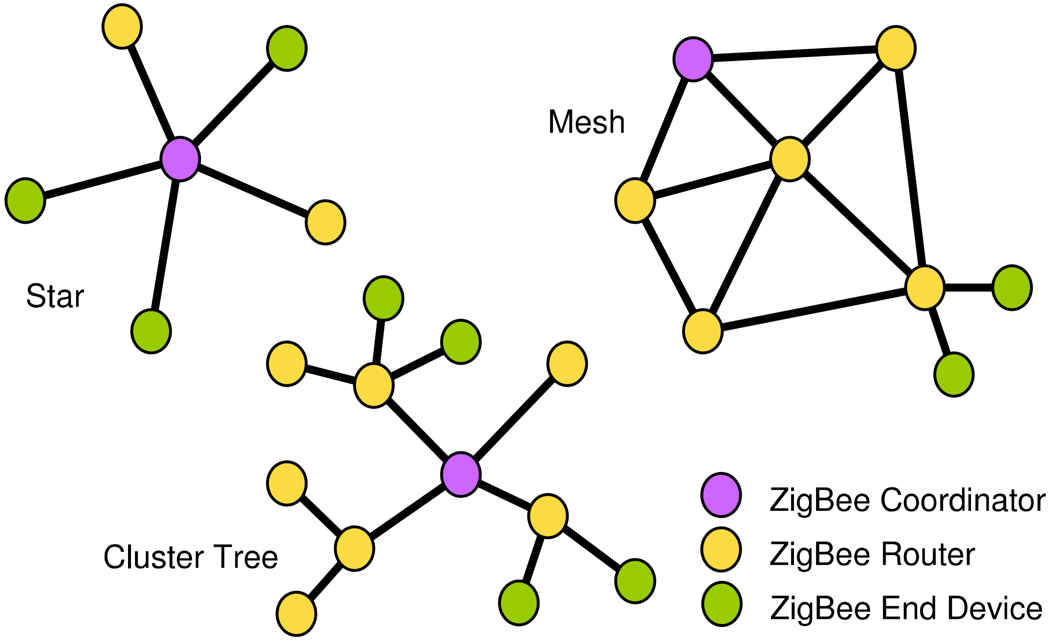
A more detailed ZigBee architecture

ZigBee

- ZigBee Application Layer
  - The responsibilities of the **ZigBee Device Object** (ZDO) are:
    - To define the role of the device within the network (ZigBee coordinator or end device),
    - To initiate and/or respond to binding requests,
    - To establish a secure relationship between network devices selecting one of ZigBee's security methods such as public key, symmetric key, etc.
  - The responsibilities of the **Application Support Layer** (APS) are:
    - The discovery, which is the ability to determine which other devices are operating in the personal operating space of a device,
    - The binding, which is the ability to match two or more devices together based on their services and their needs and forwarding messages between bound devices.

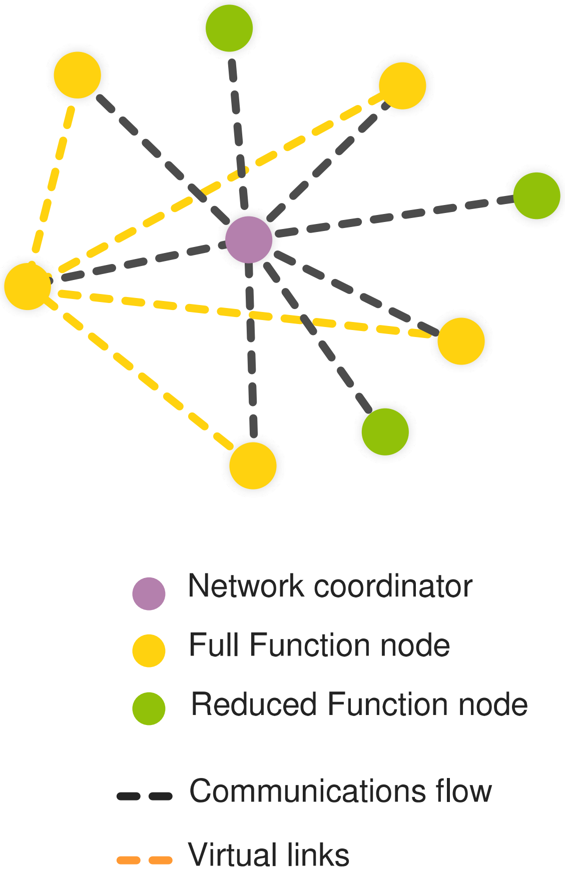
ZigBee

- ZigBee Network Layer
  - The NWK layer associates or dissociates devices using the network coordinator, implements security, and routes frames to their intended destination. In addition, the NWK layer of the network coordinator is responsible for starting a new network and assigning an address to newly associated devices.



ZigBee

- ZigBee Device Types
  - ZigBee coordinator ●
    - One required for each ZigBee network
    - Initiates network formation
  - ZigBee router ●
    - Participates in multihop routing of messages
  - ZigBee end device ●
    - Does not allow association or routing
    - Enables very low cost solutions



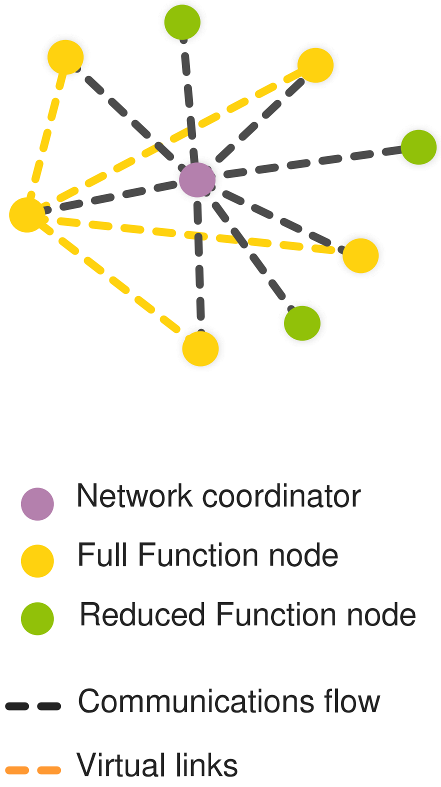
ZigBee

- ZigBee Device Types: an other denomination

● Network coordinator: The network coordinator maintains overall network knowledge. It’s the most sophisticated of the three types and requires the most memory and computing power.

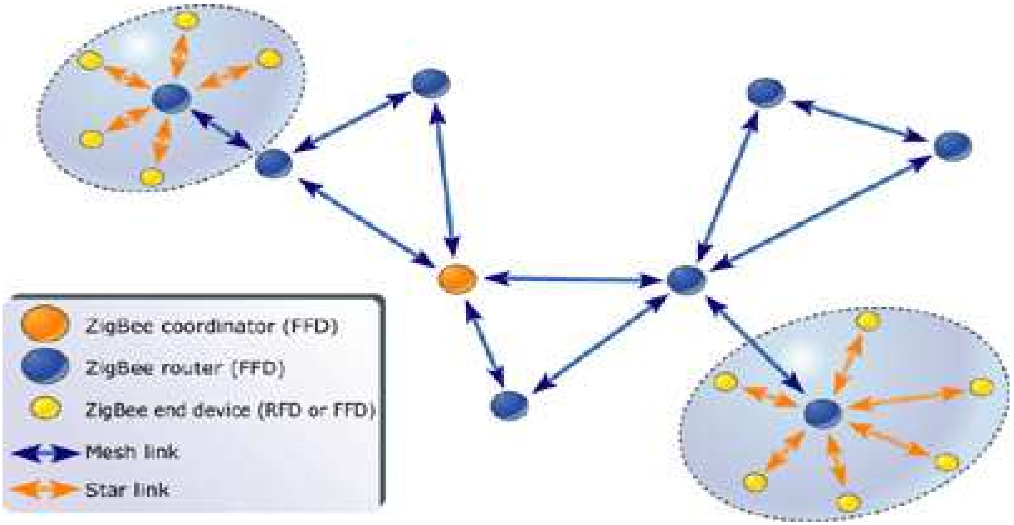
● Full function device: A full function device supports all 802.15.4 functions and features specified by the standard. It can operate as a network coordinator. Additional memory and computing power make it ideal for network router functions.

● Reduced function device: A reduced function device carries limited (as specified in the standard) functionality to lower cost and complexity. It’s generally found in network-edge devices (where the network touches the real world).



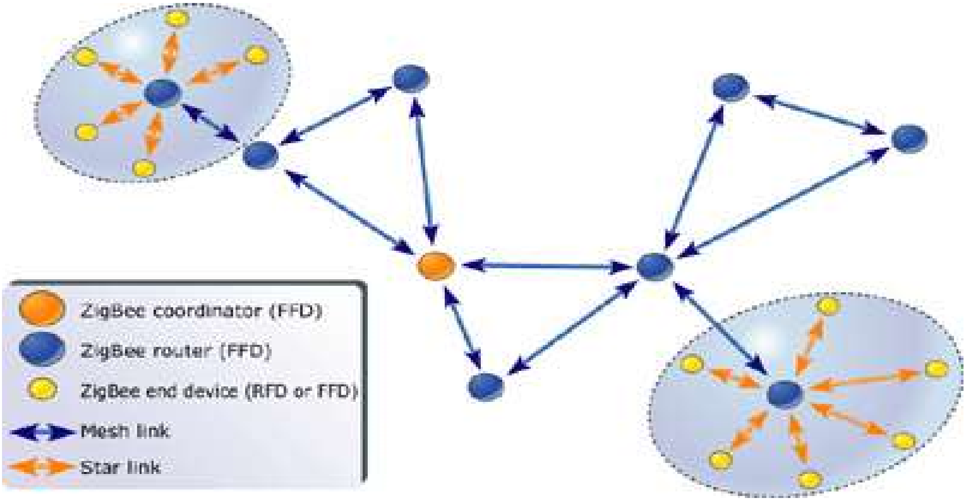
ZigBee

- ZigBee network topologies
  - Star topology
    - In a star topology, one the FFD-type devices assumes the role of network coordinator and is responsible for initiating and maintaining the devices on the network.



ZigBee

- ZigBee network topologies
  - Mesh topology
    - In a mesh topology, the ZigBee coordinator is responsible for starting the network and for choosing key networks parameters, but the network may be extended through the use of ZigBee routers. The routing algorithm uses a request-response protocol to eliminate sub-optimal routing.



ZigBee

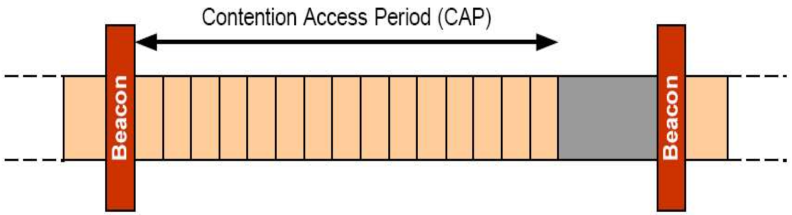
- Node Addresses
  - In a ZigBee network, each node must have unique identification. This is achieved by means of two addresses: IEEE Address and Network Address.
  - IEEE Address:
    - This is a 64-bit address, allocated by the IEEE, which uniquely identifies a device. No two devices in the world can have the same IEEE address. It is also called the MAC address or the extended address.
  - Network Address:
    - This is a 16-bit address identifies the node in the network. It is local to that network, thus two nodes on separate networks may have the same network address. Network addresses are allocated by the parent node (router or coordinator) when a node joins a network. It is also called the short address.

ZigBee

- Power and Beacons
  - Ultra-low power consumption
    - Ultra-low power consumption is how ZigBee technology promotes a long lifetime for devices with nonrechargeable batteries.
    - ZigBee networks are designed to conserve the power of the slave nodes.
    - For most of the time, a slave device is in deep-sleep mode and wakes up only for a fraction of a second to confirm its presence in the network.

ZigBee

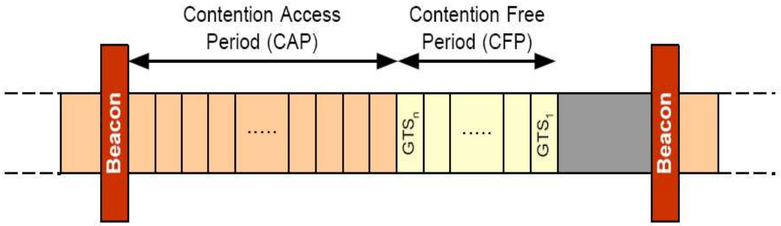
- Power and Beacons
  - Beacon or non-beacon?
    - ZigBee networks can use beacon or non-beacon environments.
    - Beacons are used to synchronize the network devices, identify the HAN, and describe the structure of the superframe.
    - The beacon intervals are set by the network coordinator and vary from 15ms to over 4 minutes.



Superframe structure

ZigBee

- Power and Beacons
  - Beacon or non-beacon?
    - Sixteen equal time slots are allocated between beacons for message delivery. The channel access in each time slot is contention-based.
    - However, the network coordinator can dedicate up to seven guaranteed time slots for non-contention based or low-latency delivery.



Superframe structure with GTS

ZigBee

- Power and Beacons
  - Beacon or non-beacon?
    - *Beacon mode* is a mechanism for controlling power consumption in extended networks such as cluster tree or mesh.
    - It enables all the clients to know when to communicate with each other. Here, the two-way radio network has a central dispatcher that manages the channel and arranges the calls.
    - The primary value of beacon mode is that it reduces the system's power consumption.

ZigBee

- Power and Beacons
  - Beacon or non-beacon?
    - Beacon mode is more suitable when the network coordinator is battery-operated.
    - Client units listen for the network coordinator's beacon (broadcast at intervals between 0.015 and 252s).
    - A client registers with the coordinator and looks for any messages directed to it. If no messages are pending, the client returns to sleep, awaking on a schedule specified by the coordinator.
    - Once the client communications are completed, the coordinator itself returns to sleep.

ZigBee

- Power and Beacons
  - Beacon or non-beacon?
    - The *non-beacon mode* is a simple, traditional multiple-access system used in simple peer and near-peer networks.
    - It operates like a two-way radio network, where each client is autonomous and can initiate a conversation at will, but could interfere with others unintentionally.
    - Non-beacon mode is typically used for security systems where client units, such as intrusion sensors, motion detectors, and glass-break detectors, sleep 99.999% of the time.

ZigBee

- Power and Beacons
  - Beacon or non-beacon?
    - Remote units wake up on a regular, yet random, basis to announce their continued presence in the network.
    - When an event occurs, the sensor wakes up instantly and transmits the alert.
    - The network coordinator, powered from the main source, has its receiver on all the time and can therefore wait to hear from each of these stations.
    - Since the network coordinator has an "infinite" source of power it can allow clients to sleep for unlimited periods of time, enabling them to save power.

ZigBee

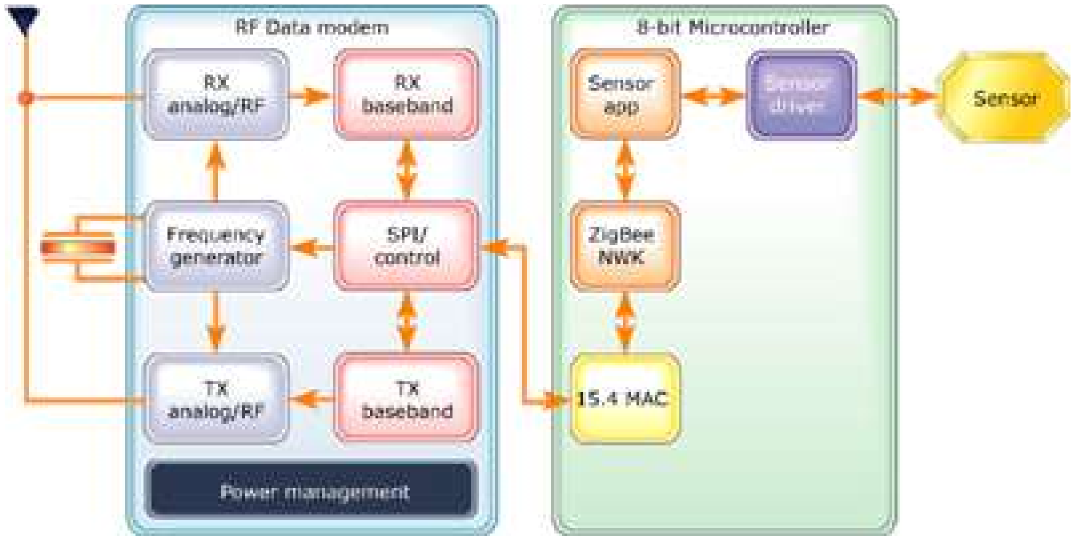
- Frame structure
  - The frame structures have been designed to keep the complexity to a minimum while at the same time making them sufficiently robust for transmission on a noisy channel.
  - Four basic frame types defined in 802.15.4:
    - A **beacon frame**, used by a coordinator to transmit beacons,
    - A **data frame**, used for all transfers of data,
    - An **acknowledgment frame**, used for confirming successful frame reception,
    - A **MAC command frame**, used for handling all MAC peer entity control transfers.

ZigBee

- ZigBee stack
  - The ZigBee stack is small in comparison to other wireless standards.
  - For network-edge devices with limited capabilities, the stack requires about 4Kb of the memory. Full implementation of the protocol stack takes less than 32Kb of memory. The network coordinator may require extra RAM for a node devices database and for transaction and pairing tables.
  - The 802.15.4 standard defines 48 primitives for the PHY and MAC layers. This number is still modest compared to 131 primitives defined for Bluetooth.
  - Such a compact footprint enables you to run Zigbee on a simple 8-bit microcontroller .

ZigBee

- ZigBee stack
  - A typical ZigBee-enabled device includes a radio frequency integrated circuit (RF IC) with a partially implemented PHY layer connected to a low-power, low-voltage 8-bit microcontroller with peripherals, connected to an application sensor or actuators. The protocol stack and application firmware reside in on-chip flash memory. The entire ZigBee device can be compact and cost efficient.

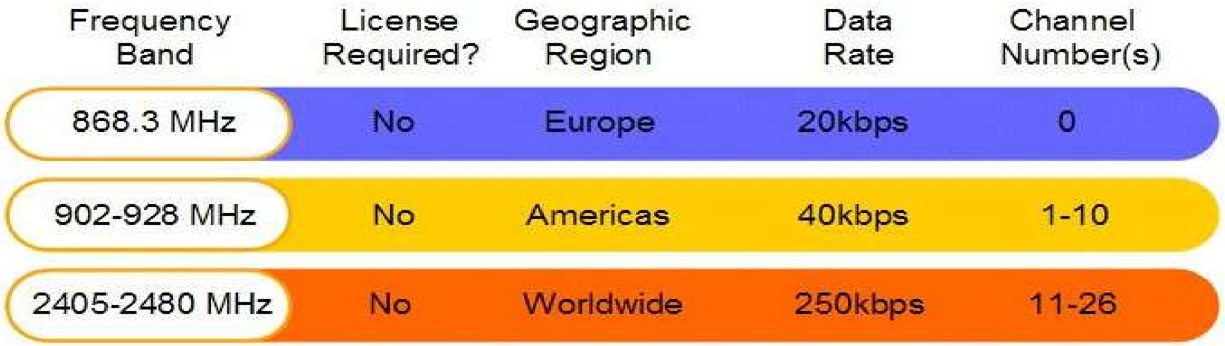


ZigBee

- Channel access
  - Two channel-access mechanisms are implemented in 802.15.4 standard:
    - For a non-beacon network, a standard ALOHA CSMA-CA (carrier-sense medium-access with collision avoidance) communicates with positive acknowledgement for successfully received packets.
    - In a beacon-enabled network, a superframe structure is used to control channel access. The superframe is set up by the network coordinator to transmit beacons at predetermined intervals (multiples of 15.38ms, up to 252s) and provides 16 equal-width time slots between beacons for contention-free channel access in each time slot. The structure guarantees dedicated bandwidth and low latency. Channel access in each time slot is contention-based. However, the network coordinator can dedicate up to seven guaranteed time slots per beacon interval for quality of service.

ZigBee

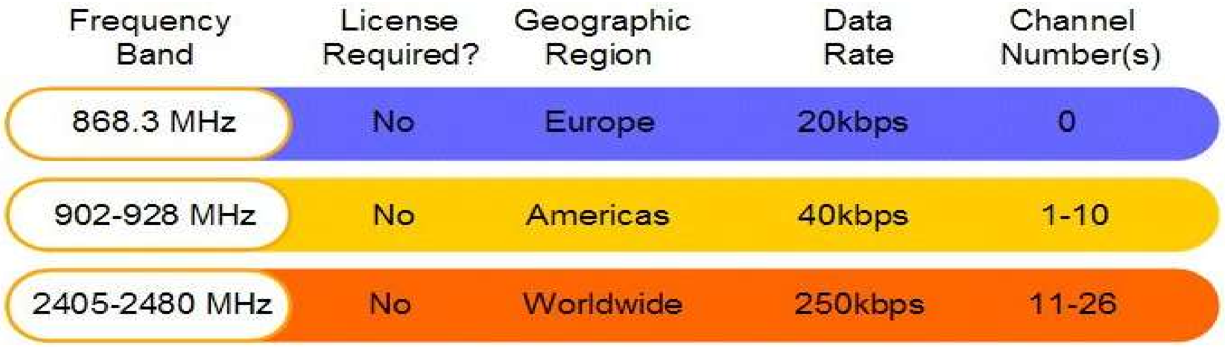
- RF transmission characteristics
  - Frequency bands:
    - ZigBee-compliant products operate in unlicensed bands worldwide, including:
      - 2.4 GHz band (global),
      - 902 to 928 MHz band (Americas),
      - 868 MHz band (Europe).



Frequency Band	License Required?	Geographic Region	Data Rate	Channel Number(s)
868.3 MHz	No	Europe	20kbps	0
902-928 MHz	No	Americas	40kbps	1-10
2405-2480 MHz	No	Worldwide	250kbps	11-26

ZigBee

- RF transmission characteristics
  - Data rate:
    - Data throughput rates of :
      - 250 kbps can be achieved at 2.4 GHz (16 channels),
      - 40 kbps at 915 MHz (10 channels),
      - 20 kbps at 868 MHz (1 channel).



Frequency Band	License Required?	Geographic Region	Data Rate	Channel Number(s)
868.3 MHz	No	Europe	20kbps	0
902-928 MHz	No	Americas	40kbps	1-10
2405-2480 MHz	No	Worldwide	250kbps	11-26