EE-432
Systeme de Telecommunication

Prof. Andreas Burg
Joachim Tapparel, Yuqing Ren, Jonathan Magnin

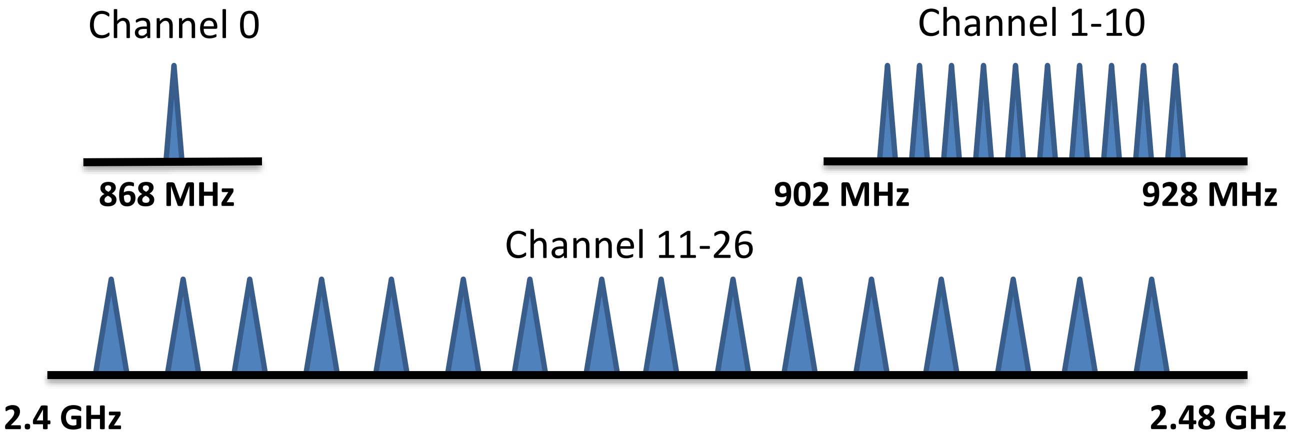
System Examples

IEEE 802.15.4 PHY/MAC

- **Physical layer (PHY) and media access control (MAC) for low-rate wireless personal area network** (**LR-WPAN**)
- **1998:** Start development by IEEE 802.15 working group as IEEE 802.15.4
- **Objectives of the standardization**
  - Low cost and low-power connectivity for sensors
  - Optimized for low duty cycle devices (efficient sleep modes)
  - Simpler and less expensive than Bluetooth (*reduced-complexity protocol stack*)
  - Support larger networks (hundreds to thousands of sensor nodes)
    for example star and point-to-point topologies
  - Large coverage area with short-medium range (10-100m) links
  - Facilitate implementation of security on higher layers
  - **2003**: Completion of the IEEE 802.15.4 standard (ratified Dec. 2004)
- **IEEE 802.15.4 is the basis for Zigbee, ISA100.11a, WirelessHART, MiWi, 6LoWPAN, Thread, and SNAP**

The 802.15.4 Physical Layer

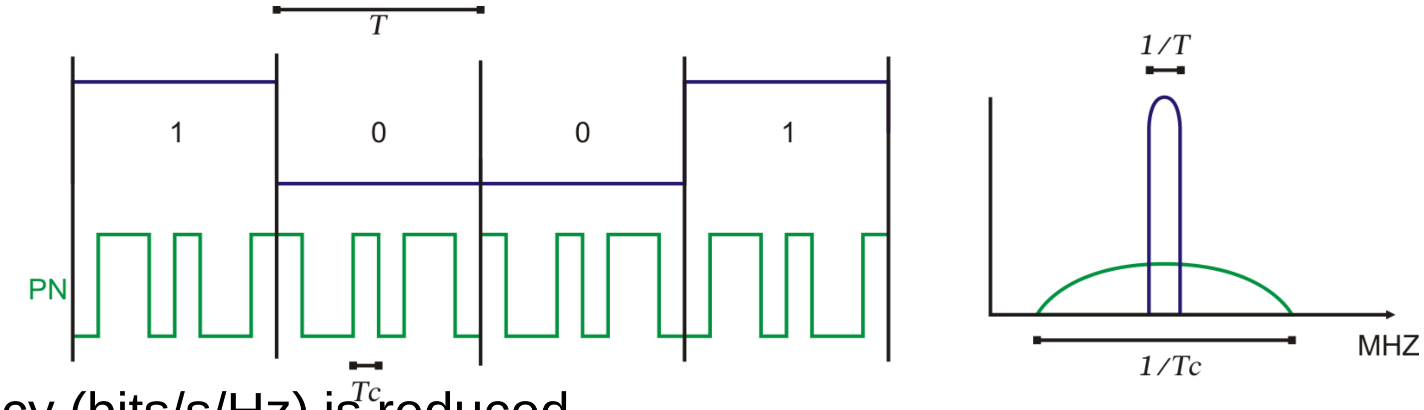
- **IEEE 802.15.4 PHY parameters**
  - Support for 3 unlicensed ISM frequency bands: 868 MHz, 915 MHz, 2.4 GHz
  - *Multiple channels in support parallel networks and avoid interference*
  - Supported data rate depend on the frequency band



Frequency	Channels	Spacing	Datarate	Region
868-870 MHz	1		20 kbit/s	Europe
902-928 MHz	10	2 MHz	40 kbit/s	America
2.4 GHz	16	5 MHz	250 kbit/s	World

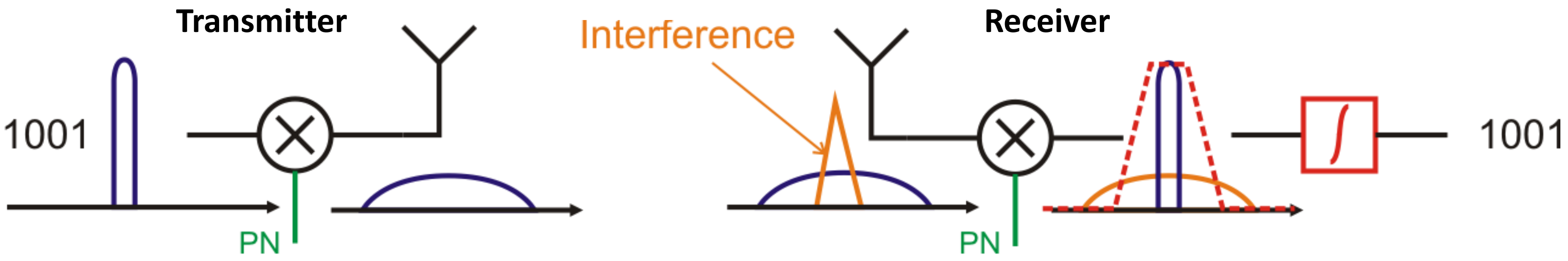
The 802.15.4 Physical Layer

- **Direct Sequence Spread Spectrum (DSSS) Modulation**
  - Each symbol is represented by a (modulated) pseudo-noise (PN) sequence (chips)
  - Chip-rate is higher than the symbol rate => signal is spread in the frequency domain



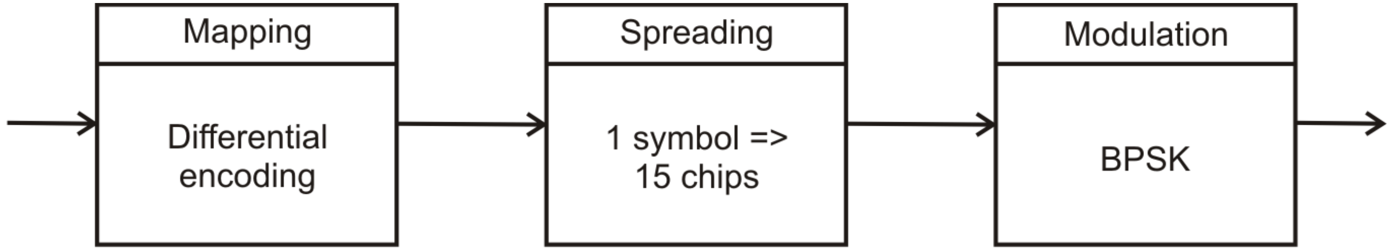
  - Spectral efficiency (bits/s/Hz) is reduced

- **Reduces interference to and from other users in the same frequency band**



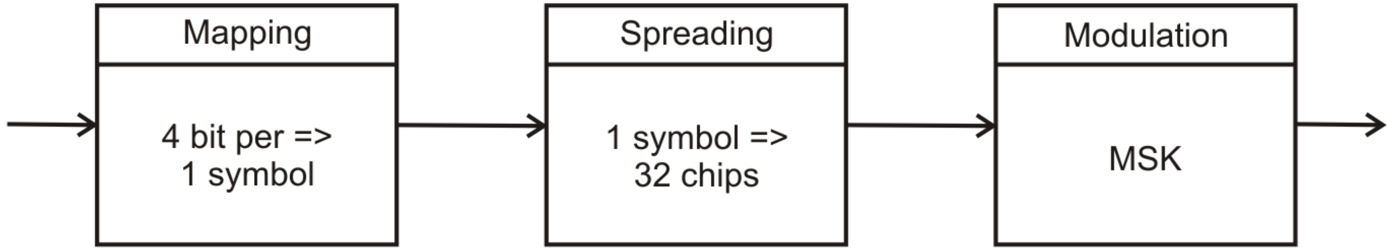
The 802.15.4 Physical Layer

- **DSSS modulation with different spreading factors**
  - The details of the modulation scheme and the spreading depend on the frequency bands



868 MHz 20 kbps 20 kHz 300 kchips/s 300 kHz

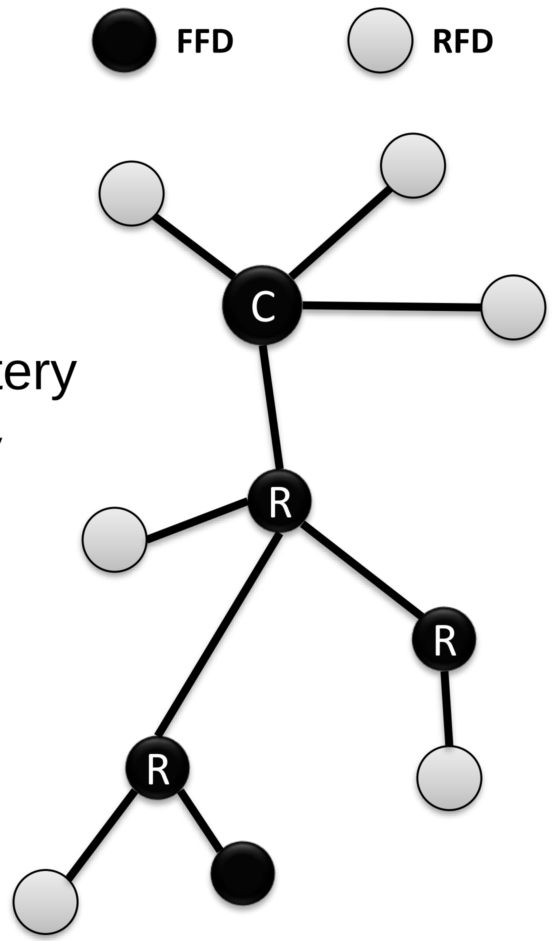
915 MHz 40 kbps 40 kHz 600 kchip/s 600 kHz



2.4 GHz 250 kbps 62.5 KHz 2 Mchips/s 2 MHz

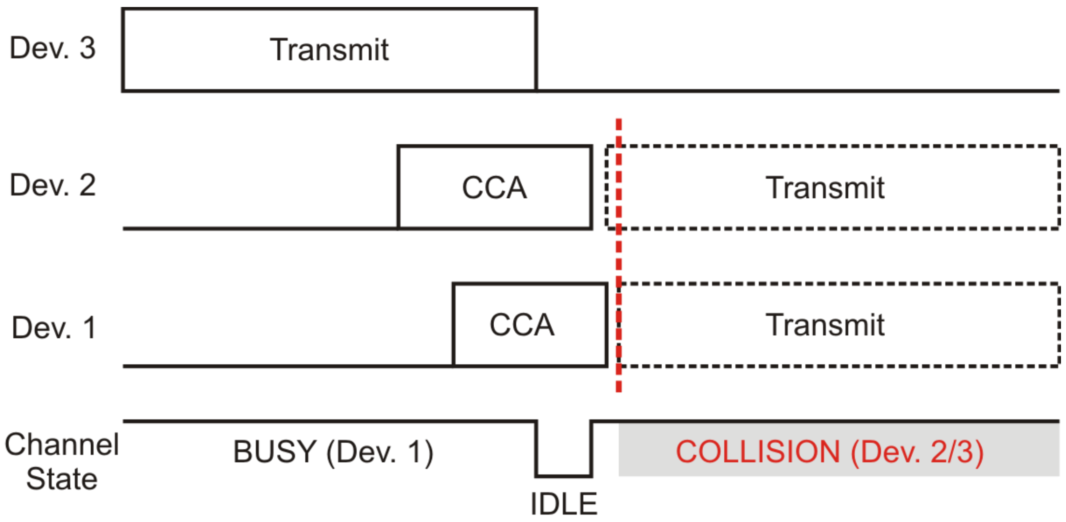
802.15.4

- **IEEE 801.15.4 knows 2 types of devices**
  - Different in cost and power consumption
- **The full function device (FFD)**
  - Can act as router and as coordinator in a network
  - Can also act as an end device
  - Typically equipped with a power connection or a stronger battery
  - Relatively complex protocol stack and need for more memory
  - Code: 15-30k; RAM: 2.5k – 4k
- **Reduced function devices (RFD)**
  - Reduced protocol stack and less memory required
  - Can only be leaves in the tree and can only talk to a router or to the coordinator
  - Code: 6k; RAM: <2k



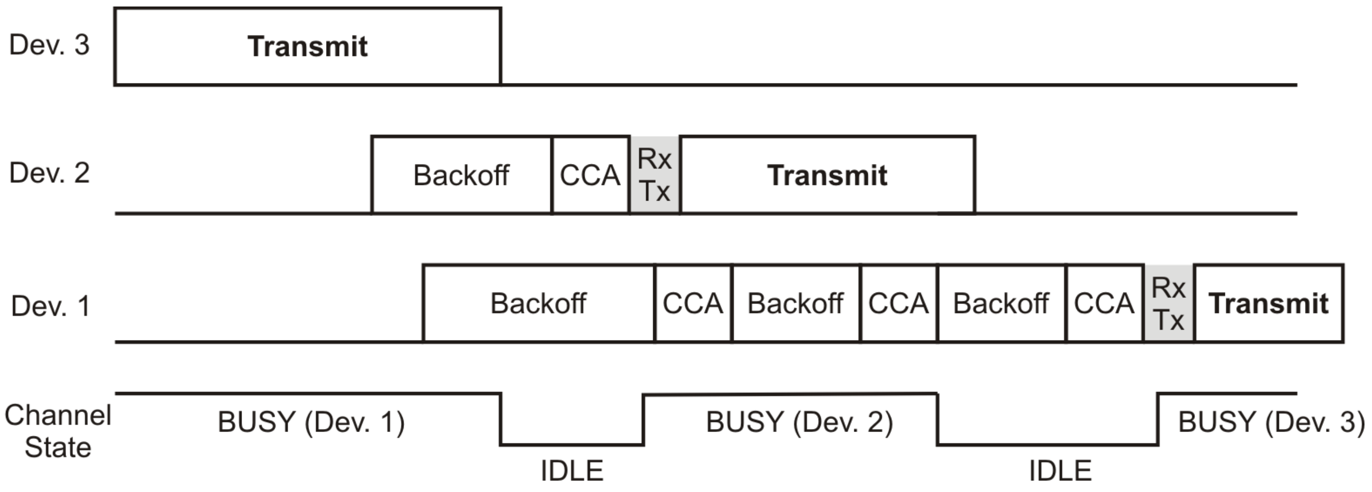
IEEE 802.15.4 Channel Access

- **Channel access**
  - Devices are not synchronized and have no assigned time slots
  - Need other means to avoid collisions between devices
- **Carrier sense multiple access (CSMA)**
  - Devices listen before sending : clear channel assessment (CCA)
  - Send only if channel has been idle for a specified period
  - Collisions still occur frequently with multiple nodes due to delays



IEEE 802.15.4 Channel Access

- **Carrier sense multiple access (CSMA)** with collision avoidance (CA): CSMA/CA
  - Wait for a randomly chosen backoff interval before CCA

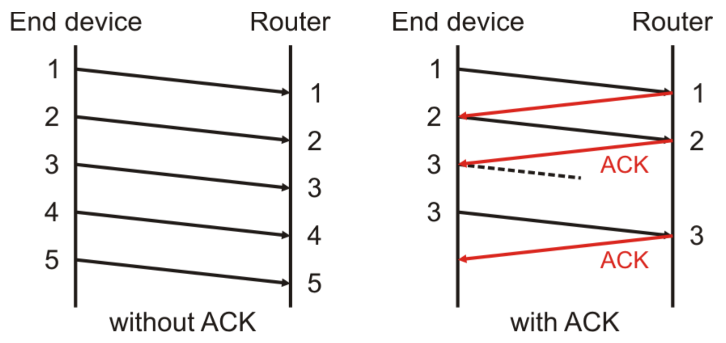


  - If CCA fails, choose a new backoff time and try again
  - For each attempt, the maximum length of the backoff interval increases exponentially

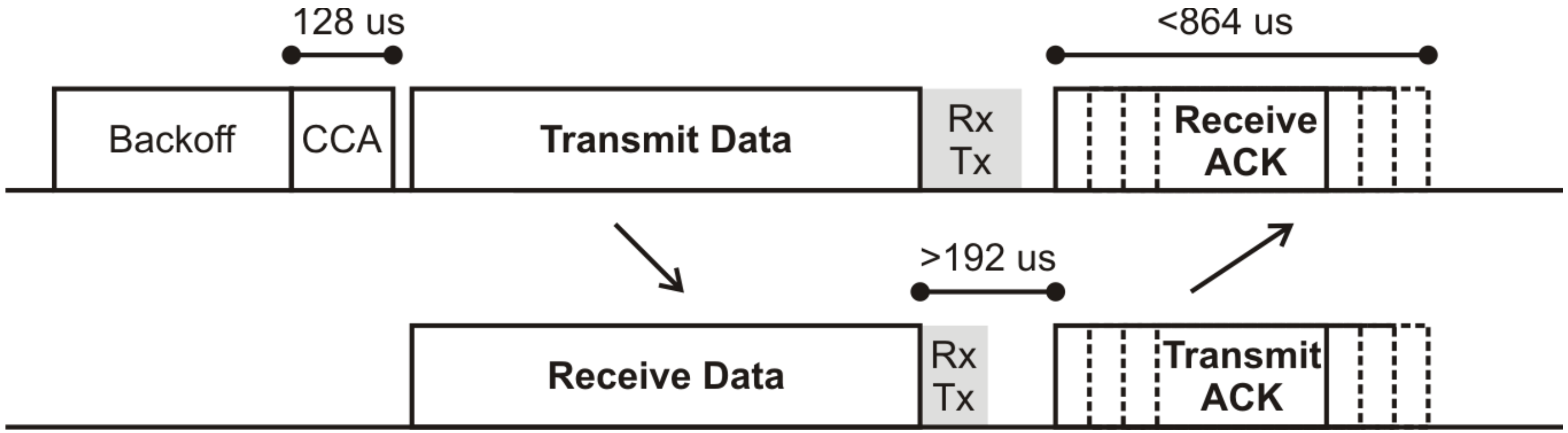
  - **Devices can sleep during backoff**

IEEE 802.15.4 Channel Access

- **Data transfer between two nodes can be *with* <u>or</u> *without* acknowledge**
  - Competing for channel access to send a short ACK is inefficient
  - A packet and its ACK should be a single, unbreakable entity to simplify packet management



- **ACK is sent without new CCA**
  - Receiver waits at least T_{ack} = 192us before sending the ACK (Rx/Tx and Tx/Rx turnaround)
  - T_{ack} is short enough to prevent other devices from capturing the channel (in most cases!)



IEEE 802.15.4 / ZigBee

Low-power low-data-rate wireless ad-hoc network with medium range for

- **Applications: home automation, industrial, medical, data collection, non-real-time control**
- **ZigBee builds on 802.15.4 PHY/MAC layer and adds network and application layers**
  - Adds routing, security, application profiles

- **ZigBee has been created and is maintained by an industry consortium: ZigBee Alliance (>300 member companies)**
  - **2002** : Foundation of the ZigBee Alliance as industry consortium
  - **2003** : Completion of the IEEE 802.15.4 standard (ratified Dec. 2004)
  - **2004** : ZigBee 1.0 (also known as ZigBee 2004) announced (now obsolete)
  - **2006/2007/…:** further releases supersede previous versions
  - **Latest version:** ZigBee 3.0 (since 2015)

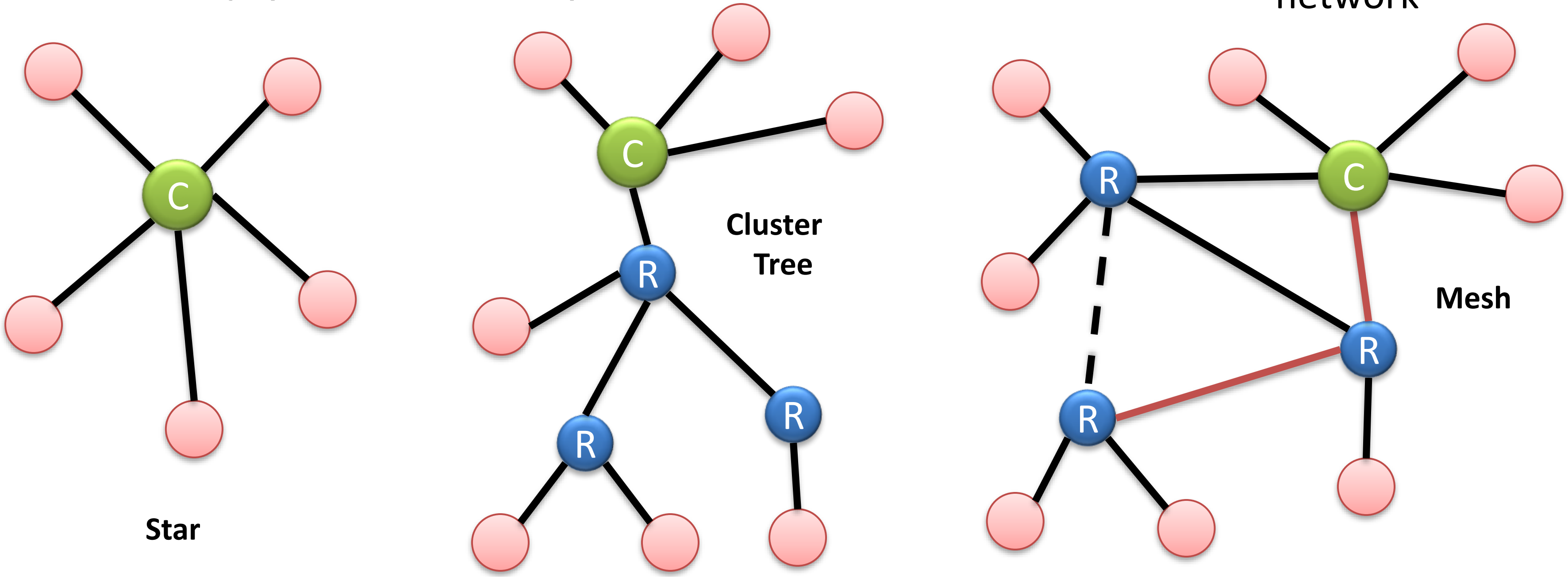
- **Main non-technical advantage of ZigBee:** rigorous certification process for device interoperability (in practice, still many hurdles)

- **Drawback**: costly certification process and complex (close-source stack) & licensing costs

ZigBee Network Topologies

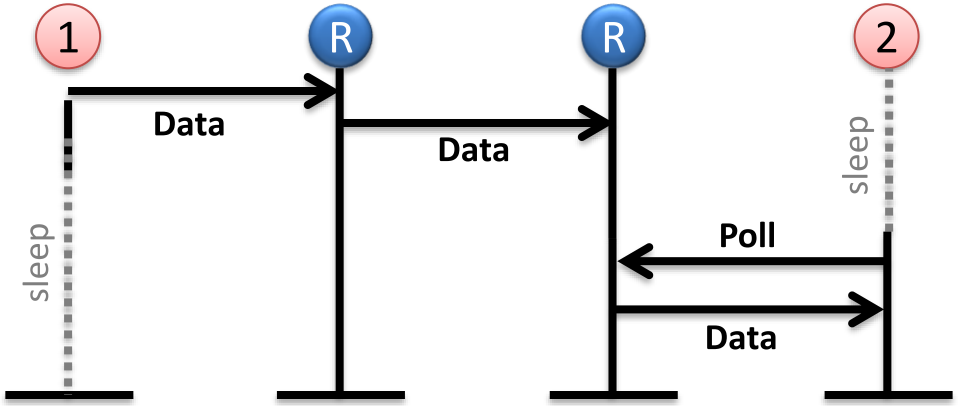
- **Self organizing ad-hoc network with 3 different roles**
  - Star
  - Cluster Tree
  - Mesh Network
    - Routers connect to multiple other routers (and endpoints)
    - Improved reliability (alternate routes)

- **End device**: connects only to one and only one router
- **Router**: multiple connections to other routers and multiple end devices
- **Coordinator**: only one per network

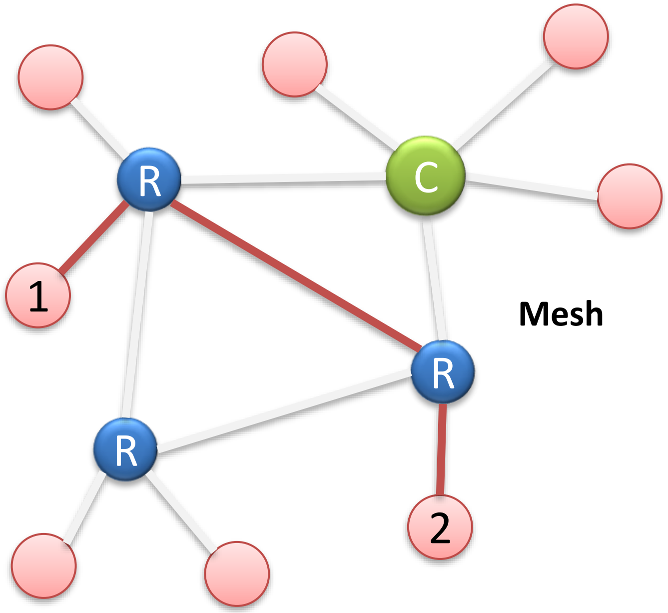


ZigBee Network Topologies

- **Self organizing ad-hoc network** with 3 different roles
  - Star
  - Cluster Tree
  - Mesh Network
- **Communication in the network**
  - **Coordinator** creates and manages the network
  - **End devices** sleep most of the time and *initiate communication* by sending data or polling a router
  - **Routers** buffer traffic for their connected end devices



- **End device**: connects only to one and only one router
- **Router**: multiple connections to other routers and multiple end devices
- **Coordinator**: only one per network



ZigBee Devices

- **Transceivers are typically available as modules or highly integrated SoCs with MCU/ROM/flash/memory**
- **Receiver sensitivity (1% PER) typically -90 to -100dBm**

NXP JN5139-Z01-M/03
30 x 18mm,
>15 USD

- **Typical power consumption**
  - Standby: < 8uW
  - Active: 60-120mW (@3V)

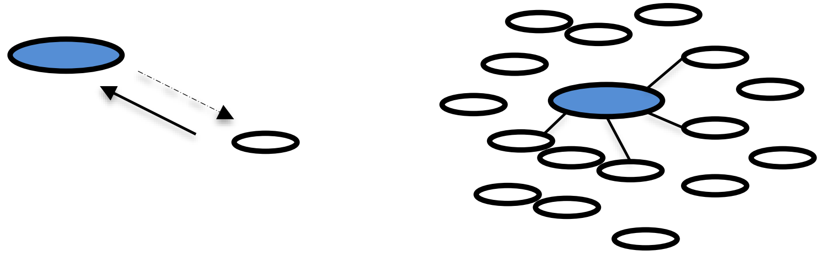
TI CC-2420/2430/2431
ZigBee Radio + MCU
6 x 6 mm, ~4-8 USD

	Vendor	Atmel	Ember		Freescale				Jennic		Microchip	Texas Instruments		
	ZigBee Chip	AT86 RF230	EM 250	EM 260	MC 13193	MC 13203	MC 13213	MC 13225	JN 5121	JN 5139	MRF 24J40	CC 2420	CC 2430	CC 2431
IEEE 802.15.4 Features	Sleep Current [uA]	0.1	1	1	1	1	1	NA	5	1.3	2	2	1	1
	RX Current [mA]	16	36	36	42	42	42	20	50	34	18	20	27	27
	TX Current [mA]	17	36	36	35	35	35	20	45	34	22	18	27	27
	RX Sensitivity [dBm]	-101	-98	-98	-92	-92	-92	NA	-90	-97	-91	-95	-92	-92
	TX Power [dBm]	+3	+5	+5	+4	+3	+3	NA	0	+3	+5	0	0	0
MCU Features	In Package		X	The ZigBee Coprocessor			X	X	X	X			X	X
	External	X			X	X					X	X		
	Core	AVR	XAP2b		HCS08	Coldfire	HCS08	ARM7	RISC	RISC	PIC	MSP430	x51	x51
	Bus Width [bits]	8	16		8	32	8	32	32	32	8	16	8	8
	RAM [kB]	8	5		4	~32	4	NA	to 96	to 96			8	8
	ROM [kB]	256	128		60	~256	60	NA	64	192			128	128
	Core Freq. [MHz]	16	12		20	50	40	26	16	16			32	32
ZB Stack	Availability	yes	yes	in ROM	yes	soon	yes	soon	yes	yes	yes	yes	yes	yes
	License Price				995 $		995 $				free	free	free	free
	Latest Version	PRO	2006	2006	2006	2006	2006	2006	2006	2006	2004	2006	2006	2006

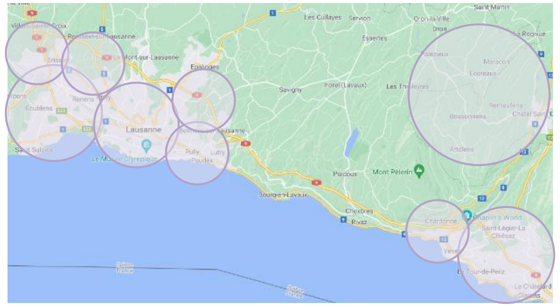
M. Varchola, M. Drutarovsky, “ZigBee Based Home Automation Wireless Sensor Network,” Acta Electronica Et Informatica, Vol. 7, No. 4, 2007

Long Range Low Power Wide Area Networks (LPWANs)

- **Highly optimized for low-cost IoT sensor nodes**
  - Support only very low data rates with very short duty cycles
  - Focused on Upling (sensor-to-cloud) traffic
  - Large number of devices per gateway (hundreds)



- **Radio access and modulation**
  - Often based on open radio standards
  - Operation in unlicensed (ISM) frequency bands
  - Mostly ad-hoc network deployment (rather unplanned)
  - Low cost and low power physical layer modems
  - Long range radio reach to minimize infrastructure needs
  - Very basic radio access protocol, optimized for ULP only



- **Low medium cost infrastructure (gateways & core network)**
  - Relatively low cost gateways (300-1000 USD)
  - Basic core network with simple radio-network protocols
  - Builds on public IP network (no dedicated fiber links or networks)

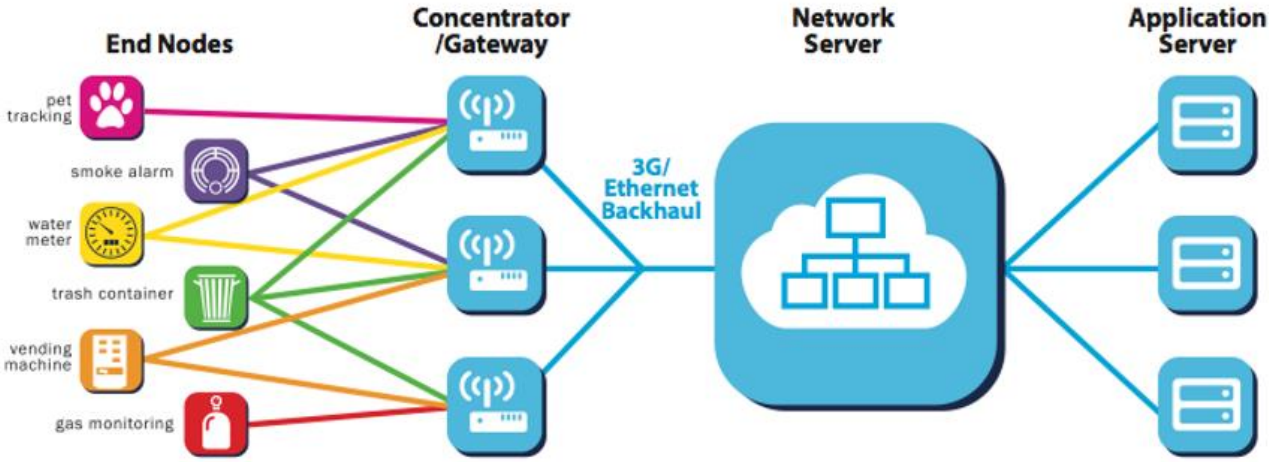
LoRa

- **Alliance between multiple companies on different levels of the stack**
- **Multiple vendor offering based on cooperation between various companies offering services around a common open concept**
- **Technology was originally developed by Cycleo (Grenoble, France) and later acquired by *Semtech (Neuchatel, Switzerland)* in 2012**
- **Semtech broadly licenses the IP to other chip manufacturers**
- **LoRa Alliance provides a certification process for new products**

- **Targets low data rates: 290 bps – 11 kbps (125 kHz), 1.16 kbps – 50 kbps (500 kHz)**
  - Symmetric up and downlink
- **Modulation provides multiple data rates using spread spectrum modulation**
  - Robustness to interferers
  - Tradeoffs between data rate and range
  - Codes of different spreading factors are almost orthogonal
- **Coverage per gateway: rural=5-10 km, urban=1-3 km**
  - Multiple gateways extend coverage area and improve robustness (diversity)
  - Network server filters duplicate packets (received by multiple gateways)

The LoRa System Architecture

- **Gateways (Connectors):**
  - Receive and demodulate long-range wireless transmissions using LoRa PHY protocol and serve as interface between the wireless connection and a Network Server with almost no further intelligence
- **Network Server (intelligence):**
  - Collects receptions from multiple gateways (diversity), filters duplicate packets, schedules acknowledgements, controls data rates and checks security. They can process messages directly or act as Cloud Server to provide services to a further layer of customers (depending on the business model)



LoRa Modulation

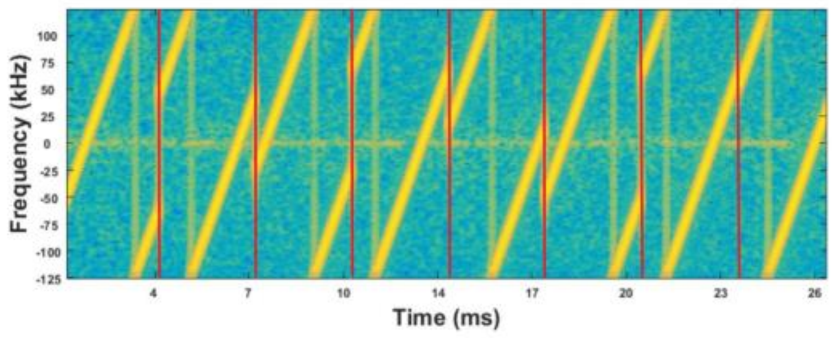
- **To cover a wide range of distances, LoRa requires a modulation that allows to adapt the energy per bit (at the cost of throughput)**
  - Spread-spectrum frequency chirp
  - Symbols are distinguished by the starting frequency

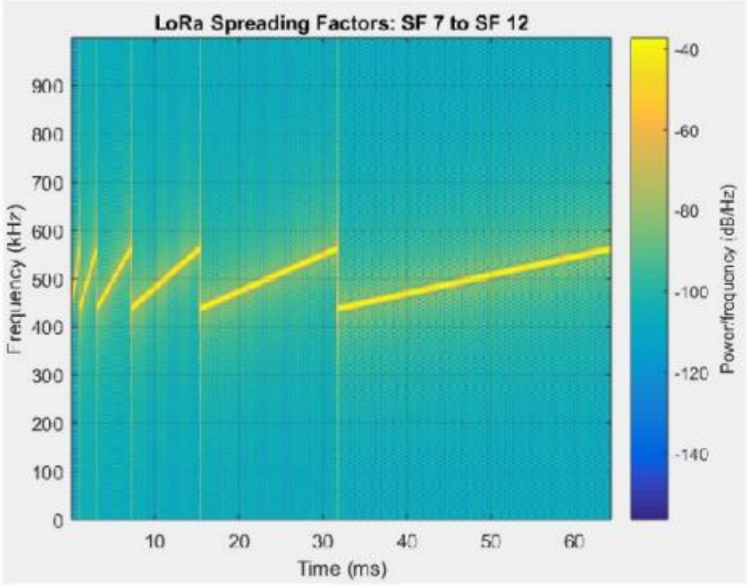
$$x[n] = e^{j2\pi\left(\frac{n^2}{2N}+\left(\frac{s}{N}-\frac{1}{2}\right)n\right)}$$

  - Six possible spreading factors adjust the symbol duration (i.e., the rate) $T_s = \frac{1}{BW} 2^{SF}$
    - Each symbol carries SF bits of information

PHY Data Rate [bps]

$$R_b = SF \cdot \frac{\frac{4}{4+CR}}{2^{SF}} \cdot BW$$





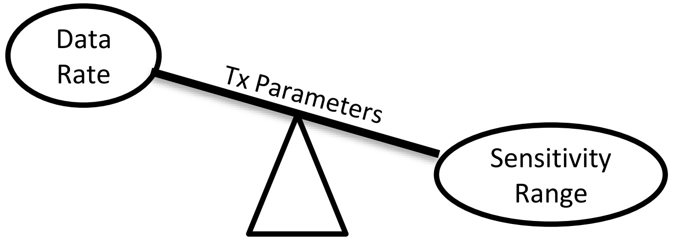
LoRa Chirps for Different Spreading Factors [1]

LoRa: RF and Physical Layer Sensitivity Examples

- **Doubling BW doubles data rate, but reduces sensitivity by 3 dB**
- **Example, based on Semtech SX1272 (860 – 1020 MHz)**

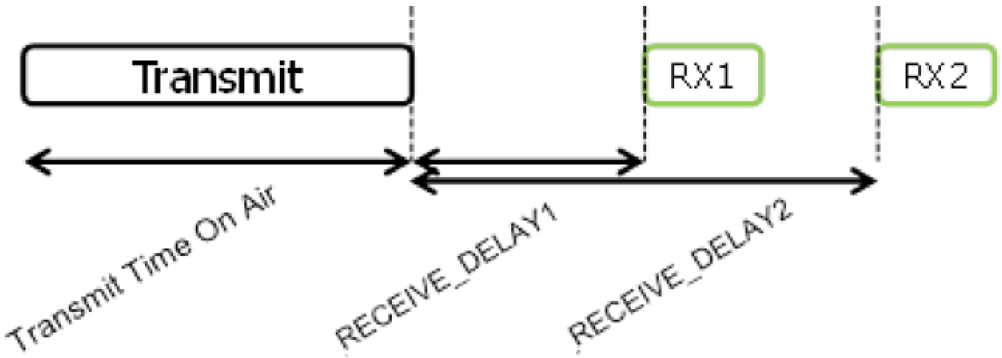
Bandwidth	SF	Code rate	Bit rate (bps)	Sensitivity [dB]
125	6	4/5	9380	-122
125	12	4/5	293	-137
250	6	4/5	18750	-119
250	12	4/5	586	-134
500	6	4/5	37500	-116
500	12	4/5	1172	-131

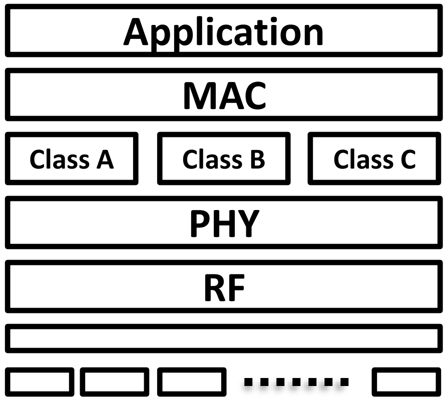
- **Range:**
  - In LOS scenario: 6 dB better sensitivity doubles the range
  - Urban environment: 12 dB better sensitivity needed for doubling the range



LoRa: Multiple Access (Class A)

- **LoRa Class A is based on the ALOHA protocol for multiple access**
  - Class A is the most frequently used type of devices with all communication initiated by end-user device with uplink msg.



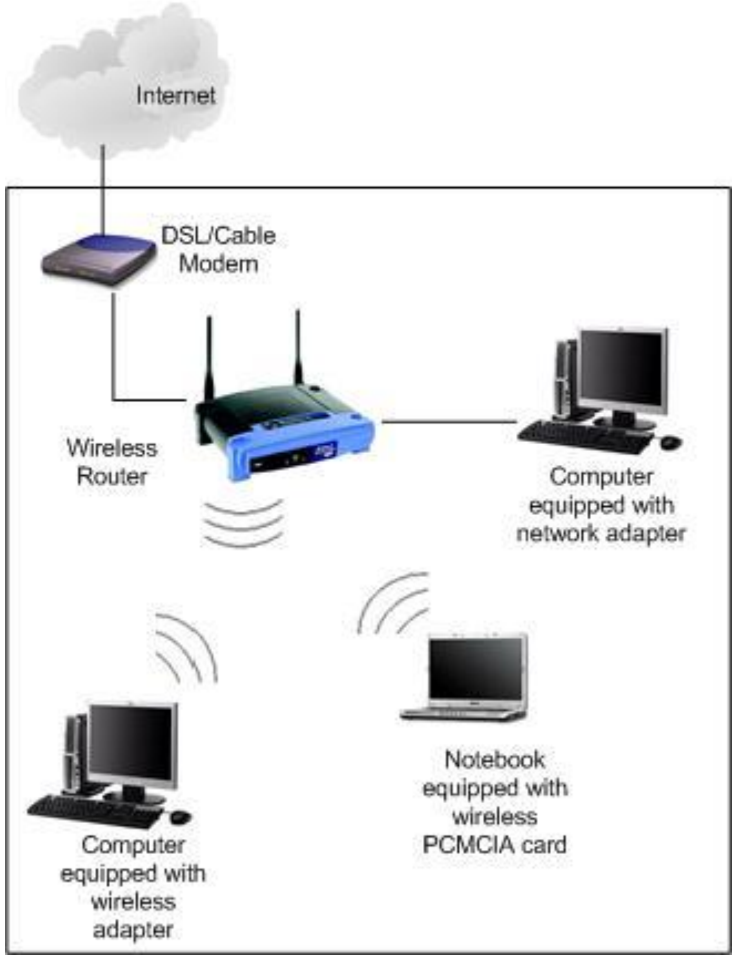


  - Orthogonality between spreading codes of different lengths allows collisions between devices that use different SFs
  - Collisions are resolved by missing ACK and retransmissions with random transmission slots
  - Target duty cycle of <1% and limited number of packets per day ensures low collision probability
  - Typical ALOHA network capacity ~18% of its maximum

  - Encryption and authentication using AES-128

WiFi Networks & Standardization

- **WiFi is a local area network with short radio range (<100m), typically arranged in a star-topology**
- **WiFi is an industry alliance that certifies devices**
- **WiFi standardized by IEEE, known as IEEE 802.11**
  - IEEE 801.11 is a family of standards that is amended regularly, e.g., 802.11b, 802.11a/g, 802.11n, 802.11ax, ...
  - New major version (generation) every roughly 4-6 years (backwards compatible)



- **Primary application: broadband connectivity**
  - Targets high data rates between devices
  - Reasonable number of devices served in parallel
  - Maintain high system capacity (aggregate capacity across all connected devices)

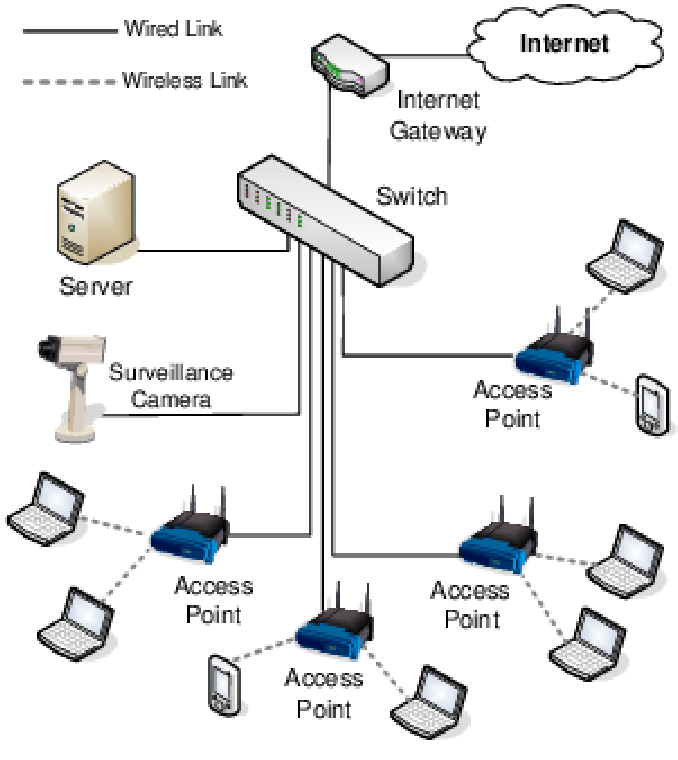
Evolution of the WiFi Standard

Generation	IEEE standard	Adopted	Maximum link rate (Mbit/s)	Radio frequency (GHz)
Wi-Fi 8	802.11bn	2028	100’000	2.4, 5, 6, 7, **42.5, 71**
Wi-Fi 7	802.11be	2024	1’376–46’120	2.4, 5, 6
Wi-Fi 6E	802.11ax	2020	574–9’608	6
Wi-Fi 6		2019		2.4, 5
Wi-Fi 5	802.11ac	2014	433–6’933	5
Wi-Fi 4	802.11n	2008	72–600	2.4, 5
(Wi-Fi 3)*	802.11g	2003	6–54	2.4
(Wi-Fi 2)*	802.11a	1999		5
(Wi-Fi 1)*	802.11b	1999	1–11	2.4
(Wi-Fi 0)*	802.11	1997	1–2	2.4

WiFi Networks and Co-Existence

- **WiFi operates in license free ISM bands**
  - Multiple WiFi networks and multiple users may collide with each other when operated at the same frequency

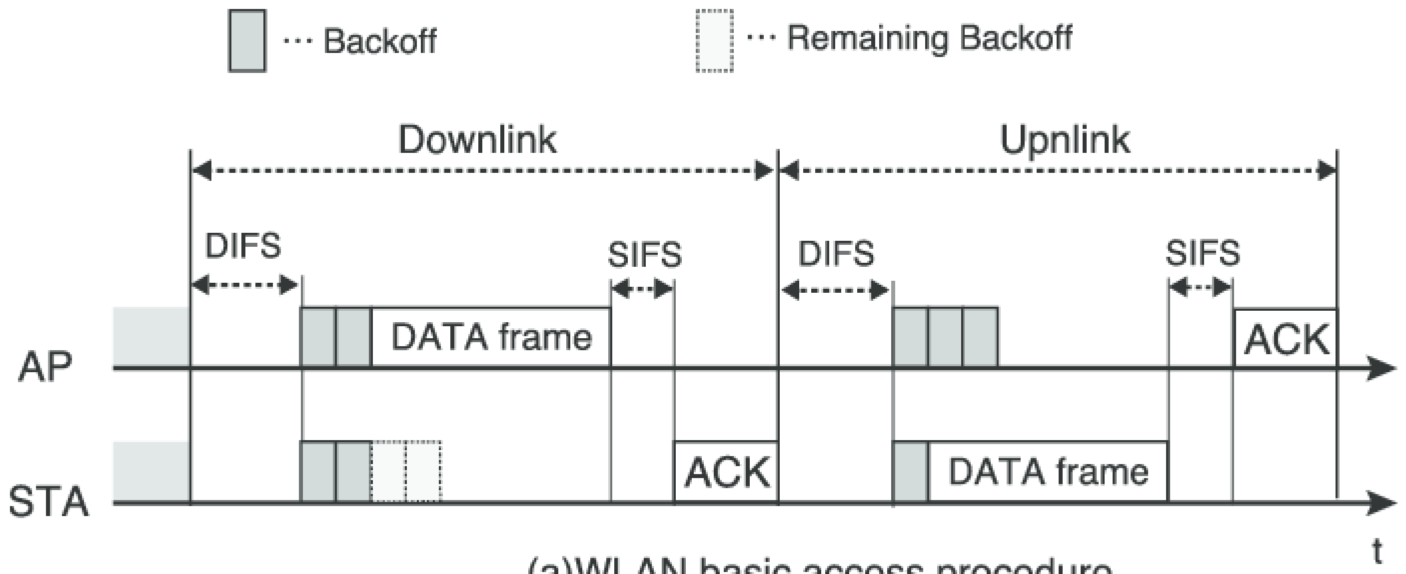
- **WiFi is a packet based communication protocol**
  - Devices in a network communicate with common access point (AP)
  - Multiple networks can co-exist in parallel
  - Communication is half-duplex (up- and down-link in same band)



(a)

Stations and APs Access the Channel Dynamically

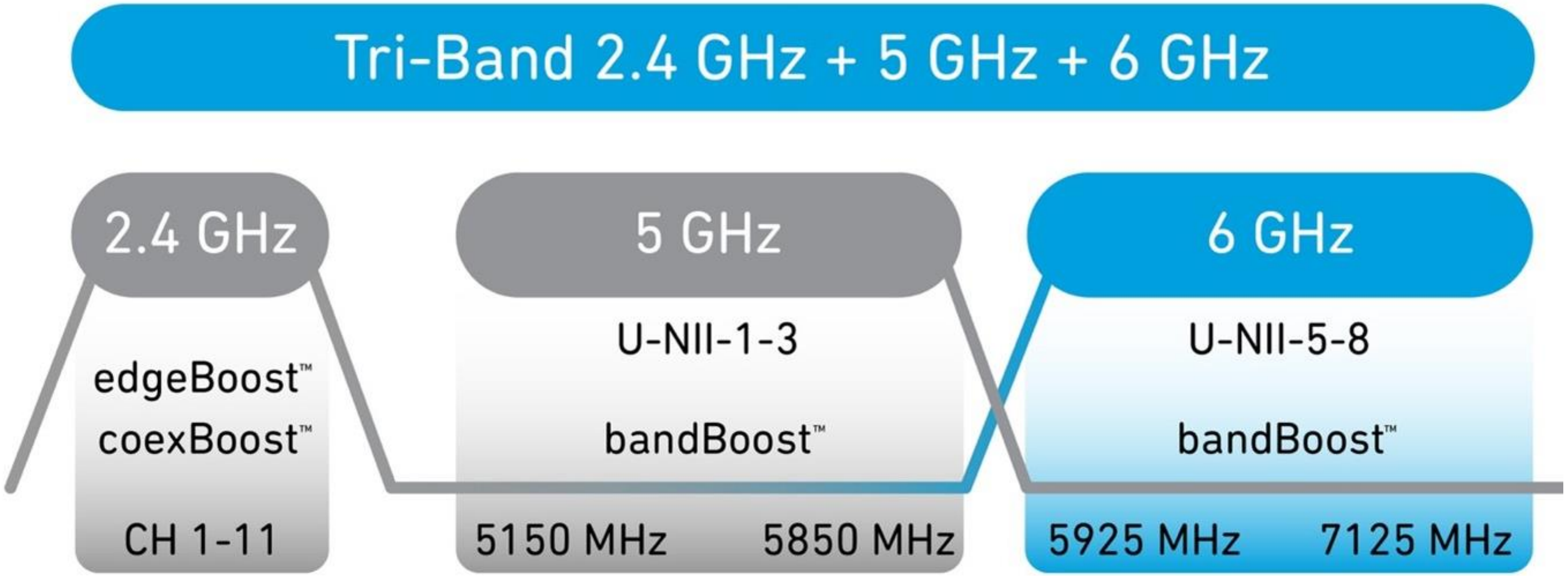
- **All devices and AP in a network share the same physical resource (channel)**
  - Need to coordinate channel access to minimize the number of collisions
- **WiFi is based on a sophisticated form of "Carrier Sense Multiple Access"**
  - Devices listen to the channel before they start transmitting
  - Random backoff: if channel is occupied, they introduce a random delay before checking again
  - Acknowledgement packets (ARQ) have priority (sent without delay)

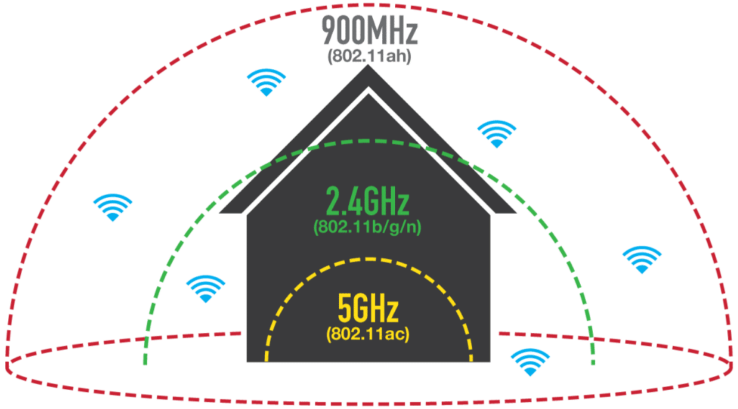


(a)WLAN basic access procedure

WiFi Frequency Bands

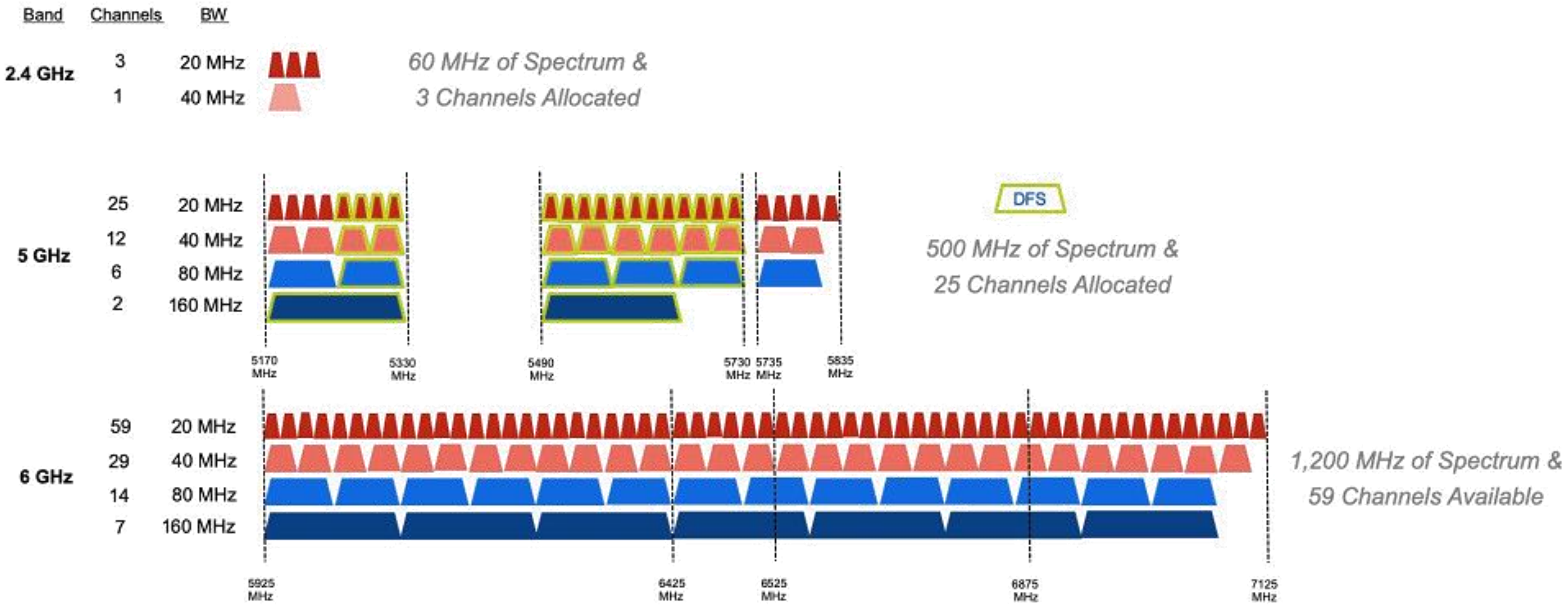
- **Technology generations have continuously added new, higher frequency ISM bands to allow for more bandwidth and more system capacity**
  - Each band is partitioned into multiple channels, with higher bands offering more channels and channels with wider bandwidth
  - Choice of frequency band is a tradeoff between available bandwidth and range





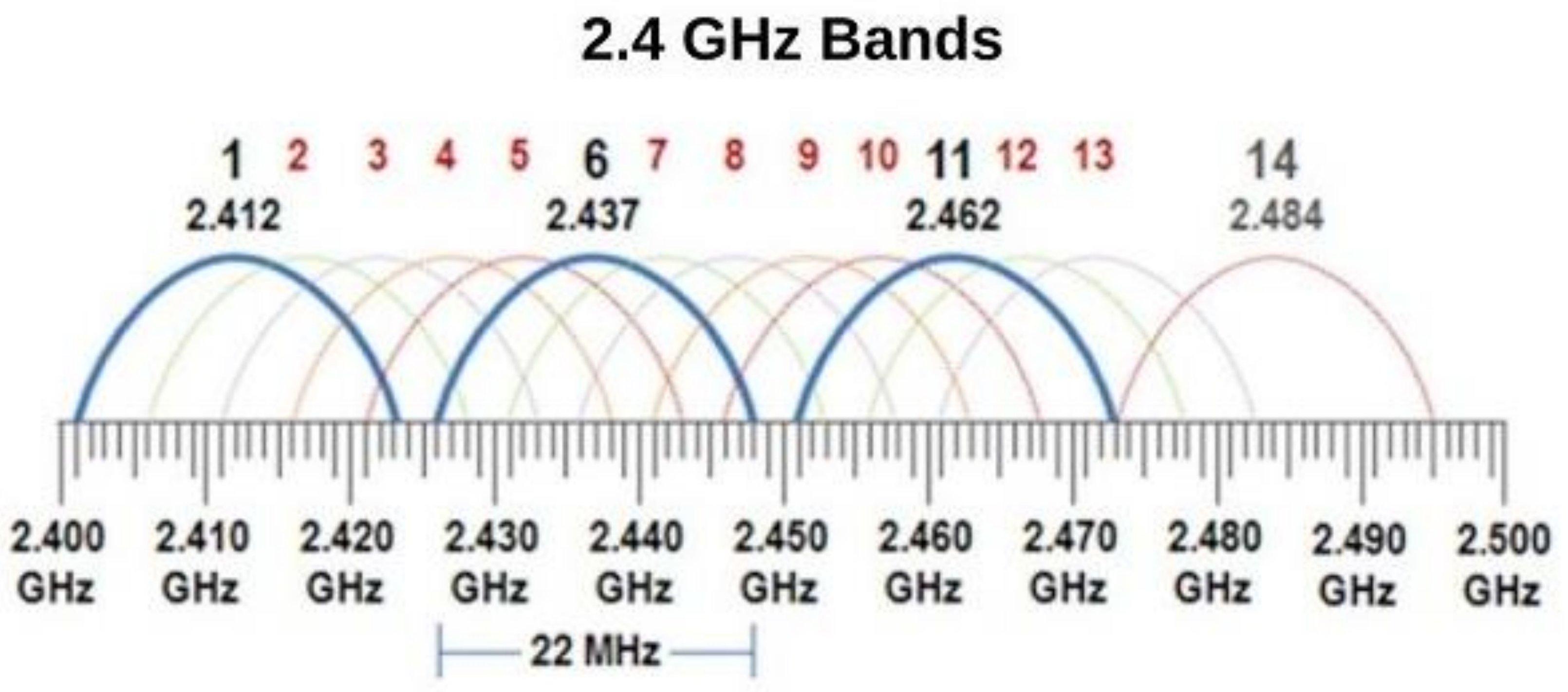
WiFi Channels

- **To separate networks (avoid collisions), WiFi offers multiple channels**
  - The number of channels depends on
    1. the available bandwidth in an ISM band
    2. the bandwidth used by the WiFi system (multiple bandwiths available, increasing over generations)



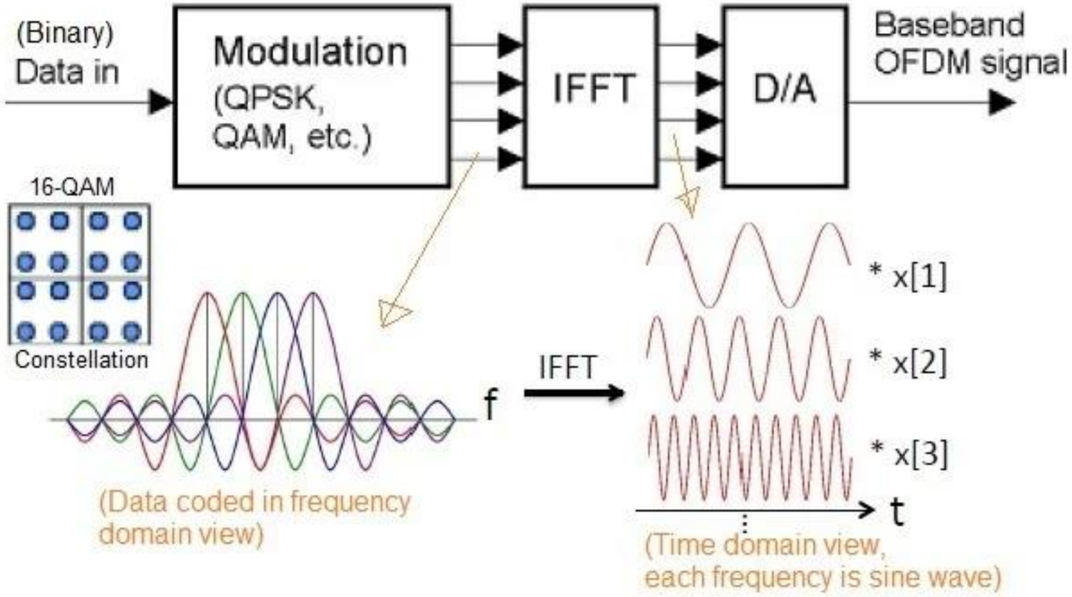
WiFi Channels in 2.4 GHz Band

- **In the narrow 2.4 GHz Band, WiFi defines many “overlapping” channels.**
  - ATTENTION: this leads to collisions even when networks are on different channels
  - Only three (3) 20MHz channels are non-overlapping:

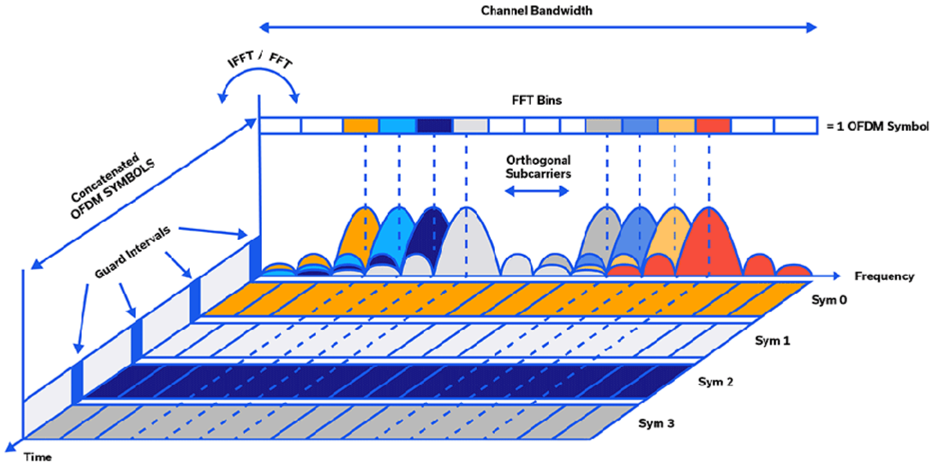


WiFi Modulation: Orthogonal Frequency Division Multiplexing (OFDM)

- **Modern WiFi (starting from 802.11a/g) is based on OFDM modulation**
  - Basic idea: break up a wide bandwidth into many parallel sub-carriers
  - Each sub-carrier is modulated with N-QAM modulation of adjustable rate

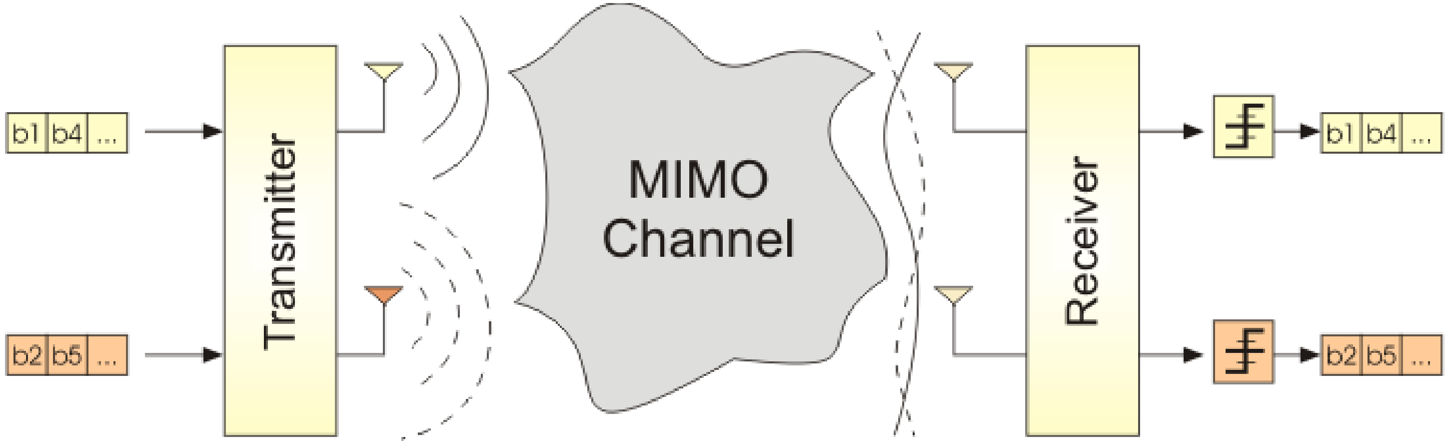


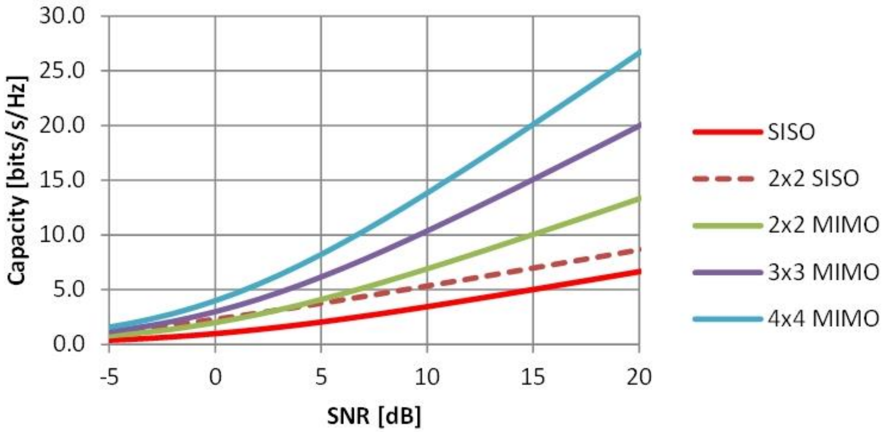
Many (N) long data symbols overlap in time
but occupy different frequencies (sub-carriers)



WiFi Modulation: MIMO

- **WiFi (as many other modern standards) use multiple-input multiple-output (MIMO) technology to increase capacity with multiple antennans**
  - Transmitter: transmit different data streams at the same time and frequency, but from different antennas
  - Receiver: multiple antennas pick up a superposition of the transmitted streams and separate them due to differences in the channel characteristics





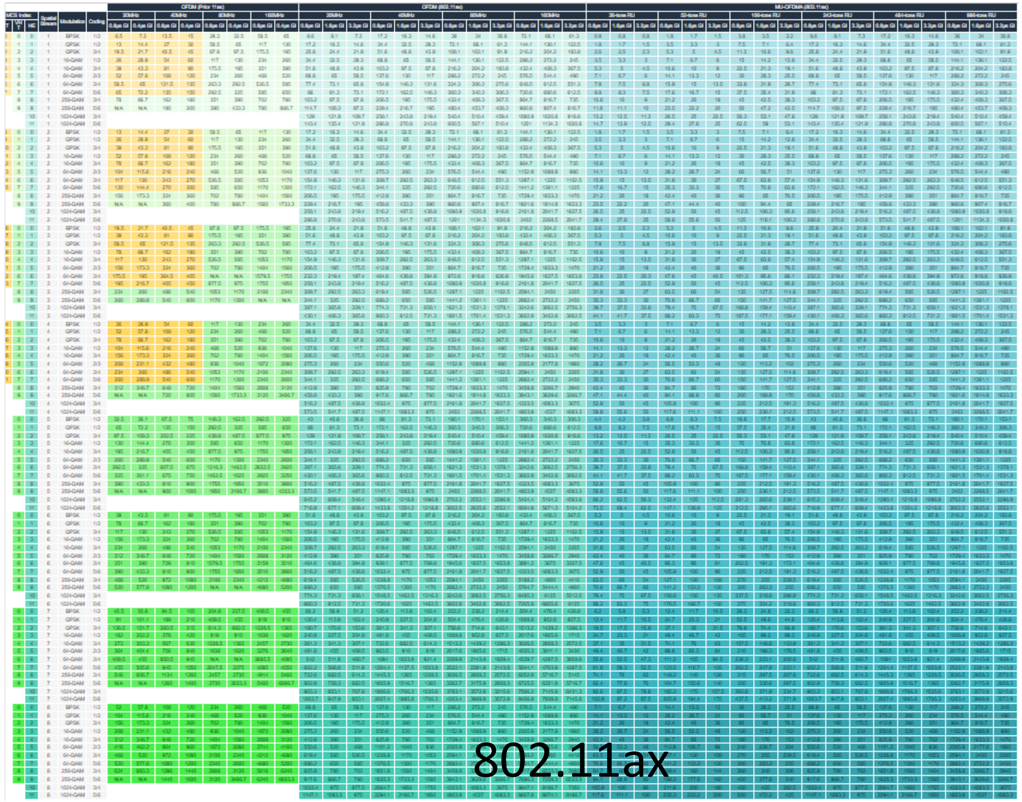
- **Under ideal conditions, MIMO increased capacity by $\min(N_{tx}, N_{rx})$**

WiFi Rate Adaptation

- **A WiFi transmitter dynamically chooses from a list of “Modulation & Coding Schemes” based on channel quality feedback the most promising rate**
  - With the arrival of MIMO, wider bandwidth, very-high-order modulation, and advanced space-time codes as well as channel codes, the number of MCSs has exploded from 11g to 11ax

Index	RxPower (dBm)	Modulation	Code Rate	PHY Rate
1	-82	BPSK	1/2	6
2	-81	BPSK	3/4	9
3	-79	QPSK	1/2	12
4	-77	QPSK	3/4	18
5	-74	16 QAM	1/2	24
6	-70	16 QAM	3/4	36
7	-66	64 QAM	2/3	48
8	-65	64 QAM	3/4	54

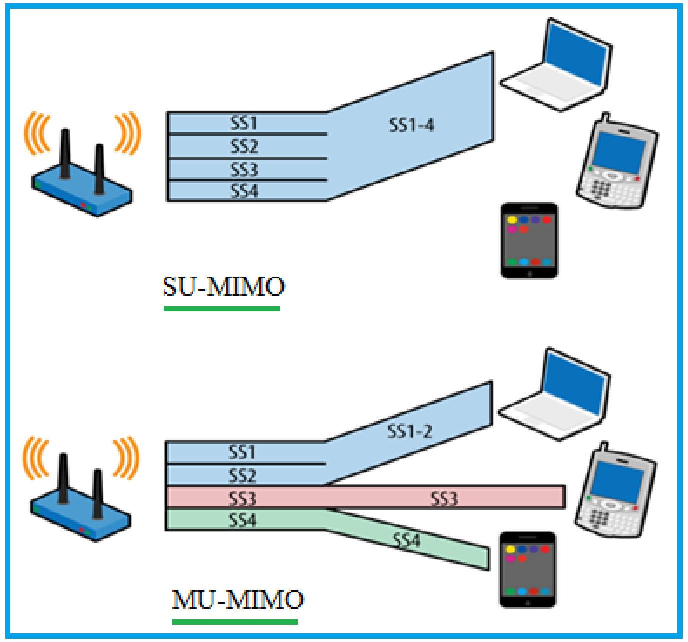
802.11a (1990s)

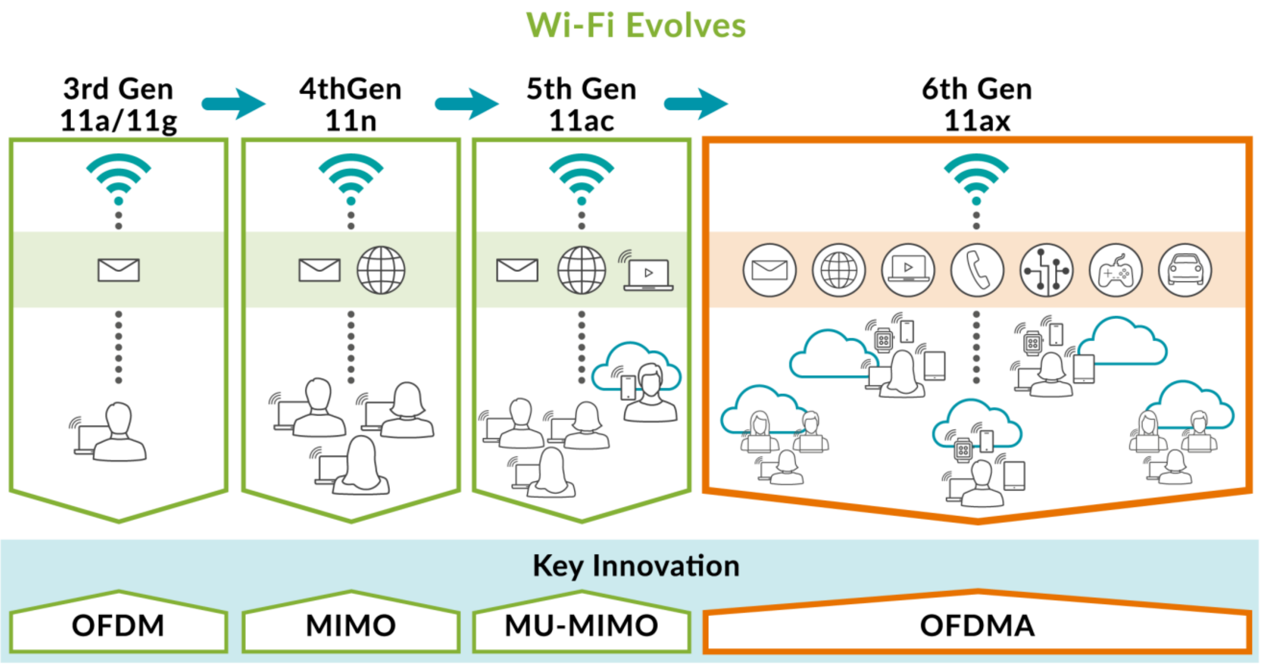


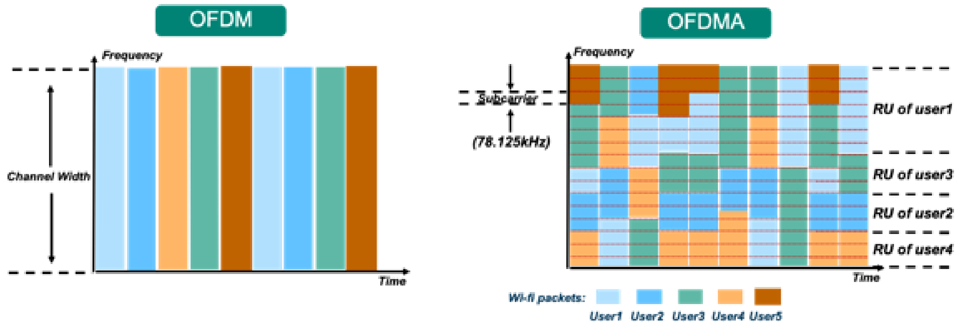
802.11ax

WiFi Latest Modes and Technologies

- **OFDM and MIMO are only the most fundamental ideas.**
  - IEEE 802.11ac and 802.11ax build on these technologies as well as on advanced channel coding to further increase capacity and stability







EE-432
Systeme de Telecommunication

Prof. Andreas Burg
Joachim Tapparel, Yuqing Ren, Jonathan Magnin

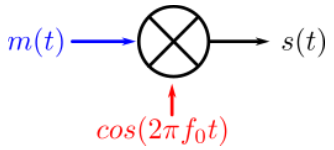
FM Modulation (Preparation for Project)

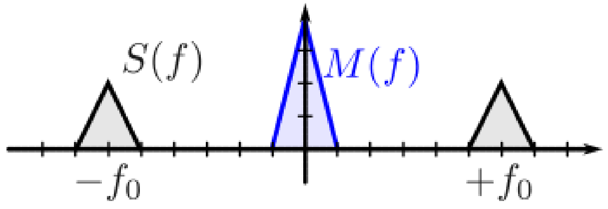
Recap: Amplitude Modulation (AM)

- **Amplitude modulation is the most basic for of linear modulation**

Modulation

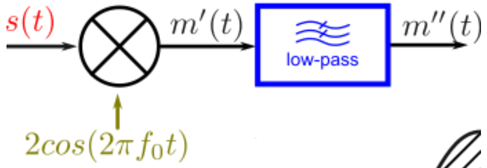
$$s(t) = m(t) \cdot \cos(2 \cdot \pi \cdot f_0 \cdot t)$$

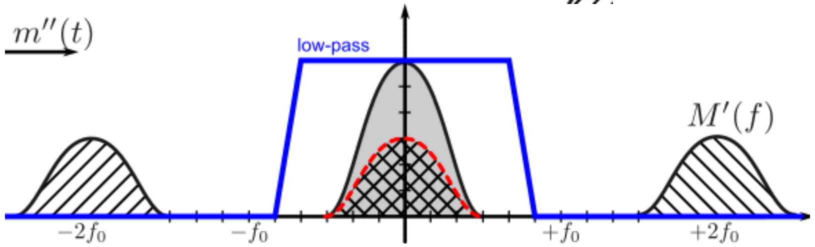




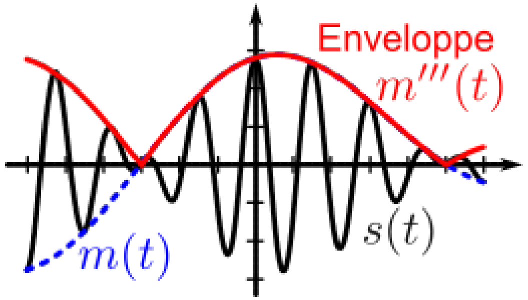
Demodulation

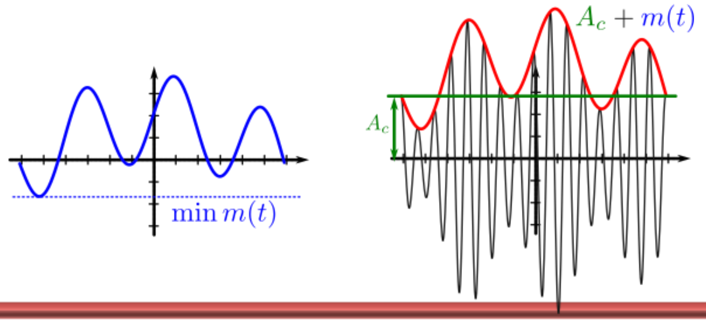
$$m''(t) = \text{LPF}\{s(t) \cdot 2\cos 2\pi f_0 t\}$$





- **To avoid the need for coherent-demodulation we often modulate the envelope**





Drawbacks of AM

- **AM modulation requires phase/frequency coherent demodulation**

- **Envelope modulation** (avoid need for coherent receiver) **is energy inefficient**

- **RF power depends on the "data" signal amplitude** (transmitter must be linear across a large dynamic range, set by the signal to be transmitted)

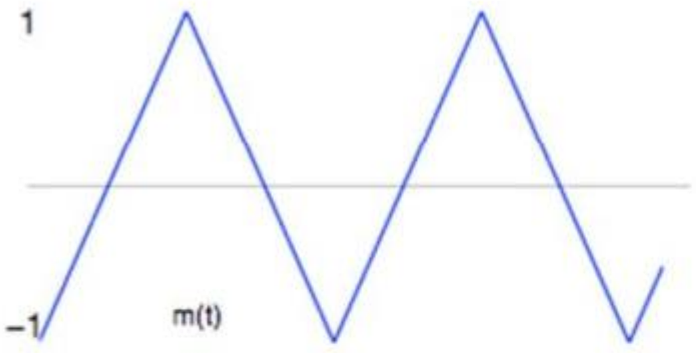
- **Any noise on the RF signal directly affects the received signal**

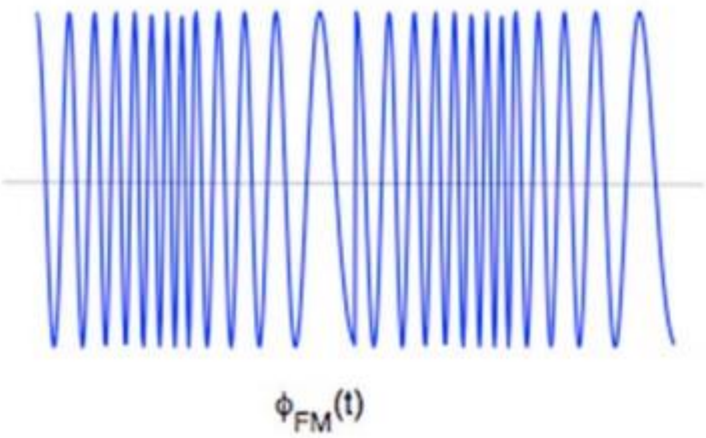
- **Demodulated signal amplitude proportional to the RF signal amplitude**

Frequency Modulation (non-linear)

- **Frequency modulation:** encodes the transmitted signal by changing the "frequency" of the carrier

$$s(t) = \cos\left(2 \cdot \pi \cdot \left(f_0 + k_f \cdot m(t)\right) \cdot t\right)$$

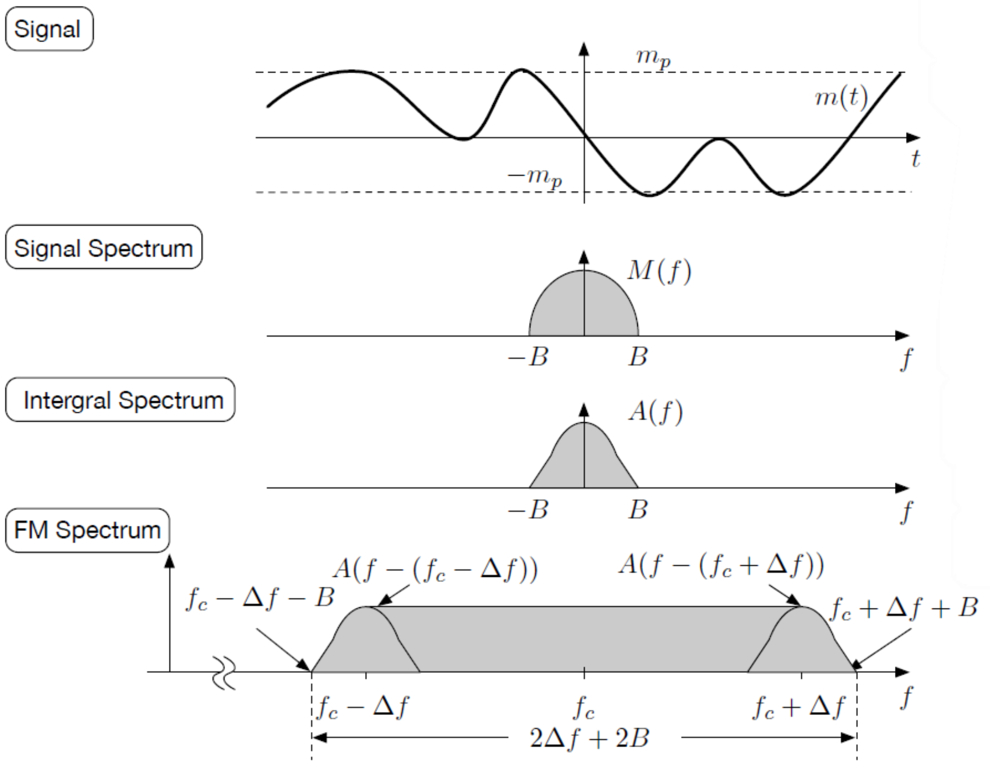




- **Remark:** FM modulation can also be seen as modulating the **phase (=derivative of the frequency)** with the integral of the data signal

$$s(t) = \cos\left(2 \cdot \pi \cdot \left(f_0 \cdot t + k_f \cdot \int_{-\infty}^{t} m(\tau)d\tau\right)\right)$$

Frequency Modulation & Bandwidth



- **FM modulation is a non-linear modulation:**
  - Modulation leads to new spectral components
  - The bandwidth of the RF signal does not correspond
  - to the bandwidth of the baseband signal

- **Bandwidth of the signal is determined by the amplitude of** $k_f \cdot m(t)$ and by the bandwidth of $m(t)$

- **Carlson's rule:** $B_{FM} \approx 2 \cdot \Delta f + 2 \cdot B_m$ with $\Delta f = k_f \cdot A_m$

- **Modulation index** β: ratio between original bandwidth and modulated bandwidth

FM Demodulation

- **Many methods exist to demodulate FM RF signals**
  - Based directly on the RF signal
  - Based on the baseband representation of the RF signal (after down-conversion)

- **Most basic idea using the baseband representation:** calculate backwards from the received signal to the modulated signal

$$s(t) = \mathrm{e}^{j2\pi\left(f_0 t + k_f \cdot \int_{-\infty}^{t} m(\tau)d\tau\right)} + \mathrm{e}^{-j2\pi\left(f_0 t + k_f \cdot \int_{-\infty}^{t} m(\tau)d\tau\right)}$$

  - Down conversion and filtering to get the modulated complex baseband:

$$s'(t) = \mathrm{LPF}\left\{s(t) \cdot \mathrm{e}^{-j2\pi f_0 t}\right\} = \mathrm{e}^{j2\pi k_f \cdot \int_{-\infty}^{t} m(\tau)d\tau}$$

$$\angle s'(t) = 2\pi k_f \cdot \int_{-\infty}^{t} m(\tau)d\tau$$

$$\frac{d\angle s'(t)}{dt} \cdot \frac{1}{2\pi k_f dt} = \frac{1}{dt}\left(\int_{-\infty}^{t} m(\tau)d\tau - \int_{-\infty}^{t-dt} m(\tau)d\tau\right) = m(t)$$

FM Demodulation

- **Digital implementation**:
  - Sampling (careful to consider the correct bandwidth): $s_n' = s'(n \cdot T_s)$

$$s'(n \cdot T_s) = \mathrm{e}^{j2\pi k_f \cdot \int_{-\infty}^{n \cdot T_s} m(\tau)d\tau}$$

  - Calculating the phase difference between $n \cdot T_s$ and $(n-1) \cdot T_s$ in the complex domain

$$s''(n \cdot T_s) = s'(n \cdot T_s) \cdot \left[s'\big((n-1) \cdot T_s\big)\right]^* = \mathrm{e}^{j2\pi k_f \cdot \int_{(n-1) \cdot T_s}^{n \cdot T_s} m(\tau)d\tau}$$

  - Get the phase from the complex valued signal

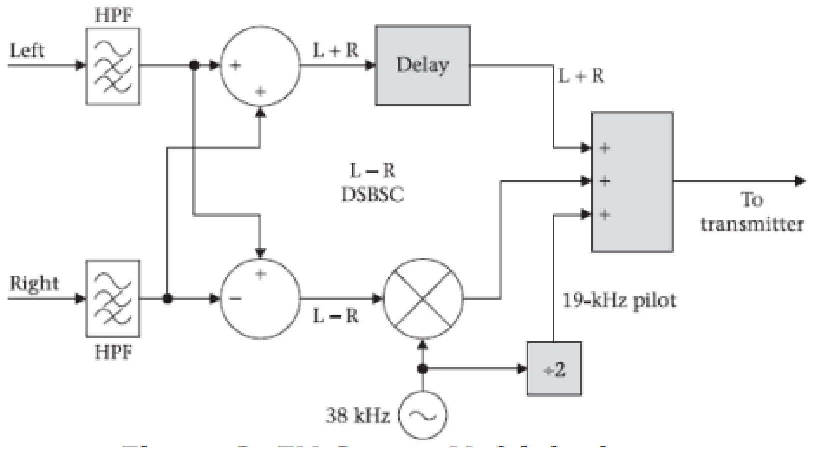
$$\angle s''(n \cdot T_s) \cdot \frac{1}{2\pi k_f} \cdot \frac{1}{T_s} = \frac{1}{T_s} \int_{(n-1) \cdot T_s}^{n \cdot T_s} m(\tau)d\tau = m(\tau)$$

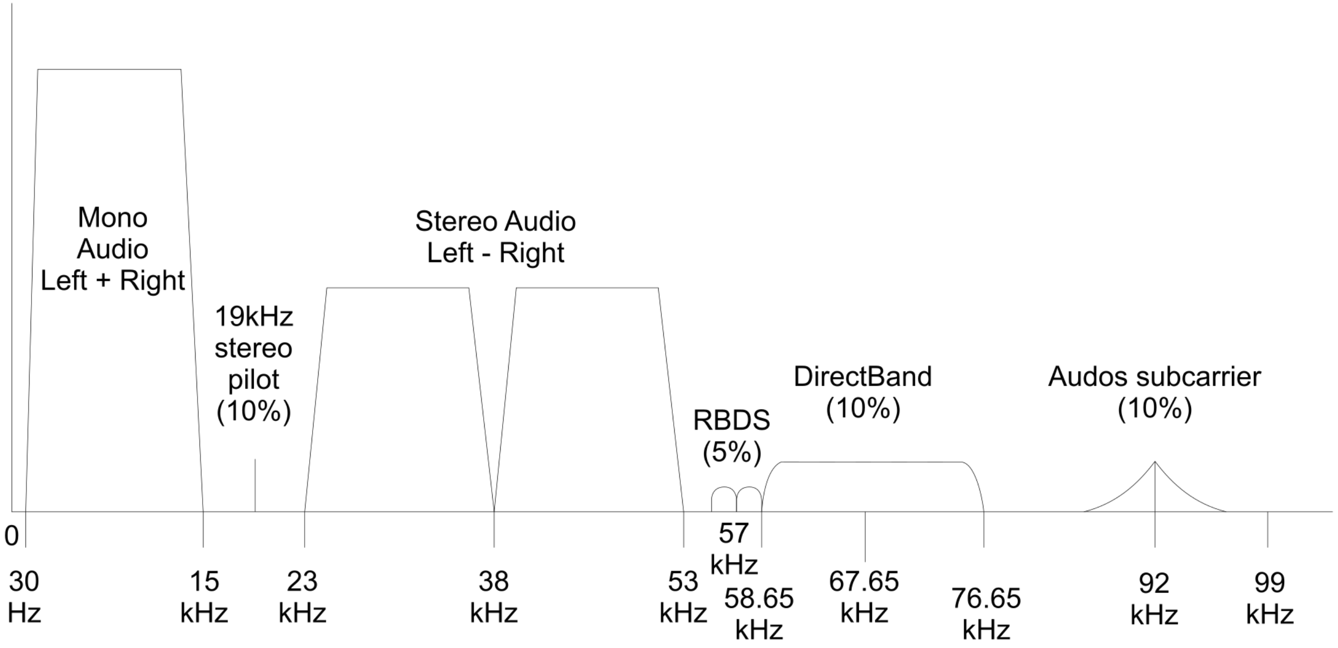
    - Assumption for the last step: $m(\tau)$ is approximately constant over duration of T_s (compare the bandwidth of the original signal with the sampling time of the modulated signal)

FM Radio Broadcast (1)

- **FM radio is a combination of AM and FM modulation**
  - AM is used to enable stereo radio by frequency multiplexing the two required audio channels
  - FM is used to modulate the stereo signal (**L+R**: **L**eft and **R**ight)

- **Stereo baseband signal:** add a second audio channel while remaining backward compatible (i.e., demodulating only one channel contains information on both channels)





FM Radio Broadcast (2)

- **The AM baseband signal (including both audio channels and other signals) is modulated using FM modulation**
  - Typical parameters:

Parameter	Symbol	Typical values (mono)	Typical values (stereo+RDS)
Peak deviation	Δf	$75\ \mathrm{kHz}$	$75\ \mathrm{kHz}$
Signal bandwidth	BW_{BB}	$15\ \mathrm{kHz}$	$59\ \mathrm{kHz}$
Modulation index	β	$\frac{75\ \mathrm{kHz}}{15\ \mathrm{kHz}} = 5$	$\frac{75\ \mathrm{kHz}}{59\ \mathrm{kHz}} = 1.27$
RF bandwidth	BW_{RF}	$180\ \mathrm{kHz}$	$268\ \mathrm{kHz}$