CZECH TECHNICAL UNIVERSITY IN PRAGUE

FACULTY OF ELECTRICAL ENGINEERING

DEPARTMENT OF TELECOMMUNICATION ENGINEERING

B2M32BTSA - Bezdrátové technologie

BE2M32BTSA - Wireless Technologies and Sensor Networks

Wi-Fi Technology

Pavel Mach

Czech Technical University in Prague

Faculty of Electrical Engineering

Department of Telecommunication Engineering

6G mobile RESEARCH LAB

Overview

Wireless basics

- Communication basics
  - (Antenna types, gain, modulation, etc.)
- Types of wireless area networks
- IEEE 802 family

802.11

- Terminology & topology
- Physical (PHY) layer
  - Types of PHY layers
- Medium access control (MAC) layer
  - Types of accessing methods
  - MAC frame
- Evolution
  - From WiFi 0 generation to WiFi 7
- Security
  - Security threats
  - Authentication protocols

Wireless basics (1/2)

Antennas & gains

- Isotropic, omnidirectional, directional, sector (e.g., 120°)
- Antenna gain (in dBi) expresses the gain compared to isotropic antenna (i.e., antenna transmitting with the same power in all directions)

Modulation

- How many bits are transmitted in a single symbol
- BPSK (1 bit), QPSK (2 bits), 16-QAM (4 bits), 64-QAM (6 bits), 256-QAM (8 bits)

Code rate $\mathrm{R} = k/n$

- Useful *k* (bits) vs redundant data in packet of size *n*
- Trade-off between **latency** and **reliability**
  - high *R* => low latency, low reliability
  - low *R* => high reliability, high latency

Bit rate (data rate)

- Modulation, Code rate, Bandwidth, Symbol duration

Wireless basics (2/2)

Multi User (MU)

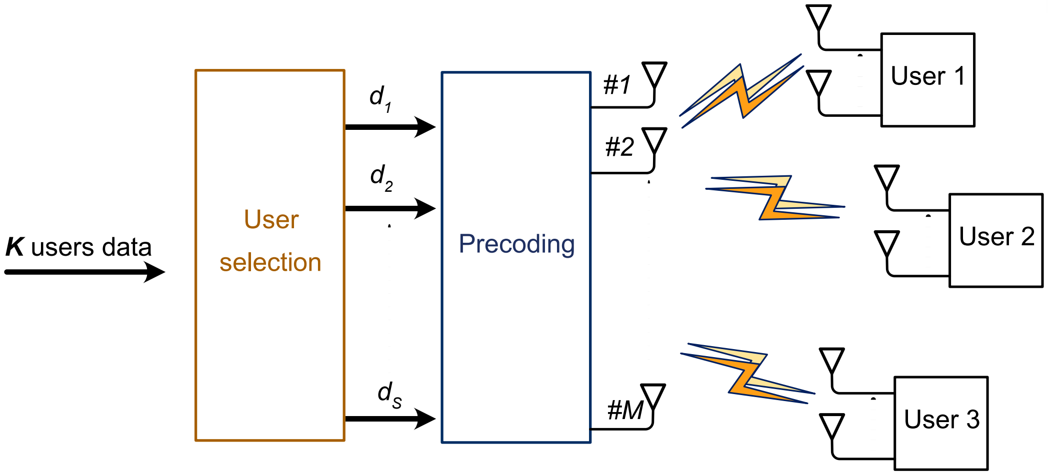
- Concurrent data connections
- Spatial separation of communication channels
- Single antenna at the transmitter (Tx) and the receiver (Rx) => Single Input Single Output (SISO)

Multiple Input Multiple Output (MIMO)

- Multiple antennas Tx and Rx
- Multiple data streams

MU-MIMO

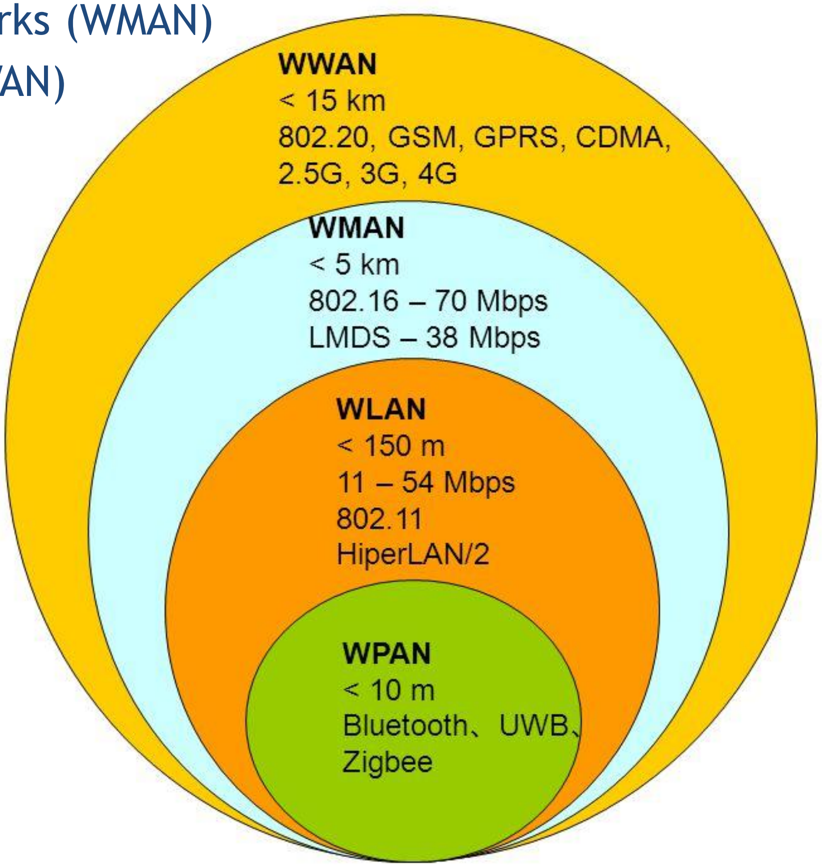
- Single Tx (e.g., access point) transmits to multiple users (multiple Rxs) simultaneously
- Increased efficiency
- Reduced latency



Types of wireless area networks

Classification:

- Wireless Personal Area Networks (WPAN)
- **Wireless Local Area Networks (WLAN)**
- Wireless Metropolitan Area Networks (WMAN)
- Wireless Wide Area Networks (WWAN)



W(X)AN differs in:

- Coverage
- Bit rates rates
- Technology

IEEE 802 family

Layers

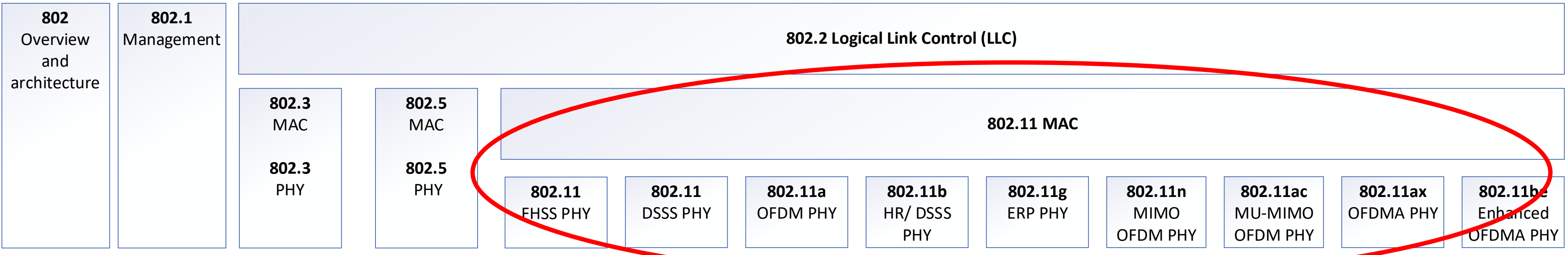
- **Physical Layer** (PHY)
- **Medium Access Control** (MAC)
- **Logical Link Control** (LLC)

Wireless Local Area Network (WLAN)

- **IEEE 802.11** – specifies **Physical Layer** (PHY) and **Medium Access Control** (MAC)

Wireless Fidelity (Wi-Fi) alliance

- Alliance of Wi-Fi device developers
- Compatibility certification



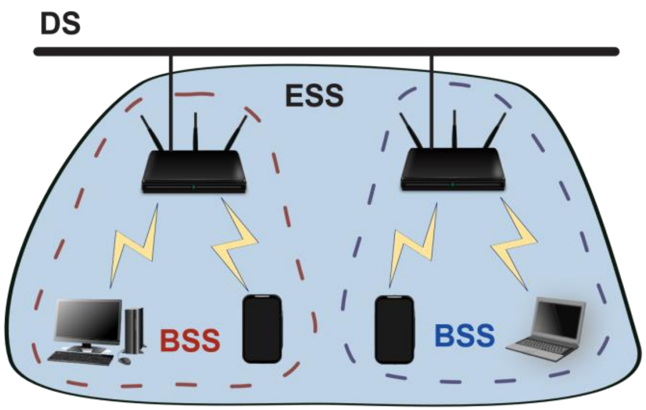
https://ieeexplore.ieee.org/browse/standards/get-program/page/series?id=68
M. Gast, "802.11 wireless networks: the definitive guide." *O'Reilly Media, Inc.*, 2005.

Topology & Terminology

Communication topology

Terminology

- **Distribution system** (DS)
  - Must provide a specified set of services, mostly exploited - Ethernet
- **Stations**
  - Clients (phones, tablets, laptops,…)
- **Access Point** (AP)
  - Provides wireless connectivity and is connected to DS
- **Basic Service Set** (BSS)
  - Group of Stations that communicate together
- **Extended station set** (ESS)
  - Multiple BSSs linked together
- **Service Set Identifiers** (SSID)
  - Name of network (BSS area)
- **Extended Service Set Identifiers** (ESSID)
  - Name of network (ESS area)
- **Basic Service Set Identifiers** (BSSID)
  - Identification of APs and clients

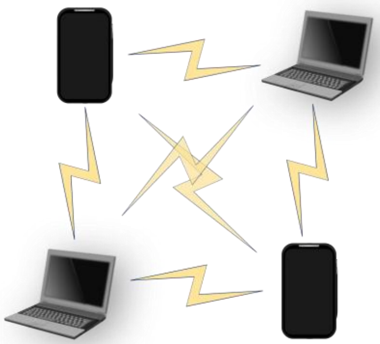


Wi-Fi topology

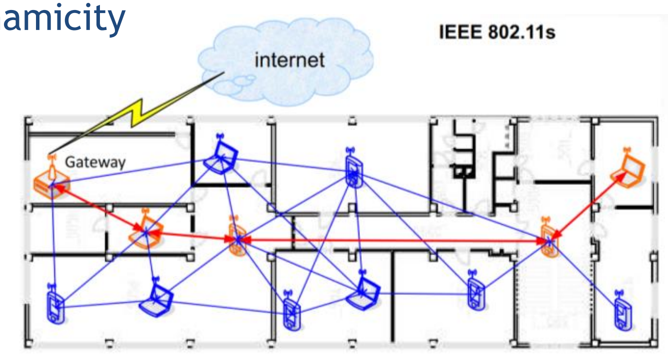
Topologies

- **Infrastructure**
  - Devices communicate through **infrastructure** (APs)

- **Ad-hoc**
  - **No centralized management**
  - **Independent BSS** (IBSS)
  - All devices equal
  - Dynamic network



- **Mesh 802.11s**
  - Mix of Ad-hoc and infrastructure
    - Devices **communicate with gateway (e.g., APs)**
    - **Device can use another device(s) to reach the gateway**
    - **Multi-hop communication**
  - Low dynamicity

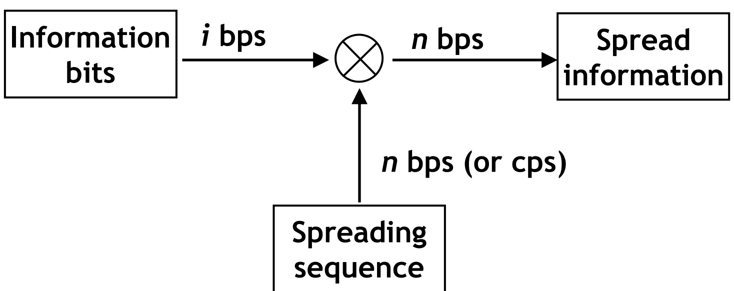


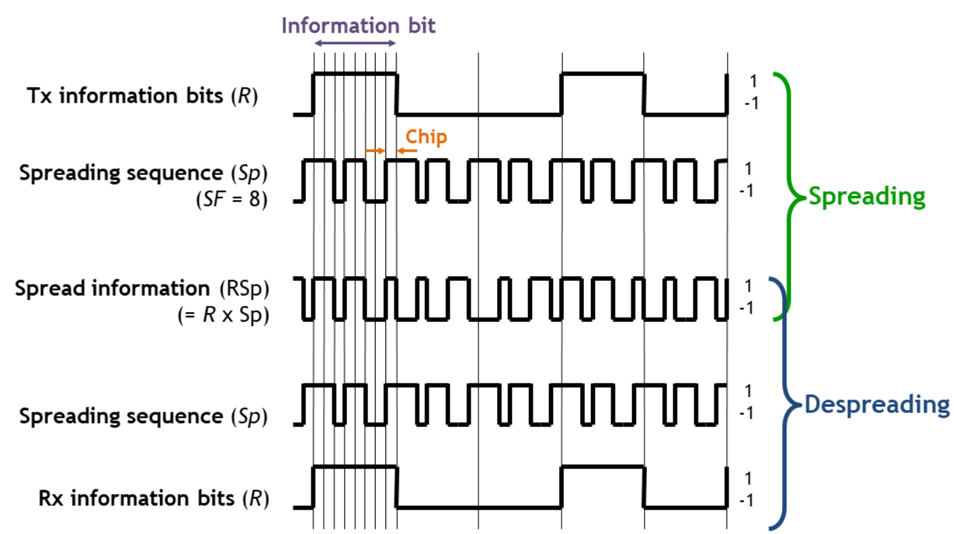
802.11: PHY layer

Direct Sequence Spread Spectrum (DSSS)

Spreading

- Each **information bit** processed by a certain number of bits of **spreading (chipping) sequence**
  - Spreading sequences at Tx and Rx identical and synchronized
- Chip – binary digit for spreading (encoding)
  - Pseudorandom noise code, must run at much higher rate than the information bits
- **Spreading Factor (SF)**
  - Ratio of spreading sequence **bitrate (n)** to **information bit rate (i)**
    - i.e., number of bits in spreading sequence per information bit ($SF = n/i$)





Pros:

- Transmission looks like noise
- Robust against jamming and interference

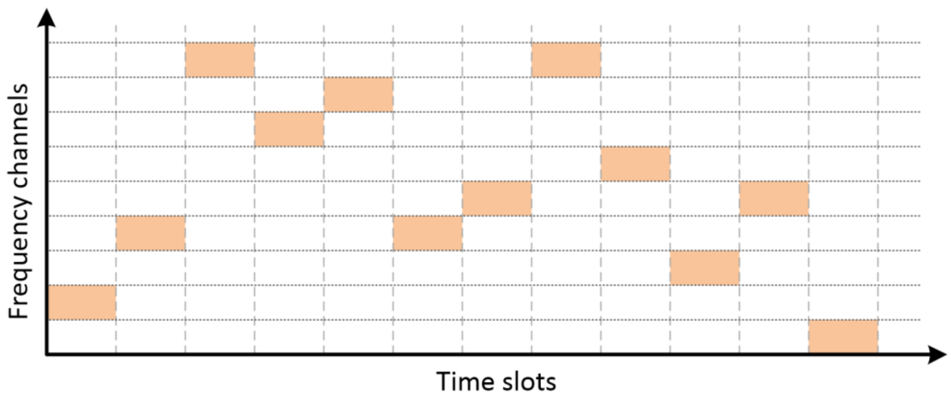
Cons:

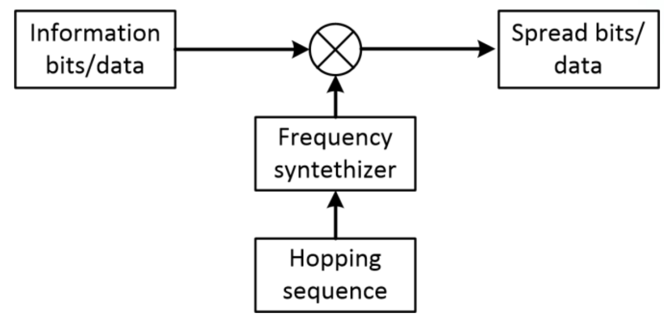
- Original DSSS has very low throughput (2 Mbit/s)
  - Enhanced with HR/DSSS => use of complementary code keying (CCK) improving rates to 11 Mbit/s

Frequency Hopping Spread Spectrum (FHSS)

Transmission frequency channels determined pseudo-randomly

- **Station "hops" between communication channels**
  - Dwell time – time spend at one frequency
- Multiple stations share communication spectrum
  - **Frequency reuse**
- Both Tx and Rx must know the hopping sequence





Pros:

- Robust transmissions in interference environment (multipath)
  - Up to 10 APs w/o significant interference

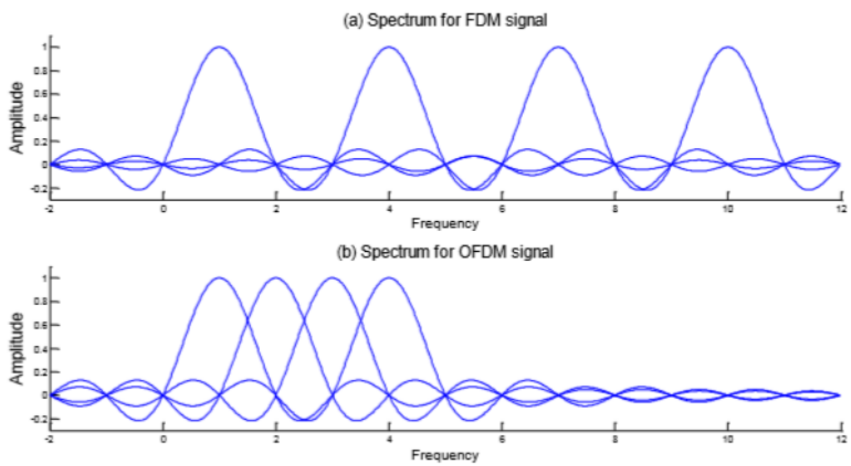
Cons:

- "Bursty" errors due to selective frequency fading
- Low coverage range
- Low data rates (only 1 or 2 Mbit/s)

Orthogonal Frequency Division Multiplex (OFDM)

Carrier multiplexing

- Overlapping but not interfering **channels** -> **orthogonal**



Pros:

- Efficient usage of spectrum wrt FDM
  - High data rates (initially up to 54 Mbit/s and improved further with newer WiFi generations)
- Resistance to frequency fading
- Inter symbol interference (ISI) eliminated with cyclic prefix (CP)

Cons:

- High peak to average power ratio => more complex power amplifier needed
- Sensitive to Doppler shift

Data rate calculation OFDM based

$$\text{Data Rate in Mbit/s} = \frac{\text{Data Subcarriers} * \text{Modulation} * \text{Coding} * \text{Spatial Streams}}{\text{Data Interval Time} + \text{Guard Interval}}$$

Example **802.11n**

- Data Subcarriers = 52 (20 MHz channel)
- Modulation = 64-QAM (6 bits/symbol)
- Coding = 5/6
- Spatial Streams = 2
- Data Interval Time = 3.2 μs
- Guard Interval = 0.4 μs

$$\text{Data Rate} = \frac{52 * 6 * 5/6 * 2}{3.2 + 0.4} = 144.4 \text{ Mbit/s}$$

https://dot11.exposed/2018/11/29/802-11-ofdm-data-rates-the-math-behind-the-numbers/
IEEE 802.11/b https://disi.unitn.it/locigno/didattica/NC/09-10/A02_report1.pdf

802.11: MAC layer

Accessing medium

Contention-based

- Multiple stations may transmit at the same time & frequency
  - ALOHA, Slotted ALOHA, CSMA/CD, **CSMA/CA (DCF, EDCF)**

Contention-free

- Collision avoided – each station uses exclusively allocated resources
  - FDMA, TDMA, CDMA, OFDMA, **CSMA/CA (PCF, HCF)**

Carrier Sense Multiple Access-Collision Avoidance (CSMA-CA)

Tailored for transmission over wireless medium

- **Carrier sense (CS)**
  - Sensing of medium before sending data => data are sent only if medium is not used by other stations (“listen before talk” approach)
- **Multiple access (MA)**
  - Several stations may access the same medium => possible collisions (if two or more stations transmit simultaneously)
- **Collision avoidance (CA)**
  - Schedule transmissions to avoid collisions (not like CSMA-Collision Detection used in wired networks)

Types of CSMA-CA

- Contention based (DCF, EDCF)
- Contention free (PCF, HCF)

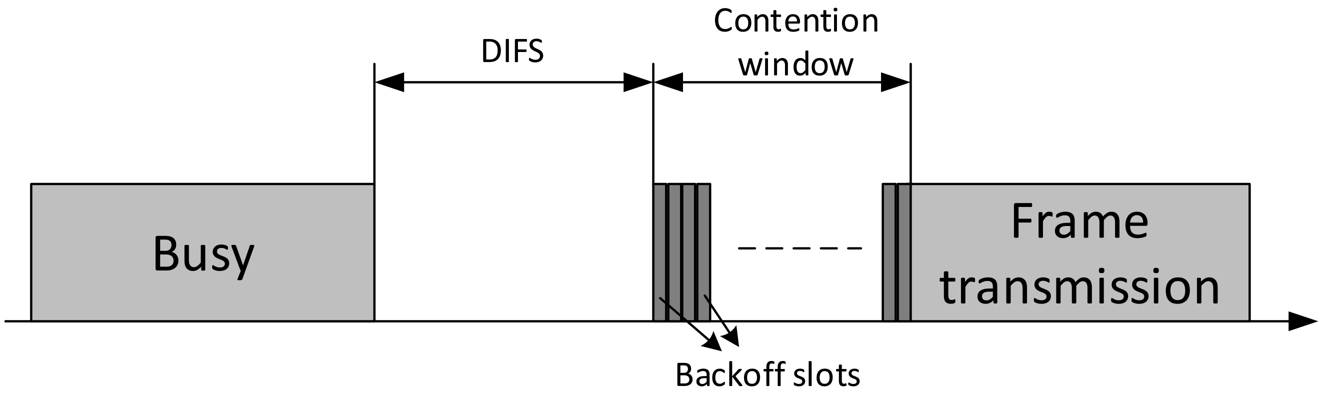
Distributed Coordination Function (DCF) (1/3)

Process of accessing the medium managed by each station

- Contention-based (no coordination at the side of AP)

Terminology

- DCF Interframe Space (DIFS)
  - Minimum idle time for contention-based services (28 and 50 microseconds)
- Contention window
  - Window divided into “backoff” slots
  - Each slot is selected with equal probability
- Frame transmission
  - Station can transmit after elapsing of DIFS+N*Number of contention slots



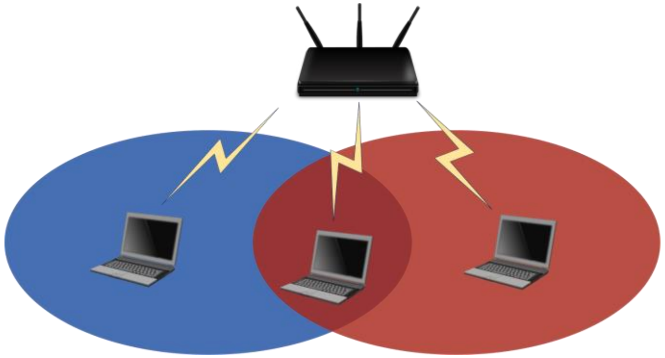
Distributed Coordination Function (DCF) (2/3)

How DCF works?

- Station monitors the activity on medium (i.e., carrier sensing)
- If medium is currently occupied
  - random backoff is initiated => after elapsing the station checks the medium again
- If medium is not occupied
  - Check the channel more thoroughly for DIFS
  - If medium is still not occupied after DIFS => random backoff is generated within contention window
  - Station selecting first slot wins
    - If collision(s) occur, the size of contention window is doubled to decrease a probability of another collision (up to 1023 slots) and random backoff is generated again

Issues of initial DCF

- Hidden node problem
  - Some stations cannot hear each other -> Collision
- Frequent sensing can deplete battery of stations



Distributed Coordination Function (DCF) (3/3)

Hidden node problem addressed by:

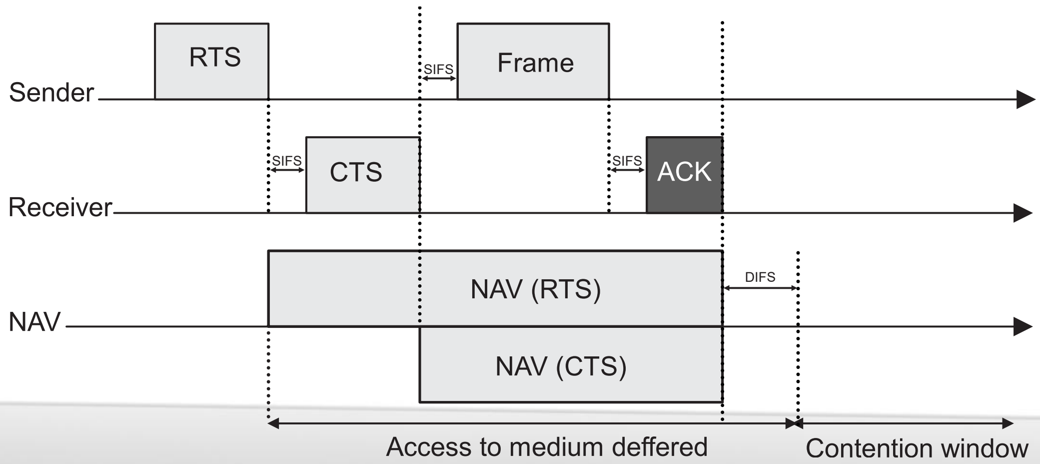
- Request to send (RTS) and Clear to send (CTS) packets
- Each packet received correctly needs to be acknowledged by ACK packet

Battery depletion problem addressed by:

- Network Allocation Vector (NAV)
  - Active station notifies all stations in range for how long the medium will be reserved
  - Other stations know how long the medium will be busy => sensing is done only if station knows medium is not busy

Short Interframe Space (SIFS)

- Dedicated for transmission with the highest priority (RTS, CTS, ACK)
- SIFS is much shorter than DIFS (10 to 16 microseconds)



Point Coordination Function (PCF)

Process of accessing the medium managed by AP

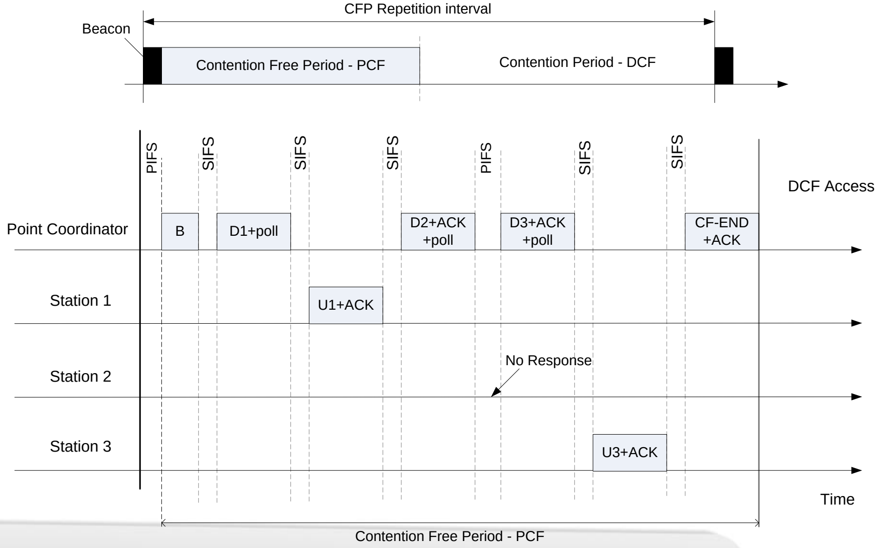
- Contention-free => no collisions

Transmits Beacon frame

- NAV set to maximum duration to lock out DCF access

Inclusion of stations into polling list

- Stations get to polling list when they associate with AP
- (CF-)Poll – license to transmit one frame by station
- (CF-)ACK – station ack receipt of frame
- If no transmission, AP moves to next station after PCF Interframe Space (PIFS)
  - Duration of PIFS is usually 19 or 30 microseconds (shorter than DIFS, longer than SIFS)
- Transmissions separated by SIFS
- CF-End – end of Contention-free period
  - Start of DCF



Quality of Service (QoS) support

Priority (0-7)	Access category	Data type
0	0	Best effort
1, 2	1	background
3, 4, 5	2	video
6, 7	3	voice

Legacy 802.11 does not support QoS

- **Throughput** not guaranteed (video)
- **Latency** not guaranteed (voice)

802.11e amendment (adopted in 2005)

- Definition of access category (AC) between 0 to 3
- Different priority and AC for different type of data

Access Methods:

- **Enhanced Distributed Channel Access** (EDCA)/EDCF
  - Extension of DCF
  - QoS traffic prioritization support via AC
    - Arbitration Inter-frame Space (AIFS) based on AC: shorter for higher priority, longer for lower priority
- **Hybrid Coordination Function** (HCF)
  - Works similarly as PCF
    - But it allows instantaneous contention free access anytime during contention based
  - Transmit Opportunity (TXOP) – time to send (multiple) frames - frame burst

MAC frame

Frame control	Duration/ ID	Address 1	Address 2	Address 3	Sequence control	Address 4	Data	FCS

Frame control (2 bytes)

- Protocol version, Type ands subtype of the frame

Duration/ID (2 bytes)

- NAV, Battery save mode (switch from standby to get all data from the AP buffer)

Address 1-4 (6 bytes each address)

- 48-bit IEEE MAC address
- Destination (DA) / Source (SA)
- Receive (RA) / Transmitter (TA)

Sequence control (2 bytes)

- Used to defragment and discard duplicate frames
- 4 bits – fragment number (FN), 12 bits – sequence number (SN)

DATA (up to 2 312 bytes)

- User data with maximum payload of 2304 B

FCS (4 bytes)

- Checksum computed from MAC header and data

Evolution of IEEE 802.11

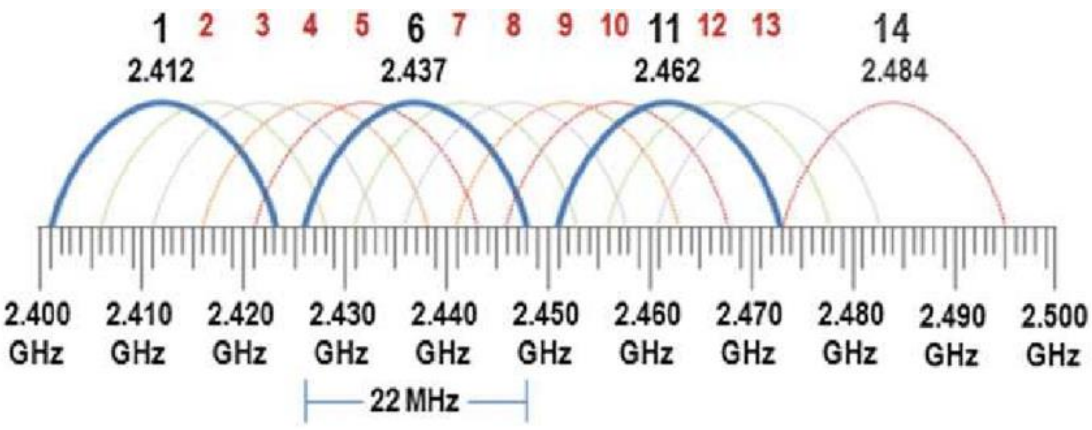
Wi-Fi Evolution (1/6)

IEEE 802.11 (Generation: Wi-Fi 0)

- Adopted in 1997
- PHY layers
  - DSSS/FSSS (also infrared is possible, but not used very often)
  - 1 or 2 Mbit/s
- Frequency bands and channels
  - 2.4 GHz,
  - EU – 13, US – 11 (3 non-overlapping channels)
  - Japan -14 (4 non-overlapping channels)

IEEE 802.11b (Wi-Fi 1)

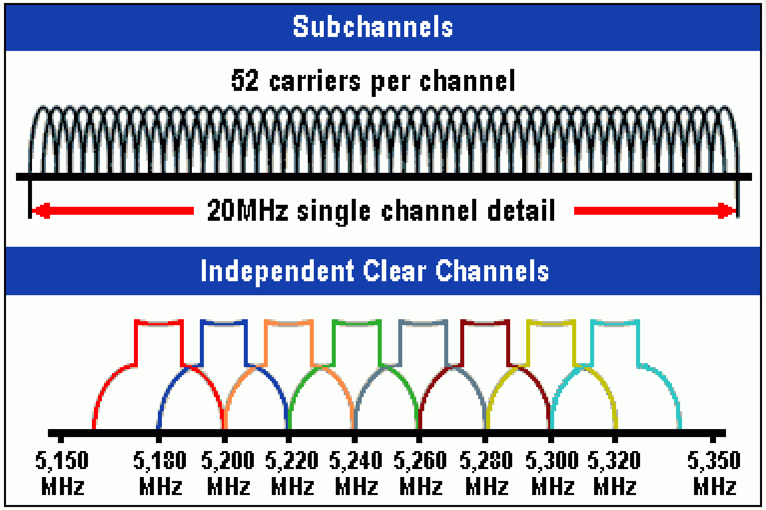
- Adopted in 1999
- PHY layers
  - HR/DSSS (BPSK, QPSK)
  - Up to 11 Mbit/s
- Freq. bands and channels
  - Same as 802.11



Wi-Fi Evolution (2/6)

802.11a (Wi-Fi 2)

- Adopted in 1999
- PHY layers
  - OFDM (BPSK, 16QAM, 64QAM)
  - Up to 54 Mbit/s
- Frequency bands and channels
  - 5 GHz with 20 MHz OFDM channel
  - 52 (sub-)carriers



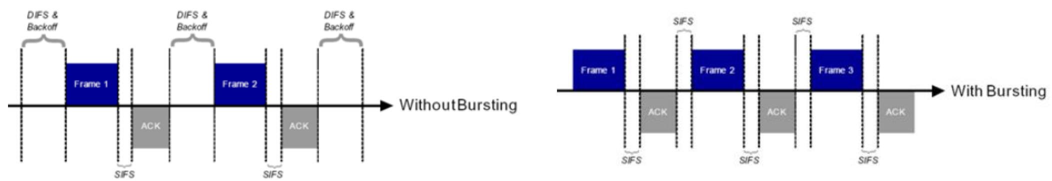
802.11g (Wi-Fi 3)

- Adopted in 2003
- PHY Layers
  - 2.4 GHz with 22 MHz OFDM channel
  - Same channels as in 802.11/b
  - Up to 54 Mbit/s
- Backward compatible with 802.11b

Wi-Fi Evolution (3/6)

802.11n (Wi-Fi 4)

- Adopted in 2008
- Main motivation is to:
  - **Improve data rates**
  - Backward compatibility with legacy devices (802.11b/g)
- Improvements at PHY layer
  - Increase of channel bandwidth from **20 MHz** to **40 MHz**
  - MIMO-OFDM
    - 4x4 (4 Tx/Rx antennas, 4 spatial streams)
  - *Optional* Low Density Parity Check (LDPC)
    - Correct great errors perfectly and leads to more reliability
- Improvements at MAC layer
  - Frame Aggregation
    - Multiple Ethernet frames wrapped in single 802.11n frame => Significant amount of overhead due to MAC header fields
  - Frame bursting
    - One station can send several frames in a row using only SIFS instead of DIFS and backoff (already introduced in 802.11e)

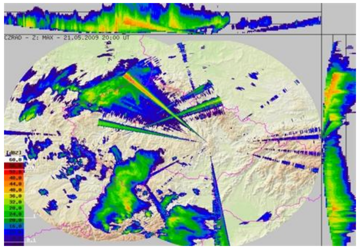


  - Block acknowledgment for multiple MAC protocol data units
- Data rates up to **600 Mbit/s** (40 MHz channel bandwidth=>108 subcarriers, 64 QAM, coding rate 5/6, 4x4 MIMO)

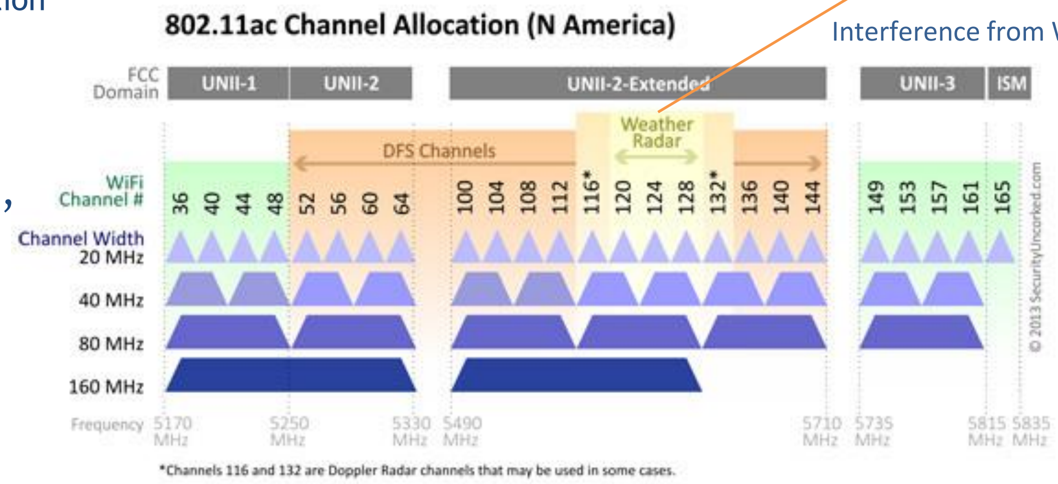
Wi-Fi Evolution (4/6)

802.11ac (Wi-Fi 5)

- Adopted in 2014
- Improvements at PHY layer wrt 802.11n
  - Increase of channel bandwidth up to **160 MHz**
  - MU MIMO-OFDM
    - **8x8** (8 Tx/Rx antennas, 8 spatial streams, 4 users)
  - Beamforming (focusing signal towards Rx)
  - 256 QAM resulting in 8 bits sent in one symbol (only for high channel quality)
- Improvements at MAC layer wrt 802.11n
  - More efficient frame aggregation
- Data rates up to **6.933 Gbit/s** (160 MHz channel bandwidth=>468 subcarriers, 256 QAM, coding rate 5/6, 8x8 MIMO)



Interference from WiFi



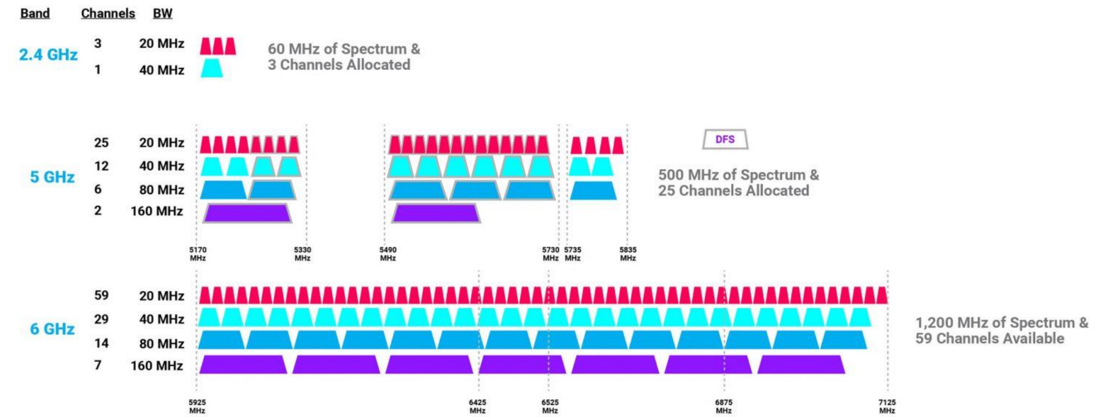
UNII - Unlicensed National Information Infrastructure

DFS - Dynamic Frequency Selection

Wi-Fi Evolution (5/6)

802.11ax (Wi-Fi 6/6e)

- Adopted in 2019 (Wi-Fi 6) and 2020 (Wi-Fi 6e)
- Motivation to reduce **energy consumption** besides data rates improvement
- Improvements at PHY layer wrt 802.11ac
  - **Orthogonal Frequency Multiple Access** (OFDMA)
    - Much more efficient than CSMA-CA => increases user data rates and reduces latency, especially for large numbers of devices with short frames or low data rate requirements (IoT devices)
    - Transmission divided in time and frequency domains, called resource units (RUs)
    - Multiple users can use different RUs at the same time
    - (Adopted also in 4G and beyond)
  - 1024 QAM resulting in 10 bits sent in one symbol
  - Mandatory LDPC for large bands
- Improvements at MAC layer wrt 802.11ac
  - Target Wake Time (TWT) – wake client at a defined time
    - Reduces energy consumption
- Data rates up to **9.608 Gbit/s**



Wi-Fi Evolution (6/6)

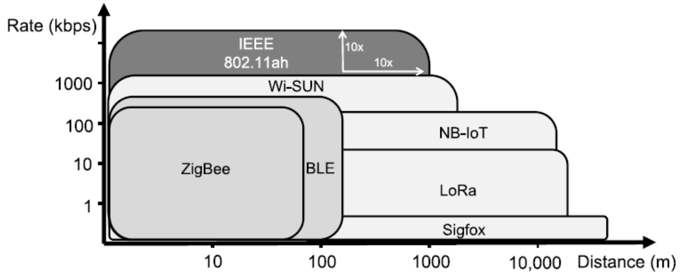
802.11be (Wi-Fi 7)

- Adopted in ~ 2024
- Extremely High Throughput (EHT)
  - Expected up to 46.120 Gbit/s
- Build on IEEE 802.11ax
- Bands 2.4/5/6 GHz
  - 320 MHz bandwidth
  - 4096 QAM
  - 16 spatial streams
  - Multi-Band aggregation
- Multi-AP Coordination
  - Coordinated and joint transmission
  - Coordinated beamforming

IEEE 802.11 - others

802.11ah – HaLow

- Adopted in 2017
- **High reach Low Power consumption**
  - **Internet of Things (IoT)** - Up to 8192 stations connected to one AP
  - Higher energy efficiency than IEEE 802.15.4 (ZigBee)
- **OFDM, 900 MHz bands**
  - 1/2/4/8/16 channel bandwidth
  - 1 km coverage
- Mechanisms
  - Relay mechanisms (between AP and user)
  - Power saving & TWT



MCS index	Modulation	Coding rate	Data rate (kbit/s) 1 MHz	2 MHz	4 MHz	8 MHz
0	BPSK	1/2	300	650	2925	5850
1	QPSK	1/2	600	1300	5850	11700
2	QPSK	3/4	900	1950	8775	17550
3	16-QAM	1/2	1200	2600	11700	23400
4	16-QAM	3/4	1800	3900	17550	35100
5	64-QAM	2/3	2400	5200	23400	46800
6	64-QAM	3/4	2700	5850	26325	52650
7	64-QAM	5/6	3000	6500	29250	58500
8	256-QAM	3/4	3600	7800	35100	70200
9	256-QAM	5/6	4000	-	39000	78000
10	BPSK	1/2 with 2x repetition	150	-	-	-

T. Le, S. Santi, A. Seferagić, J. Lan, and J. Famaey, "Wi-Fi HaLow for the Internet of Things: An up-to-date survey on IEEE 802.11 ah research." *Journal of Network and Computer Applications* 182 (2021): 103036.

IEEE 802.11 others

802.11ad (WiGig)

- Band V of mmWaves - 60 GHz (57-71 GHz) -> coverage a few meters
- Channels – each occupy 2160 MHz and provide 1760 MHz bandwidth
  - USA – 6 channels, EU, Japan, Australia – 4 channels, China – channels 2 & 3

802.11ay

- Improvements of 802.11ad
- 60 GHz with 8.64 GHz bandwidth

802.11af

- White-Fi – operation in TV white spectrum (VHF, UHF)
- Cognitive radio

802.11j

- Amendments for communication in 4.9 or 5 GHz in Japan

WiFi Direct

- Single hop
- Device to Device communication (printers, cammeras, …)
- Miracast - Streaming to displays

Security in 802.11

Typical threats/attacks in wireless networks

Denial of service (DoS)

- Sending large amount of data (packets) so the wireless medium is not accessible

Man-in-the-middle (MITM)

- Eavesdropping within range of AP to capture sensitive information

Unauthorized/rogue AP

- Fool devices into connecting with a false AP

Freeloading

- Piggybacking on a connection or intercepting file sharing

Wi-Fi Authentication - Overview

802.11 defines two types of authentication

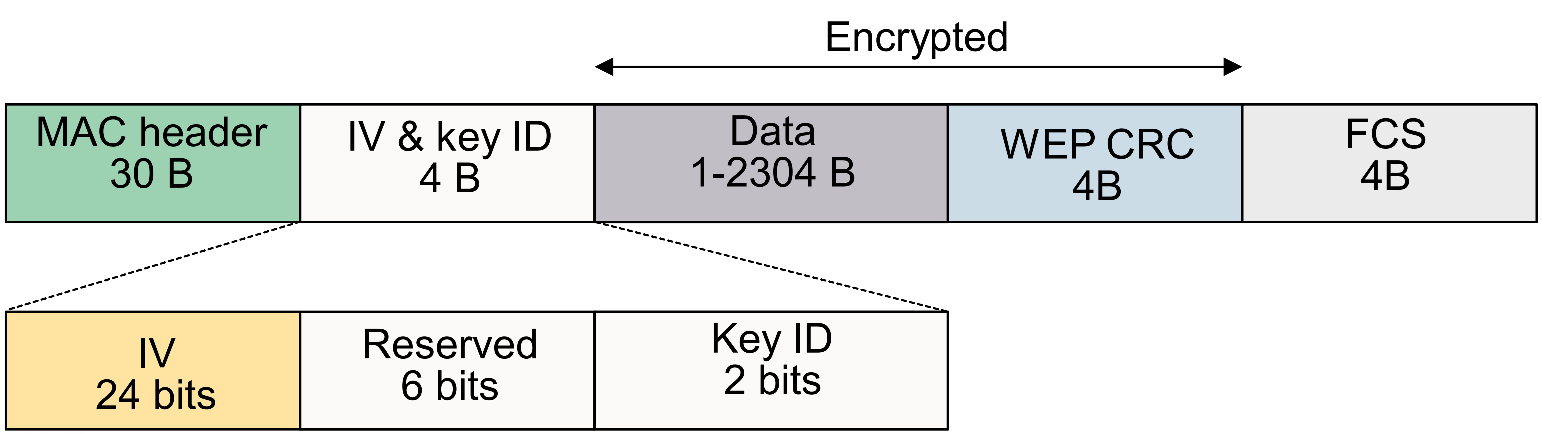
- Open system authentication
  - 1. Authentication request sent from station to AP containing typically MAC address
  - 2. Authentication response from AP with success or failure
  - Only method required by 802.11
- Shared-key
  - Wired Equivalent Privacy (WEP)
  - Wi-Fi Protected Access (WPA1-3)

Wired Equivalent Privacy

Wired Equivalent Privacy (WEP)

- Introduced to legacy 802.11 in 1997
- Key length 64,128 (default) and 256 bits
  - **Static keys** -> entered manually and does not change during session
  - 24 bit Initiation Vector (IV)
    - transmitted in an open form & changing in each frame
- Data encryption via RC4 algorithm
  - Symmetric stream cipher
  - Exclusive OR (XOR) -> vulnerability

Not secure => Encryption can be easily cracked => Superseded by WPA in 2003

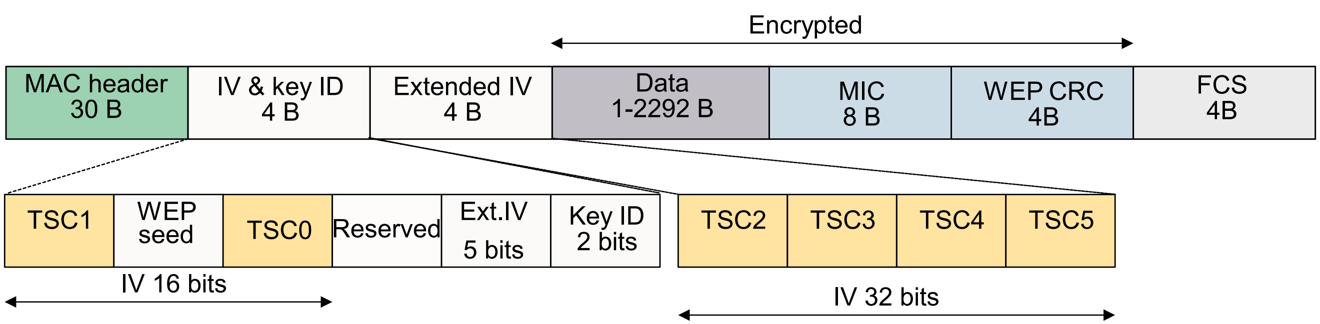


Wi-Fi Protected Access (1/2)

Wi-Fi Protected Access (WPA)

- Based on 802.11i
- Temporal Key Integrity Protocol (TKIP)
  - 64 or 128 bit encryption key with 48 bit IV
  - Support for **dynamic** keys -> different key for each packet
- Algorithm Michael (MIC)
  - MIC + CRC32 solves possibility of swapping bits within the frame
    - Out of order frames discarded
  - Prevents multiple use of IV (replay attacks)
- Pre-shared key (PSK)

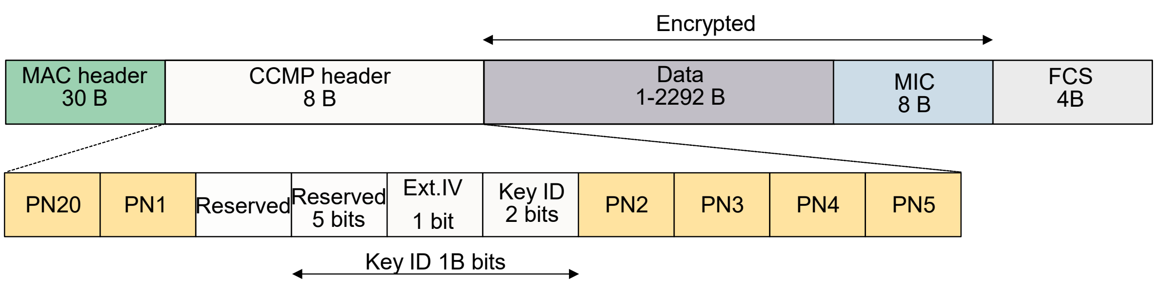
Still not secure enough due to TKIP and MIC limitations => Superseded by WPA2 in 2004



Wi-Fi Protected Access (2/2)

WPA2

- Based on IEEE 802.11i
- **Incompatible** HW between **WPA and WPA2**
- Mandatory support of Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) instead TKIP
  - Advanced Encryption Standard (AES) 128 bit



WPA3

- Required for **Wi-Fi 6 certification**
- Certified in 2018
- PSK replaced with Simultaneous Authentication of Equals (SAE)
  - More secure initial key exchange
  - Mitigate security issues posed by weak passwords

Literature

References

- M. Gast, “802.11 wireless networks: the definitive guide.” *O'Reilly Media, Inc.*, 2005.
- A. Kaoutar, "Study and optimisation of IEEE 802.11 PHY and MAC protocols towards a new generation integrated in 5G." PhD diss., *Ecole nationale supérieure Mines-Télécom Atlantique Bretagne Pays de la Loire*, 2019.
- IEEE 802.11 - https://ieeexplore.ieee.org/browse/standards/get-program/page/series?id=68
- Data rates
  - https://dot11.exposed/2018/11/29/802-11-ofdm-data-rates-the-math-behind-the-numbers/
  - IEEE 802.11/b https://disi.unitn.it/locigno/didattica/NC/09-10/A02_report1.pdf
- Encapsulation
  - https://support.mangocomm.com/docs/wlan-user-guide/mac/framework_high_eth_encap.html
- T. Le, S. Santi, A. Seferagić, J. Lan, and J. Famaey, "Wi-Fi HaLow for the Internet of Things: An up-to-date survey on IEEE 802.11 ah research." *Journal of Network and Computer Applications* 182 (2021): 103036.
- C. Deng, F. Xuming, H. Xiao, W. Xianbin, Y. Li , H. Rong, L. Yan, and G. Yuchen. "IEEE 802.11 be Wi-Fi 7: New challenges and opportunities." *IEEE Communications Surveys & Tutorials* 22, no. 4 (2020): 2136-2166.
- E. Khorov, A. Kiryanov, A. Lyakhov, and G. Bianchi. "A tutorial on IEEE 802.11 ax high efficiency WLANs." *IEEE Communications Surveys & Tutorials* 21, no. 1 (2018): 197-216.
- Wi-Fi ALIANCE, “WPA3™ Specification Version 3.0”, 2020.

CZECH TECHNICAL UNIVERSITY IN PRAGUE

FACULTY OF ELECTRICAL ENGINEERING

DEPARTMENT OF TELECOMMUNICATION ENGINEERING

Questions?

machp2@fel.cvut.cz