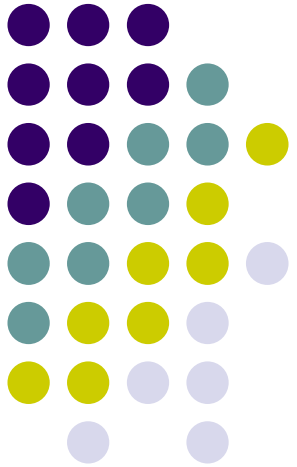
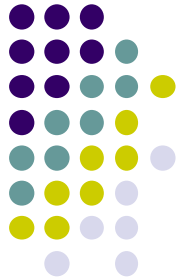
ZigBee

Evangéline BENEVENT

Università Mediterranea di Reggio Calabria
DIMET

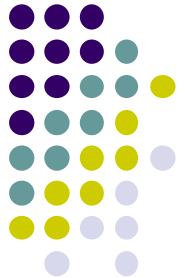


ZigBee



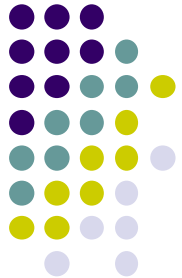
- OUTLINE
  - 1. Why is ZigBee needed?
  - 2. What is ZigBee?
  - 3. What are the ZigBee benefits?
  - 4. How does ZigBee operate?
  - Conclusion

ZigBee



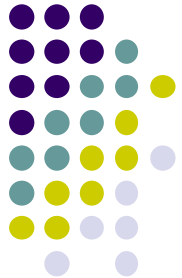
- OUTLINE
  - 1. Why is ZigBee needed?
  - 2. What is ZigBee?
  - 3. What are the ZigBee benefits?
  - 4. How does ZigBee operate?
  - Conclusion

ZigBee



- Why is ZigBee needed?
  - For the last few years, we have seen a great expansion of remote control devices in our day-to-day life. Ten years ago, infrared remotes for the television were the only such devices in our homes.
  - Now, more and more devices are remotely controlled in a house. They are not interchangeable and they don't support more than one device. Because most remotely controlled devices are proprietary, even those remotes used for the same function are not interchangeable with similar remotes from different manufacturers.
  - To interact with all these remotely controlled devices, we will need to put them under a single standardized control interface that can interconnect into a network, specifically home-area network (HAN).
  - One of the most promising home-area network protocols is ZigBee, a software layer based on the IEEE 802.15.4 standard.

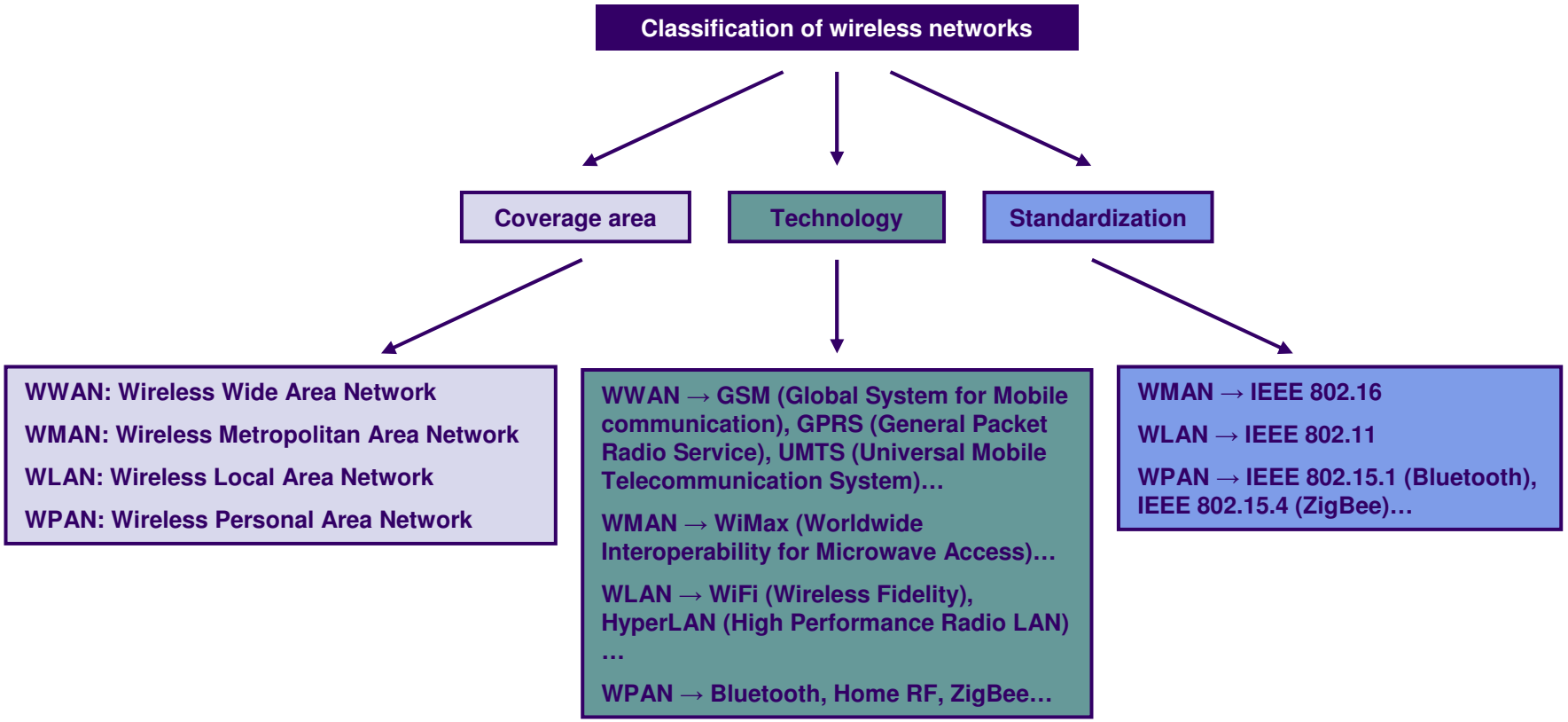
ZigBee



- Requirements for Home-Area Networks:
  - If we take a look at the type of data that circulates within a network of sensors and actuators, we may find that most of it is small packets that control devices or obtain their status. For many applications, the device mostly stays in deep-sleep mode and only sends a short burst of information if a trigger event occurs.
  - The main requirements for devices in such types of networks are:
    - Extremely low power consumption,
    - The ability to sleep for a long time,
    - Simplicity,
    - Low cost.
  - A home network should also support different configurations, such as a star or mesh network, to effectively cover a household area of 30 to 70 meters.

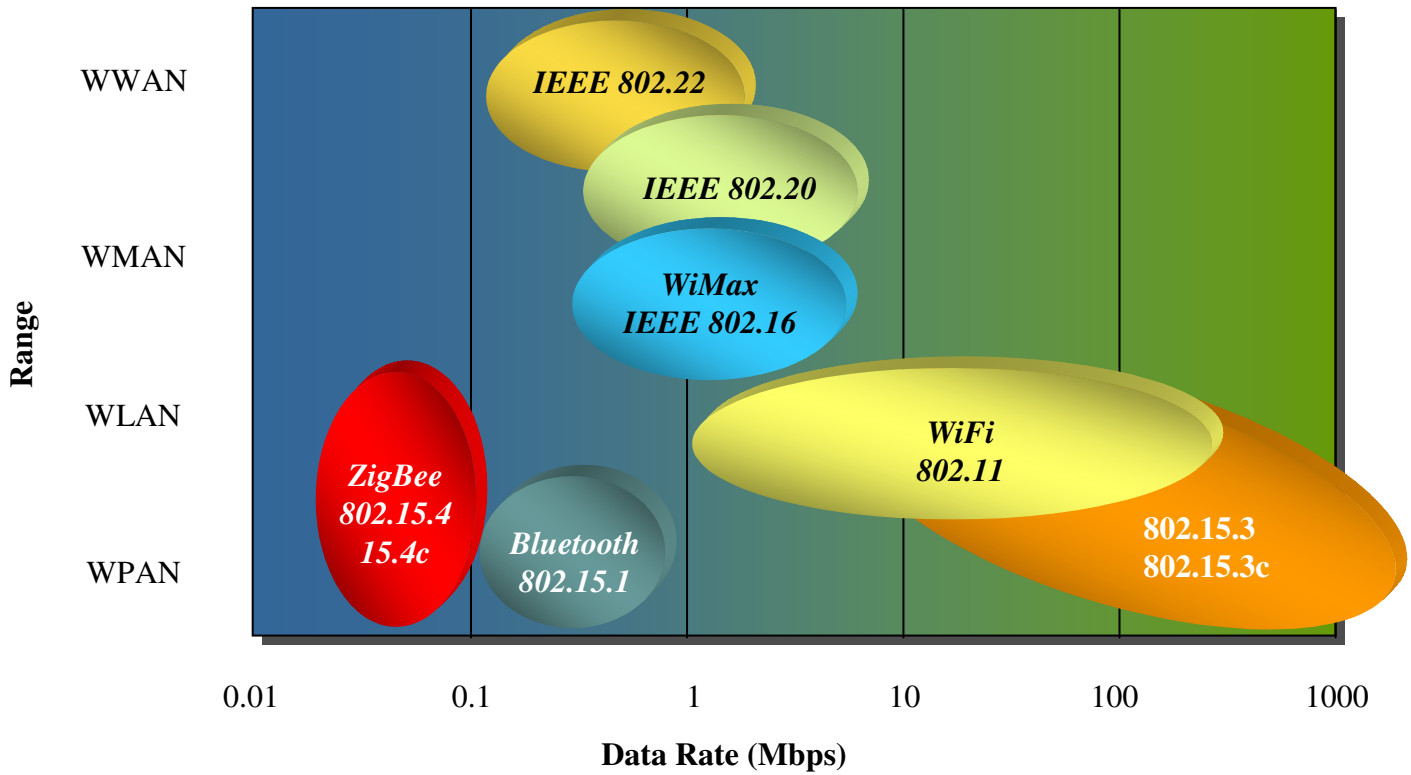
ZigBee

- ZigBee position in wireless standard spectrum

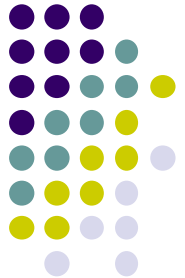


ZigBee

- The IEEE 802 wireless space:
  - ZigBee standard uniquely fills a gap for low data rate applications.

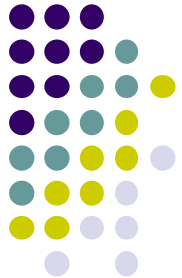


ZigBee



- OUTLINE
  - 1. Why is ZigBee needed?
  - 2. What is ZigBee?
  - 3. What are the ZigBee benefits?
  - 4. How does ZigBee operate?
  - Conclusion

ZigBee



- What is ZigBee?
  - ZigBee is a home-area network designed specifically to replace the proliferation of individual remote controls.
  - ZigBee was created to satisfy the market's need for a:
    - cost-effective,
    - standards-based wireless network that supports:
      - low data rates,
      - low power consumption,
      - security,
      - and reliability.

ZigBee

- ZigBee Alliance

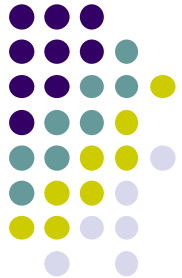
www.zigbee.org

  - To address this new market's need, the ZigBee Alliance, an industry working group, is developing standardized application software on top of the IEEE 802.15.4 wireless standard.
  - The alliance is working closely with the IEEE to ensure an integrated, complete, and interoperable network for the market.
  - The ZigBee Alliance will also serve as the official test and certification group for ZigBee devices.
  - ZigBee is the only standards-based technology that addresses the needs of most remote monitoring and control and sensory network applications.

ZigBee

- ZigBee Alliance
  - ZigBee promoters:

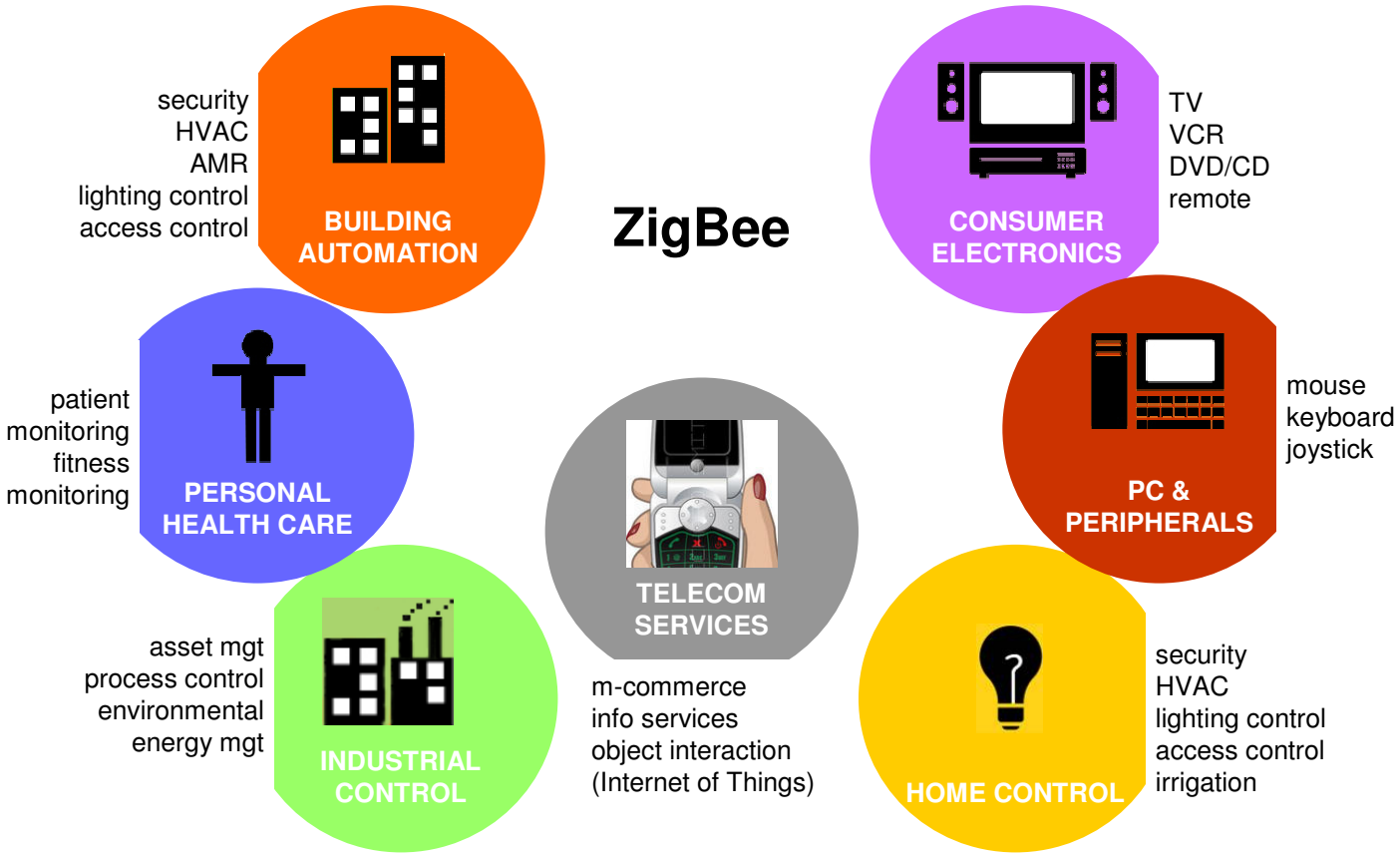
ZigBee



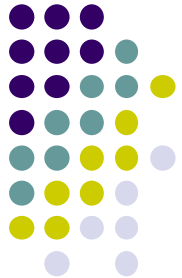
- ZigBee Alliance
  - Focus:
    - Defining the network, security and application software layers,
    - Providing interoperability and conformance testing specifications,
    - Promoting the ZigBee brand globally to build market awareness,
    - Managing the evolution of the technology.
  - The initial markets for the ZigBee Alliance include:
    - Consumer electronics,
    - Energy management and efficiency,
    - Health care,
    - Home automation,
    - Telecommunication services,
    - Building automation,
    - Industrial automation.

ZigBee

- ZigBee applications

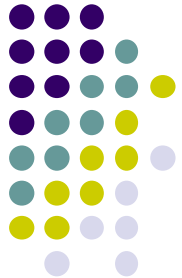


ZigBee



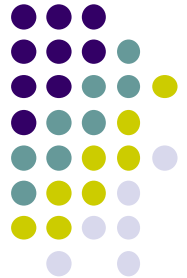
- An example of ZigBee applications: office lighting
  - Several manufacturers have developed inexpensive sensors for fluorescent tubes that let lights be turned on and off by battery-powered wall switches, with no wires between switch and tubes.
  - The light switch is the end device, powered by a button cell battery that will last for years. The switch wakes up and uses battery power only when flipped on or off to transmit the new state to fluorescent tubes' routers. The routers are already connected to the mains and are not concerned with battery conservation. Any one of the fluorescent tubes can contain the coordinator.
  - The implication are enormous for new office construction: no more electrical runs for lighting and the ability to reconfigure lighting controls at almost zero cost.
  - ZigBee extends similar benefits to a wide range of industrial automation and control applications.

ZigBee



- OUTLINE
  - 1. Why is ZigBee needed?
  - 2. What is ZigBee?
  - 3. What are the ZigBee benefits?
  - 4. How does ZigBee operate?
  - Conclusion

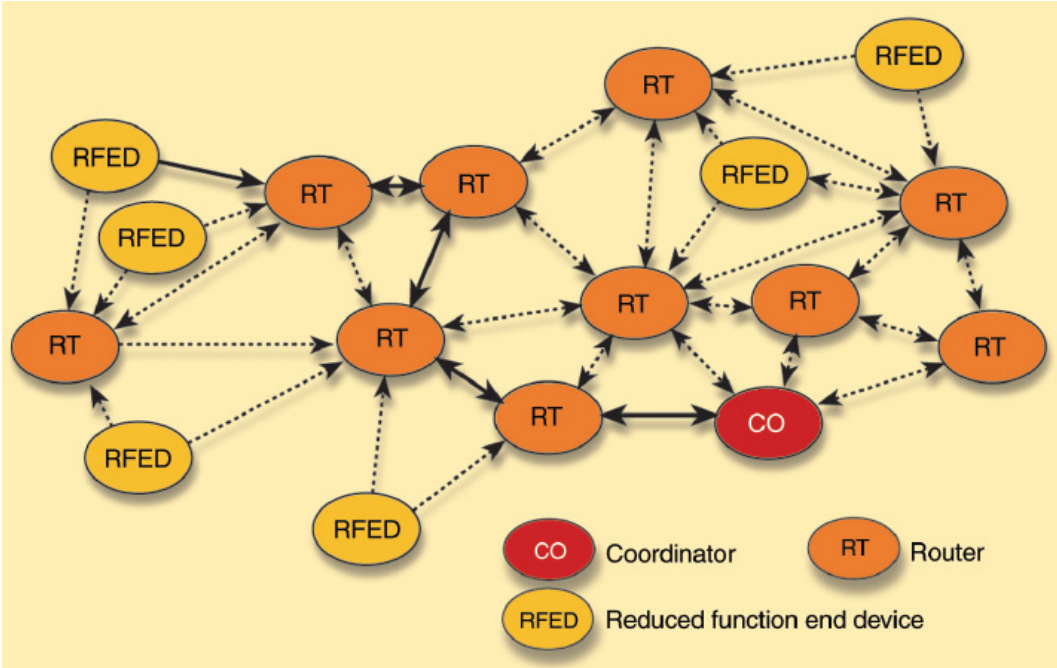
ZigBee



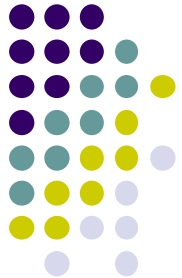
- What are the ZigBee benefits?
  - Low-cost
    - The low prices provide an economic justification for extending wireless networking to even the simplest of devices.
  - Range and obstruction issues avoidance
    - ZigBee routers double as input devices and repeaters to create a form of mesh network.
    - If two network points are unable to communicate as intended, transmission is dynamically routed from the blocked node to a router with a clear path to the data's destination. This happens automatically, so that communications continue even when a link fails unexpectedly.
    - The use of low-cost routers can also extend the network's effective reach. When the distance between the base station and the remote node exceeds the devices' range, an intermediate node or nodes can relay transmission.

ZigBee

- What are the ZigBee benefits?
  - Heavy lines show a signal that begins at a end device and passes through multiple routers to reach a coordinator: Lighter lines show possible alternative signal path.

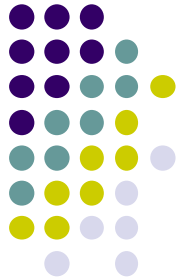


ZigBee



- What are the ZigBee benefits?
  - Multisource products
    - As an open standard, ZigBee provides customers with the ability to choose vendors as needed.
    - ZigBee Alliance working groups define interoperability profiles. A ZigBee-certified radio will interoperate with any other ZigBee-certified radio adhering to the same profile.
    - This promotes compatibility and competition between manufacturers.
  - Low power consumption
    - Basic ZigBee radios operate at 1 mW RF power and can sleep when not involved in transmission.
    - This makes battery-powered radios more practical than ever, and promotes the development of wireless devices.

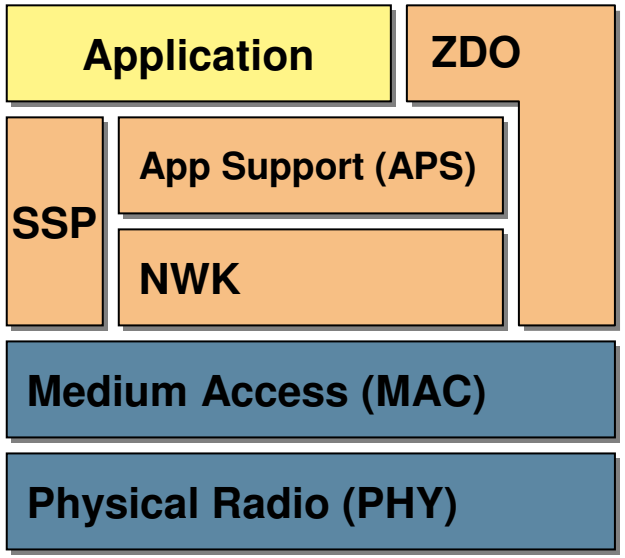
ZigBee



- OUTLINE
  - 1. Why is ZigBee needed?
  - 2. What is ZigBee?
  - 3. What are the ZigBee benefits?
  - 4. How does ZigBee operate?
  - Conclusion

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.

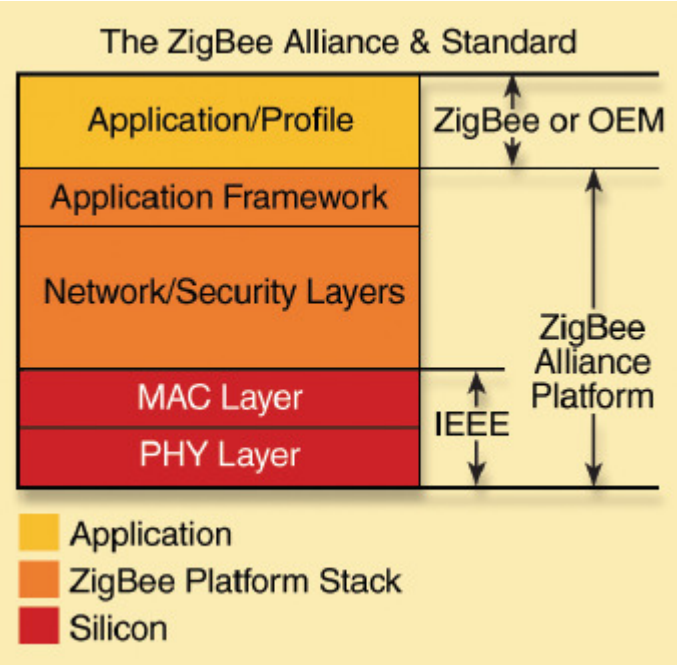


ZDO: ZigBee Device Object
SSP: Security Service Provider
APS: Application Support sub-layer
NWK: Network layer

IEEE 802.15.4 standard

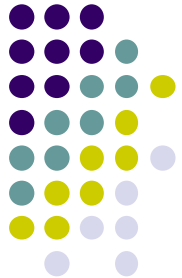
ZigBee

- 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

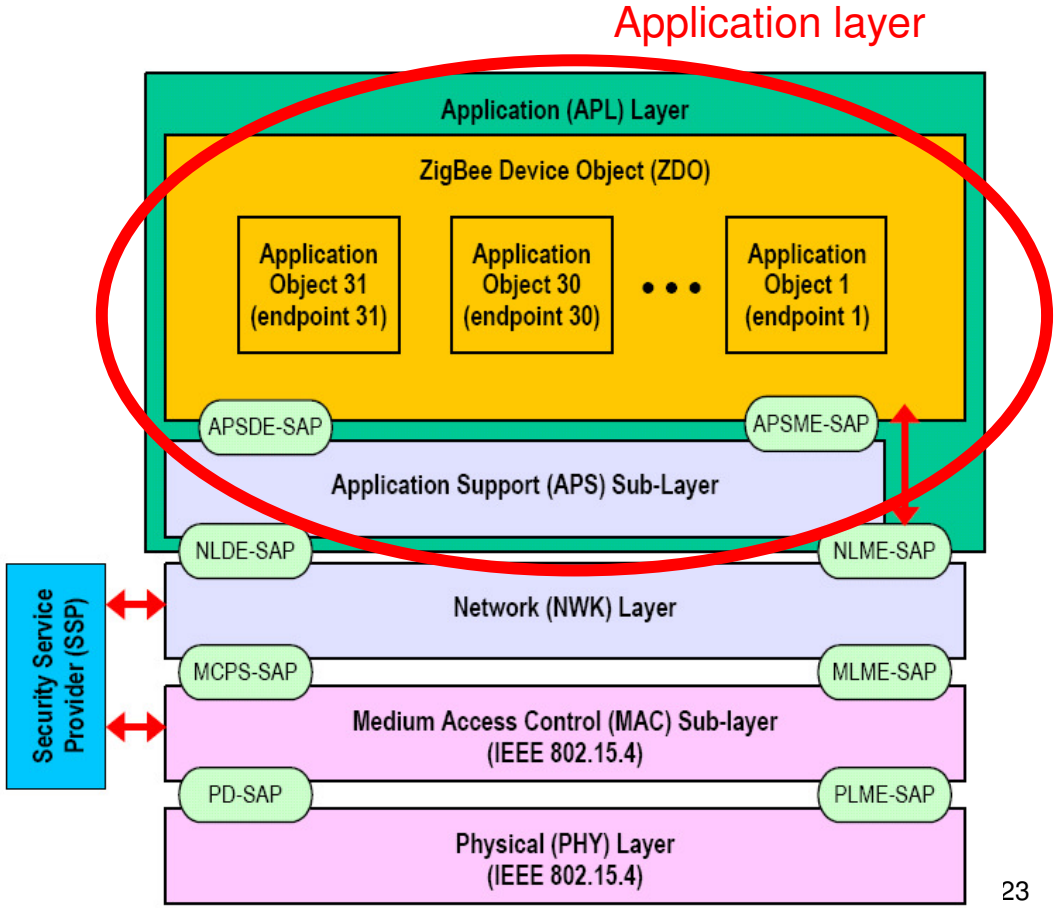
ZigBee



- 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.

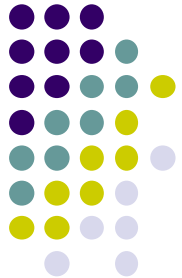
ZigBee

- 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.



A more detailed ZigBee architecture

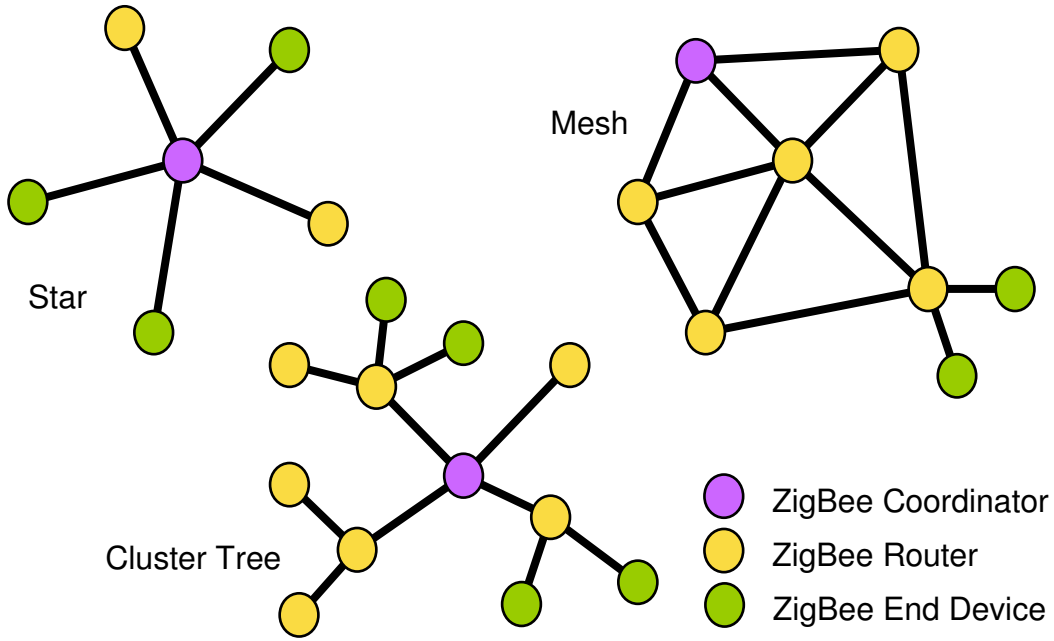
ZigBee



- 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.

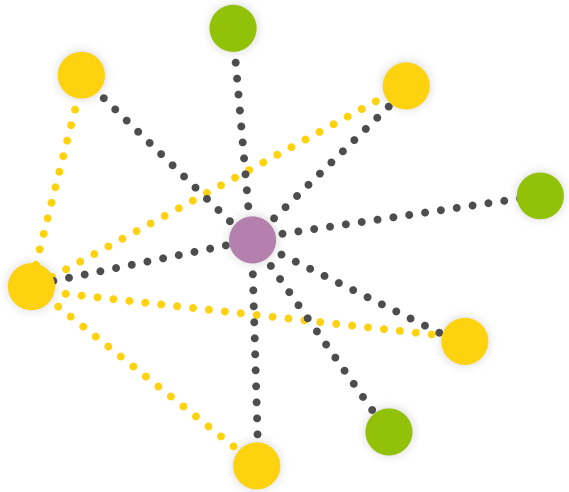
ZigBee

- 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



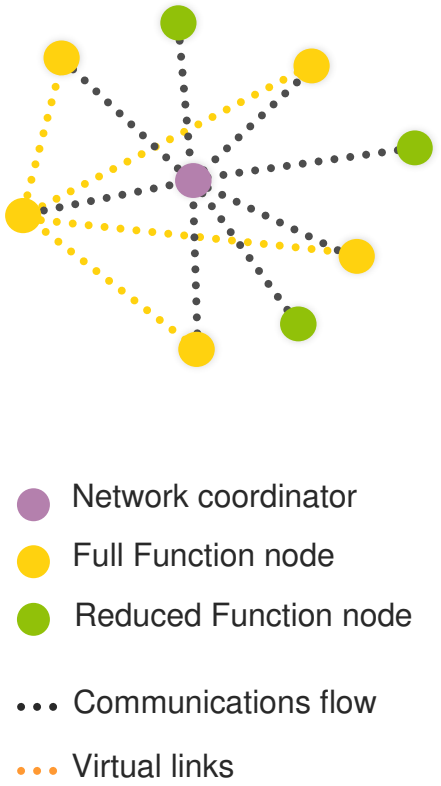
ZigBee

- 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.

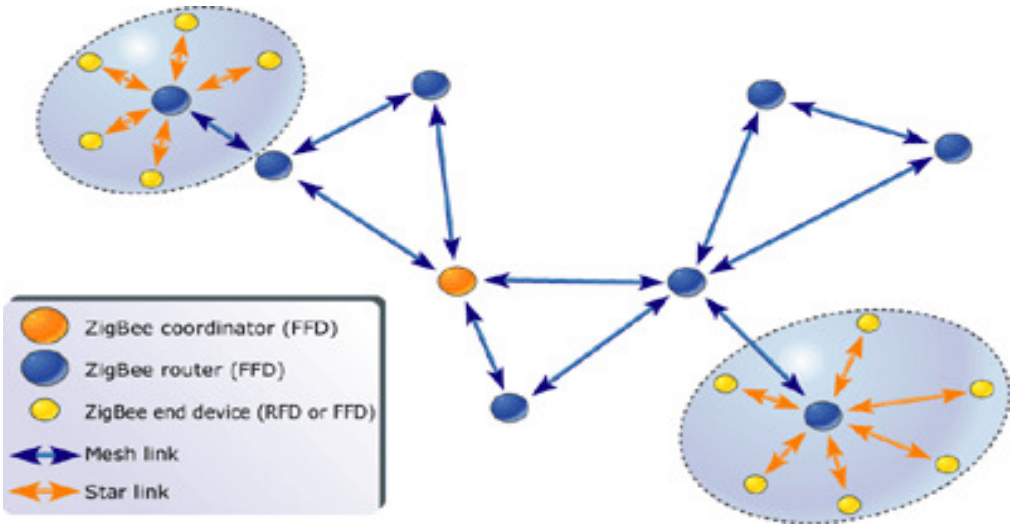
Full function device: A full function device supports all 802.15.4 functions and features specified by the standard. It can operate as a network coordinator. Additional memory and computing power make it ideal for network router functions.

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).



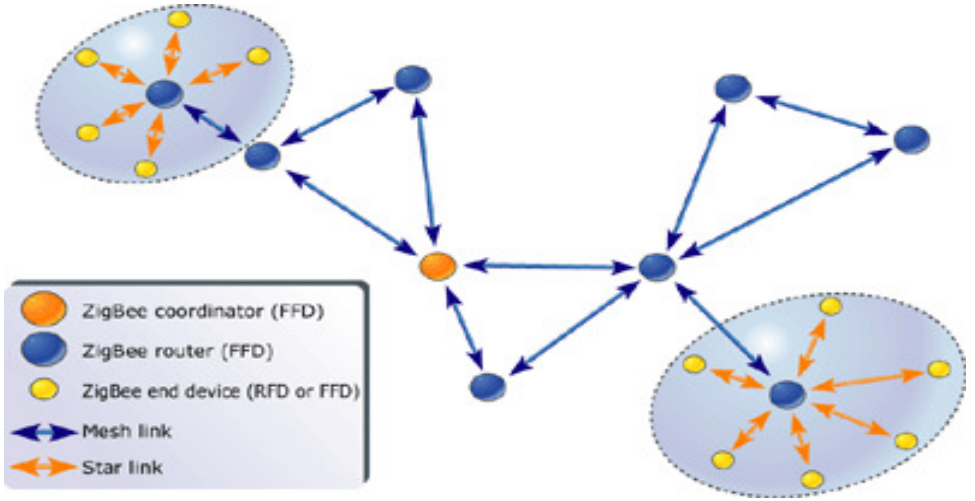
ZigBee

- 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.

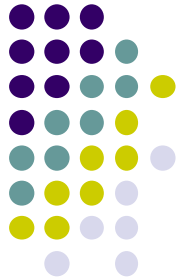


ZigBee

- 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.

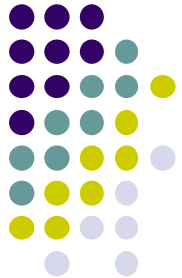


ZigBee



- 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.

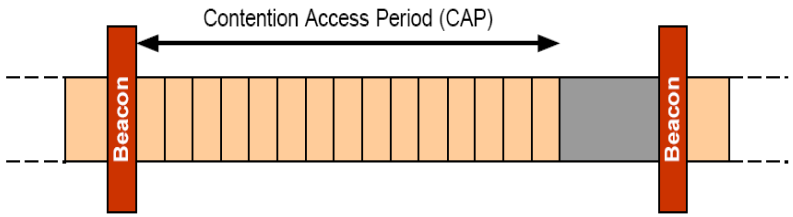
ZigBee



- 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

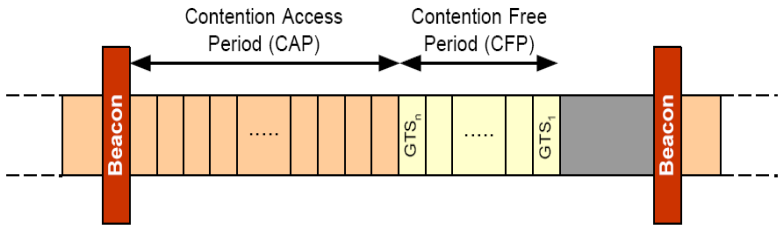
- Power and Beacons
  - Beacon or non-beacon?
    - ZigBee networks can use beacon or non-beacon environments.
    - Beacons are used to synchronize the network devices, identify the HAN, and describe the structure of the superframe.
    - The beacon intervals are set by the network coordinator and vary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



Superframe structure

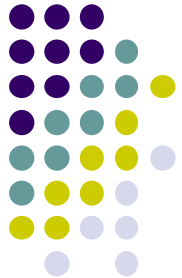
ZigBee

- 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.



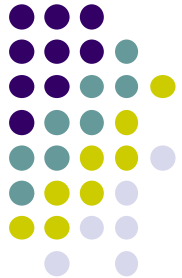
Superframe structure with GTS

ZigBee



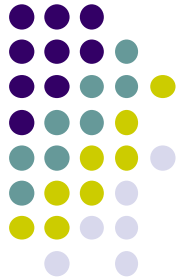
- Power and Beacons
  - Beacon or non-beacon?
    - *Beacon mode* is a mechanism for controlling power consumption in extended networks such as cluster tree or mesh.
    - It enables all the clients to know when to communicate with each other. Here, the two-way radio network has a central dispatcher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

ZigBee



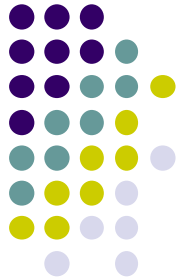
- Power and Beacons
  - Beacon or non-beacon?
    - Beacon mode is more suitable when the network coordinator is battery-operated.
    - Client units listen for the network coordinator's beacon (broadcast at intervals between 0.015 and 252s).
    - A client registers with the coordinator and looks for 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



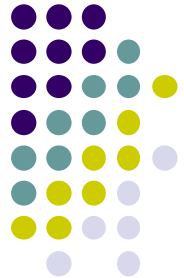
- Power and Beacons
  - Beacon or non-beacon?
    - The *non-beacon mode* is a simple, traditional multiple-access system used in simple peer and near-peer networks.
    - It operates like a two-way radio network, where each client is autonomous and can initiate a conversation at will, but could interfere 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.

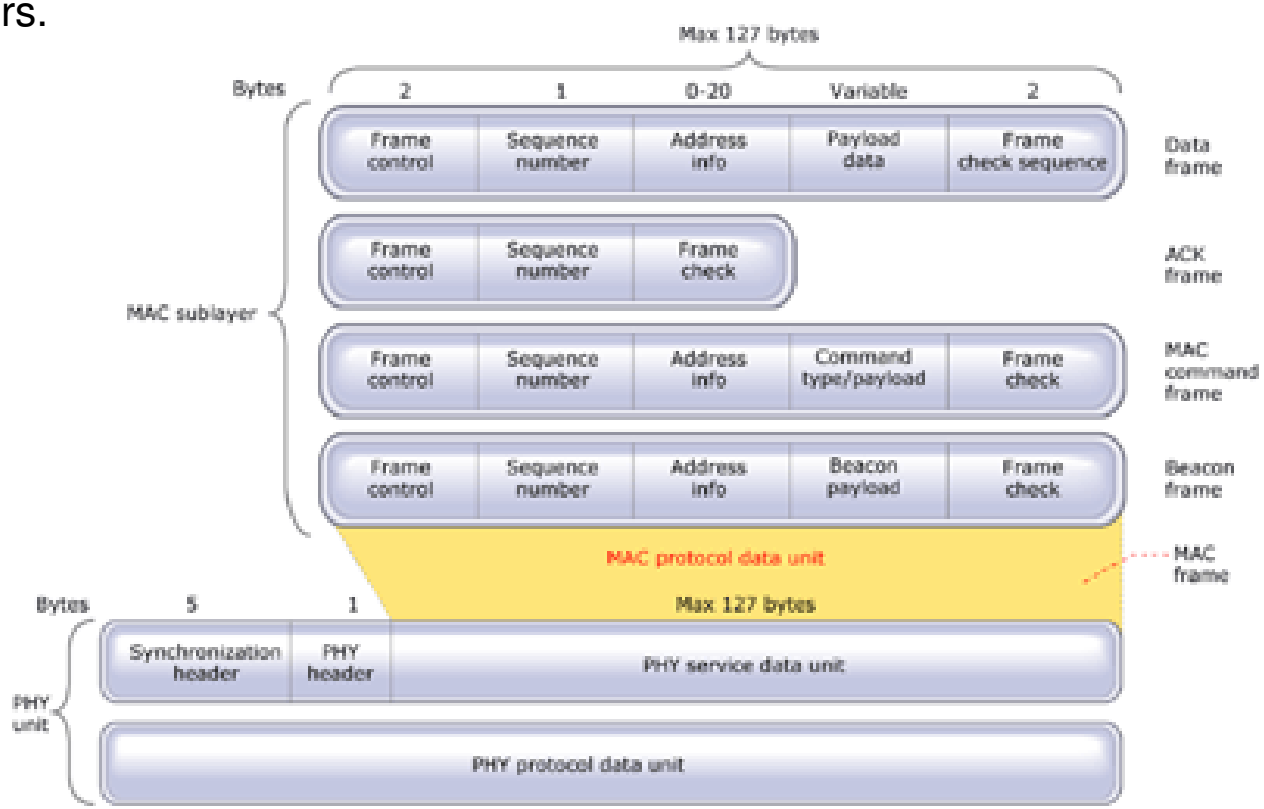
ZigBee



- 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.

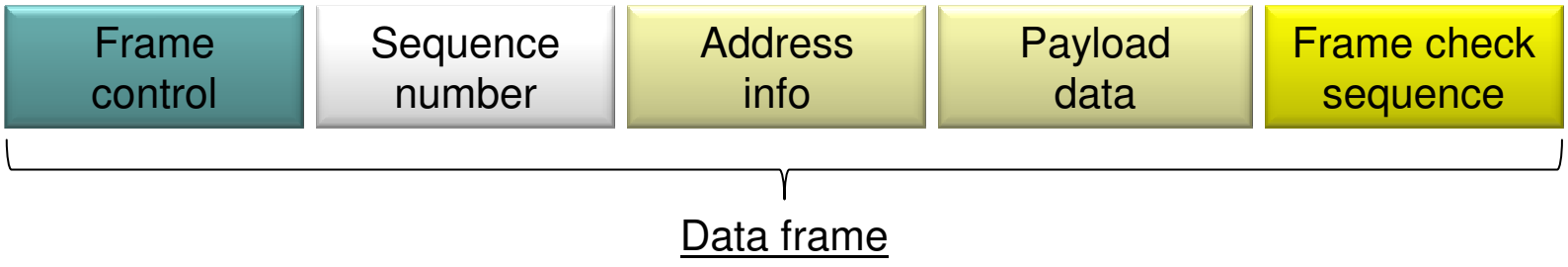
ZigBee

- Frame structure
  - Each successive protocol layer adds to the structure with layer-specific headers and footers.



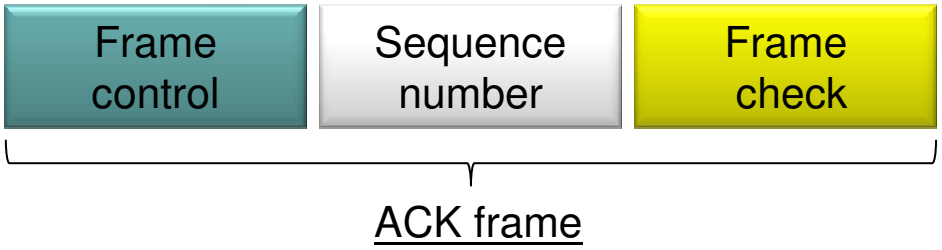
ZigBee

- Frame structure
  - Data frame
    - The *data frame* provides a payload of up to 104 bytes.
    - The frame is numbered to ensure that all packets are tracked.
    - A frame-check sequence ensures that packets are received without error.
    - This frame structure improves reliability in difficult conditions.



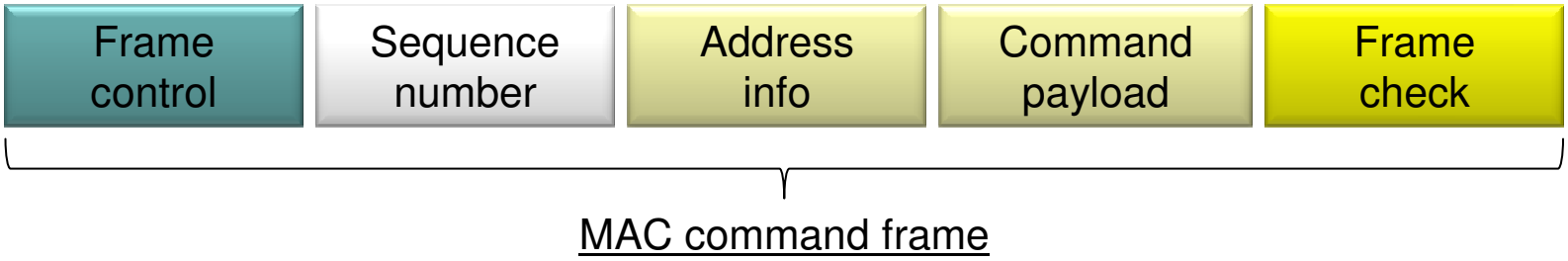
ZigBee

- Frame structure
  - ACK frame
    - Another important structure for 802.15.4 is the *acknowledgment (ACK) frame*.
    - It provides feedback from the receiver to the sender confirming that the packet was received without error.
    - The device takes advantage of specified "quiet time" between frames to send a short packet immediately after the data-packet transmission.



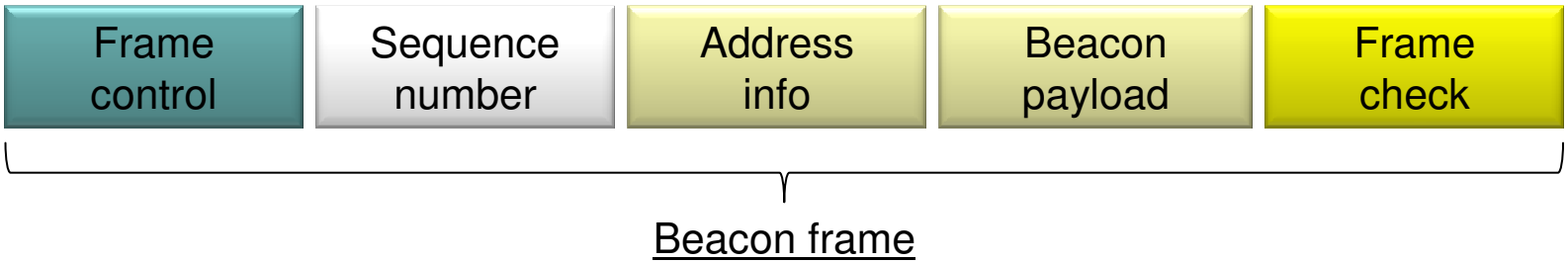
ZigBee

- Frame structure
  - MAC command frame
    - A *MAC command frame* provides the mechanism for remote control and configuration of client nodes.
    - A centralized network manager uses MAC to configure individual clients' command frames no matter how large the network.

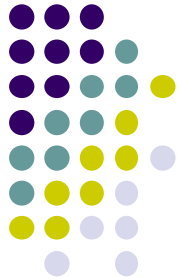


ZigBee

- Frame structure
  - Beacon frame
    - Finally, the *beacon frame* wakes up client devices, which listen for their address and go back to sleep if they don't receive it.
    - Beacons are important for mesh and cluster-tree networks to keep all the nodes synchronized without requiring those nodes to consume precious battery energy by listening for long periods of time.



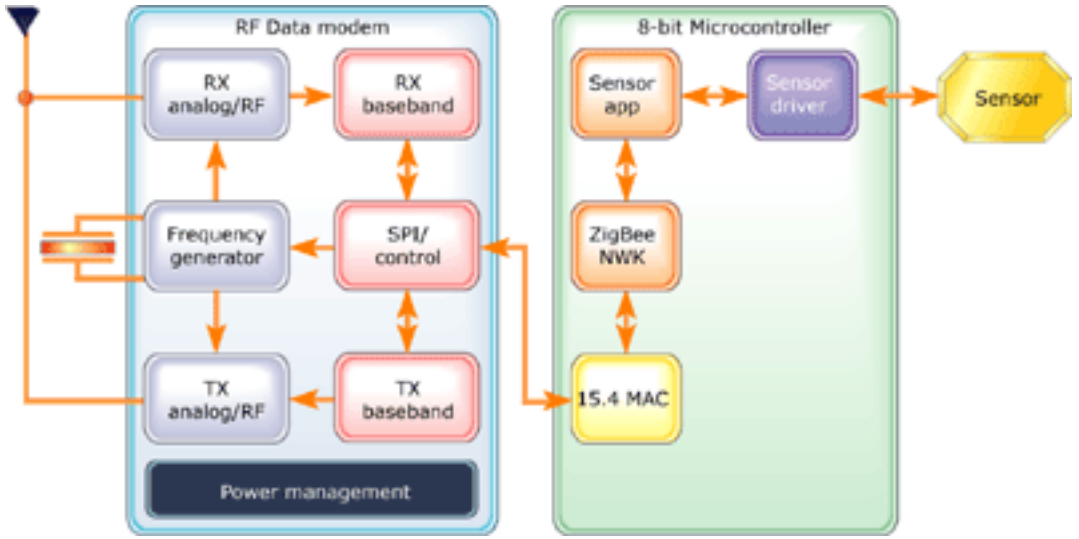
ZigBee



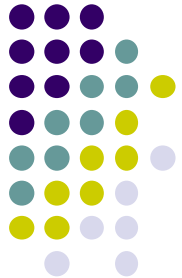
- ZigBee stack
  - The ZigBee stack is small in comparison to other wireless standards.
  - For network-edge devices with limited capabilities, the stack requires about 4Kb of the memory. Full implementation of the protocol stack takes less than 32Kb of memory. The network coordinator may require extra 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



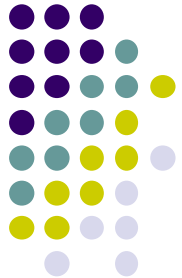
- Channel access
  - Two channel-access mechanisms are implemented in 802.15.4 standard:
    - For a non-beacon network, a standard ALOHA CSMA-CA (carrier-sense medium-access with collision avoidance) communicates with positive acknowledgement for successfully received packets.
    - In a beacon-enabled 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

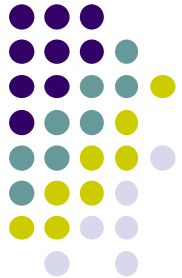
ZigBee



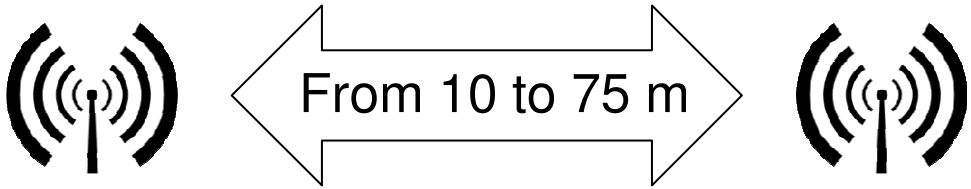
- RF transmission characteristics
  - Data rate:
    - Data throughput rates of :
      - 250 kbps can be achieved at 2.4 GHz (16 channels),
      - 40 kbps at 915 MHz (10 channels),
      - 20 kbps at 868 MHz (1 channel).

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

ZigBee



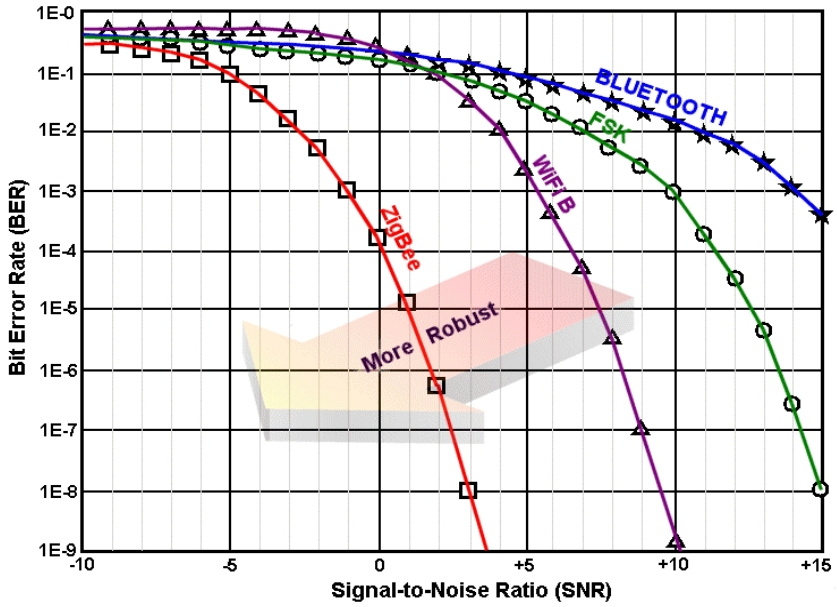
- RF transmission characteristics
  - Transmission distance:
    - The transmission distance is expected to range from 10 to 75 m, depending on power output and environmental characteristics.



  - Modulation and channel:
    - Like Wi-Fi, ZigBee uses direct-sequence spread spectrum in the 2.4 GHz band, with offset-quadrature phase-shift keying modulation.
    - Channel width is 2 MHz width, with 5 MHz channel spacing.
    - The 868 and 900 MHz bands also use direct-sequence spread spectrum but with binary-phase-shift keying modulation.

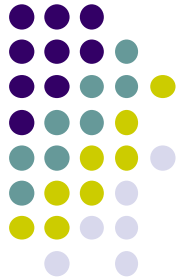
ZigBee

- RF transmission characteristics
  - Robustness:
    - ZigBee technology relies upon IEEE 802.15.4, which has excellent performance in low SNR environments.



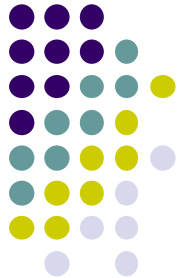
Reliable operation:
WHY?

ZigBee



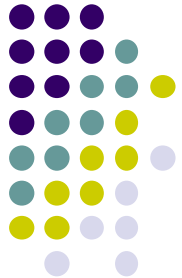
- Reliable operation
  - ZigBee employs a range of techniques to ensure reliable communications, that is to ensure communications reach their destinations uncorrupted. Corruption could result, for example, from radio interference or poor transmission/reception conditions.
    - Channel selection:
      - When a ZigBee network is initialized, the channels of the chosen RF band are assessed for activity. The result can be used to automatically select a quiet channel for the network to operate in.
    - Listen before sending:
      - To avoid conflicting transmissions (more than one device transmitting in the same frequency channel at the time), before beginning a transmission, a node will listen on the relevant channel to check whether it is clear. It will only transmit if no activity is detected on the channel, otherwise the node waits for a random period of time before re-trying.

ZigBee



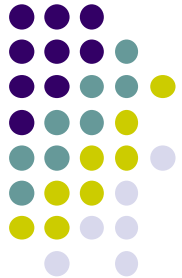
- Reliable operation
  - Data coding:
    - ZigBee networks apply a coding mechanism to radio transmissions. Due to this coding, there is a higher probability that a message will get through to its destination intact, even if there are conflicting transmissions.
  - Acknowledgements:
    - A system of message ACK is available in ZigBee to confirm that messages reach their destinations. If the sending device does not receive an ACK within a certain time interval, it resends the original message.
  - Route discovery:
    - In a mesh topology, if the default route to the destination node is down, due to failed intermediate node or link, the network can “discover” and use alternative routes for message delivery.

ZigBee



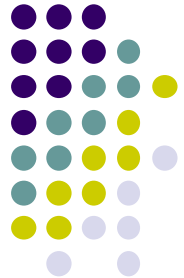
- Co-existence and interoperability
  - Any device designed for use in a ZigBee network must comply with the ZigBee standard.
  - Two levels of compliance:
    - Co-existence:
      - The ability of a device to exist in the same network as other devices without preventing them from working.
    - Interoperability:
      - The ability of a device to operate in conjunction with other devices, that is to communicate and function with them.

ZigBee



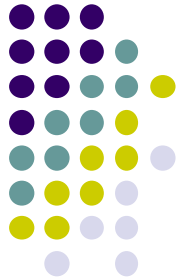
- Security
  - Security and data integrity are key benefits of the ZigBee technology. ZigBee leverages the security model of the IEEE 802.15.4 MAC sublayer which specifies four security services:
    - access control: the device maintains a list of trusted devices within the network,
    - data encryption, which uses symmetric key 128-bit advanced encryption standard,
    - frame integrity to protect data from being modified by parties without cryptographic keys,
    - sequential freshness to reject data frames that have been replayed: the network controller compares the freshness value with the last known value from the device and rejects it if the freshness value has not been updated to a new value.
  - The security implementation is specified by the implementer using a standardized toolbox of ZigBee security software.

ZigBee



- OUTLINE
  - 1. Why is ZigBee needed?
  - 2. What is ZigBee?
  - 3. What are the ZigBee benefits?
  - 4. How does ZigBee operate?
  - Conclusion

ZigBee

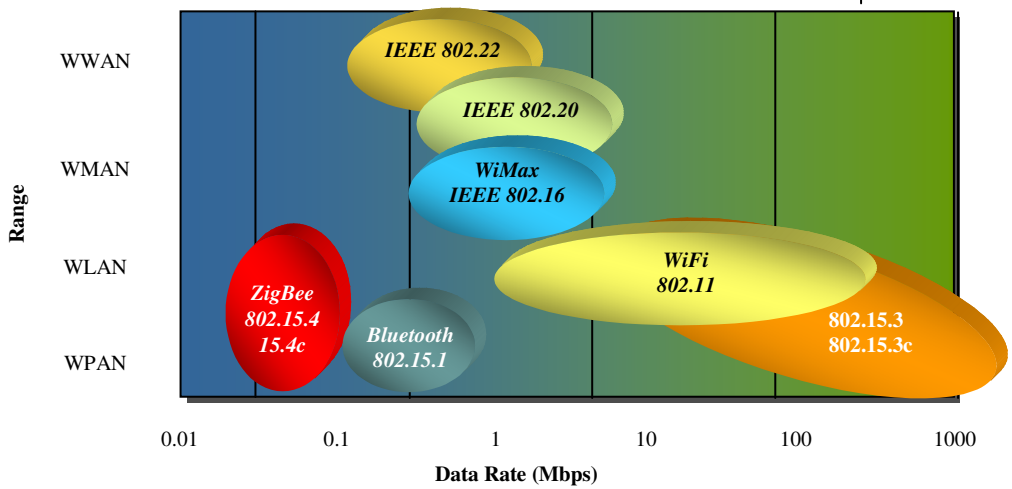


- Conclusion
  - Sensor/Control Network Requirements:
    - Networks form by themselves, scale to large sizes and operate for years without manual intervention
    - Extremely long battery life
      - Low infrastructure cost (low device & setup costs)
      - Low complexity and small size
    - Low device data rate and QoS
    - Standardized protocols allow multiple vendors to interoperate

ZigBee

- Conclusion
  - ZigBee Alliance

ZigBee™ Alliance

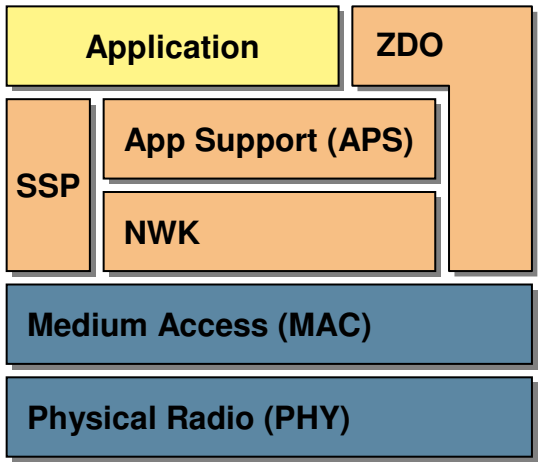


  - To address this new market's need, the ZigBee Alliance, an industry working group, is developing standardized application software on top of the IEEE 802.15.4 wireless standard.

  - Focus:
    - Defining the network, security and application software layers,
    - Providing interoperability and conformance testing specifications,
    - Promoting the ZigBee brand globally to build market awareness,
    - Managing the evolution of the technology.

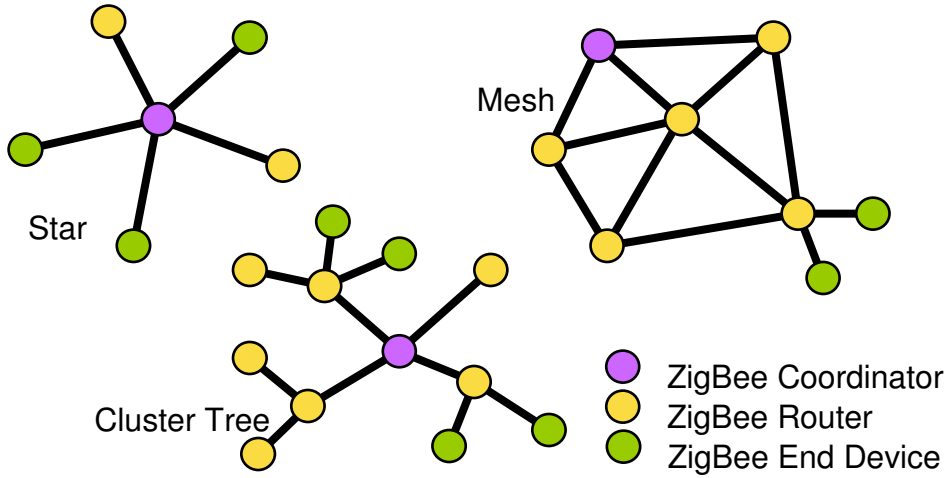
ZigBee

- Conclusion
  - Basic network characteristics:
    - Optimized for timing-critical applications and power management.
    - Optimized for low duty-cycle applications (< 0.1 %).
  - Architecture:



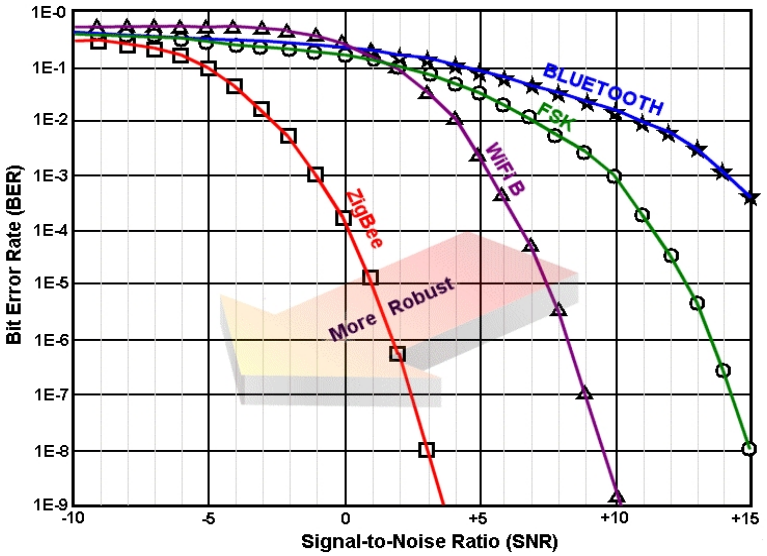
ZigBee

- Conclusion
  - Basic network characteristics:
    - 3 network topologies: star, mesh, cluster tree topology
    - 3 device types: network coordinator, router, end device
    - Beacon and non-beacon networks



ZigBee

- Conclusion
  - RF transmission:
    - ISM band
    - PHY and MAC layer defined by IEEE 802.15.4 standard

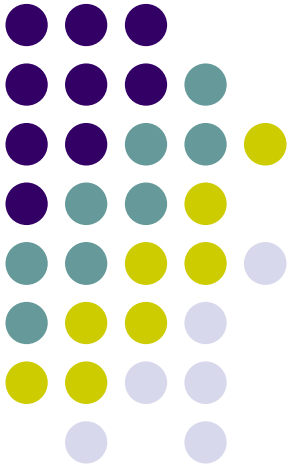


Frequency Band	License Required?	Geographic Region	Data Rate	Channel Number(s)
868.3 MHz	No	Europe	20kbps	0
902-928 MHz	No	Americas	40kbps	1-10
2405-2480 MHz	No	Worldwide	250kbps	11-26

ZigBee

Evangéline BENEVENT

Università Mediterranea di Reggio Calabria
DIMET



Thank you for your attention