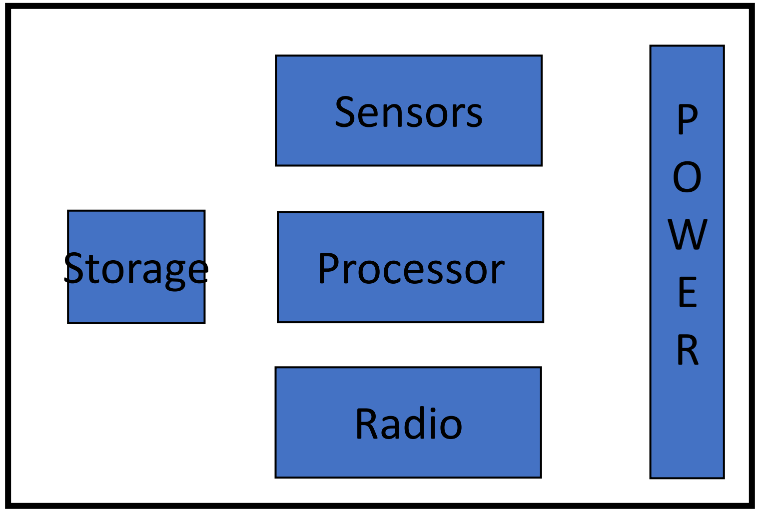
What are wireless sensor networks (WSNs)?

- A wireless sensor network (WSN) is a wireless network using sensors to cooperatively monitor physical or environmental conditions
- Networks of typically small, battery-powered, wireless devices (often MANY, sometimes heterogeneous)
  - On-board processing,
  - Communication, and
  - Sensing capabilities.

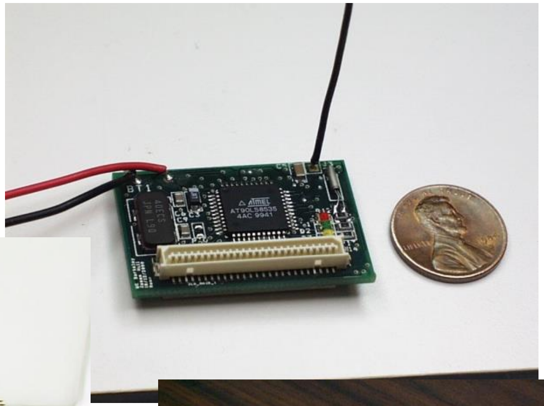
Or…

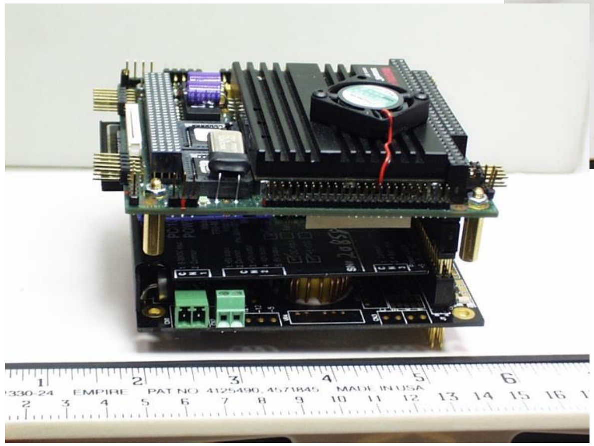
➢ Wireless sensing + Data Networking!
  ➢ Group of sensors linked by wireless media to perform distributed sensing tasks

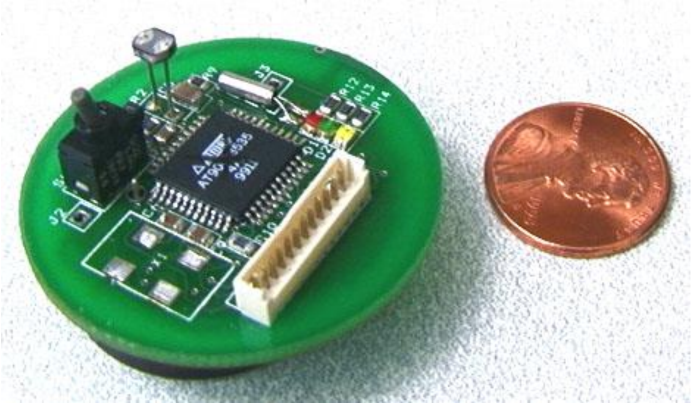


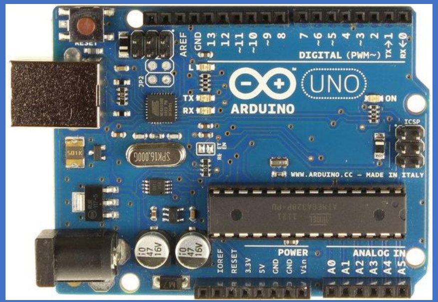
WSN device schematics

Sensor Nodes and platforms



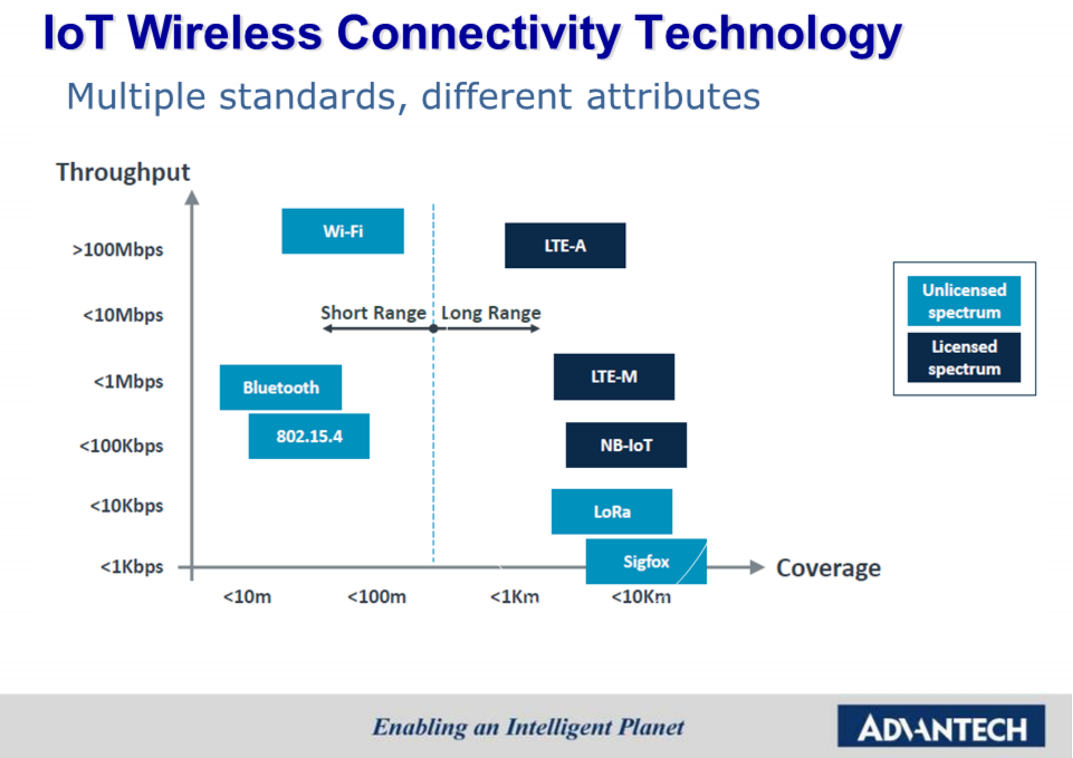






IoT Wireless Connectivity

As with wireless in general, multiple standards with different properties

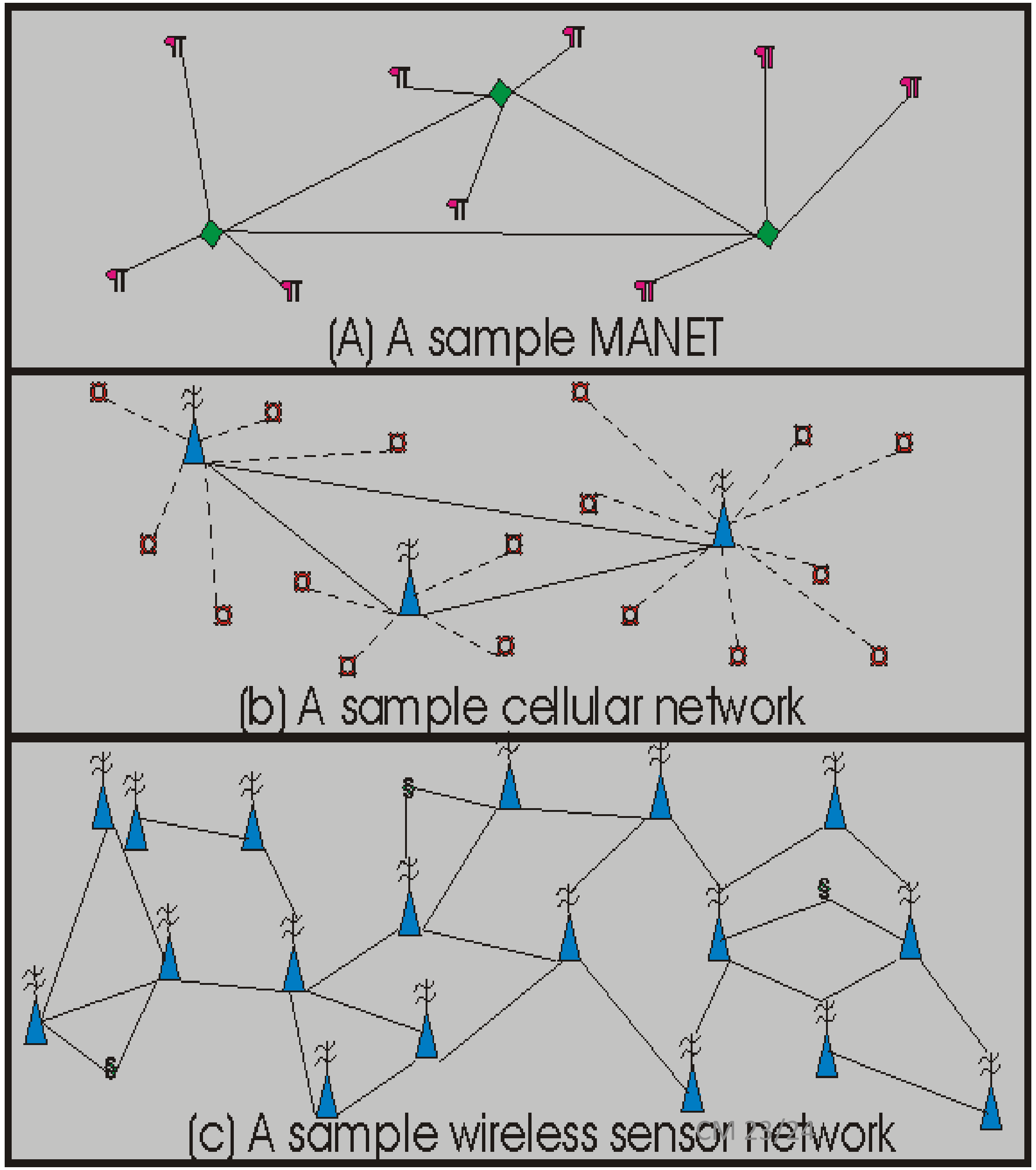


MIoT and HIoT are different

- IoT has multiple scenarios, from human-oriented to machine-oriented, and from industrial to forest environments
- WSN need to adapt to these environments.

	Manufacturing IoT	Consumer IoT
Goal	Manufacturing-industry Centric	Consumer Centric
Devices	Machines, Sensors, Controllers, Actuators, Smart meters	Consumer devices and Smart appliances
Working Environment	Harsh (vibration, noisy, extremely high/low temperature)	Moderate
Data rate	High (usually)	Low or average
Delay	Delay sensitive	Delay tolerant
Mission	Mission-critical	Non-mission-critical

Types of wireless Networks

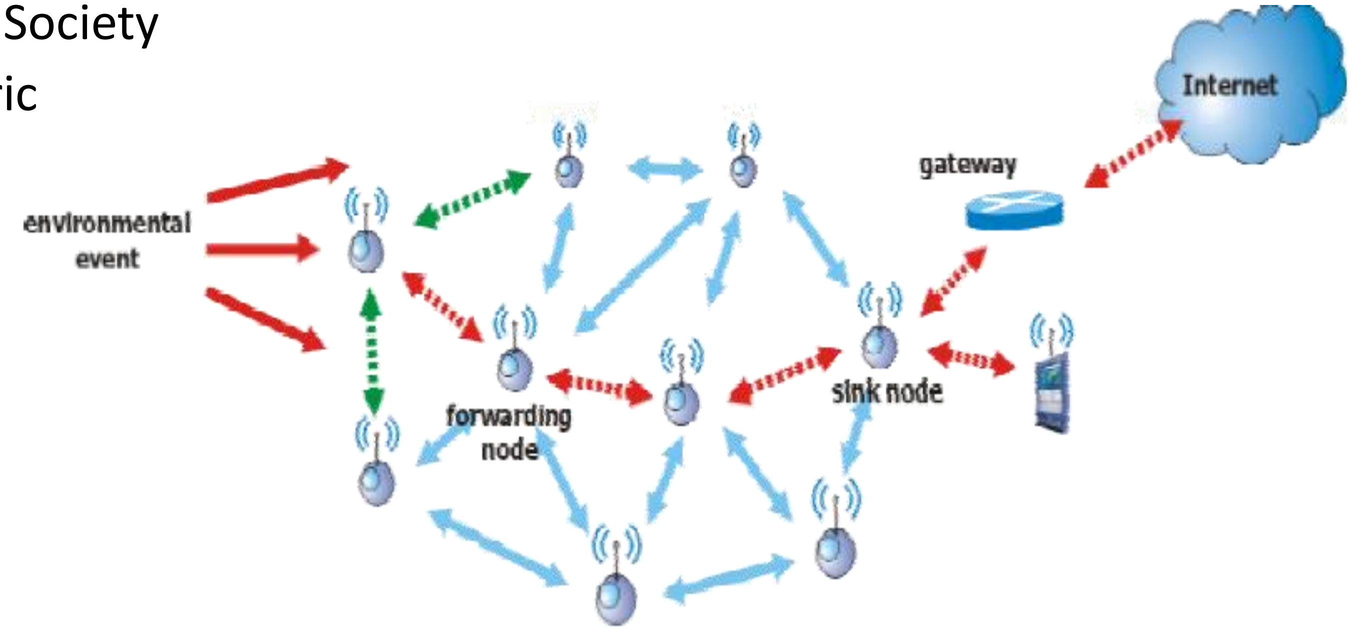


MANET – Mobile Ad-hoc network

WSN can explore the **architecture and protocol** concepts both of MANETs (mobile ad-hoc networks) and of celular networks.

Wireless Sensor Network

- Focus on:
  - Ubiquitous Computing
  - Ubiquitous Network Society
  - (often) Human-centric
- Ubiquitous
  - Anytime
  - Anyone
  - Anywhere
  - Any Device
  - Affordable
  - All Security
  - Any Information/Service



MAC: challenges for wireless networking

- MAC is a critical layer for networking
- Traditional problems
  - Fairness
  - Latency
  - Throughput
- For Sensor Networks, more problems are added
  - Power efficiency
  - Scalability

MAC challenges for WSN

- Sensor networks are deployed in an ad hoc fashion, with individual nodes remaining largely **inactive for long periods of time**, but then becoming **suddenly active** when something is detected.
- These characteristics of sensor networks and applications motivate a MAC that is different from traditional wireless MACs :
  - **Energy conservation** and **self-configuration** are primary goals.
  - Per-node fairness and latency are less important.

Challenges in WSN’s

- Energy and Power Consumption
- Self-organization
- Communication Heterogeneity
- Adaptability
- Security
- Scalability

Design Challenges

Why are WSNs challenging/unique?

- Typically, severely energy constrained.
  - Limited energy sources (e.g., batteries).
  - Trade-off between performance and lifetime.
- Self-organizing and self-healing.
  - Remote deployments.
- Scalable.
  - Arbitrarily large number of nodes.

Design Challenges

- Heterogeneity.
  - Devices with varied capabilities.
  - Different sensors.
  - Hierarchical deployments.
- Adaptability.
  - Adjust to operating conditions and changes in application requirements.
- Security and privacy.
  - Potentially sensitive information.
  - Hostile environments.

Sensor Network MAC Protocols

- The major sources of energy wastage are:
  - Collisions – *interfering packets*
  - Overhearing – *hearing more than required from a packet*
  - Control packet overhead – *control versus data*
  - Idle listening – *hearing for nothing*

Typical solutions in wireless MACs

- Carrier Sensing
  - Only during low traffic load.
- Contention
  - RTS-CTS only during high traffic load.
- Backoff
  - Backoff in application layer is desired other than in MAC layer.

Achieving good scalability and collision avoidance capability is necessary.

Challenges

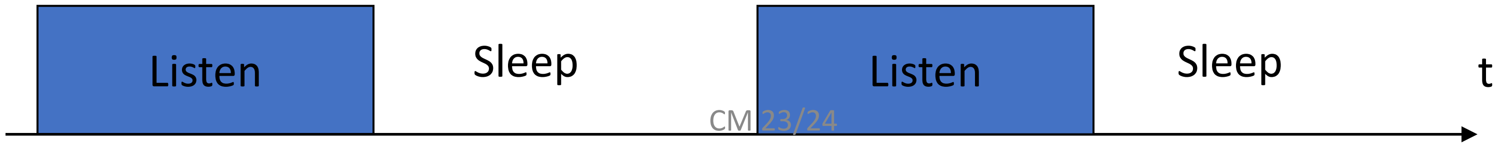
1. Energy Efficiency:
   - Sensor nodes are not connected to any energy source.
   - Energy efficiency is a dominant consideration no matter what the problem is.
   - Many solutions, both hardware and software related, have been proposed to optimize energy usage.
2. Ad hoc deployment (adaptability):
   - Most sensor nodes are deployed in regions which have no infrastructure.
   - We must cope with the changes of connectivity and distribution.

Challenges

3. Unattended operation:
    - Generally, once sensors are deployed, there is no human intervention for a long time.
    - Sensor network must reconfigure by itself when certain errors occur.
4. Dynamic changes (self-healing and scalability)
    - As changes of connectivity due to addition of more nodes or failure of nodes, Sensor network must be able to adapt itself to changing connectivity, to arbitrary large numbers of nodes
5. Security
    - Both Sensors and Actuators carry sensitive information in an hostile environment

Sensor-MAC (S-MAC)

- S-MAC is a medium-access control (MAC) protocol designed for wireless sensor networks.
  - Explores typical solutions also found in many other sensor MACs.
  - **Nodes periodically sleep, and sleep during other nodes' transmissions**
    - Nearby nodes form virtual clusters to synchronize their wake-up and sleep periods
  - Trades **energy efficiency for lower throughput and higher latency**
    - Message passing is used to reduce the contention latency and control overhead



802.15.4 and Zigbee

What is ZigBee?

- Technological Standard Created for Control and Sensor Networks
  - Based on the IEEE 802.15.4 Standard
  - Centered in small radios
- Created by the ZigBee Alliance
  - 200+ members
- History
  - *May 2003: IEEE 802.15.4 completed*
  - December 2004: ZigBee specification ratified
  - June 2005: public availability

What Does ZigBee Do?

- Designed for wireless controls and sensors
  - Operates in Personal Area Networks (PAN's) and device-to-device networks
  - Connectivity between small packet devices
  - Examples: control of lights, switches, thermostats, appliances, etc.

Zigbee?

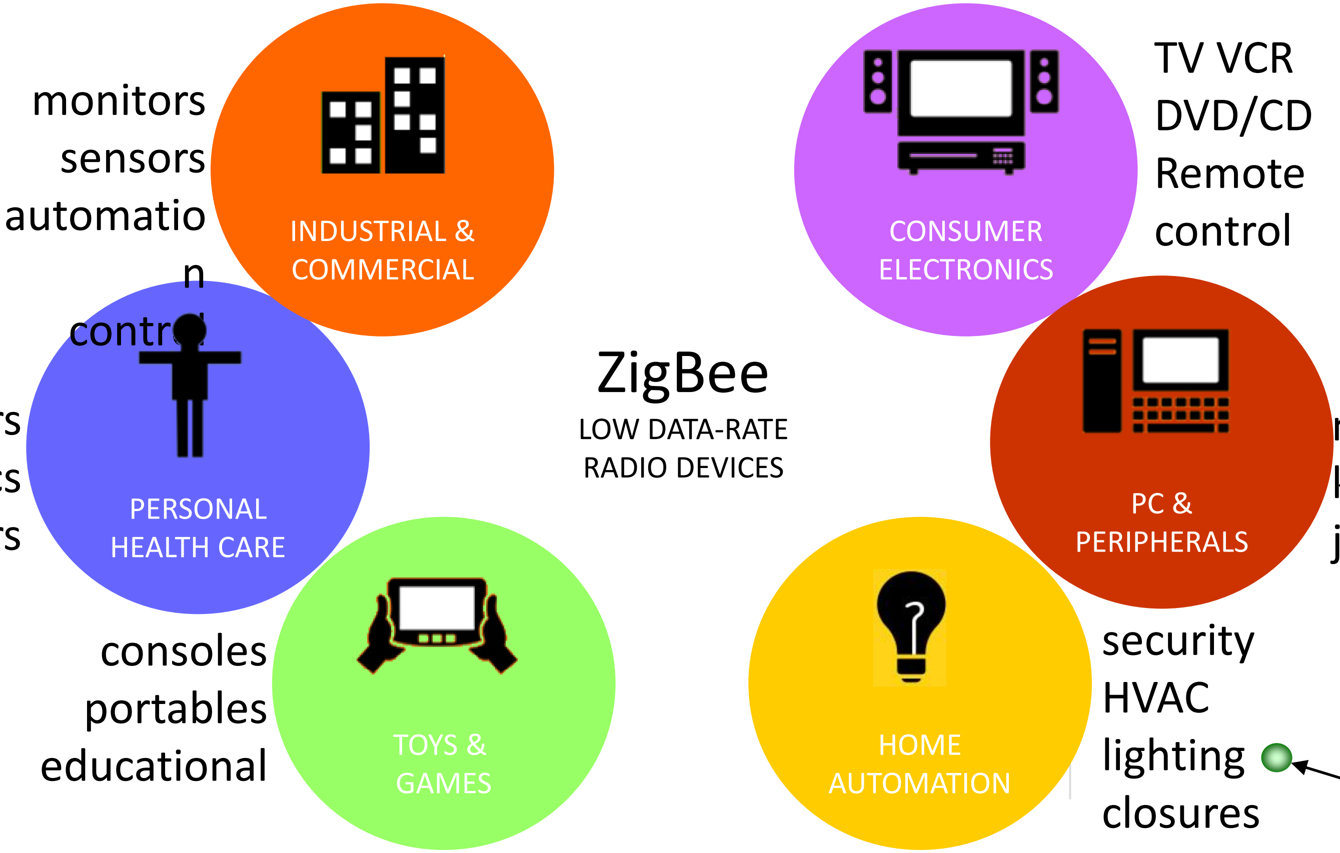
  - Named for erratic, zig-zagging patterns of bees between flowers
  - Symbolizes communication between nodes in a mesh network
  - Network components "seen as analogous" to queen bee, drones, worker bees

ZigBee network applications

monitors
sensors
automatio
n
control

monitors
diagnostics
sensors

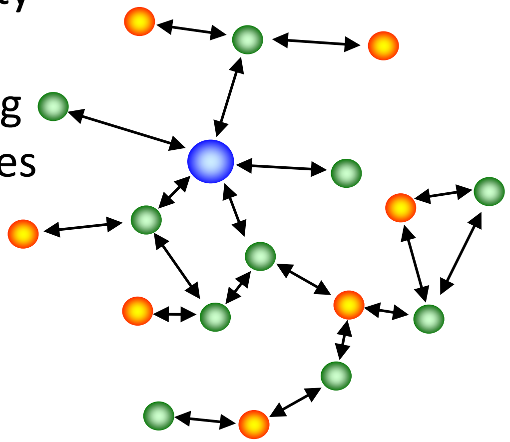
consoles
portables
educational



TV VCR
DVD/CD
Remote
control

mouse
keyboard
joystick

security
HVAC
lighting
closures



- Just everything you can imagine for wireless sensor nodes or in general short range communications

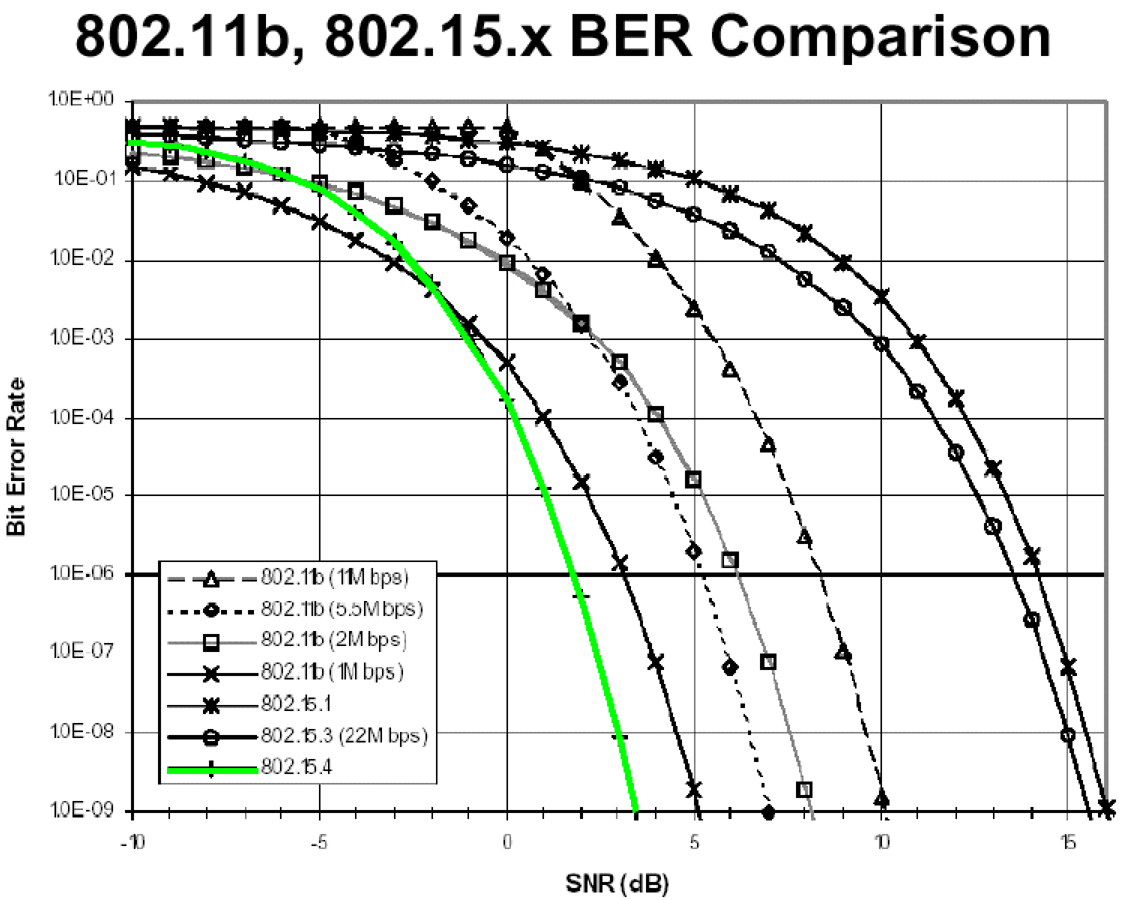
ZigBee and Other Wireless Technologies

Market Name Standard	ZigBee™ 802.15.4	--- GSM/GPRS CDMA/1xRTT	Wi-Fi™ 802.11b	Bluetooth™ 802.15.1
Application Focus	Monitoring & Control	Wide Area Voice & Data	Web, Email, Video	Cable Replacement
System Resources	4KB - 32KB	16MB+	1MB+	250KB+
Battery Life (days)	100 - 1,000+	1-7	.5 - 5	1 - 7
Network Size	Unlimited (2^{64})	1	32	7
Bandwidth (KB/s)	20 - 250	64 - 128+	11,000+	720
Transmission Range (meters)	1 - 100+	1,000+	1 - 100	1 - 10+
Success Metrics	Reliability, Power, Cost	Reach, Quality	Speed, Flexibility	Cost, Convenience

Source: http://www.zigbee.org/en/about/faq.asp

Why do we need another "WPAN" standard?

- Power consumption
  - ZigBee: 10mA <==> BT: 100mA
- Production costs
  - ZigBee: 1.1 $ <==> BT: 3 $
- Development costs
  - Codesize ZB/codesize BT = ½
- Bit-error-rate (BER)



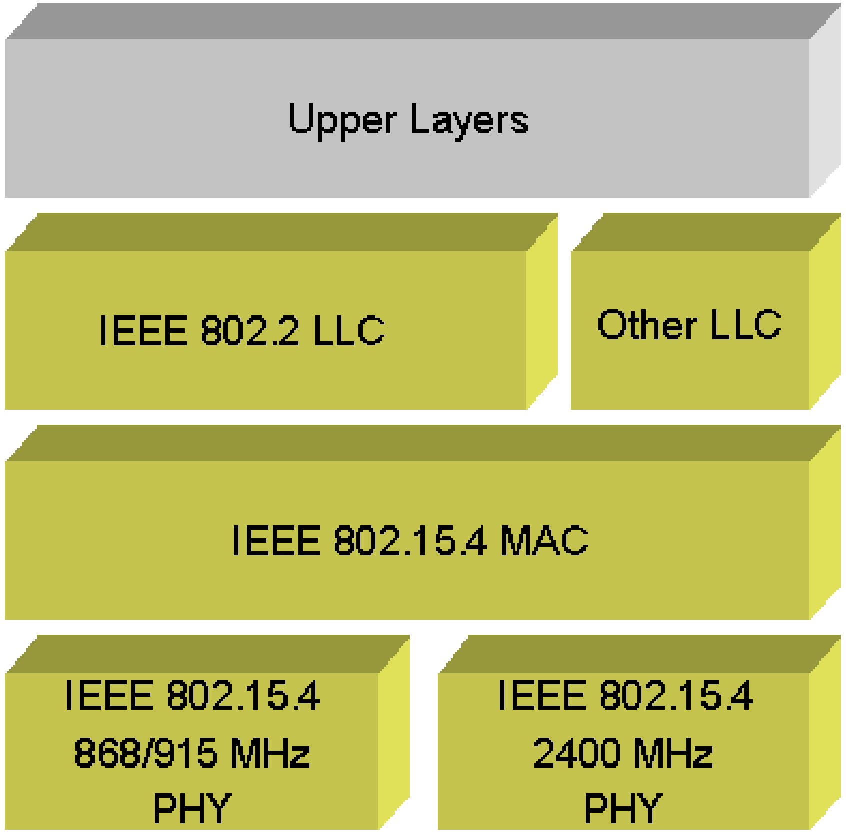
- Sensitivity
- flexibility
  - No. of supported nodes
  - ZigBee: 65536 (in a mesh) <==> BT: 7
- Security
- Latency requirements
- Range
  - ZigBee: up to 75 m in LOS condition <==> BT: 10 m

ZigBee/IEEE 802.15.4 features

- Low power consumption
- Low cost
- Small packet
- Low offered message throughput
- Supports large network orders (<= 65k nodes)
- Low to no QoS guarantees
- Flexible protocol design suitable for many applications

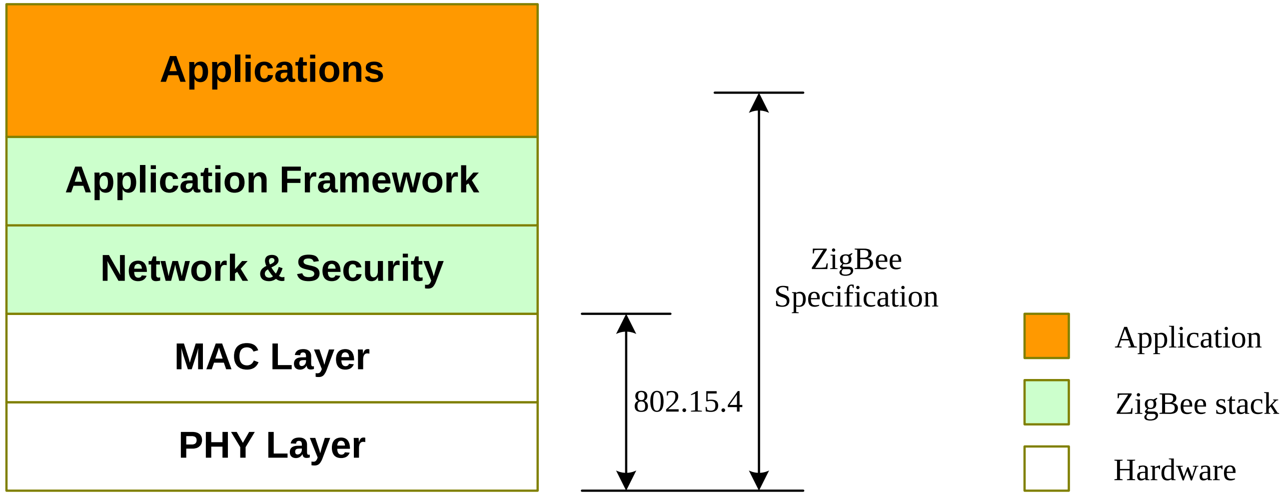
IEEE 802.15.4 - Overview

- Low Rate WPAN (LR-WPAN)
  - E.g. Sensor networks
- Simple and low cost
  - Fully handshake protocol
- Low power consumption
  - Years on lifetime using standard batteri
- Different topologies
  - Star, peer-to-peer, combined
- Data rates: 20-250 kbps
  - Low latency support
- Operates at different frequencies
  - 868 Mhz, 915 Mhz, 2.4 GHz

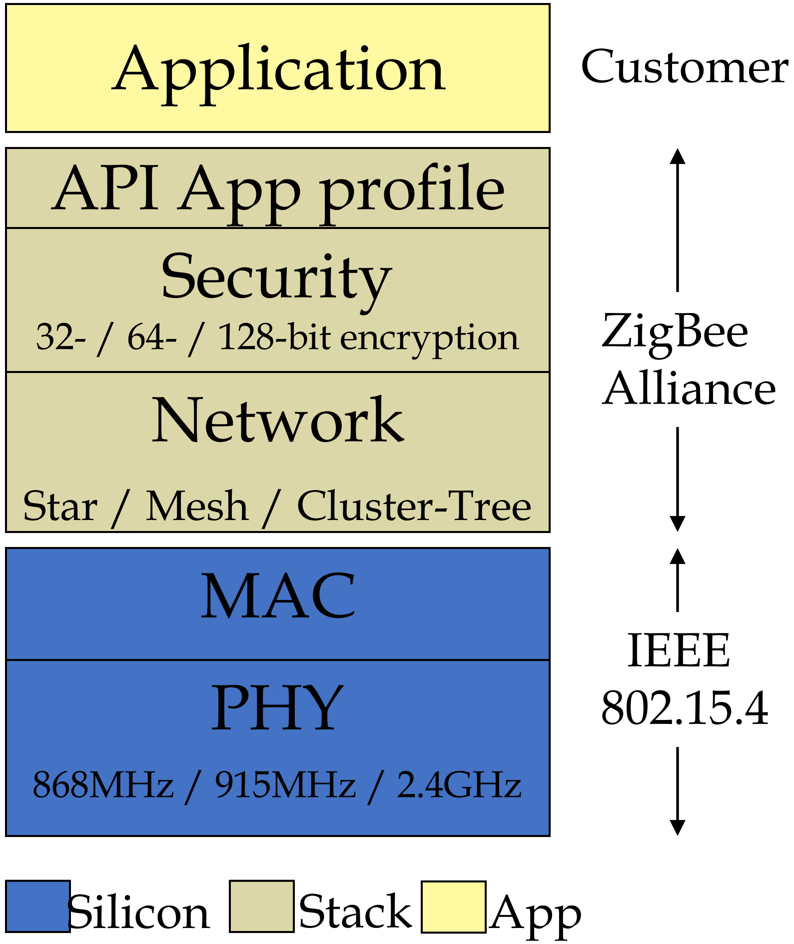


ZigBee/802.15.4 architecture

- ZigBee Alliance
  - Companies: semiconductor manufacturers, IP providers, OEMs, etc.
  - Defining upper layers of protocol stack: from network to application, including application profiles
  - First profiles published mid 2003
- IEEE 802.15.4 Working Group
  - Defining lower layers of protocol stack: MAC and PHY



IEEE 802.15.4 & ZigBee In Context



ZigBee Alliance

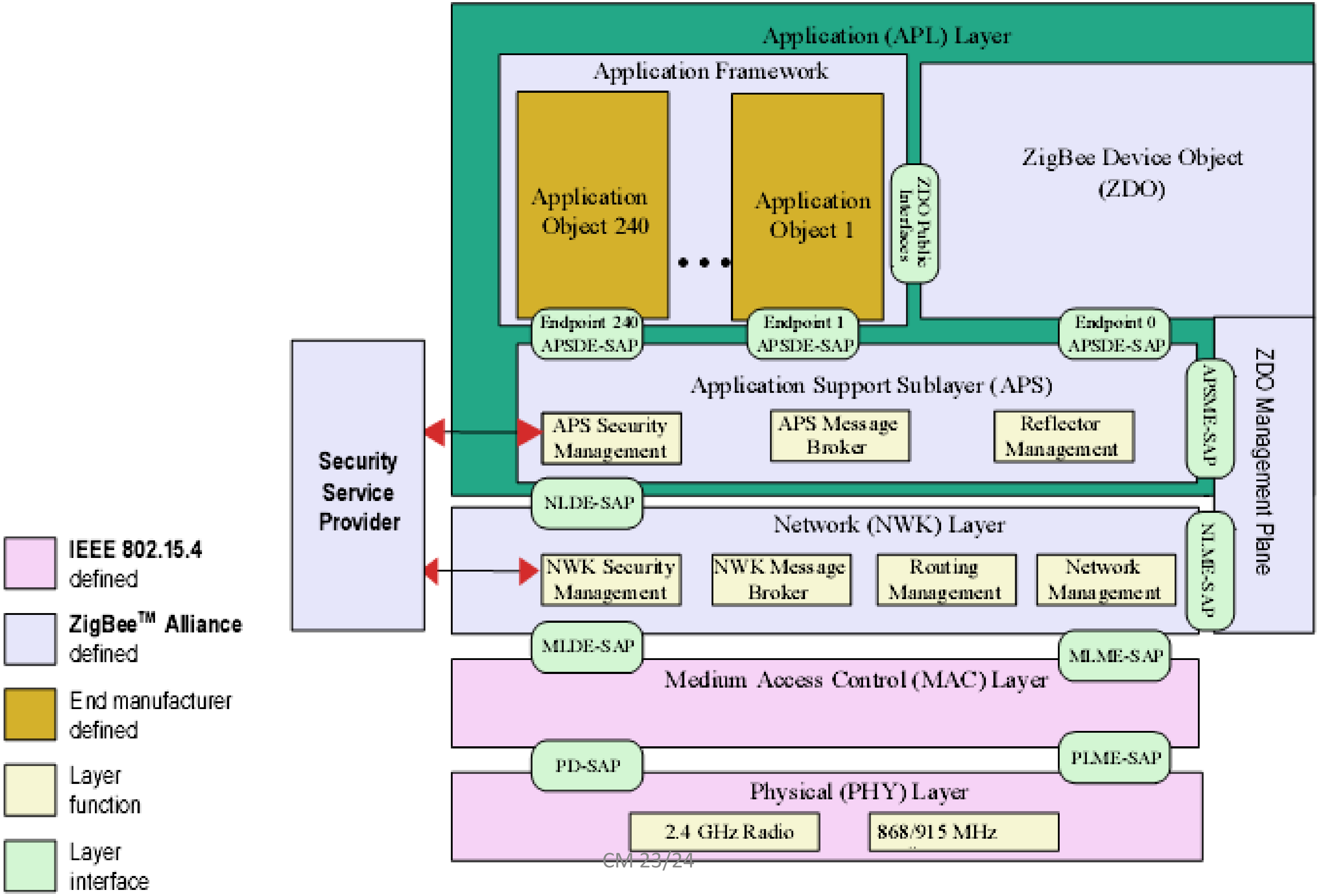
- "the software"
- Network, Security & Application layers
- Brand management

IEEE 802.15.4

- "the hardware"
- Physical & Media Access Control layers

Source: http://www.zigbee.org/resources/documents/IWAS_presentation_Mar04_Designing_with_802154_and_zigbee.ppt

Protocol Stack



How ZigBee Works

- Topology
  - Star
  - Cluster Tree
  - Mesh
- Network coordinator, routers, end devices
- 2 or more devices form a PAN/WSN

How ZigBee Works

- States of operation
  - Active
  - Sleep
- Devices
  - Full Function Devices (FFD’s)
  - Reduced Function Devices (RFD’s)
- Modes of operation
  - Beacon
  - Non-beacon
- Traffic types
  - Intermittent
  - Repetitive
  - Periodic

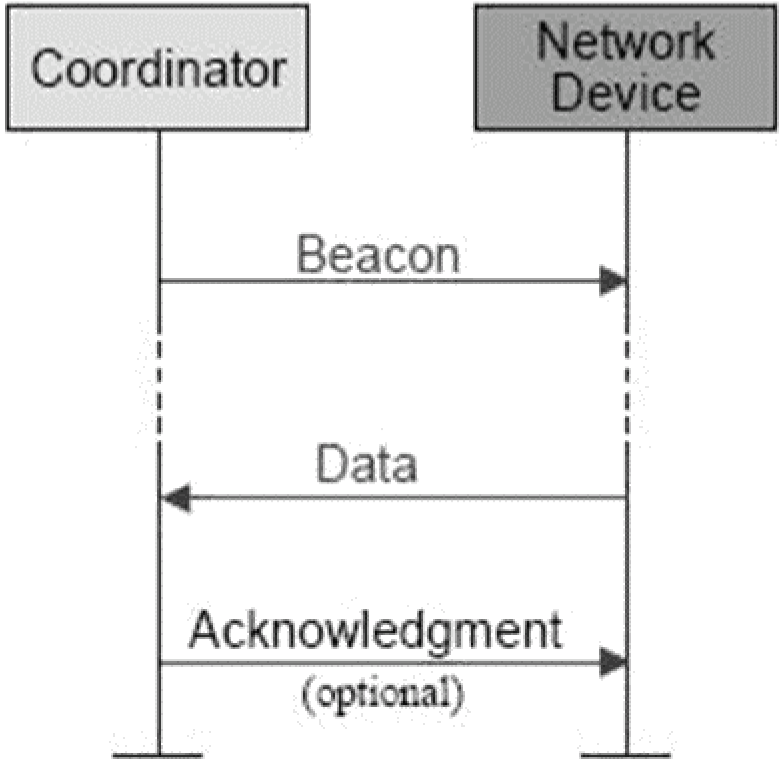
Traffic-Types

- Data is periodic
  - application dictates rate (e.g. sensors)
- Data is intermittent
  - application or stimulus dictates rate (optimum power savings), e.g. light switch
- Data is repetitive (fixed rate a priori)
  - device gets guaranteed time slot (e.g. heart monitor)

Traffic-Modes

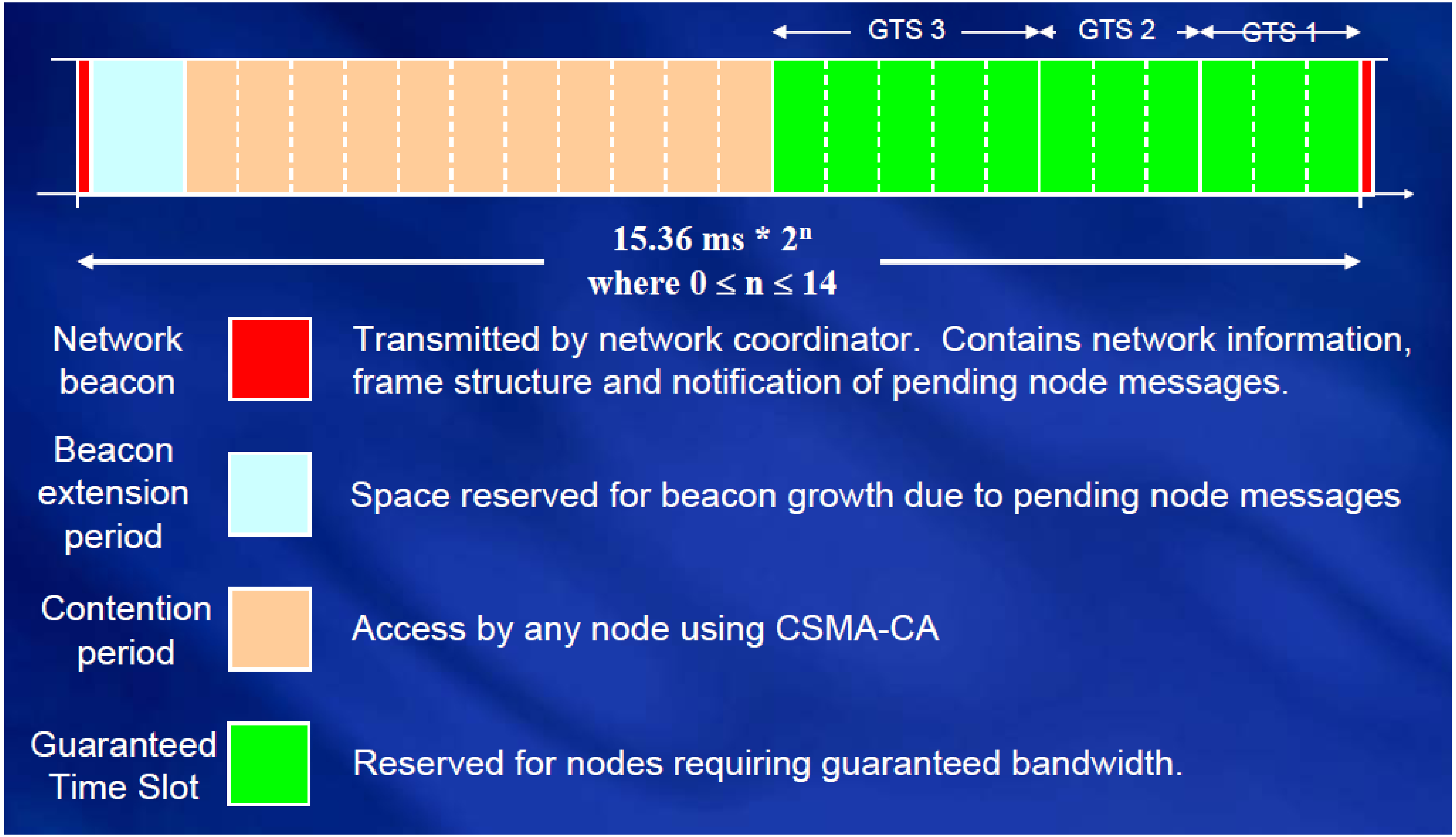
Beacon mode:

- beacon sent periodically
- Coordinator and end device can go to power save
- Lowest energy consumption
- Precise timing needed
- Beacon period (ms-m)



Beacon Mode

GTS – Guaranteed Time Slots



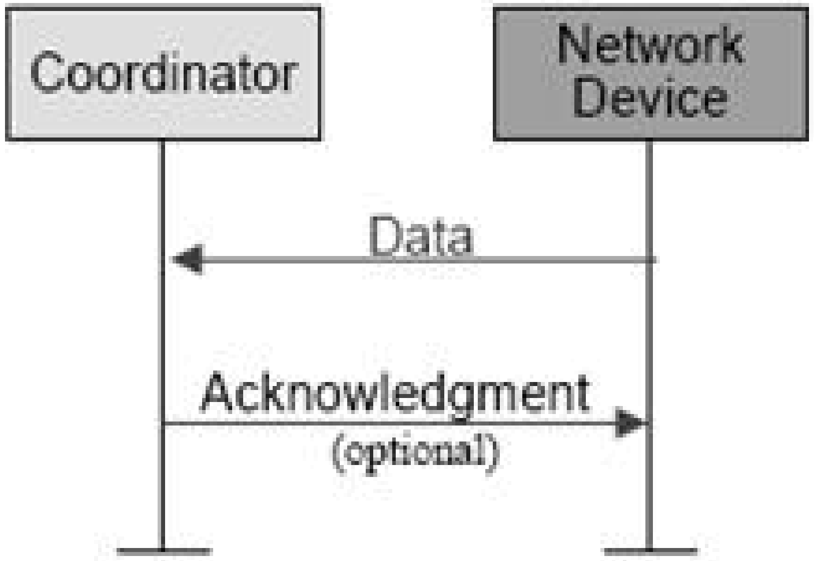
Traffic-Modes

Non-Beacon mode:

- coordinator/routers have to stay awake

  (robust power supply needed)

- heterogeneous network
- asymmetric power



ZigBee Node-Types

ZigBee Coordinator (ZBC) (IEEE 802.15.4 FFD)

- only one in a network
- initiates network
- stores information about the network
- all devices communicate with the ZBC
- routing functionality
- bridge to other networks

ZigBee Router (ZBR) (IEEE 802.15.4 FFD)

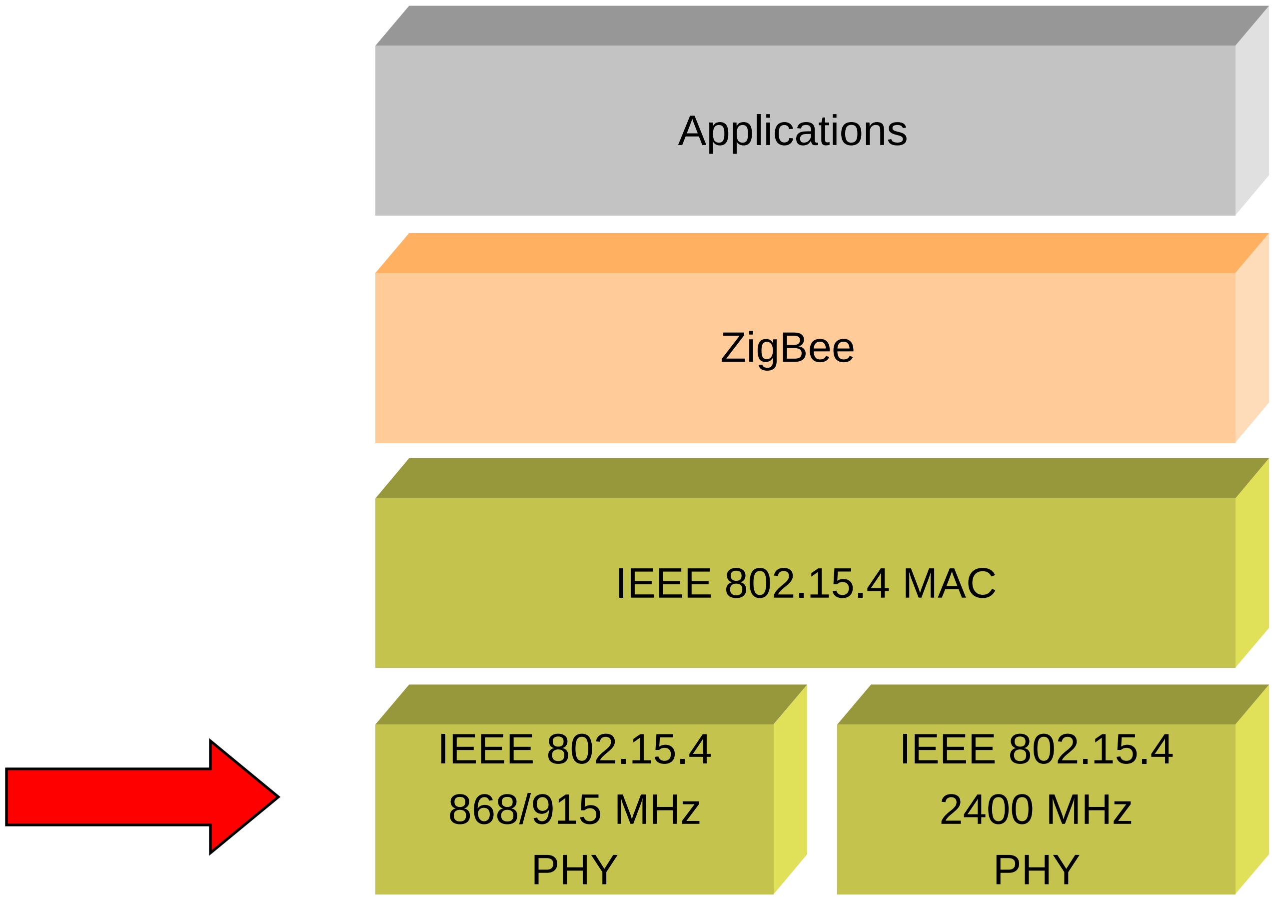
- optional component
- routes between nodes, network backbone
- extends network coverage
- manages local address allocation/de-allocation

ZigBee End Device (ZBE) (IEEE 802.15.4 RFD)

- optimized for low power consumption
- cheapest device type
  - sensor would be deployed here

Remember: FFD – Full Function Device
RFD – Reduced Function Device

802.15.4 / ZigBee Architecture



- Packet generation
- Packet reception
- Data transparency
- Power Management

IEEE 802.15.4 basics

- 802.15.4 is a simple packet data protocol for lightweight wireless networks
  - Channel Access is via **Carrier Sense Multiple Access with collision avoidance** and optional time slotting
  - Message acknowledgement and an optional beacon structure
  - Multi-level security
  - Works well for
    - Long battery life, selectable latency for controllers, sensors, remote monitoring and portable electronics
  - Configured for maximum battery life, has the potential to last as long as the shelf life of most batteries

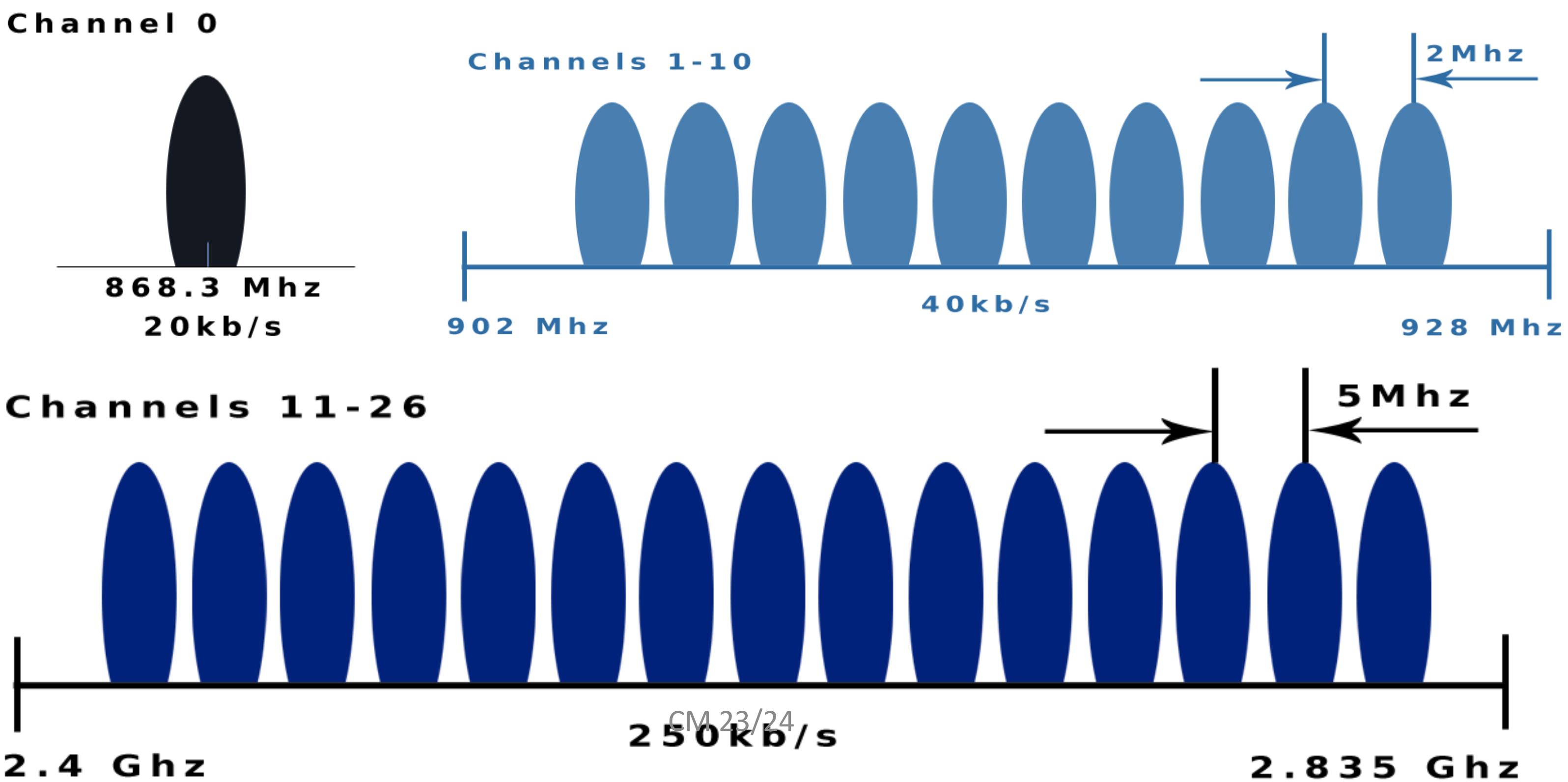
802.15.4 General characteristics

- Data rates of 250 kbps , 20 kbps and 40kpbs.
- Star or Peer-to-Peer operation.
- Support for low latency devices.
- CSMA-CA channel access, with CCA detection
  - Clear Channel Assessment
- Dynamic device addressing.
- Fully handshaked protocol for transfer reliability.
- Low power consumption.
- 16 channels in the 2.4GHz ISM band
- 10 channels in the 915MHz ISM band
- one channel in the European 868MHz band.
- Extremely low duty-cycle (<0.1%)

802.15.4 frequency bands

Operates in Unlicensed Bands

- ISM 2.4 GHz Global Band at 250kbps
- 868 MHz European Band at 20kbps
- 915 MHz North American Band at 40kbps

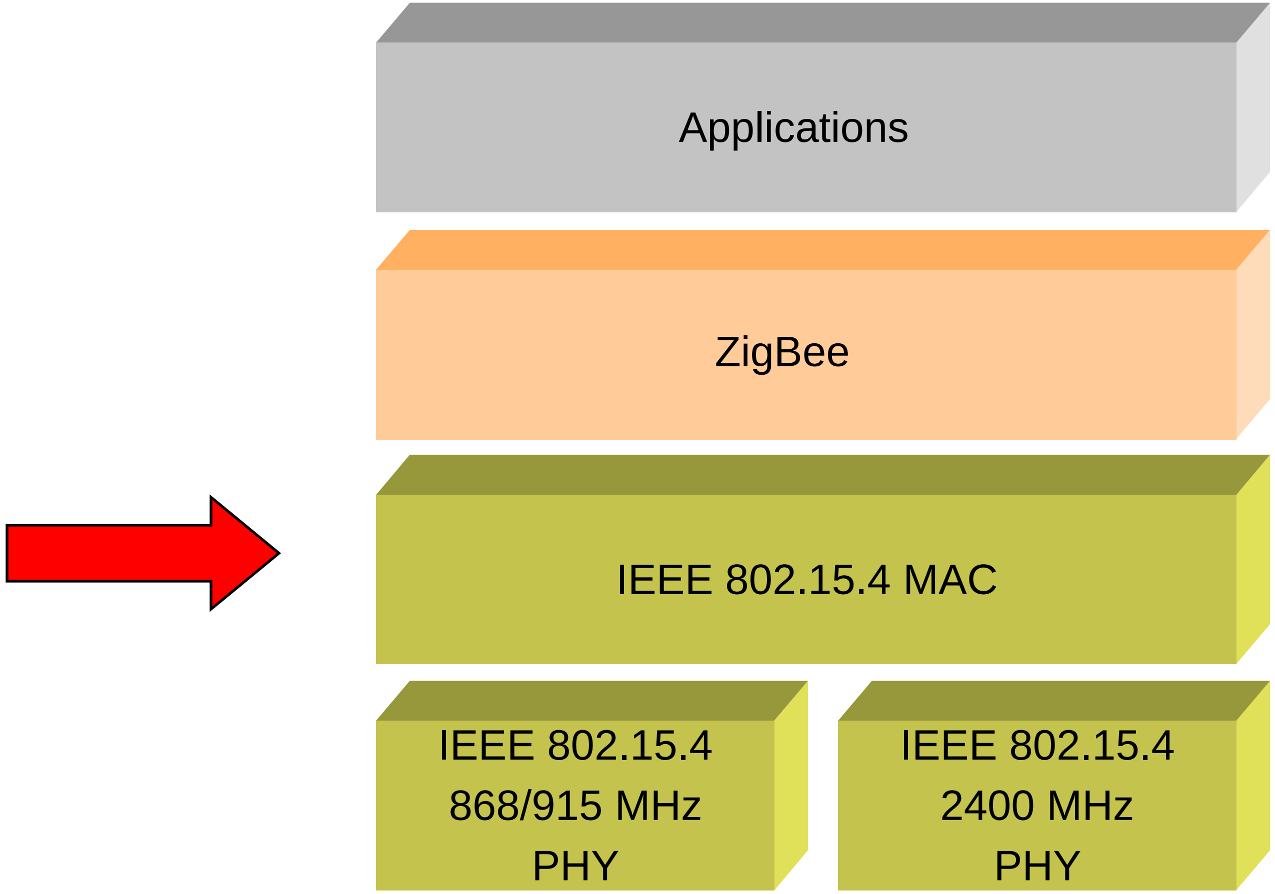


PHY frame structure

- PHY packet fields
  - Preamble (32 bits) – synchronization
  - Start of packet delimiter (8 bits) – shall be formatted as “11100101”
  - PHY header (8 bits) –PSDU length
  - PSDU (0 to 127 bytes) – data field

Sync Header		PHY Header		PHY Payload
Preamble	Start of Packet Delimiter	Frame Length (7 bit)	Reserve (1 bit)	PHY Service Data Unit (PSDU)
4 Octets	1 Octets	1 Octets		0-127 Bytes

802.15.4 Architecture (MAC)



- Channel acquisition
- Contention management
- (super)Frame structure
- NIC address
- Error Correction

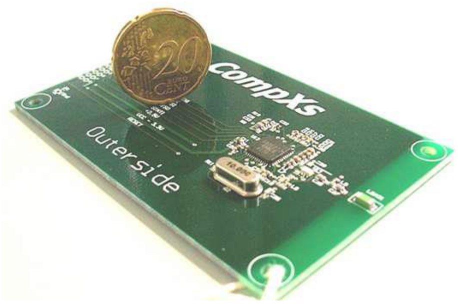
IEEE 802.15.4 MAC Design Drivers

- Extremely low cost
- Ease of implementation
- Reliable data transfer
- Short range operation
- Very low power consumption

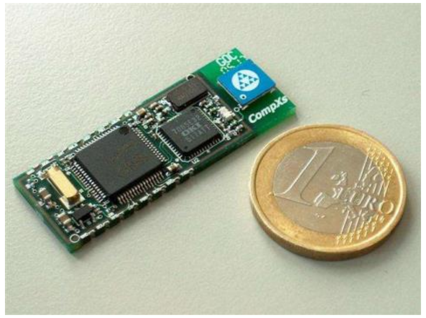
Simple but flexible protocol

IEEE 802.15.4 MAC Overview

Device Classes

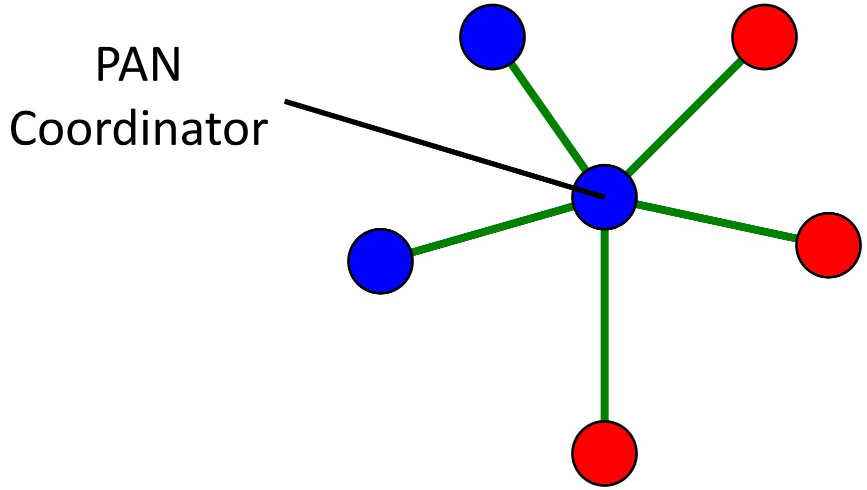


- Full function device (FFD)
  - Any topology
  - Network coordinator capable
  - Talks to any other device
  - The FFD can operate in three modes serving
    - Device
    - Coordinator
    - PAN coordinator
- Reduced function device (RFD)
  - Limited to star topology
  - Talks only to a network coordinator
    - Cannot become a network coordinator
  - Very simple implementation



IEEE 802.15.4 MAC Overview

Star Topology



Master/slave

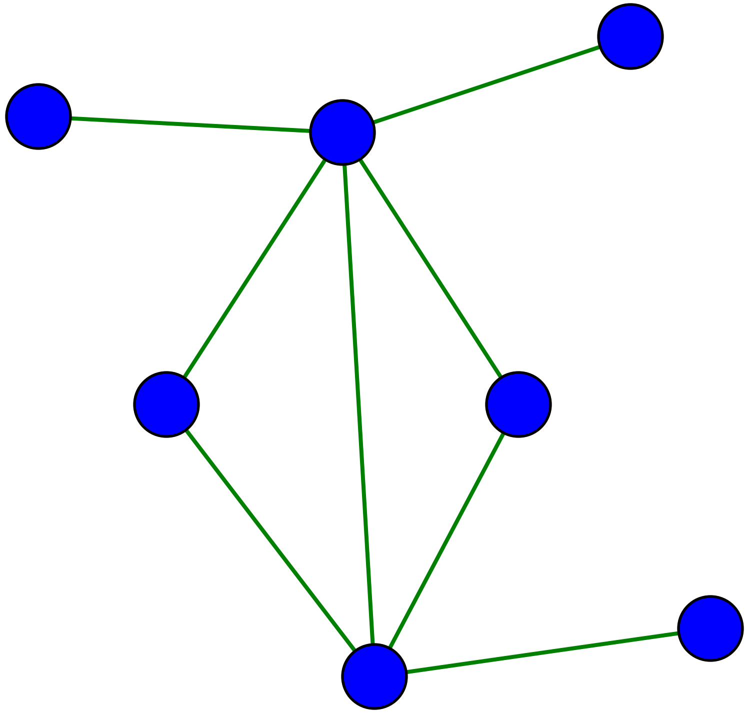
Full function device

Communications flow

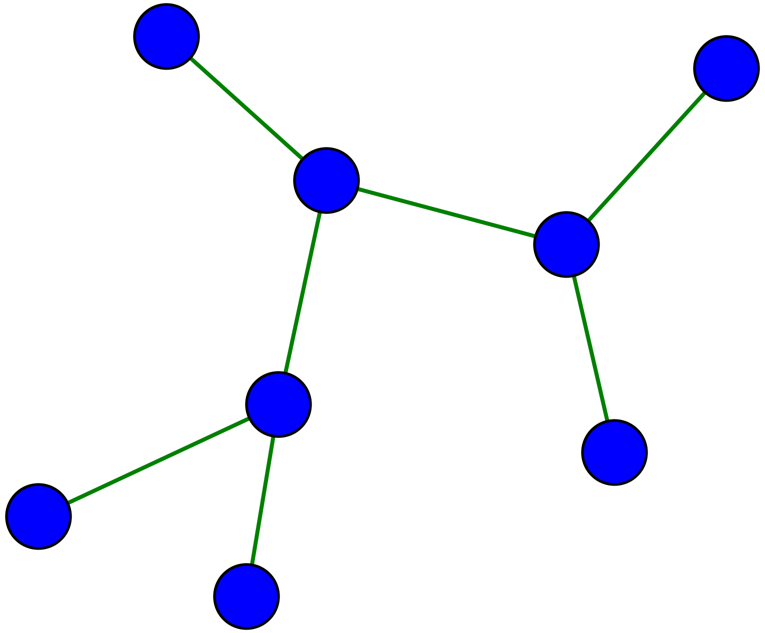
Reduced function device

IEEE 802.15.4 MAC Overview

Mesh (Peer-Peer) and cluster tree topologies



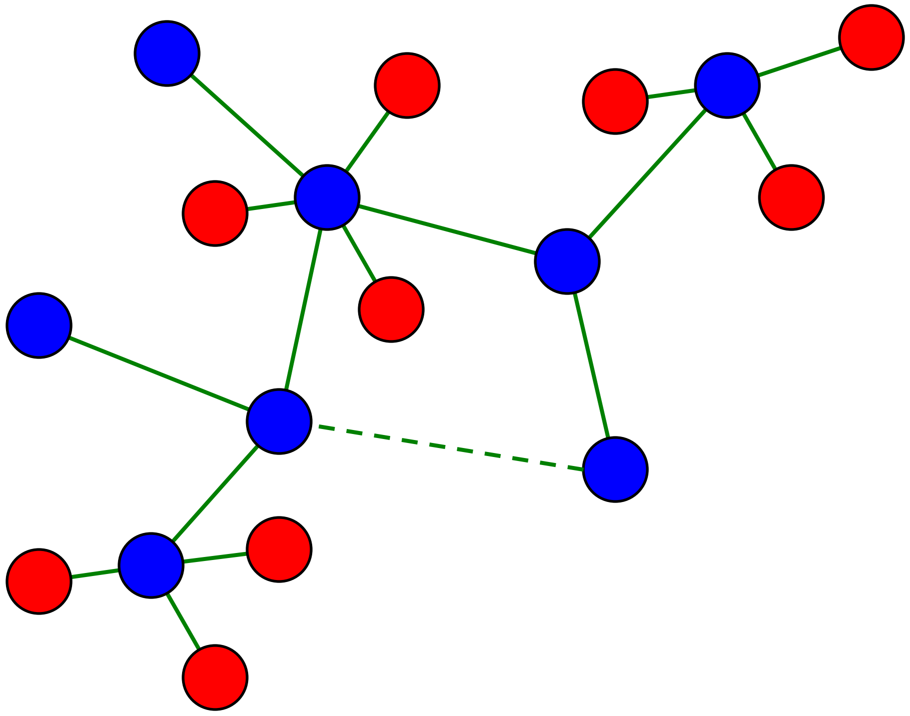
Mesh



Cluster tree

IEEE 802.15.4 MAC Overview

Combined Topology



Clustered stars - for example, cluster nodes exist between rooms of a hotel and each room has a star network for control.

May have a mesh structure in some cases as well

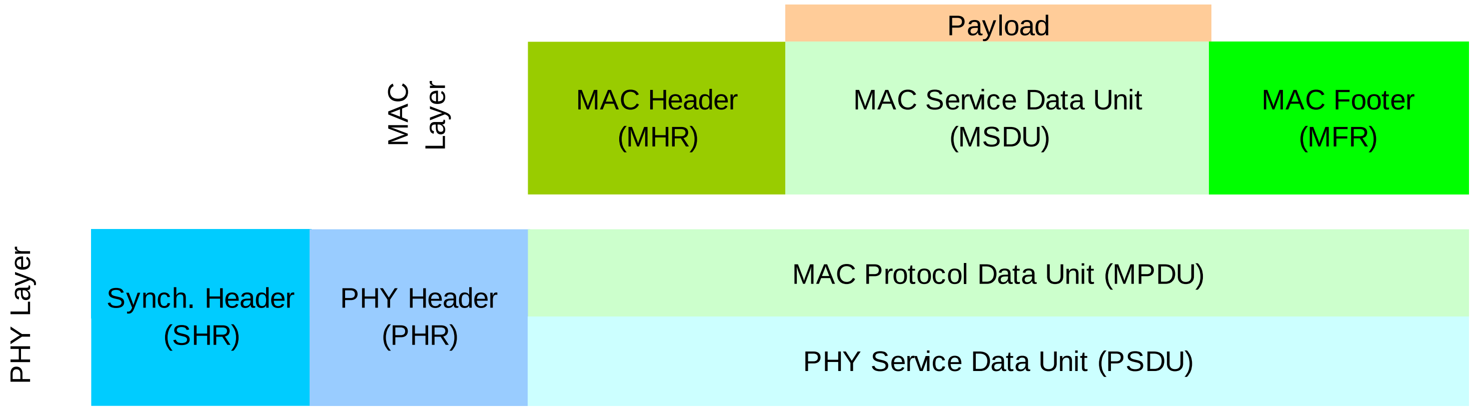
Full function device

Reduced function device

Communications flow

IEEE 802.15.4 MAC Overview

General Frame Structure



4 Types of MAC Frames:

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

MAC layer

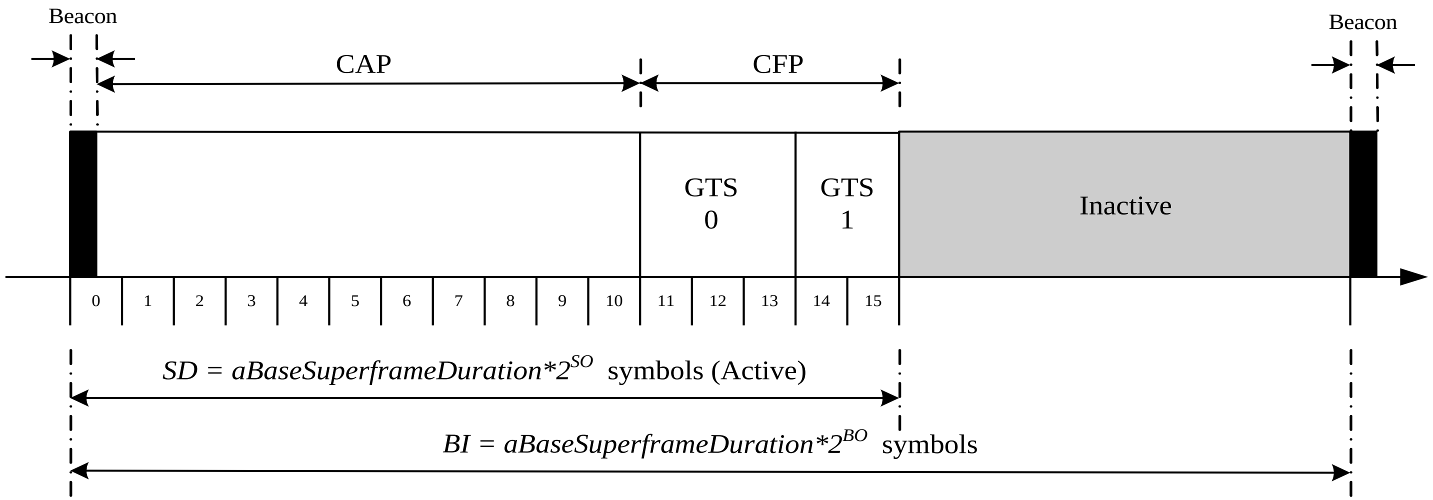
Managing PANs

- Channel scanning (Energy Detection, active, passive, orphan – verifies if it still has a parent)
- PAN ID conflict detection and resolution
- Starting a PAN
- Sending beacons
- Device discovery, association/disassociation
- Synchronization (beacon/nonbeacon)
- Orphaned device realignment

Transfer handling

- Transaction based (indirect transmission)
  - Beacon indication
  - Polling
- Transmission, Reception, Rejection, Retransmission
  - Acknowledged / Not acknowledged
- GTS management
  - Allocation/deallocation/Reallocation
  - Usage

Superframe



- A coordinator in a PAN can optionally bound channel time using a SuperFrame structure
  - bound by beacon frames
- A superframe is divided into two parts
  - Inactive: all devices sleep (including the coordinator
  - Active:
    - Active period will be divided into 16 slots
    - 16 slots can further be divided into two parts
      - Contention access period
      - Contention free period

CAP – Contention Access Period
CFP – Contention Free Period
SD – Superframe Duration
BI – Beacon Interval

Superframe

- Beacons are used for
  - starting superframes
  - synchronizing with associated devices
  - announcing the existence of a PAN
  - informing pending data in coordinators
- In a beacon enabled network,
  - Devices use the slotted CSMA/CA mechanism to contend for the usage of channels
  - FFDs which require fixed rates of transmissions can ask for *guarantee time slots* *(GTS)* from the coordinator