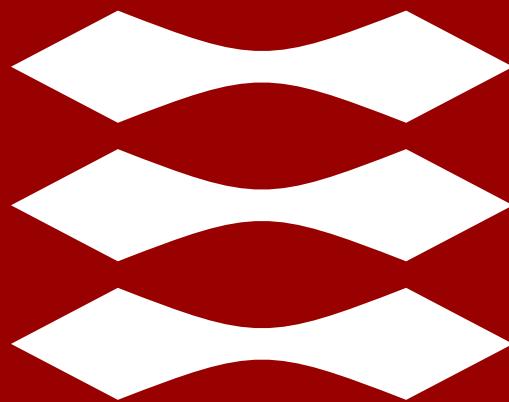


**DTU**



02116/02226 - Networked Embedded Systems

# Week 8: Wireless Networked Embedded Systems

**Charalampos (Haris) Orfanidis**

Assistant Professor

chaorf@dtu.dk

[www.compute.dtu.dk/~chaorf](http://www.compute.dtu.dk/~chaorf)

Slides by Xenofon (Fontas) Fafoutis

# Wireless vs Wired Embedded Systems

- Wireless Networked Embedded Systems
  - Necessary in mobile embedded systems (wearables, vehicles)
  - Necessary for embedded systems that are deployed in areas without easy access to infrastructure
  - Generally, cheaper, more flexible, and easier to install
  - They can be reliable and secure, but...
- Wired Networked Embedded Systems
  - More reliable (less vulnerable to interference and environmental noise)
  - More secure (less vulnerable to physical attacks)



# Basics of Wireless Communications

- Transmission
  - The radio transmitter generates an electric current and supplies it to the antenna
  - The antenna radiates energy as an electromagnetic wave (radio wave)
  - Data are encoded in the physical properties of the radio wave (frequency, phase, etc)
- Reception
  - The antenna produces an electric current based on the electromagnetic waves that reach it
  - The radio receiver processes filters and amplifies the signal, and recovers the transmitted data via demodulation



# Radio Waves and Decibels

- As a radio wave propagates through 3D space its power attenuates very fast (exponentially)
  - Analogy: An balloon becoming thinner as it expands
  - Example: signal is transmitted at 0.2 W and reaches the receiver with power 0.1 pW
  - Result: The power of radio signals has a huge dynamic range
- Power is typically expressed in Decibels (dB)
  - A relative unit in logarithmic scale
  - Expresses how big or small is something with respect to some reference
- dB arithmetic
  - Addition in logarithmic domain is multiplication in linear domain
  - Rules of thumb
    - +3 dB approximately equal to x2
    - -3 dB approximately equal to /2
    - +10 dB approximately equal to x10
    - -10 dB approximately equal to /10

$$P_{dB} = 10 \log_{10} \frac{P}{P_o}$$

Q: +17dB is approximately equal to?

# Radio Waves and Decibels

- As a radio wave propagates through 3D space its power attenuates very fast (exponentially)
  - Analogy: A balloon becoming thinner as it expands
  - Example: signal is transmitted at 0.2 W and reaches the receiver with power 0.1 pW
  - Result: The power of radio signals has a huge dynamic range
- Power is typically expressed in Decibels (dB)
  - A relative unit in logarithmic scale
  - Expresses how big or small is something with respect to some reference
- dB arithmetic
  - Addition in logarithmic domain is multiplication in linear domain
  - Rules of thumb
    - +3 dB approximately equal to x2
    - -3 dB approximately equal to /2
    - +10 dB approximately equal to x10
    - -10 dB approximately equal to /10

$$P_{dB} = 10 \log_{10} \frac{P}{P_o}$$

Q: +17dB is approximately equal to?

A:  $+17\text{dB} = +10\text{dB} + 10\text{dB} - 3\text{dB} = 10 \times 10 / 2 = \times 50$

# Decibels: Typical Power References

- Amplification/Attenuation Processes
  - The output power is expressed with reference to the input power
  - Example: A 3dB power amplifier doubles the power of the signal it receives

$$P_{dB} = 10 \log_{10} \frac{P_{OUT}}{P_{IN}}$$

- Absolute Power
  - The power is expressed with reference to 1mW (dBm)
  - Example: A -10dBm signal has power that is  $\sim 1/10$  of the power of 1mW, or  $\sim 0.1\text{mW}$

$$P_{dB} = 10 \log_{10} \frac{P}{1\text{mW}}$$

- Combination
  - If I amplify a -10dBm signal using a 3dB amplifier, I get:  
 $-10\text{dBm} + 3\text{dB} = -7\text{dBm} (\sim 0.2\text{mW})$

Power	Example
296 dBm	Power output of the sun
80 dBm	Transmission power of FM radio station
60 dBm	Radiated power of microwave ovens
30 dBm	Maximum transmission power of a Wifi router
27 dBm	Maximum transmission power of a cellular phone
0 dBm	Typical transmission power of small embedded systems
-20 dBm	Received signal power of WiFi at very short distance
-100 dBm	Minimal received signal power of WiFi
-174 dBm	Thermal noise

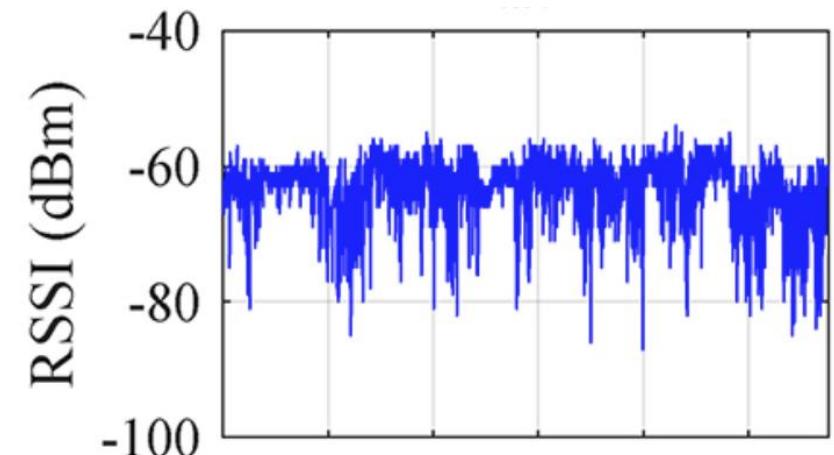
# Link Budget

- A received signal power approximator:  $P_{RX} = P_{TX} + G_{TX} - L_{TX} - L_P + G_{RX} - L_{RX}$  where:
  - $P_{RX}$  is the received power (dBm)
  - $P_{TX}$  is the transmission power (dBm)
  - $G_{TX}$  is the transmitter antenna gain (dBi)
  - $L_{TX}$  is the transmitter losses: cables, connectors, etc (dB)
  - $L_P$  is the path loss (dB)
  - $G_{RX}$  is the receiver antenna gain (dBi)
  - $L_{RX}$  is the receiver losses: cables, connectors, etc (dB)
- The path loss ( $L_P$ ) depends on:
  - The distance between transmitter and receiver
  - The frequency of the signal
  - The propagation environment
- The Received Signal Strength Indicator (RSSI) can be used to estimate the path loss



# Path Loss

- Path Loss is very predictable in free space, but very dynamic down on Earth!
- Multipath fading
  - A wireless signal reflects on surfaces or the air
  - Multiple rays reach the receiver
  - Rays may arrive with small delays due to longer travel paths (phase shifts)
  - Rays may interfere constructively or destructively
- Shadowing
  - Obstacles in between can attenuate signals
  - Metallic objects block completely the signals
- Path loss is very dynamic even when the transmitter and receiver are static (constant distance)
  - Figure shows the RSSI of a static link in an office environment during working hours



# Antenna Gain

- Antennas are passive components
  - They do not amplify the signal
  - They reshape the signal sending/receiving more energy in some directions than others
- Isotropic Antenna
  - A theoretical antenna that emits/collect energy equally in all 3D directions
  - Used as reference for directivity
- Directivity
  - Real-world antennas emit/collect more energy at some locations
  - Measured as peak power gain relative to isotropic antenna (dBi)
  - High directivity means high gain in one direction, but low gain in all others!
    - Low directivity is good when source location is unknown (e.g. mobility)
    - High directivity is good when source location is known (e.g. P2P links)
  - Antenna Gain is directivity minus losses

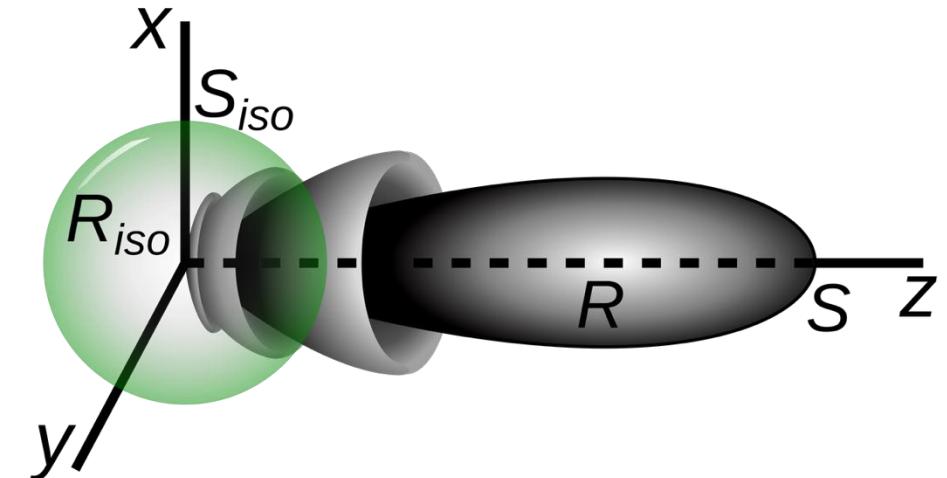


Image source: Wikipedia

# Connecting Antennas to Radios

- External Antennas
  - Connect to the PCB via SMA or u.FL connectors
- Printed Antennas
  - Copper trace printed on the PCB
- Matching Circuit
  - Maximise power emitted
  - Minimise power reflected back
- Balun
  - Chip that converts the balanced output of a specific radio to unbalanced input for an antenna
  - With integrated matching circuit
- Some radios have integrated balun so you just connect the antenna

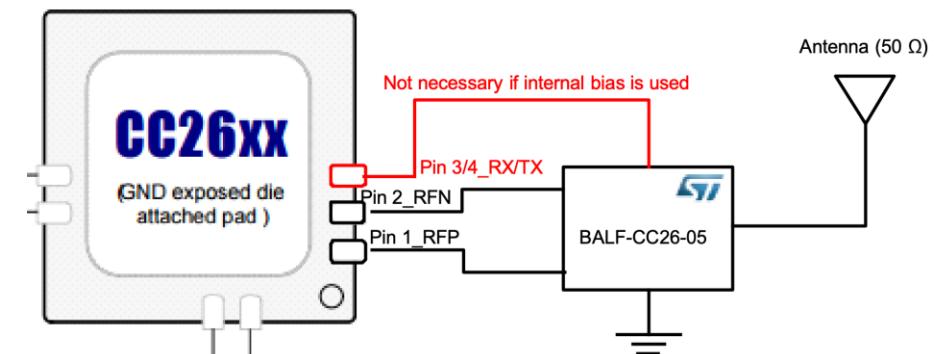
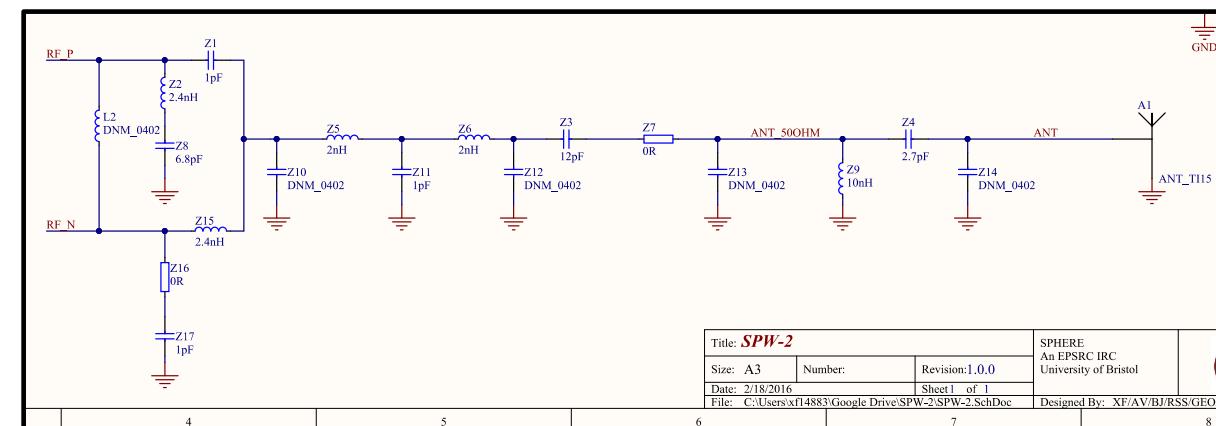
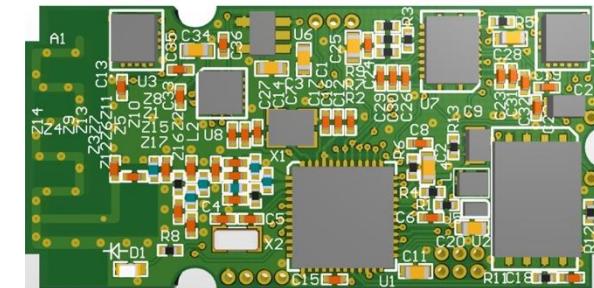


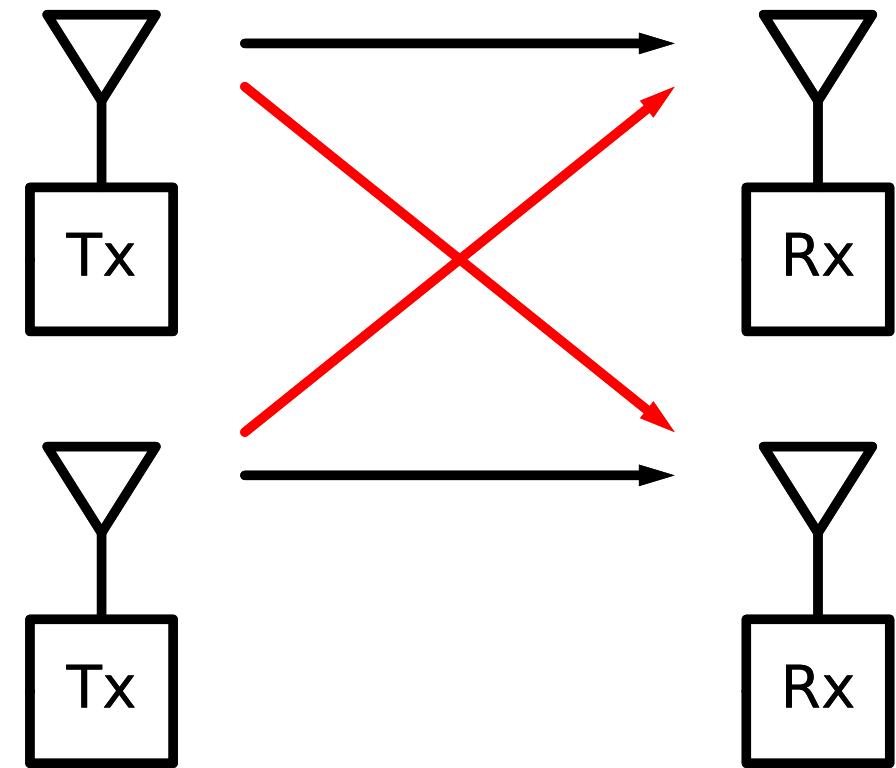
Image source: BALF-CC26-05D3 Datasheet by STMicroelectronics (bottom)

# Requirements for a Successful Reception

- There are two requirements for successful packet reception
- The received signal needs to be sufficiently powerful to be perceived by the receiver
  - A radio receiver typically has a sensitivity threshold, e.g. -97dBm
  - It is the lowest signal power level from which the receiver can extract information
  - If the received signal is weaker, the receiver will perceive the signal as noise
- The received signal needs to be sufficiently more powerful than the sum of any external interference signals also captured by the receiver antenna
  - External interference can introduce bit errors in the decoding process
  - Wireless environments are exposed to interference so typically received power higher than the sensitivity is required for robust communication

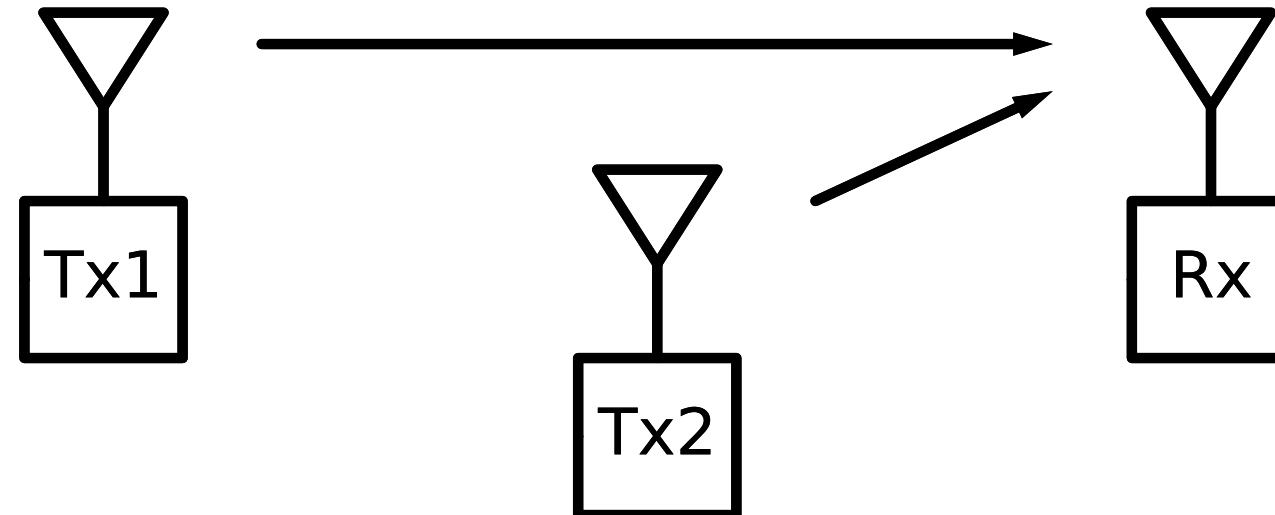
# Interference

- Wireless Interference
  - All wireless signals are broadcasted in the environment
  - Receivers collect all of them
  - To successfully decode a signal, it must be sufficiently stronger than all others received
- Interference is subjective
  - A signal creates interference to others
  - Analogy: speaking/listening
- Sources of interference
  - Other transmitters of the same network
  - Transmitters from overlapping networks
  - Other electronics (microwaves, lights, etc)



# Capture Effect

- Assume two simultaneous packet transmissions from Tx1 and Tx2 with equal Tx power
- The closest transmission from Tx2 can be received without errors
  - From the perspective of Tx2 the interference is low
  - From the perspective of TX1 the interference is high



# Wireless Coverage

- Often simplified as a circle or a cell
- However, real world is not so simple
  - RSSI is very dynamic due to multipath fading and shadowing
  - Bit Error Rate (BER) is very dynamic due to interference
- Packet Error Rate (PER), depends on:
  - Transmission power and antennas
  - Distance
  - Environment
  - Interference
  - Transmission rate
  - Packet size

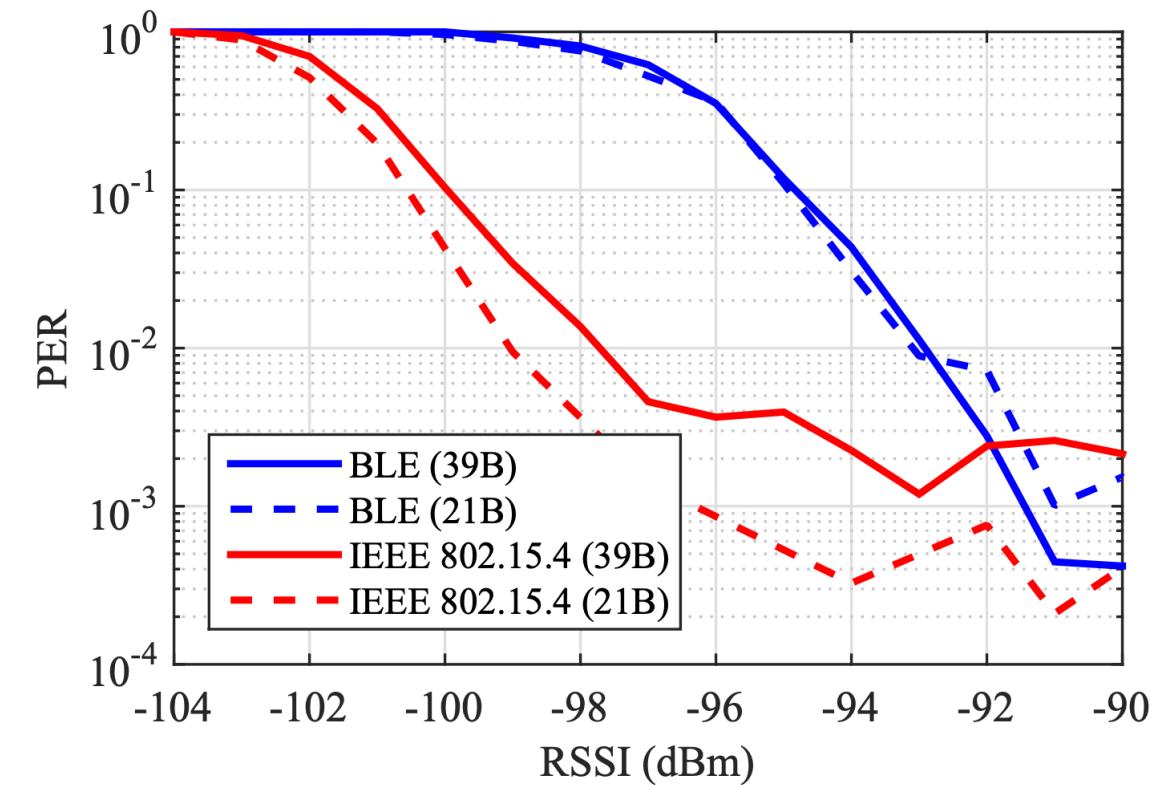


Image source: <http://dx.doi.org/10.4108/eai.1-12-2016.151713>

# Carrier Wave

- Information is encoded in the physical properties of a radio wave (amplitude, frequency, phase, etc)
- The modifications that represent '0' and '1' are done on top of a carrier wave with frequency  $f_c$
- Example: BFSK (Binary Frequency Shift Keying)
  - '0' is represented as  $f_c-f_0$
  - '1' is represented as  $f_c+f_0$
- Advantage:
  - Receiver can use a **bandpass filter** to filter out all signals that are not near the carrier wave
  - Limits interference to signals close to carrier frequency
  - Parallel interference-free transmissions in different frequencies

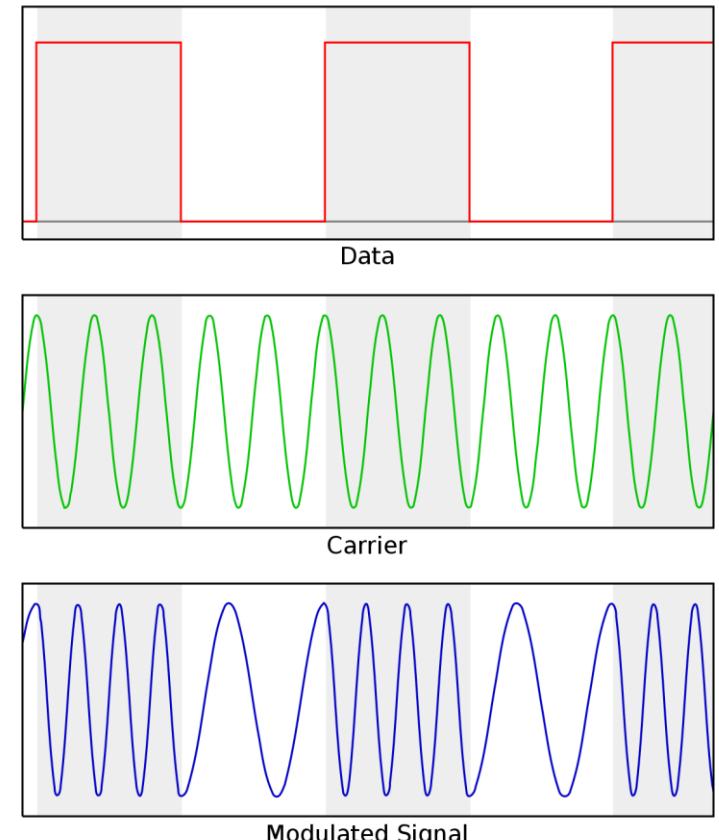


Image source: Wikipedia

# Frequency Band: Trade-offs

- Lower Frequency Band
  - Lower path loss
  - More obstacle penetration
  - More coverage
  - More interference
  - Less capacity for data
  - Lower bitrate
  - Bigger antennas
- Above visible light EM radiation is dangerous
- Digital systems typically communicate with radio waves and microwaves (300 MHz to 300 GHz)
  - 300 MHz - 1 GHz (Sub-GHz): UHF radar band
  - 1 GHz - 30 GHz: UHF and SHF bands
  - 30 GHz - 300 GHz (millimetre wave): EHF band

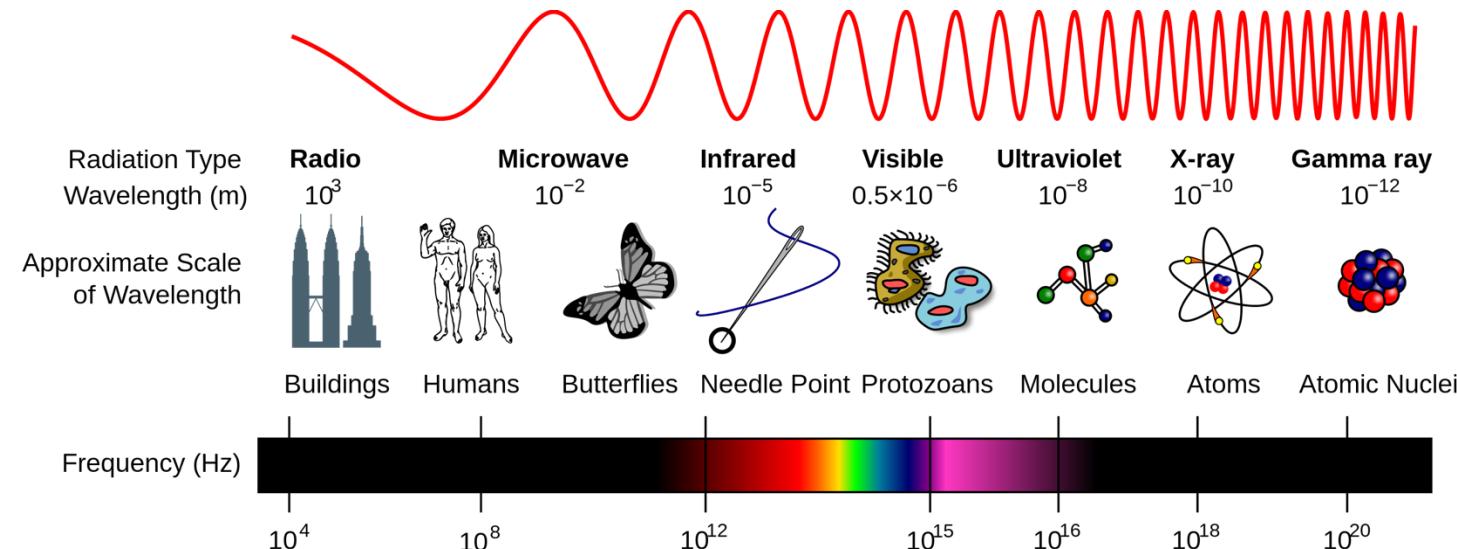


Image source: Wikipedia

# Frequency Bands: Rules

- Frequency bands are limited, thus regulated by governments
  - Who can use them
  - How often they can be used
  - What is the maximum transmission power
- Licensed bands
  - Illegal to transmit unless you have a license
  - Government, aviation, military, etc
  - Rented to telecom providers (cellular)
- Unlicensed bands
  - OK to use without a license
  - ISM (industrial, scientific and medical) by ITU (International Telecommunication Union)
  - 863-870 MHz band in Europe

Frequency range	Availability	
6.765 MHz	6.795 MHz	Subject to local acceptance
13.553 MHz	13.567 MHz	Worldwide
26.957 MHz	27.283 MHz	Worldwide
40.66 MHz	40.7 MHz	Worldwide
433.05 MHz	434.79 MHz	Europe, Africa, Middle East
902 MHz	928 MHz	North/South America
2.4 GHz	2.5 GHz	Worldwide
5.725 GHz	5.875 GHz	Worldwide
24 GHz	24.25 GHz	Worldwide
61 GHz	61.5 GHz	Subject to local acceptance
122 GHz	123 GHz	Subject to local acceptance
244 GHz	246 GHz	Subject to local acceptance

# Wireless Channels

- We can further split a band in channels
- Overlapping Channels
  - Interfere with each other
- Orthogonal Channels
  - Do not interfere with each other
- FDMA (Frequency Division Multiple Access)
  - Transmitters can transmit in parallel at different orthogonal channels without interfering with each other

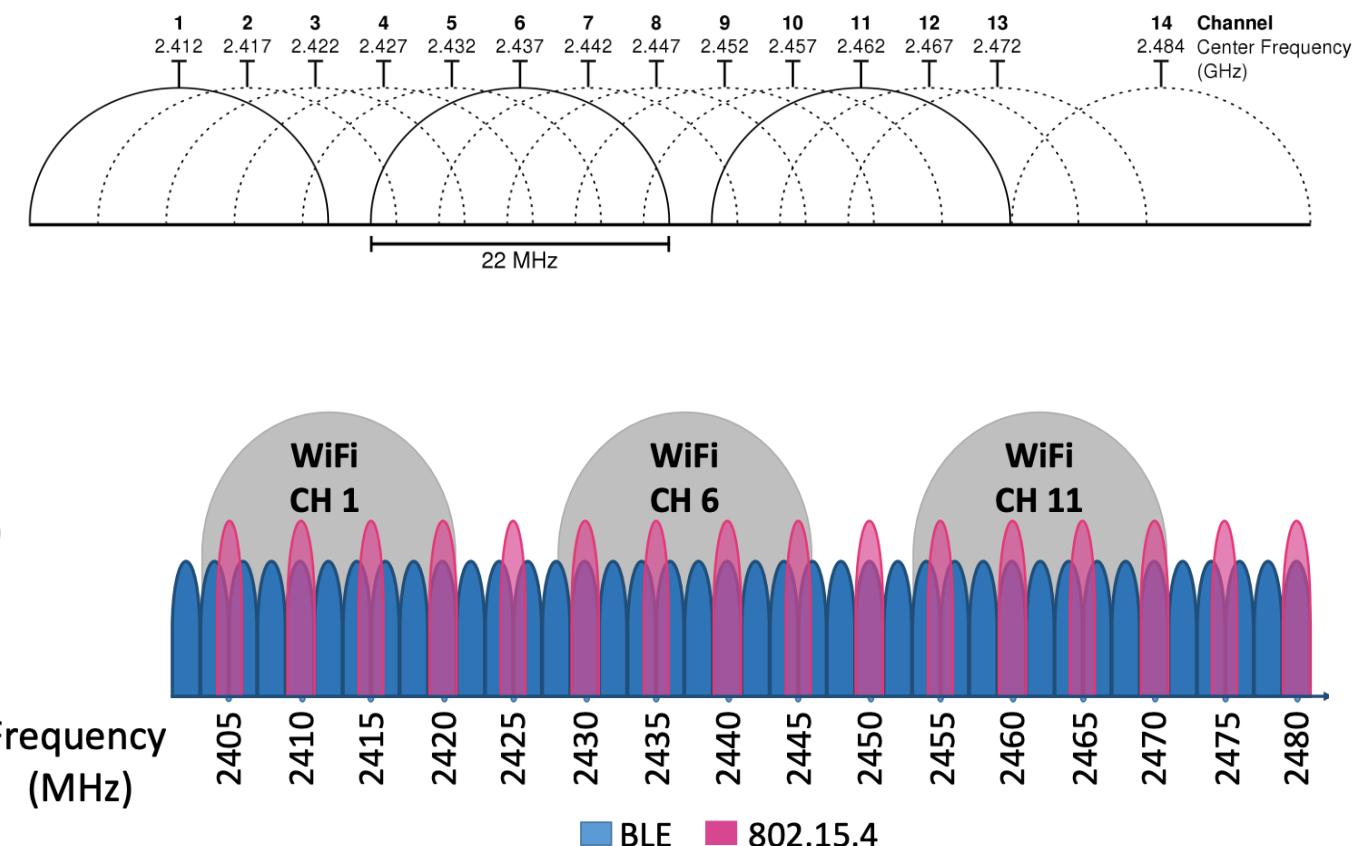
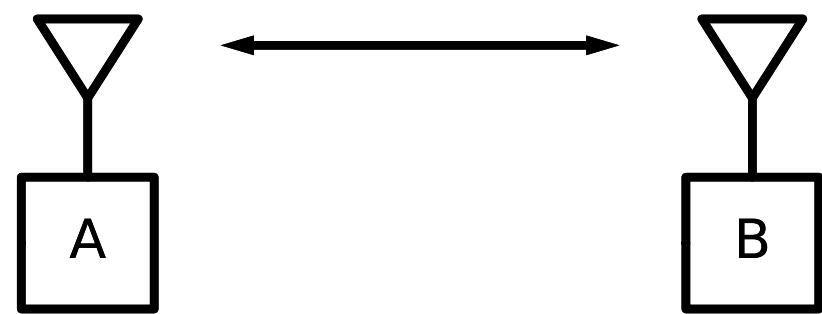


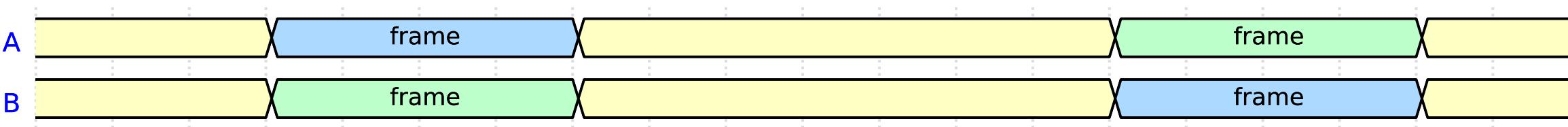
Image source: Wikipedia (top) and <https://doi.org/10.1109/PIMRC.2017.8292262> (bottom)

# Radio States

- The receiver filters, amplifies and decodes an incoming signal
  - Each frame starts with a preamble (i.e., a synchronisation phrase)
  - Receive (receive data) and Listen (receive noise) are the same state
- Wireless radios have two modes: Transmit and Receive
  - Devices cannot receive while they transmit
  - Collisions cannot be detected as they happen
  - Devices need to be in receive mode when idle to detect incoming frames

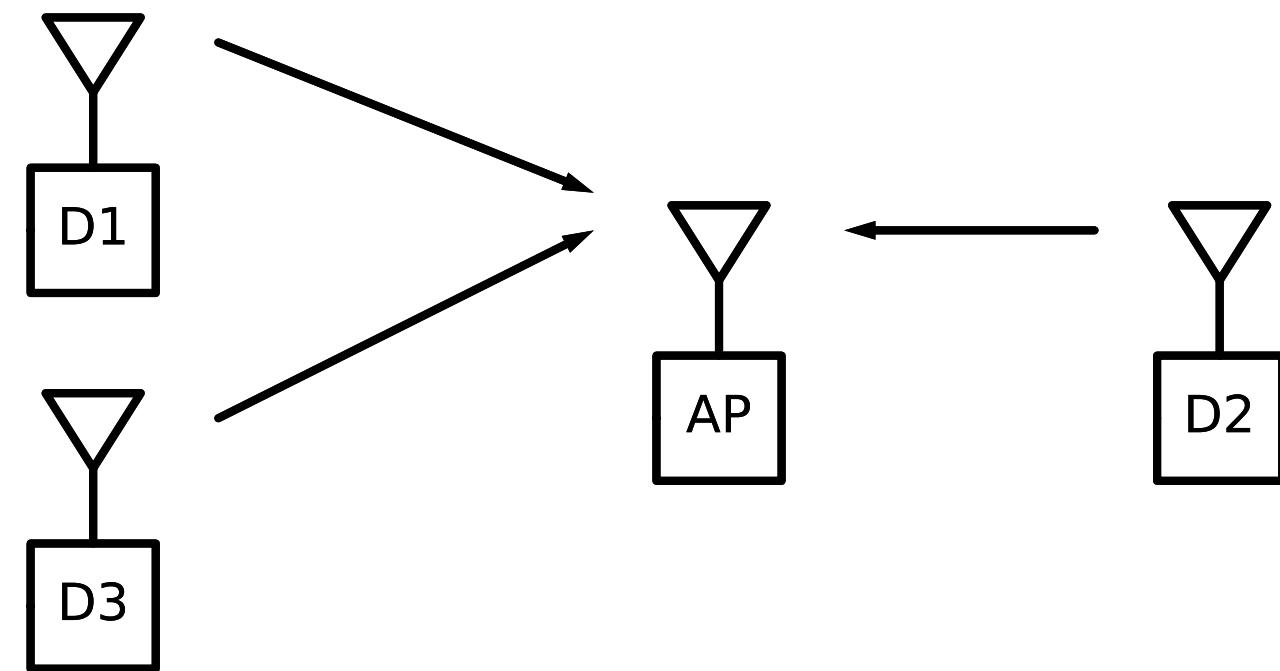


Blue: transmit  
Green: receive  
Yellow: listen

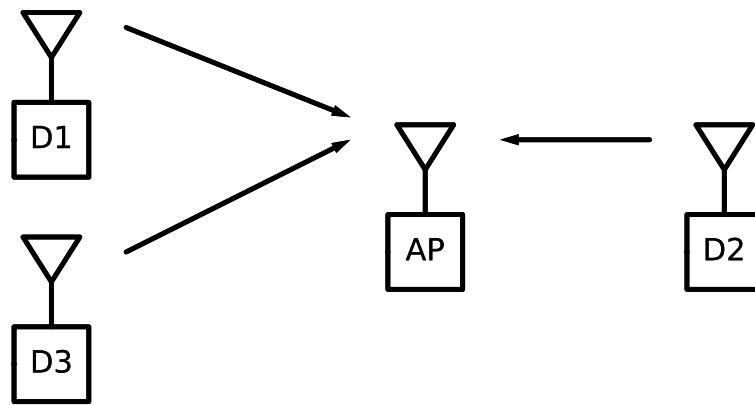


# Medium Access Control: Sharing a Channel

- Star Topology
- Access Point (AP)
  - One node collects data or bridges the wireless network to the wired
  - Aka Sink or Gateway (GW)
- Wireless devices talk directly to the AP
- Vulnerable to collisions and interference
- Overlapping networks can use a different channel to mitigate interference

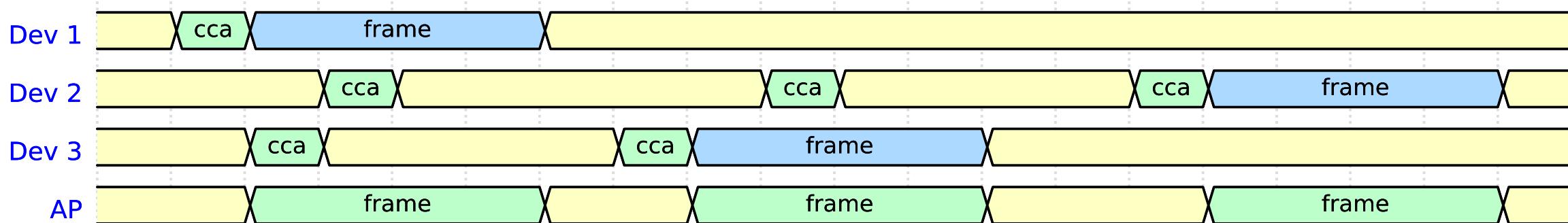


# CSMA/CA

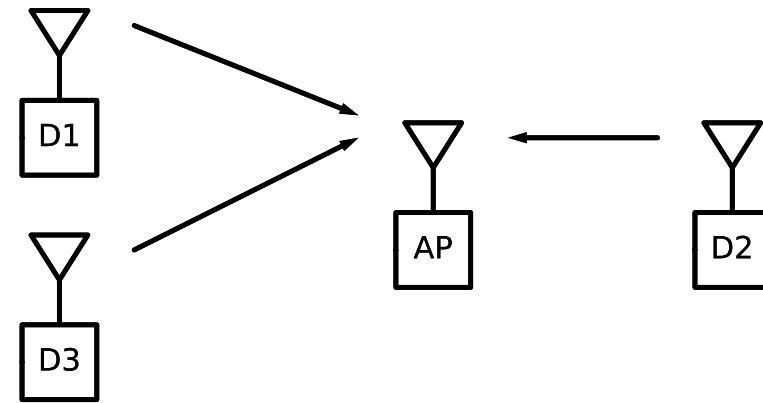


- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)
  - Sense the channel before transmitting (Clear Channel Assessment, CCA)
  - If channel free, transmit
  - If channel busy, wait some time randomly before attempting first transmission
    - Binary exponential backoff
- Used by IEEE 802.11 (WiFi)

Blue: transmit  
Green: receive  
Yellow: listen

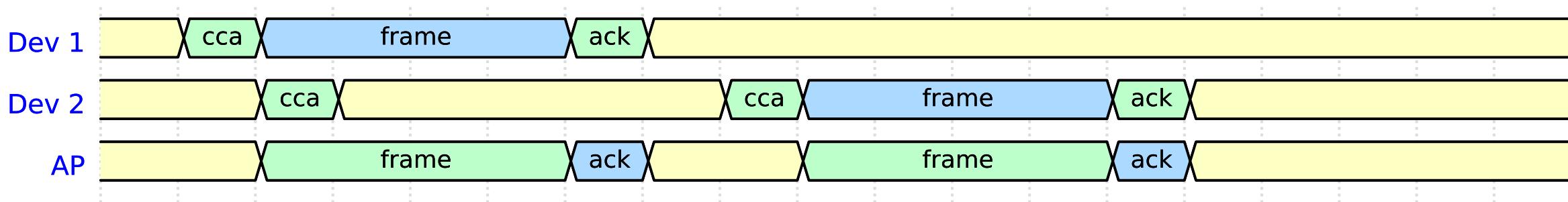


# Acknowledgements



- Channel errors are more likely than wired networks
  - CA reduces the probability of collisions, but collisions can still happen
  - Interference from other nodes of the same network, other overlapping networks, etc
  - Signal might arrive weaker due to environmental issues, such as an obstacle
- Acknowledgements (ACK) at the end of each frame
  - If no ACK, retransmit
  - If maximum number of retransmission attempts reached, drop frame

Blue: transmit  
Green: receive  
Yellow: listen



# Radio Duty Cycle

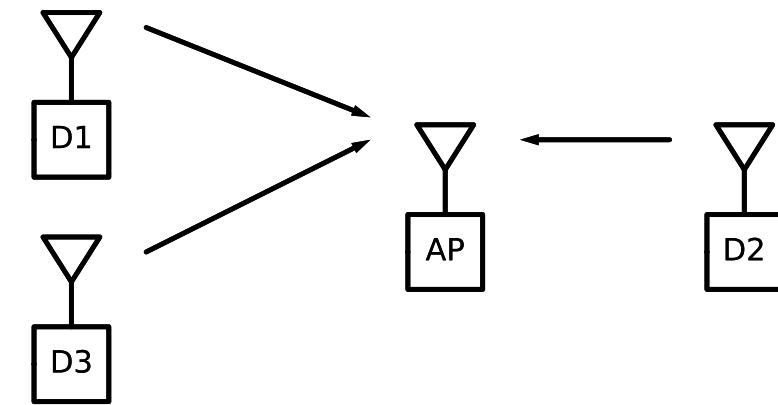
- Often devices have energy constraints
  - Battery-powered
  - Energy Harvesting
- The radio consumes a lot of energy when active (i.e. TX or RX mode)
  - Listening requires the same power as receiving
  - Idle listening wastes energy resources
- Solution: Radio Duty Cycle
  - Turn radio off when not used
  - Radio has three states (TX, RX, Sleep)
- Challenge
  - How does the receiver know when the transmitter is about to transmit, to wake up and put the radio in RX mode?

Radio RX <sup>(1)</sup>	5.9	mA
Radio RX <sup>(2)</sup>	6.1	
Radio TX, 0-dBm output power <sup>(1)</sup>	6.1	
Radio TX, 5-dBm output power <sup>(2)</sup>	9.1	

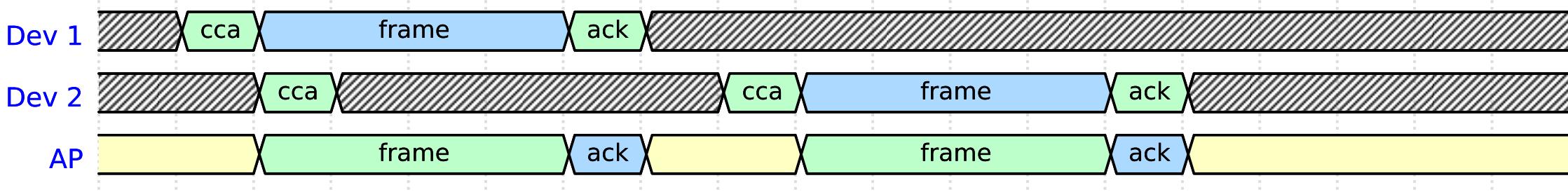
Image source: CC2650 Datasheet by Texas Instruments

# Asymmetric Energy Availability

- Star Topology
  - The AP/GW is mains-powered (no energy limitations)
  - The wireless device are energy-constrained and need to be duty cycled
- MAC Protocol: Duty-Cycled CSMA
  - AP/GW always in RX mode unless it transmits (no duty cycle)
  - Nodes wake up when having data to transmit
    - If CCA succeeds, transmit packet and switch to RX mode waiting for the ACK
    - If CCA fails, go to sleep and try again later

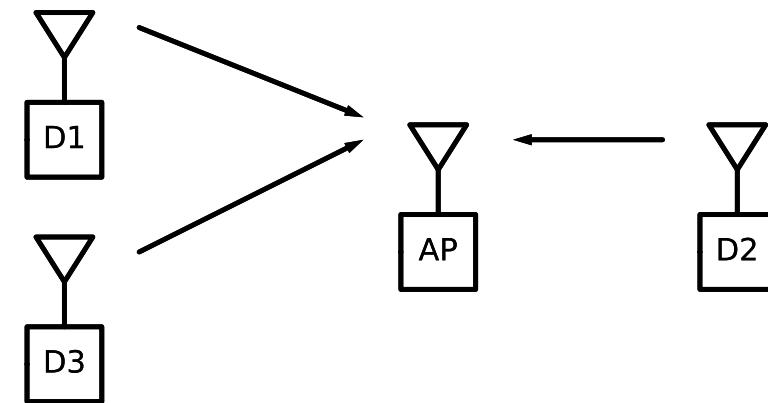


Blue: transmit  
Green: receive  
Yellow: listen  
Gray: sleep



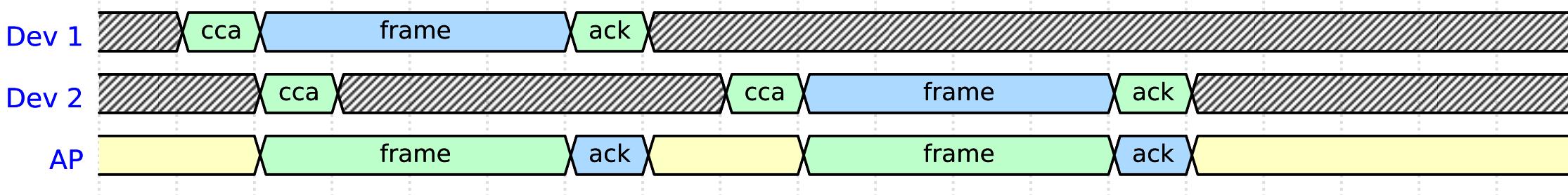
# Asymmetric Energy Availability

- Star Topology
  - The AP/GW is mains-powered (no energy limitations)
  - The wireless device are energy-constrained and need to be duty cycled
- MAC Protocol: Duty-Cycled CSMA
  - AP/GW always in RX mode unless it transmits (no duty cycle)
  - Nodes wake up when having data to transmit
    - If CCA succeeds, transmit packet and switch to RX mode waiting for the ACK
    - If CCA fails, go to sleep and try again later



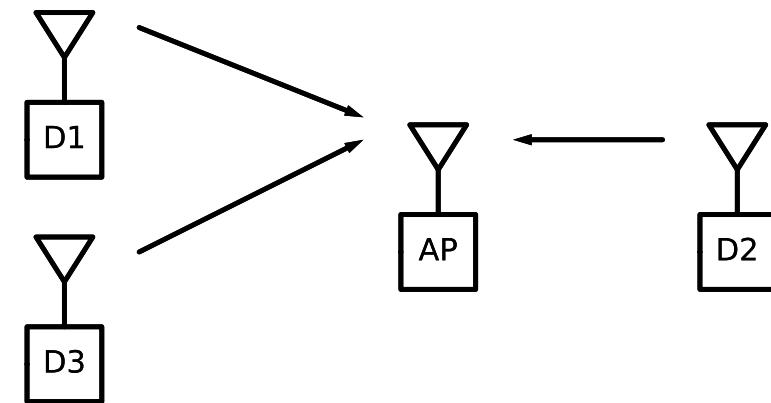
Blue: transmit  
Green: receive  
Yellow: listen  
Gray: sleep

Challenge: OK for uplink, but how does the AP send data to the devices?

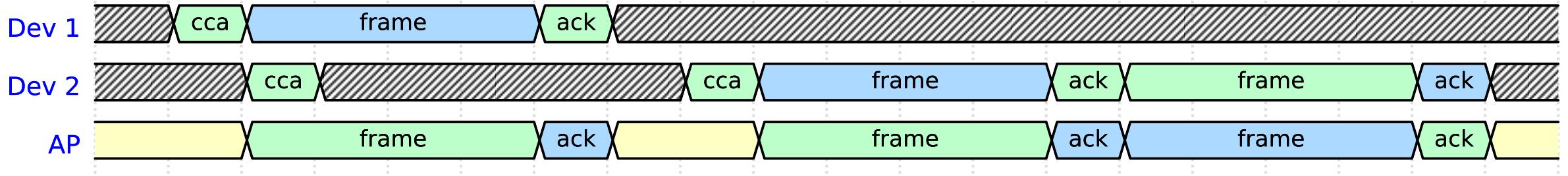


# Downlink Traffic

- Star Topology
  - The AP/GW is mains-powered (no energy limitations)
  - The wireless device are energy-constrained and need to be duty cycled
- MAC Protocol: Duty-Cycled CSMA Downlink
  - AP/GW cannot initiate a data transfer to duty-cycled nodes
  - AP/GW can request in the ACK the node to remain awake in RX mode (receive window)



Blue: transmit  
Green: receive  
Yellow: listen  
Gray: sleep



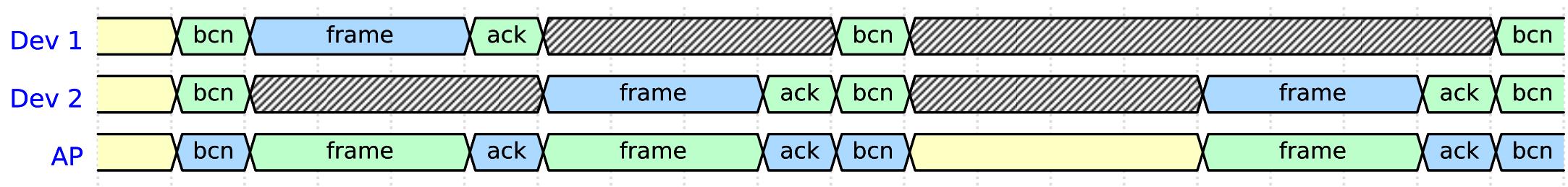
# Contention-based vs Contention-free MAC

- CSMA/CA is a contention-based MAC: devices compete for the medium
  - Efficient at low-medium traffic conditions and sporadic traffic
  - No guarantees that important devices will find the medium free
  - Many collisions at high traffic conditions
- Contention-Free MAC: transmission slots are allocated to specific devices
  - Efficient at high traffic conditions
  - Important devices are guaranteed to find the medium free
    - Still vulnerable to external interference
  - Inefficient at unpredictable traffic
    - When nothing to transmit, the allocated slots are wasted
  - Less flexible to changes, overhead with making the slot allocation
- Analogy: Car lanes vs Bus lanes

# Guaranteed Time Slots

- AP/GW transmits a beacon with a schedule indicating when each device can transmit
  - Devices transmit at their dedicated transmit slot
  - If nothing to transmit, the slot is idle
- TDMA (Time Division Multiple Access)
- When joining the network, a device needs to be in RX mode until it gets the first beacon

Blue: transmit  
Green: receive  
Yellow: listen  
Gray: idle

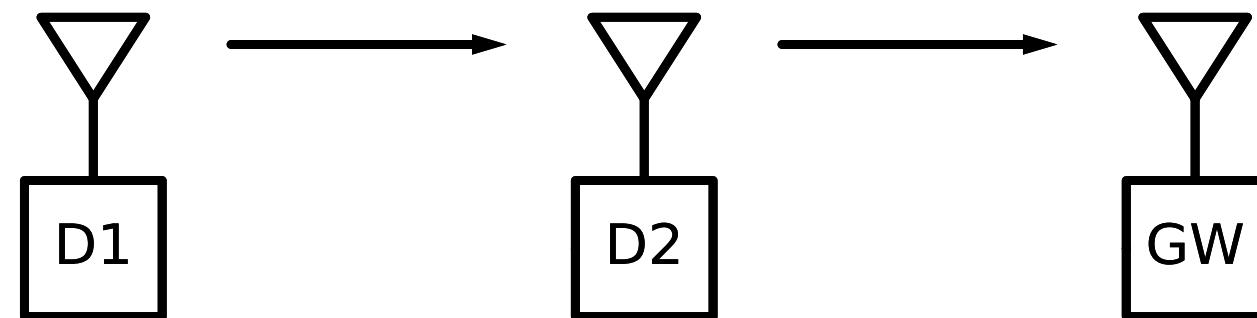


# Radio Duty Cycling with Asymmetric Energy Availability

- Advantages
  - Simple to implement and maintain
  - Very energy-efficient for end devices
  - Overhead of synchronisation falls on AP/GW
- Disadvantages
  - Can only be used when receiver has no energy constraints
  - Cannot support device-to-device and multi-hop topologies (mesh networks)
  - Delay for downlink traffic
- Variations of the paradigm used:
  - IEEE 802.15.4 (Zigbee, Thread)
  - BLE (Bluetooth Low Energy)
  - LoRaWAN
  - Low-Power WiFi

# Multi-hop Topology

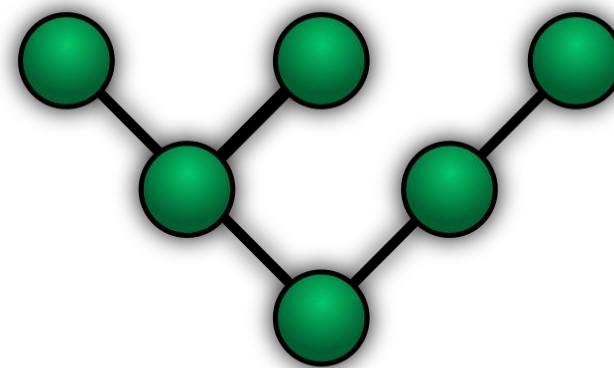
- A device may not have direct access to the gateway
  - Too far away
  - Too weak signal (e.g. basement)
- Coverage can be extended using multi-hop topologies
  - Normal nodes forward frames to the gateway on behalf of other nodes
  - Cost increase: A frame is transmitted/received multiple times to reach the GW
  - Cost decrease: Short links are more robust than long links (retransmissions are reduced)



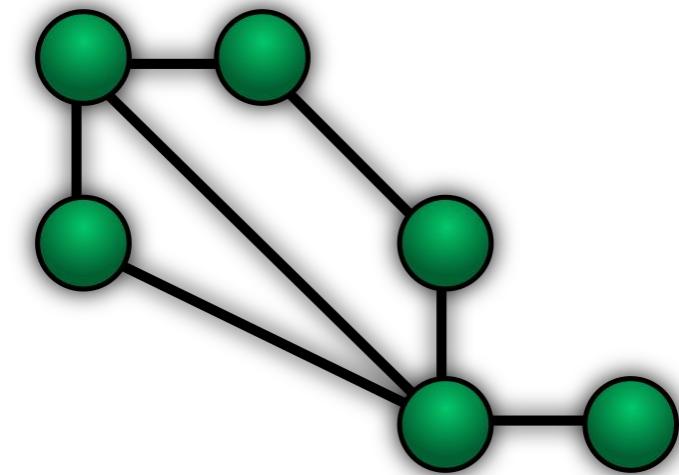
# Types of Multi-Hop Topologies



**Line**



**Tree**



**Mesh**

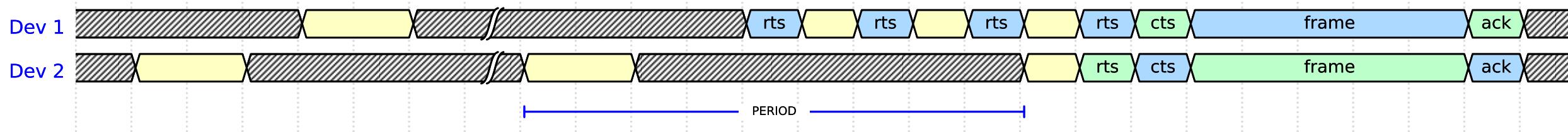
# Symmetric Energy Limitations

- Both the transmitter and the receiver need to duty cycle their radios to preserve energy
- Typical in multi-hop topologies (line, tree or mesh topologies)
- Also in star topologies when the GW is battery-powered
- Example: Walkie-Talkie
  - Alice and Bob want to communicate with two battery-powered walkie-talkies
  - When powered on, the walkie-talkie is in listen mode, user presses button to speak
  - They both want to keep them off as much as possible to preserve their batteries
  - Before they separate, they have the opportunity to agree on a radio duty cycle strategy
  - How can they synchronise their transmissions/receptions?

# Sender-Initiated Asynchronous MAC

- Also known as Preamble Sampling or Low-Power Listening (LPL)
- Protocol
  - Nodes do not synchronise their duty cycles (asynchronous)
  - When idle, nodes periodically turn their radios in RX mode and sample the channel
    - If nothing is detected, they go back to sleep
    - If preamble is detected, they send a CTS (clear to send) message and receive frame
  - Nodes with data to send, transmit a preamble (or RTS, ready to send) and listen for CTS
    - If CTS received, transmit the frame
    - If no CTS received, send preamble again and repeat
- The listening PERIOD bounds idle listening and defines senders delay/energy costs

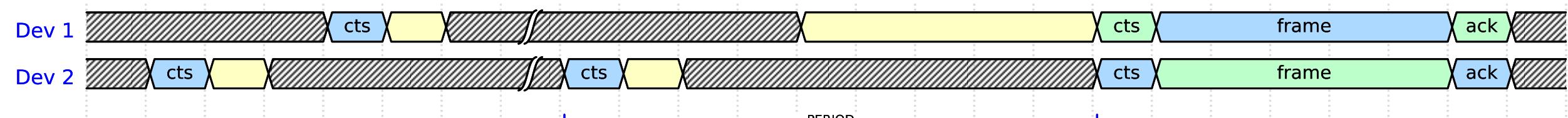
Blue: transmit  
Green: receive  
Yellow: listen  
Gray: sleep



# Receiver-Initiated Asynchronous MAC

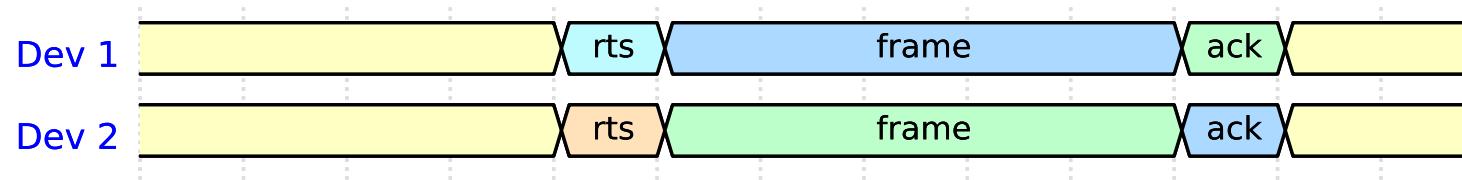
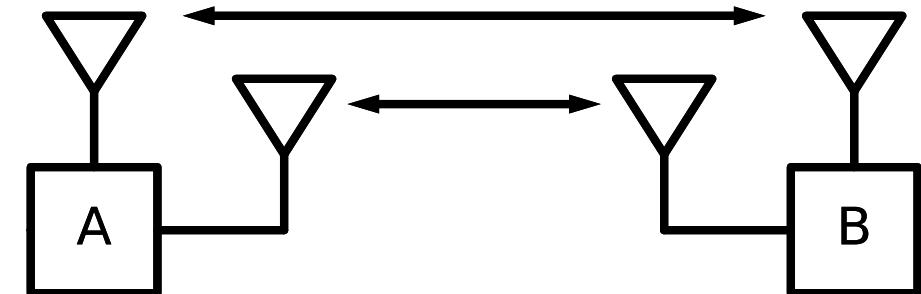
- Protocol
  - Nodes do not synchronise their duty cycles (asynchronous)
  - When idle, nodes periodically transmit a beacon (or CTS, clear to send) and put radios in RX mode to a while
    - If nothing is detected, they go back to sleep
    - If preamble is detected, they stay in RX mode and receive whole frame
  - Nodes with data to send, put their radio in RX mode and listen until they get the CTS
- The listening PERIOD bounds idle listening and defines senders delay/energy costs
- The performance of receiver-initiated and sender-initiated approaches is comparable

Blue: transmit  
Green: receive  
Yellow: listen  
Gray: sleep



# Asynchronous MAC with Wakeup Radio

- Devices employ an extra radio: Wakeup Radio
  - Very low-power to keep in listen mode continuously
  - Very low data rates (just enough to send an ID)
  - Limited coverage (typically)
- Protocol
  - When idle, main radio is off, wakeup radio is in RX mode
  - Nodes with data to transmit, send a RTS message via the wakeup radio
    - The sender then puts the main radio in TX mode and sends the frame
    - The receiver of the RTS message, puts main radio in RX mode and waits for the frame

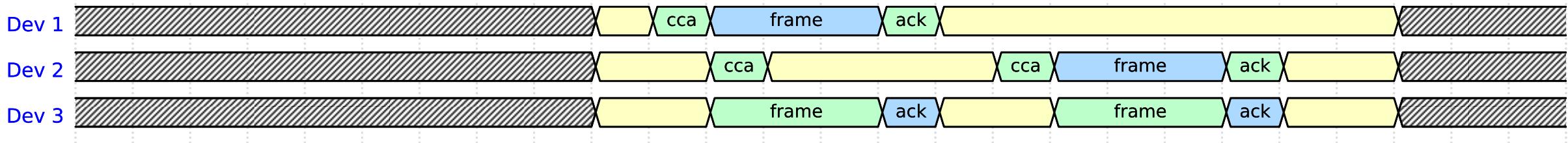


Blue: transmit (main)
Green: receive (main)
Light Blue: transmit (wakeup)
Orange: receive (wakeup)
Yellow: listen (wakeup)

# Synchronous MAC

- Devices synchronise their duty cycles
  - Switch between active and sleep periods
  - During the active period, use any MAC scheme, like CSMA/CA or guaranteed time slots
- Duty cycle is controlled by the duration of active/sleep periods
- Idle listening is reduced but not eliminated
- Requires a common notion of time (periodic time synchronisation)

Blue: transmit  
Green: receive  
Yellow: listen  
Gray: sleep



# Classification of MAC Protocols

- Duty Cycle
  - No Energy Constraints (no Duty Cycle)
  - Energy Constraints only on end devices (end devices Duty Cycle)
  - Energy Constraints on all devices (all devices Duty Cycle)
    - Synchronous Duty Cycles
    - Asynchronous Duty Cycles
      - Sender-Initiated
      - Receiver-Initiated
      - Wakeup Radio
- Contention Handling
  - Contention-free
  - Contention-based