Part 2.2: Wireless Technologies for IoT

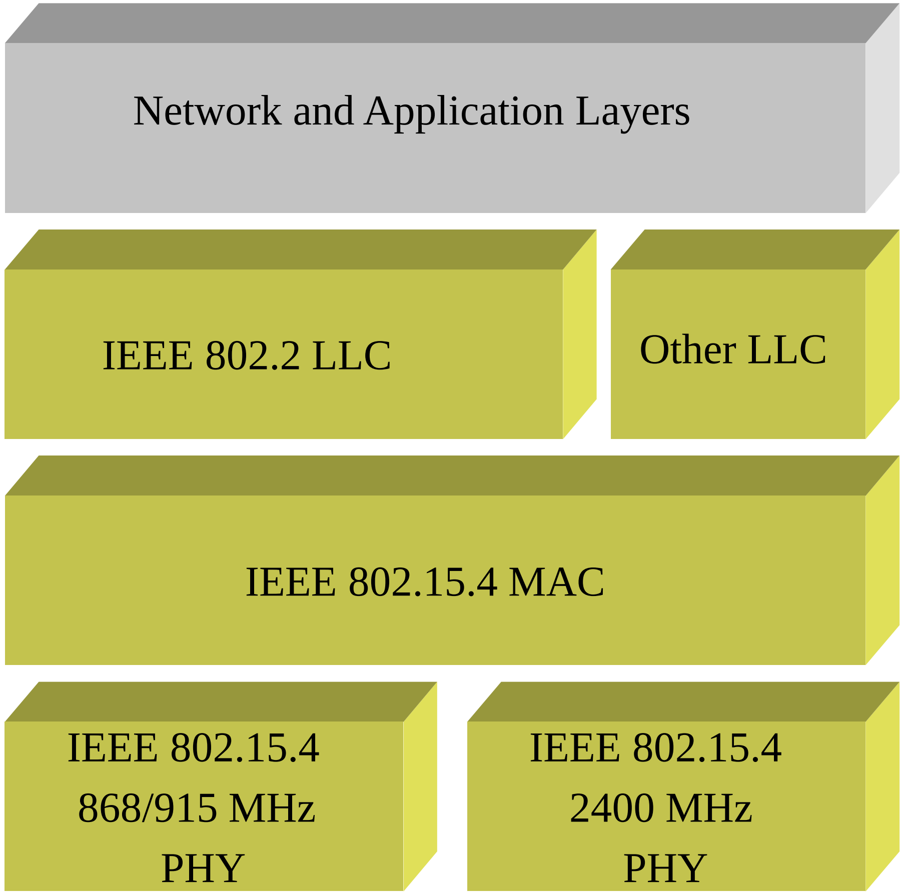
Queen Mary
University of London

Outlines

- Principles and challenges of MAC in WSNs and IoT
- MAC schemes for WSNs and IoT
  - Contention based protocols
    - S-MAC
    - T-MAC
    - WiseMAC
    - LEACH
- Zigbee/IEEE802.15.4
- Low Power WiFi
- LoRa

PRINCIPLES AND CHALLENGES

WSN Protocol Stack



Logical Link Control Sub-Layer

- The LLC is on the top of the MAC sub-layer and is in-charge of achieving good utilization and providing a reliable service to the layers above it. They are achieved with the following functions.

  - **Framing**: Data units must be encapsulated into LLC sub-layer frames to add necessary information to perform the sub-layer function. The frame size must be kept to minimum to save energy.

  - **Error Control:** Error detection and error correction mechanism must be embedded to detect and correct bit errors introduced in the media.

Logical Link Control Sub-Layer

– **Flow Control:** The LLC sub-layer includes the mechanism to control the flow of information and avoid overflowing the receiver. However, in Low data rate WSN's flow control is not important and is embedded in error control mechanism.

– **Link Management:** Neighbor discovery, link setup, maintenance and tear down and link quality estimation are among the most important link management functions. Neighbor discovery and link quality estimation are functions utilized by many topology control protocols to save energy.

The MAC Sub-Layer

- MAC protocols have the responsibility of providing fair access to all nodes sharing a common communication channel.

- Although WSN are also wireless networks facing the same issues, the MAC sub-layer is WSN’s has different goals and performance concerns than other wireless networks.

MAC protocols

- **Medium access in WSNs** is difficult mainly because of

  – WSN devices usually send very small frames and use the channel occasionally, either periodically or whenever an important event occurs.

  – As a result, fairness is not as important as in other networks where there is a chance that one would monopolize he use of the channel. In WSN's nodes rarely compete for the channel.

  – WSN's are data centric without hard delay requirements. Fast access under some reporting models is required but is not as important as in other networks.

MAC protocols

– Achieving good channel utilization is not as important as nodes are idle most of the time.

– In WSN energy is the most important issue which pose Requirements

- High throughput and other relevant metrics are traded for energy consumption
- Energy efficiency, handle switched off devices

MAC protocols – Energy Problems

- Recall: Transceiver consumes a significant share of energy in other networks as

  – Sending is costly; Receiving costs are often almost the same

  – Idling is cheaper, but about as expensive as receiving

MAC protocols – Energy Problems

- Derived energy problems regarding the MAC protocol which must be handled/ avoided in WSN's are
  - **Collision:** Waste of effort when two packets collide
  - **Overhearing:** Waste of effort when receiving a packet that was directed at another destination
  - **Protocol overhead:** Waste of effort due to MAC-related overhead and the protocol complexity
  - **Idle listening:** Waste of effort when waiting for incoming packets, but nobody is sending
  - **Overemitting:** Waste of effort when transmitting a message when the destination node is not ready

MAC protocols – Communication Patterns

- There are three basic communication patterns followed in WSNs

  – **Broadcast:** Sink (base station) to transmit some information to all sensor nodes of the network. e.g. The sink can query sensors on the location of a certain event.

  – **Local Gossip:** The sensors that detect an intruder communicate locally. I.e. A sensor sends a message to its neighbouring nodes within a range.

  – **Convergecast:** The sensors that detect an intruder then need to send what they preceive to the information center. i.e. a group of sensors communicate to specific sensor.

MAC protocols – Centralized Medium Access

- Idea: A central station controls, when a node may access the medium (also known as **fixed assignment**)

– Example: Polling, centralized computation and assignment of time slots (TDMA)

- Simple and efficient, but burden to the central station

- Not feasible for large WSNs, but if network is divided into smaller groups, this approach can be useful

MAC protocols – Distributed Medium Access

- **Contention-based protocols**

  – Risk of colliding packet is deliberately taken

  – Mechanisms to avoid/reduce collisions required (often random)

MAC protocols – Distributed Medium Access

- **Schedule-based protocols:** TDMA component provides a schedule regulating which participant may use which resource at which time
  - Typical resource : frequency band
  - Implicit idle listening avoidance mechanism

– Schedule can be fixed or computed on-demand
  - Sometimes mixed

– Collisions, Overhearing and Idle listening are no issues
  - ➢ BUT: time-synchronization is needed

Contention-based MAC protocols I

Basic options (also termed as **random assignment**)

– ALOHA → not good in most cases

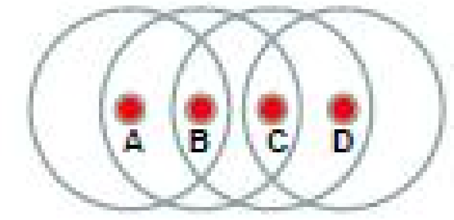
– Listen before talk (CSMA)

BUT: sender is not knowing what is going on at the receiver

→ might destroy packets despite listening

• Besides, receiver needs possibility to inform possible senders in its neighborhood upcoming transmission

→ "**shut them up**" for this duration



– Recall:

• Hidden Terminal Problem

• Exposed Terminal Problem

Contention-based MAC protocols II

- Receiver informs potential interferers

– **While a reception is on-going**

- By sending out a signal indicating the reception (Busy tone protocol)
- Problem: cannot use the same channel on which the reception takes place → use separate channel for signaling

– **Before a reception is on-going**

- Can use the same channel
- Receiver itself needs to be informed

CONTENTION-BASED PROTOCOLS

Multiple Access with Collision Avoidance (MACA)

- Sender B asks receiver C whether C is able to receive a transmission ***Request to Send (RTS)***
- Receiver C agrees, sends out a ***Clear to Send*** (***CTS***)
- Potential interferers overhear either RTS or CTS and know about impending transmission and for how long it will last
  - Store this information in a ***Network Allocation Vector***
- B sends, C ACKs

! ***MACA protocol*** (used e.g. in ***IEEE 802.11***)

MACA Problems

- **Problem:**

  – In WSNs most of the time nothing happens, i.e. there is only a low data rate

  – For low data rates, MACA's idle listening is unsuitable

- Idea: use 'rendezvous' mechanism

  – turn off nodes and ensure that neighboring nodes turn on simultaneously to allow packet exchange

Contention-based MAC protocols– S-MAC I

- Proposal of this approach: S-MAC

– S-MAC = **Sensor-MAC**

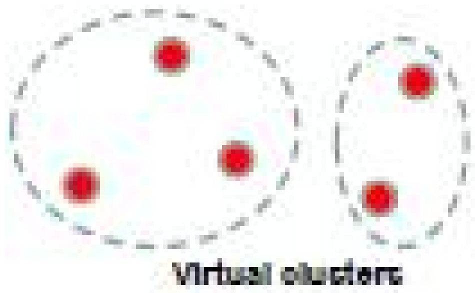
– S-MAC is energy efficient and provides collision avoidance and overhearing

Contention-based MAC protocols– S-MAC I

- The Sensor-MAC protocol solves the energy consumption related problems of Idle listening, collision and overhearing.
- S-MAC considers that nodes do not need to be awake at all times and reduces the idle listening problem by turning off and on periodically by dividing time in two parts.
- Only in the ‘listen periods data will be exchanged
  - Sending & receiving
- Nodes Periodically sleep
- Trades energy efficiency for lower throughput and higher latency
- Sleep during other node’s transmission

Contention-based MAC protocols– S-MAC II

- In order to synchronize, nodes broadcast their schedule to all neighbors with the help of SYNCH frame
    - Forming of virtual clusters "synchronized islands"
- Data transfer
    - Perform RTS/CTS
    - Transfer data, ACK
- Not affected nodes change to sleep mode



Contention-based MAC protocols– T-MAC

- In S-MAC the 'listen period' is of fixed length

- Problem

– What happens when there is no traffic?

→ nodes have to stay awake unnecessarily

Contention-based MAC protocols– T-MAC

- **Idea:**

  – Prematurely go back to sleep mode when there is no traffic for a certain time (timeout)

  adaptive duty cycle

- Implementation of this idea: T-MAC

  – Timeout**-MAC**

  – As S-MAC, but uses timeout to reduce listen period

Contention-based MAC protocols– Preamble Sampling

- Until now, periodic sleep was used to synchronize the sleep and wake up phases of the nodes

- Alternative: Don’t try to explicitly synchronize nodes

  – Regularly sample the medium to check for activity, rest of the time change to sleep mode

Contention-based MAC protocols– Preamble Sampling

- Use long preambles to ensure that receiver stays awake to catch the actual packet
- Sensor nodes go to sleep and wake up independently of others.
- Sensor nodes only wake up to check if the channel is busy. In which case they stay awake.

- – e.g. WiseMAC
  - A sensor node wanting to transmit sends a long preamble to overlap the sampling time of the receiver and subsequently sends data.

Contention-based MAC protocols– B-MAC I

- B-MAC combines several of the mentioned approaches
  - Tries to provide practically relevant solutions

- Clear Channel Assessment

  – Sampling of the medium to estimate the noise floor.

  – When a node wants to transmit, it takes the sample of the channel and compares it with noise floor.

  – If the sample energy level is below the noise floor then channel is assumed to be clear.

    - Samples are exponentially averaged

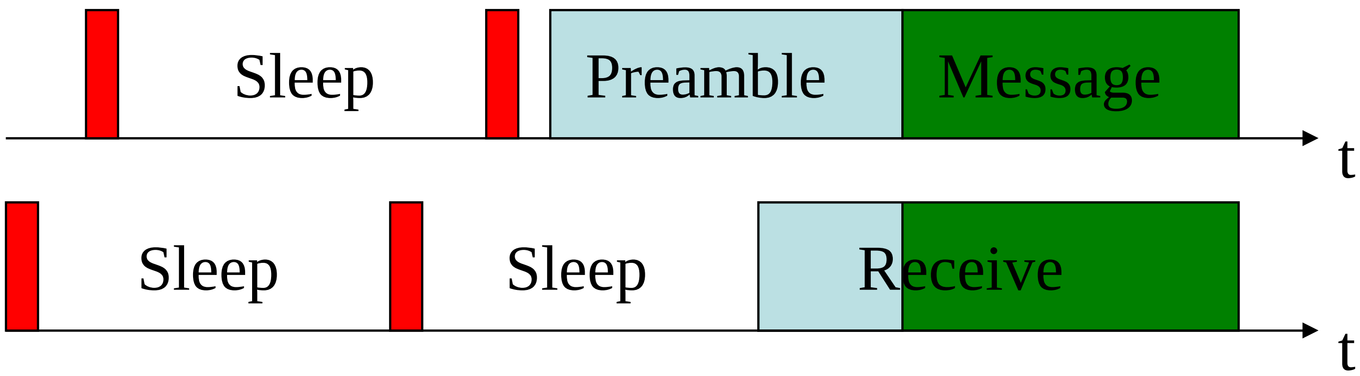
Contention-based MAC protocols– B-MAC I

– For actual assessment when sending a packet, look at five channel samples

channel is assumed as free, when even a single sample is significantly below noise

– Optional: Random back-off, if channel is found busy

- Preamble sampling to cater idle listening problem.



Contention-based MAC protocols– B-MAC II

Low Power Listening

– Preamble sampling

– Uses the clear channel assessment techniques to decide whether there is packet arriving when node wakes up

– Timeout puts node back to sleep if no packet arrived

- **B-MAC does not have**
  - Synchronization
  - RTS/CTS
- **BUT:**
  - This results in simpler and slimmer implementation
  - Clean and simple interface
- Currently, B-MAC is considered as default MAC protocol

Schedule-based MAC protocols – LEACH I

- LEACH: Low-Energy Adaptive Clustering Hierarchy
  - Given:
    - Dense network of sensor nodes reporting to a central sink
    - Each node can reach the sink directly

- Idea: Group nodes into "clusters", each controlled by a cluster-head (CH)
  - About 5% of nodes become CH (scenario dependent)
  - Role of CH rotates to share the burden
  - Cluster-head organizes
    - CDMA code for all members of the cluster
    - TDMA schedule that is used within the cluster

Schedule-based MAC protocols – LEACH II

- Setup phase

  – CHs advertise themselves → other nodes join the CH with the strongest signal; broadcast schedule is distributed by the CH

- Steady-state phase

  – CH collects and aggregates data from all cluster members

  – CH reports aggregated data to sink using CDMA

ZIGBEE/IEEE 802.15.4

Content

- Overview
- Topologies
- Superframe structure
- Frame formatting
- Data service
- Management service
- Interframe spacing
- CSMA procedure

Zigbee/IEEE802.15.4

- IEEE 802.15.4 deals with only PHY layer and MAC layer.
- The higher-layer protocols are left to industry and the individual applications.
- The Zigbee Alliance is an association of companies involved with building higher-layer standards based on IEEE 802.15.4. This includes network, security, and application protocols.

IEEE 802.15.4

- IEEE standard for low-rate WPAN applications
- Goals: low-to-medium bit rates, moderate delays without too stringent guarantee requirements, low energy consumption
- Physical layer
  - 20 kbps over 1 channel @ 868-868.6 MHz
  - 40 kbps over 10 channels @ 905 – 928 MHz
  - 250 kbps over 16 channels @ 2.4 GHz
- MAC protocol
  - Single channel at any one time
  - Combines contention-based and schedule-based schemes
  - Asymmetric: nodes can assume different roles

Wakeup radio MAC protocols

- Simplest scheme: Send a wakeup "burst", waking up all neighbors ! Significant overhearing
  - Possible option: First send a short ***filter packet*** that includes the actual destination address to allow nodes to power off quickly
- Not quite so simple scheme: Send a wakeup burst including the receiver address
  - Wakeup radio needs to support this option
- Additionally: Send information about a (randomly chosen) data channel, CDMA code, … in the wakeup burst
- Various variations on these schemes in the literature, various further problems
  - One problem: 2-hop neighborhood on wakeup channel might be different from 2-hop neighborhood on data channel
  - Not trivial to guarantee unique addresses on both channels

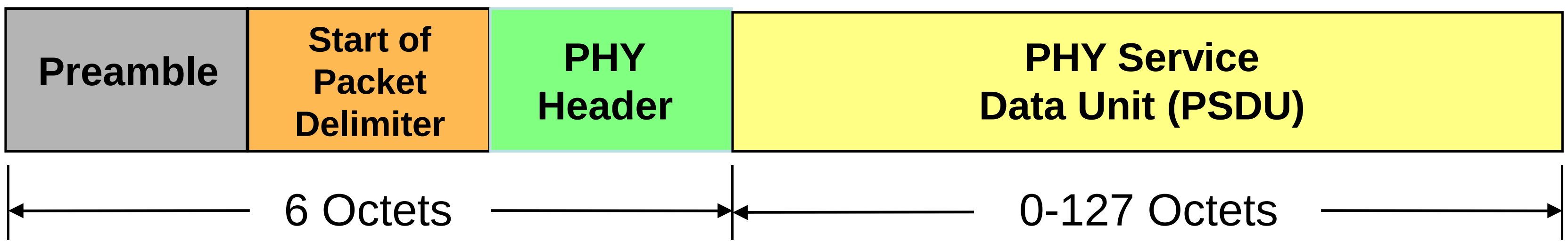
PHY Overview

The PHY is responsible for:

- Activation and deactivation of the radio transceiver
- ED within the current channel
- LQI for received packets
- CCA for CSMA-CA
- Channel frequency selection
- Data transmission and reception

PHY Packet Fields

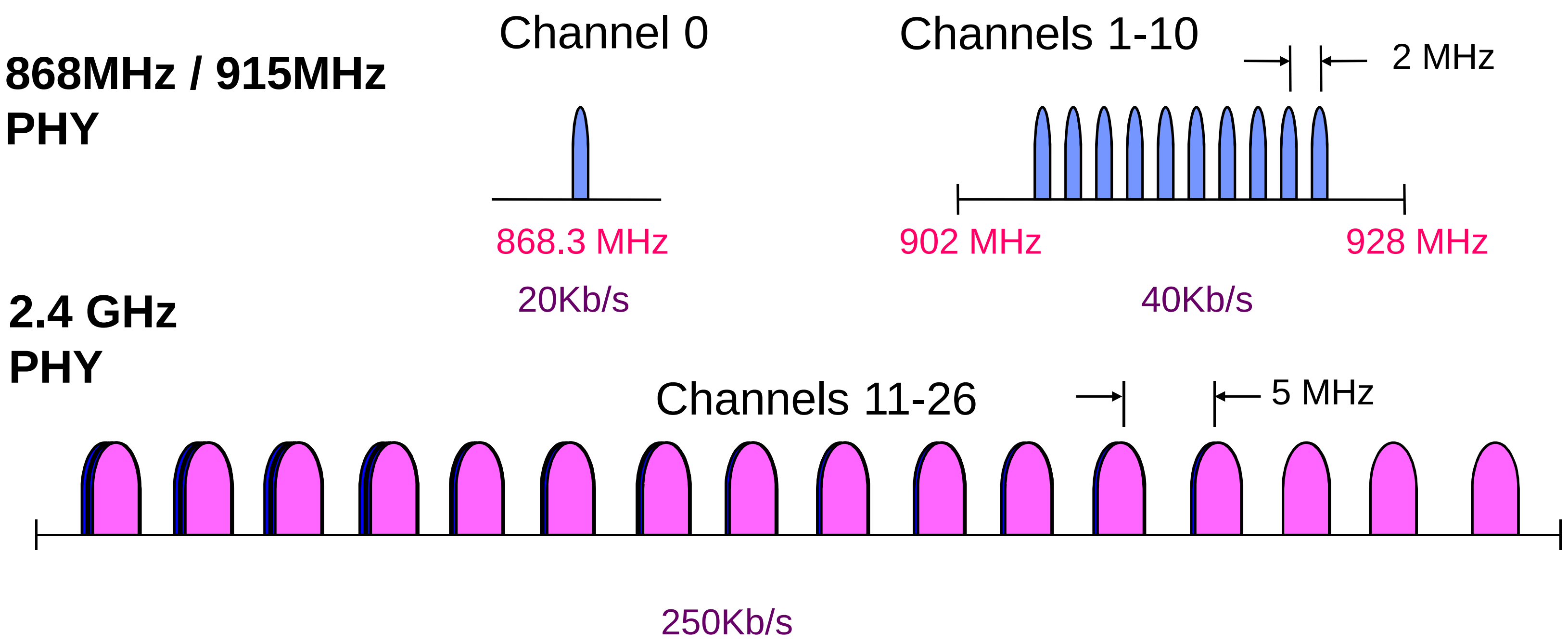
- Preamble (32 bits) - synchronization
- Start of packet Delimiter (8 bit)
- PHY Header (8 bits) – PPDU length
- PPDU (0 to 1016 bits) – Data field



PHY Overview

The radio shall operate at one of the following license free bands:

- 868-868.6 MHz (e.g., Europe)
- 902-928 MHz (e.g., North America) or
- 2400-2483.5 MHz (worldwide)



Protocol Objectives

- Extremely low cost
- Ease of installation
- Reliable data transfer
- Short range operation
- Reasonable battery life

MAC Overview

- Star and peer-to-peer topologies
- Optional frame structure
- Association
- CSMA-CA channel access mechanism
- Packet validation and message rejection
- Optional guaranteed time slots
- Guaranteed packet delivery
- Facilitates low-power operation
- Security

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

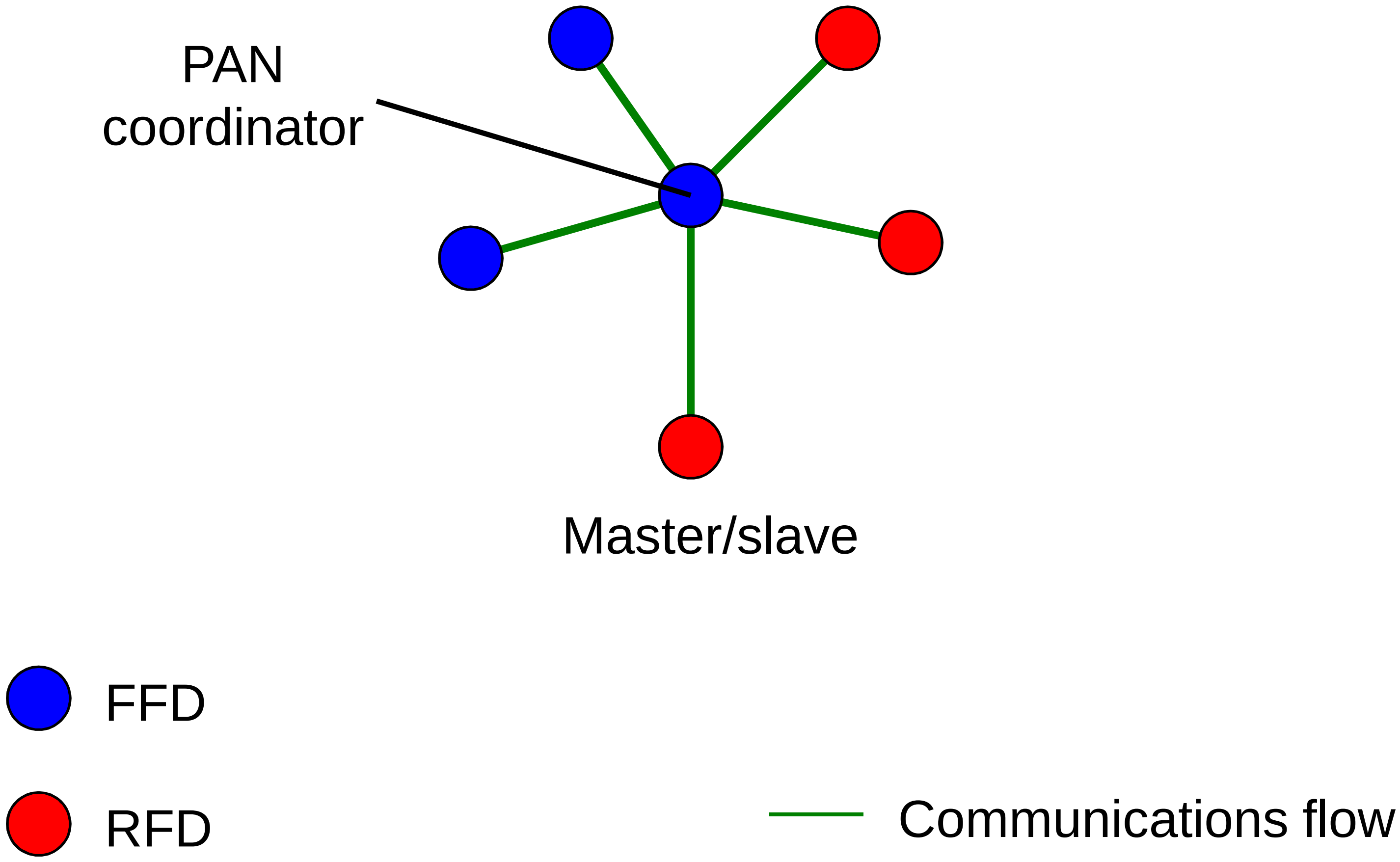
IEEE 802.15.4 Definitions

- Network Device: An RFD or FFD implementation containing an IEEE 802.15.4 medium access control and physical interface to the wireless medium.
- Coordinator: An FFD with network device functionality that provides coordination and other services to the network.
- PAN Coordinator: A coordinator that is the principal controller of the PAN. A network has exactly one PAN coordinator.

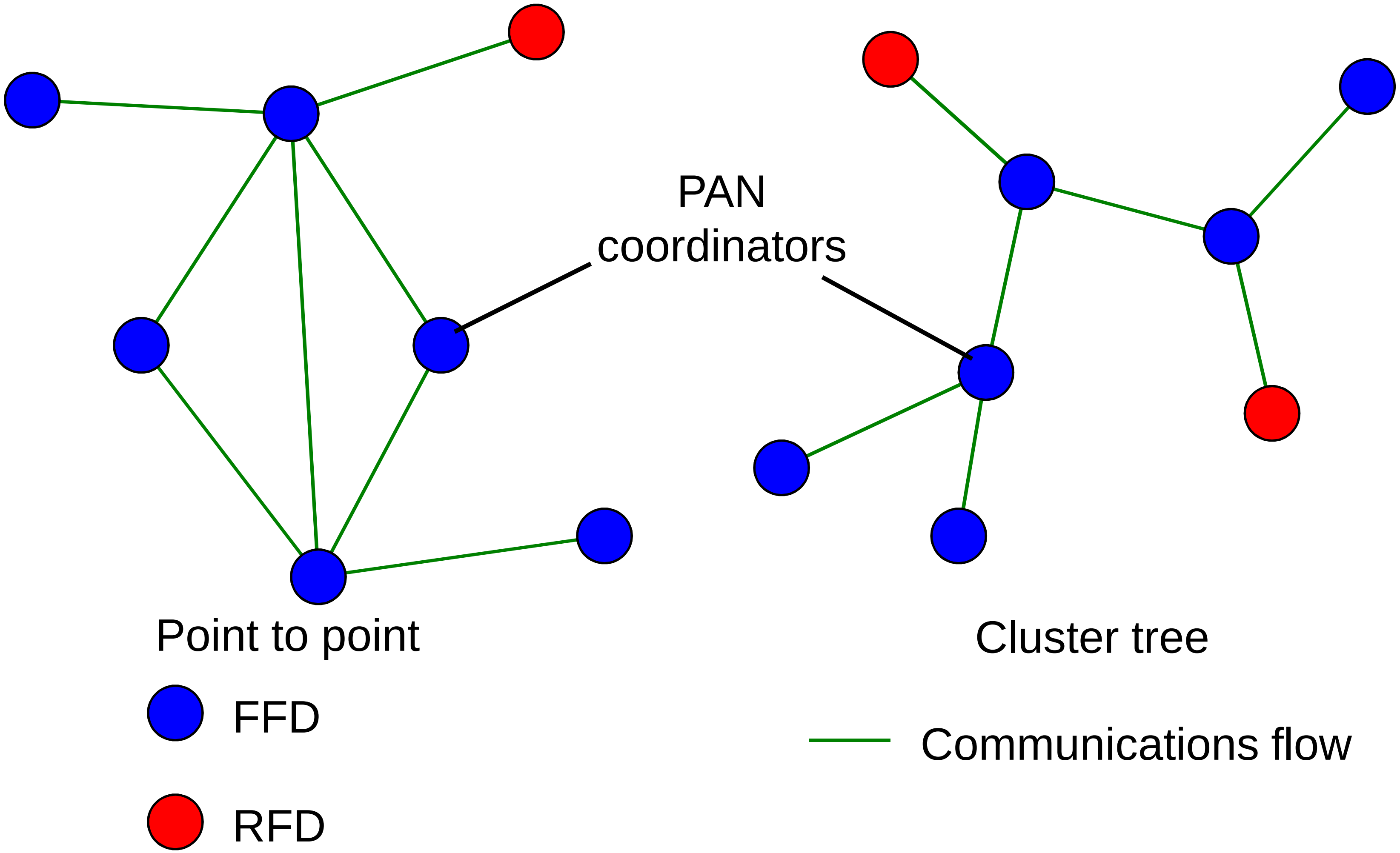
Low-Power Operation

- 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

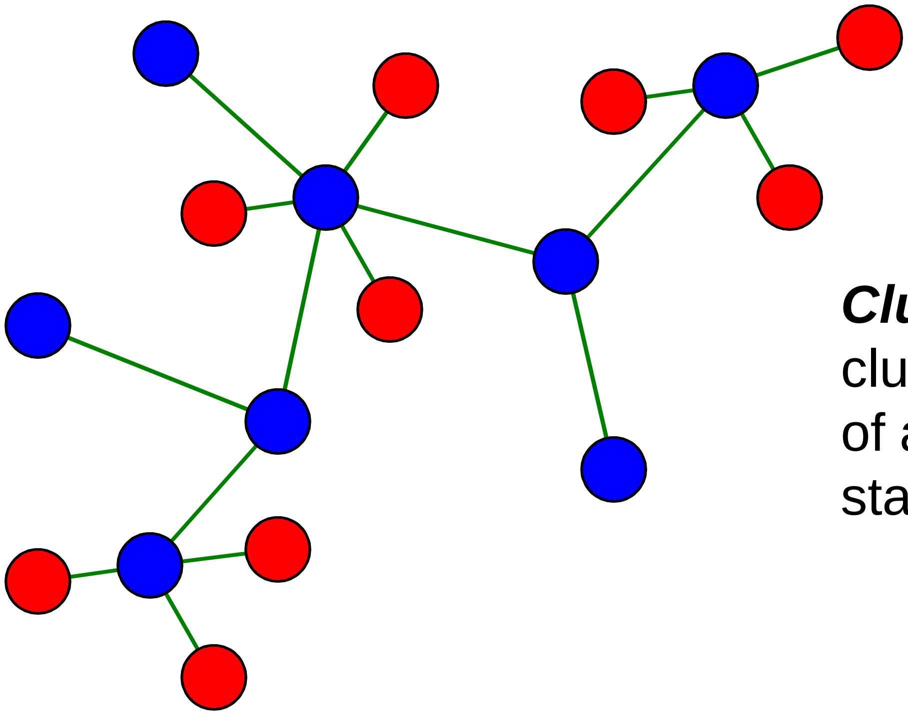
Star Topology



Peer-Peer Topology



Combined Topology



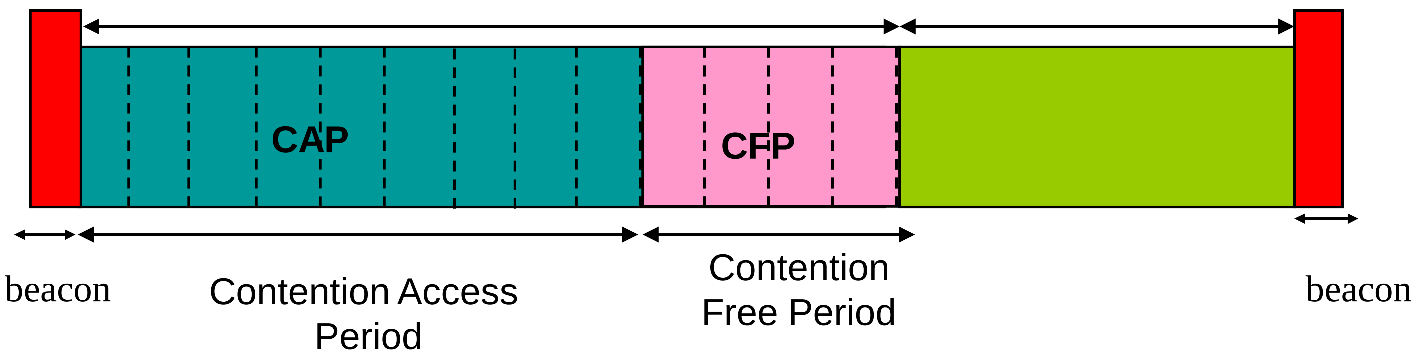
Clustered stars - for example, cluster nodes exist between rooms of a hotel and each room has a star network for control.

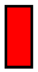
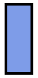
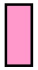
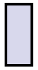
FFD

RFD

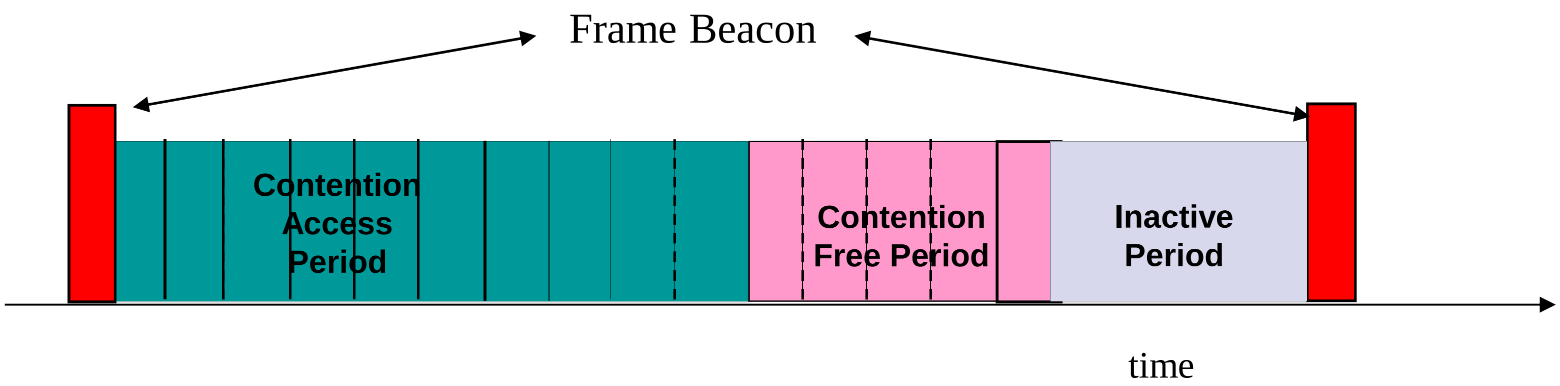
Communications flow

Optional Superframe Structure



Network beacon		Transmitted by network coordinator. Contains network information, frame structure and notification of pending node messages.
Contention period		Access by any node using CSMA-CA
Guaranteed Time Slot		Reserved for nodes requiring guaranteed bandwidth
Inactive Period		Sleep period

Guaranteed Time Slot (GTS)



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

Frame control field

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**

- Command Frame Types
  - Association request
  - Association response
  - Disassociation notification
  - Data request
  - PAN ID conflict notification
  - Orphan Notification
  - Beacon request
  - Coordinator realignment
  - GTS request

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**

Data Service

- Data transfer to neighboring devices
  - Acknowledged or unacknowledged
  - Direct or indirect
  - Using GTS service
- Maximum data length (MSDU) *aMaxMACFrameSize* (102 bytes)

IEEE 802.11.AH

IEEE 802.11ah

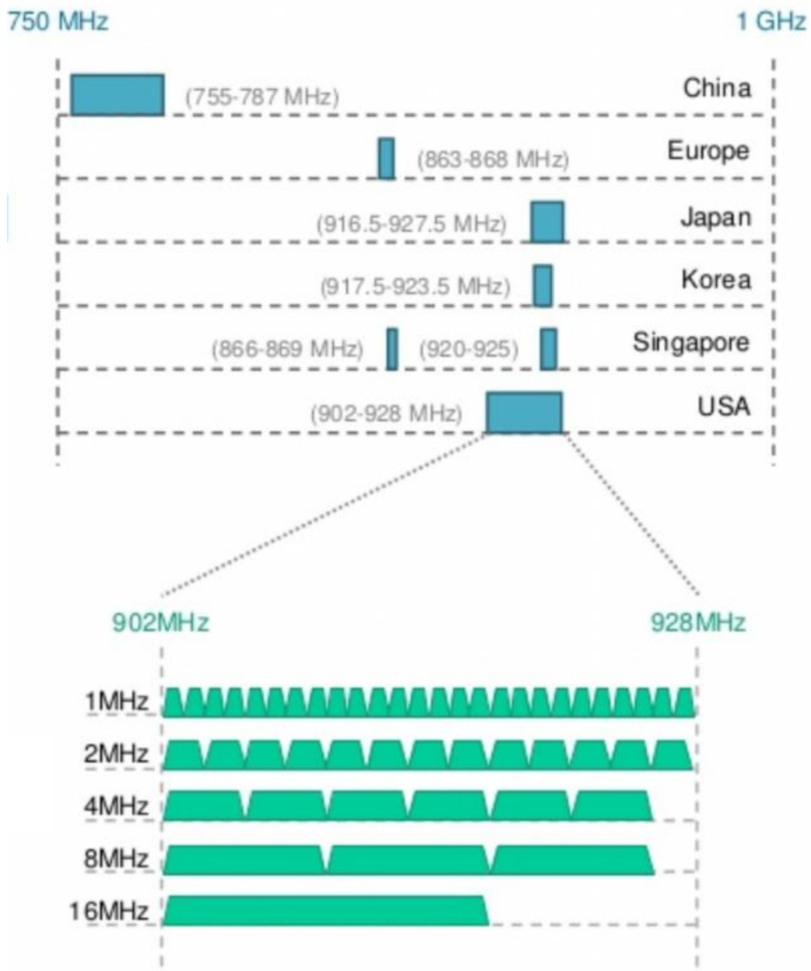
- Defines an OFDM PHY operating in the ISM band below 1GHz.
- Enhancements to the IEEE802.11 MAC to support this PHY.
  - Transmission rate up to 1 km
  - Data rates > 100kbps
  - Support up to 8196 connected devices

Advantages of transmitting in sub 1 GHz

- Spectrum characteristics
  - Good propagation and penetration
  - Large coverage area in one hop reach
- Reliability
  - Less congested frequency band
  - High sensitivity and link margin
  - Available diversity (frequency, time, space)
- Battery operation
  - Longer battery life
  - Short data transmission

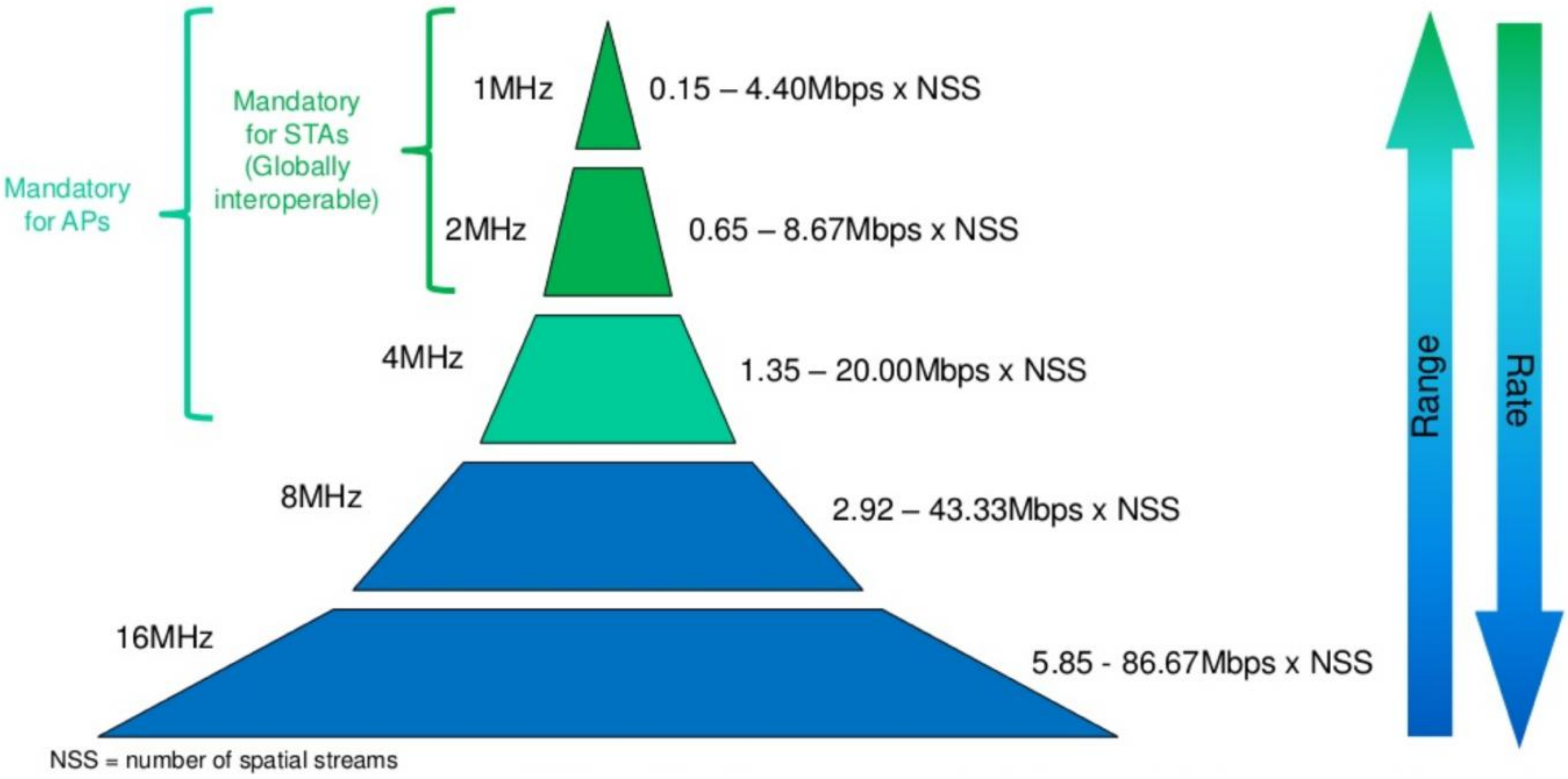
IEEE 802.11ah: Channelisation

- Each regulatory domain defines a different band and different tx power limits.
- Configurable bandwidth (channel bonding) of: 1, 2, 4, 8 and 16MHz



IEEE 802.11ah: Throughput and coverage

- Expected throughput vs. coverage



IEEE802.11ah: MAC (1)

- Need to reduce overhead: low data rates + short frames
- Short MAC headers:
  - Removed fields (Duration, QoS control, HT control, optionally Sequence control)
  - Option to use only two addresses instead of three
    - Option to use 2B AIB instead of 6B MAC address
  - E.g
    - Legacy: 100MB of data + 36B of header + FCS → 26% overhead
    - 11ah short MAC header: 100B of data + 14B of header + FCS → 12% overhead

IEEE802.11ah: MAC (2)

- Short Beacons
  - Beacons are sent frequently at the lowest rate → short (more frequent) and full beacons (less frequent).
- Implicit acknowledgment (no ACK needed)
  - Reduces channel access attempts, number of frames exchanged → increases channel efficiency, battery lifetime

IEEE802.11ah: MAC (4)

- Support thousands of associated devices (increases coverage → increases reachable STAs)
  - Legacy 802.11 limited to 2007 assocatied STAs
  - 11ah increases to ~8000

IEEE802.11ah: MAC (5)

- Thousands of STAs → huge collision probability
  - Restricted Access Windows:
    - Divide STAs into groups
    - Split channel access into time slots
    - Assign slots to group (AP indicates RAW allocation and slot assignments in its Beacons)
    - Different backoff rules apply during RAW (due to different contention conditions)

Long Range Radio (LoRa)

- Wireless Technology mainly targetting M2M and IoT Networks.
- Range-2.5 Km in dense urban and 15 km in suburban areas.
- Frequency band: ISM 868-915MHz
  - Standard: 802.15.4g
- Supports thousands of nodes.
- Longer Battery Life (Several Hours)

Summary