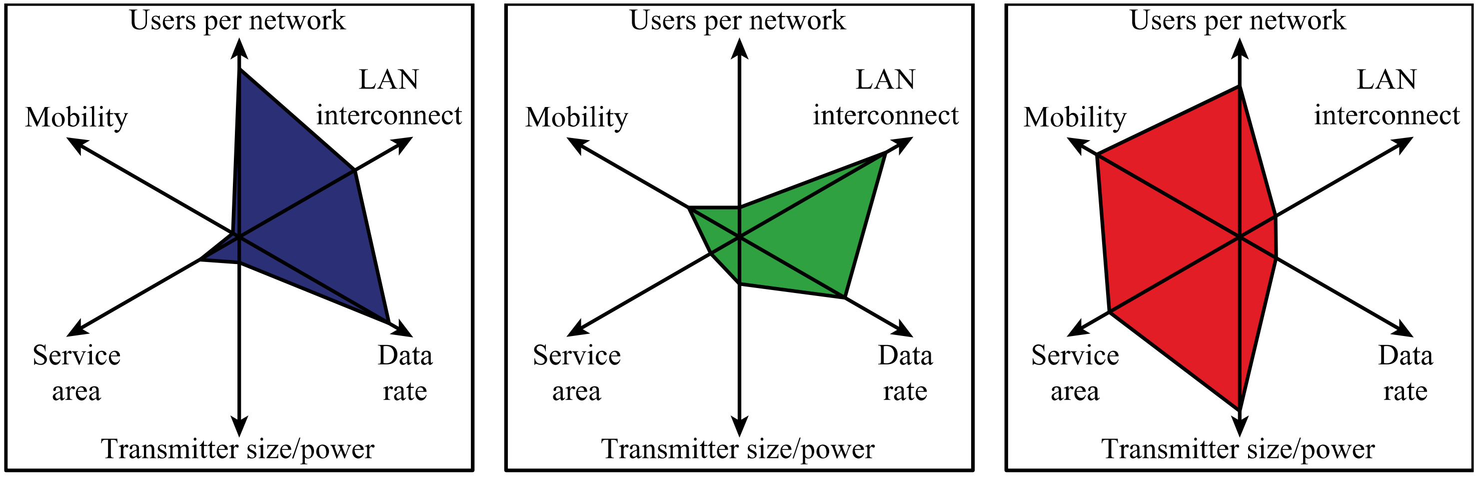
Wireless Networks and Protocols

Wireless Local Area Networks

Manuel P. Ricardo

Faculdade de Engenharia da Universidade do Porto

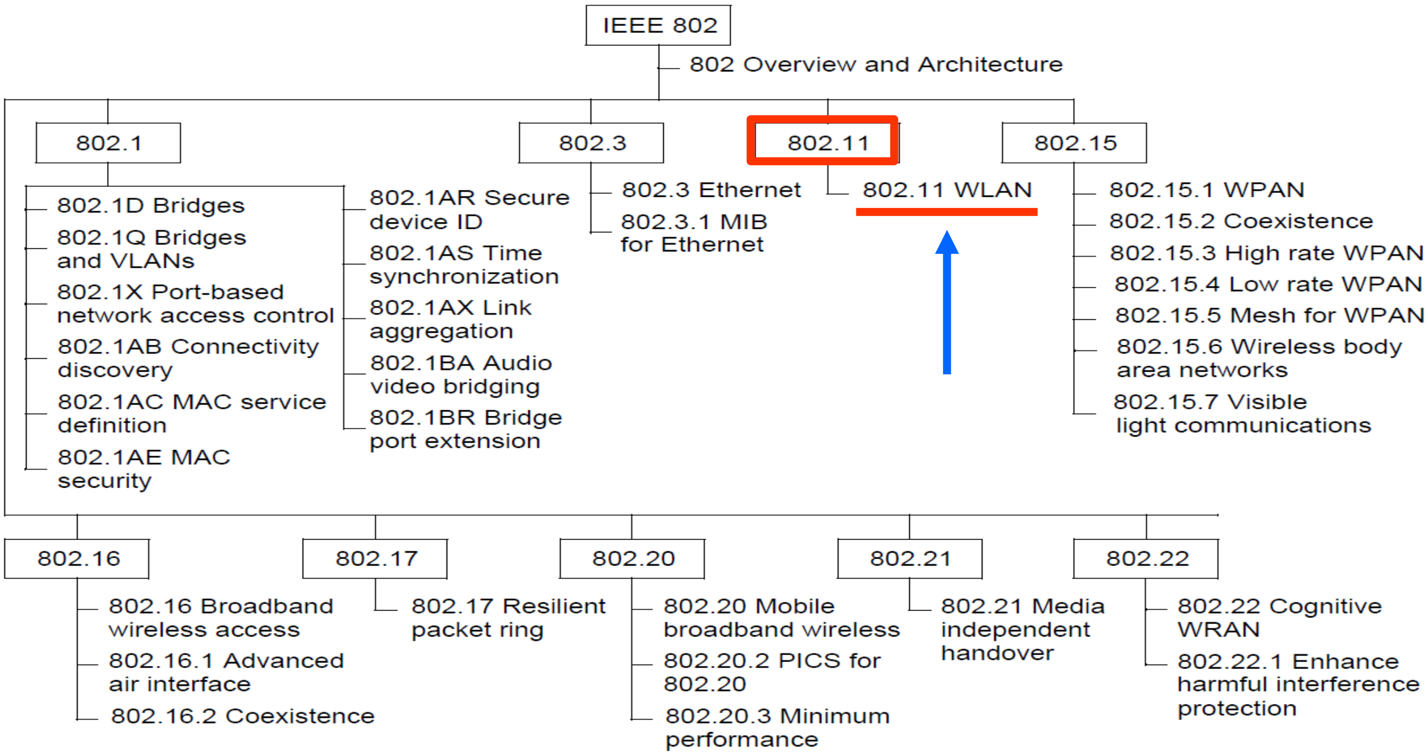
Kiviat Graphs for Data Networks



(a) Wired LANs **(b) Wireless LANs** **(c) Mobile data networks**

Wireless LAN 802.11

IEEE Standards – Family of IEEE 802 Standards



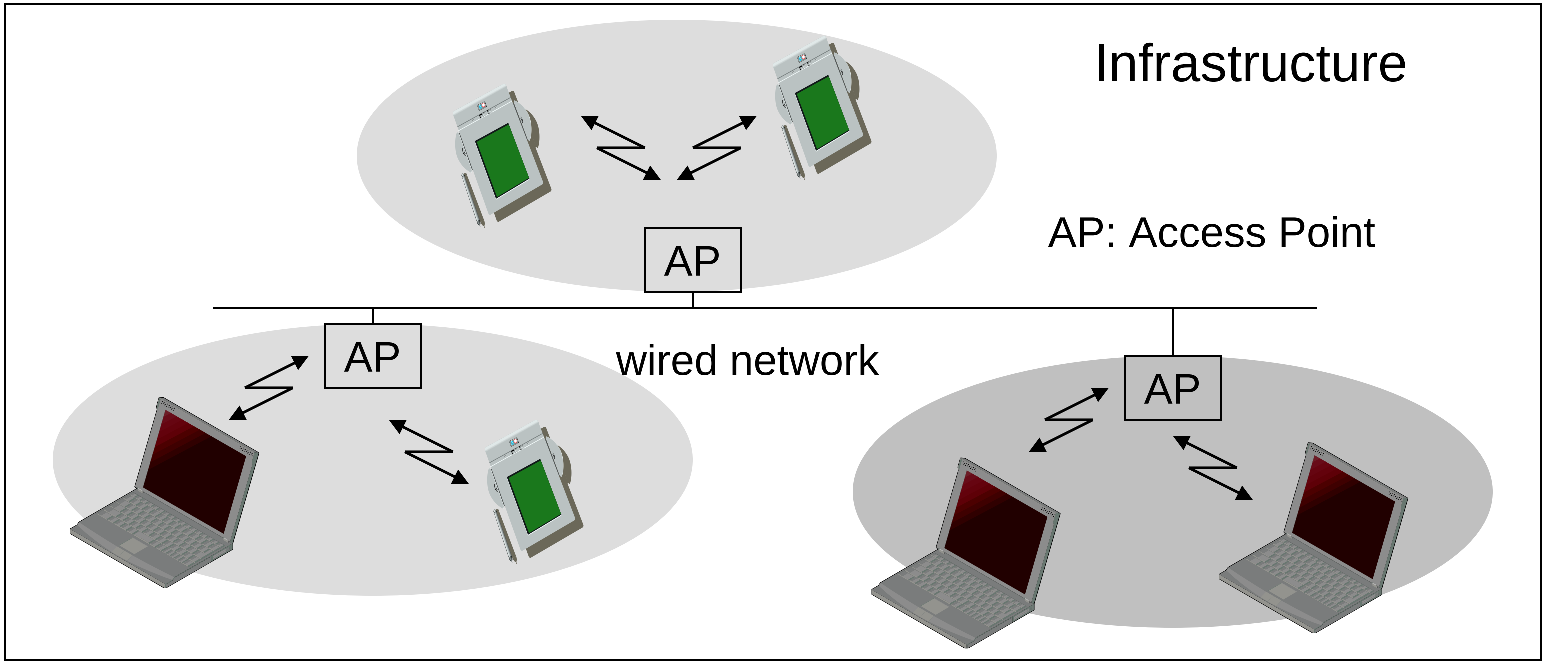
- http://standards.ieee.org/about/get/
- 802.11 - Wireless LAN (WLAN)

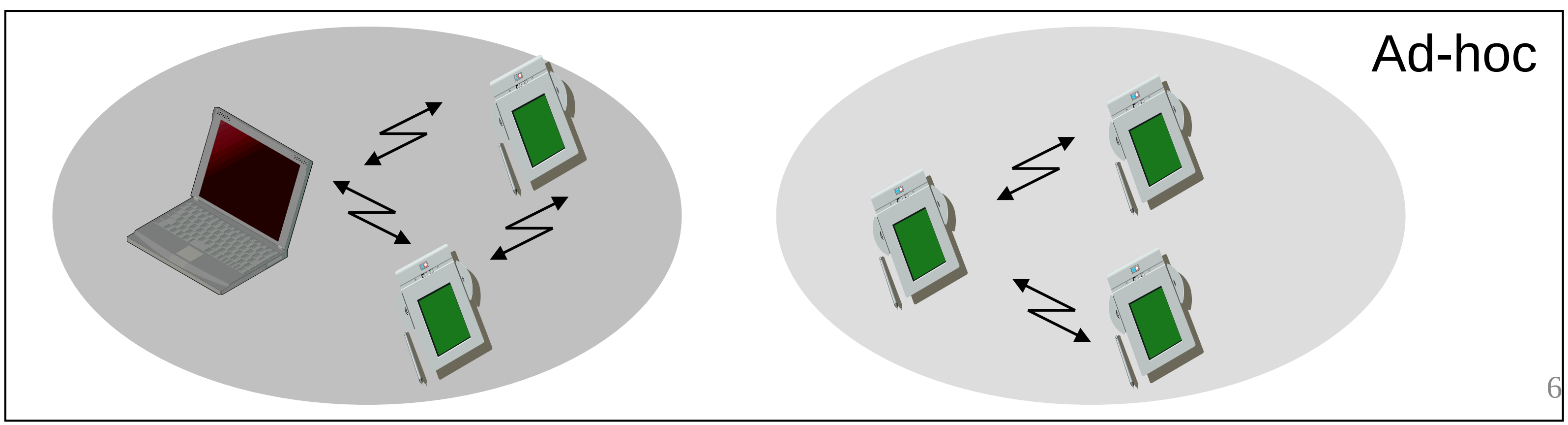
IEEE 802.11 Standards

Standard	Date	Scope
IEEE 802.11	1997	Medium access control (MAC): One common MAC for WLAN applications
		Physical layer: Infrared at 1 and 2 Mbps
		Physical layer: 2.4-GHz FHSS at 1 and 2 Mbps
		Physical layer: 2.4-GHz DSSS at 1 and 2 Mbps
IEEE 802.11a	1999	Physical layer: 5-GHz OFDM at rates from 6 to 54 Mbps
IEEE 802.11b	1999	Physical layer: 2.4-GHz DSSS at 5.5 and 11 Mbps
IEEE 802.11c	2003	Bridge operation at 802.11 MAC layer
IEEE 802.11d	2001	Physical layer: Extend operation of 802.11 WLANs to new regulatory domains (countries)
IEEE 802.11e	2007	MAC: Enhance to improve quality of service and enhance security mechanisms
IEEE 802.11f	2003	Recommended practices for multivendor access point interoperability
IEEE 802.11g	2003	Physical layer: Extend 802.11b to data rates >20 Mbps
IEEE 802.11h	2003	Physical/MAC: Enhance IEEE 802.11a to add indoor and outdoor channel selection and to improve spectrum and transmit power management
IEEE 802.11i	2007	MAC: Enhance security and authentication mechanisms
IEEE 802.11j	2007	Physical: Enhance IEEE 802.11a to conform to Japanese requirements
IEEE 802.11k	2008	Radio Resource Measurement enhancements to provide interface to higher layers for radio and network measurements

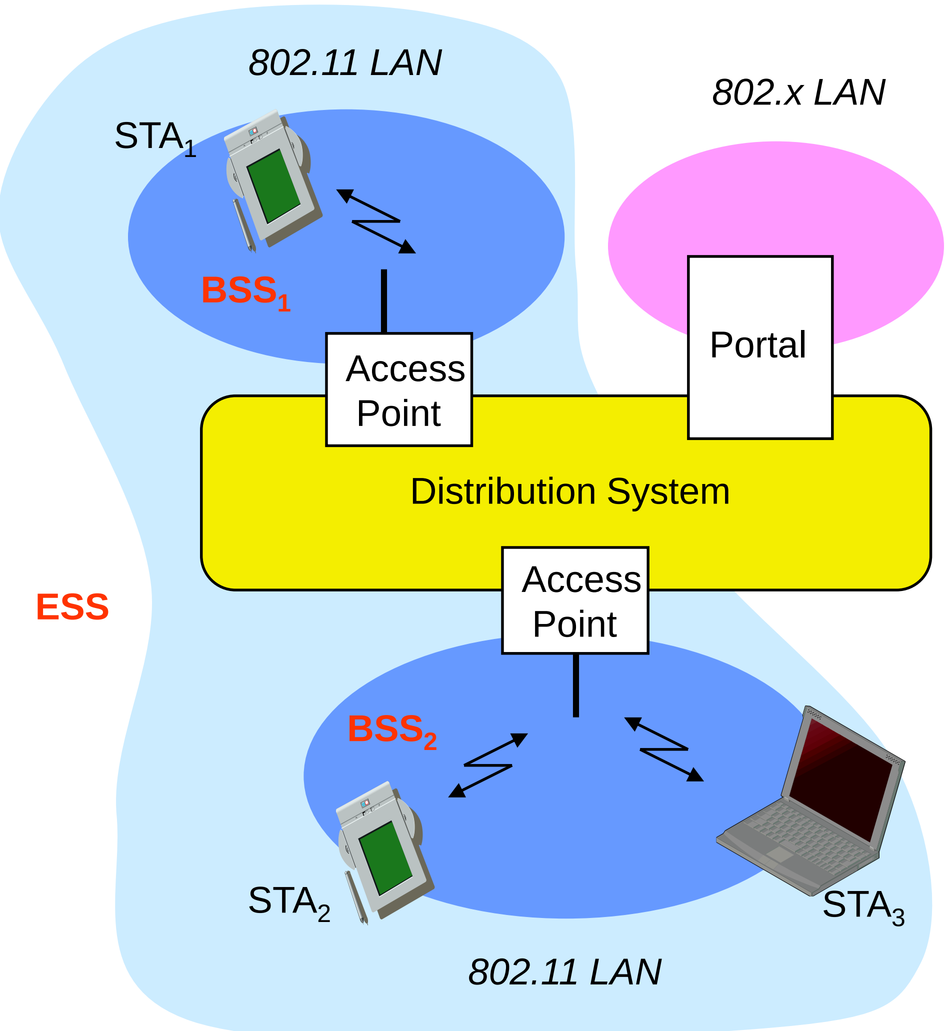
Standard	Date	Scope
IEEE 802.11m	Ongoing	This group provides maintenance of the IEEE 802.11 standard by rolling published amendments into revisions of the 802.11 standard.
IEEE 802.11n	2009	Physical/MAC: Enhancements to enable higher throughput
IEEE 802.11p	2010	Wireless Access in Vehicular Environments (WAVE)
IEEE 802.11r	2008	Fast Roaming/Fast BSS Transition
IEEE 802.11s	2011	Mesh Networking
IEEE 802.11T	Abandoned	Recommended Practice for Evaluation of 802.11 Wireless Performance
IEEE 802.11u	2011	Interworking with External Networks
IEEE 802.11v	2011	Wireless Network Management
IEEE 802.11w	2009	Protected Management Frames
IEEE 802.11y	2008	Contention Based Protocol
IEEE 802.11z	2010	Extensions to Direct Link Setup
IEEE 802.11aa	2012	Video Transport Stream
IEEE 802.11ac	Ongoing	Very High Throughput <6Ghz
IEEE 802.11ad	2012	Very High Throughput in 60 GHz
IEEE 802.11ae	2012	Prioritization of Management Frames
IEEE 802.11af	Ongoing	Wireless LAN in the TV White Space
IEEE 802.11ah	Ongoing	Sub 1GHz
IEEE 802.11ai	Ongoing	Fast Initial Link Set-up
IEEE 802.11aj	Ongoing	China Milli-Meter Wave (CMMW)
IEEE 802.11ak	Ongoing	Enhancements For Transit Links Within Bridged Networks
IEEE 802.11aq	Ongoing	Pre-Association Discovery (PAD)
IEEE 802.11ax	Ongoing	High Efficiency WLAN (HEW)

Infrastructure Networks vs Ad-Hoc Networks



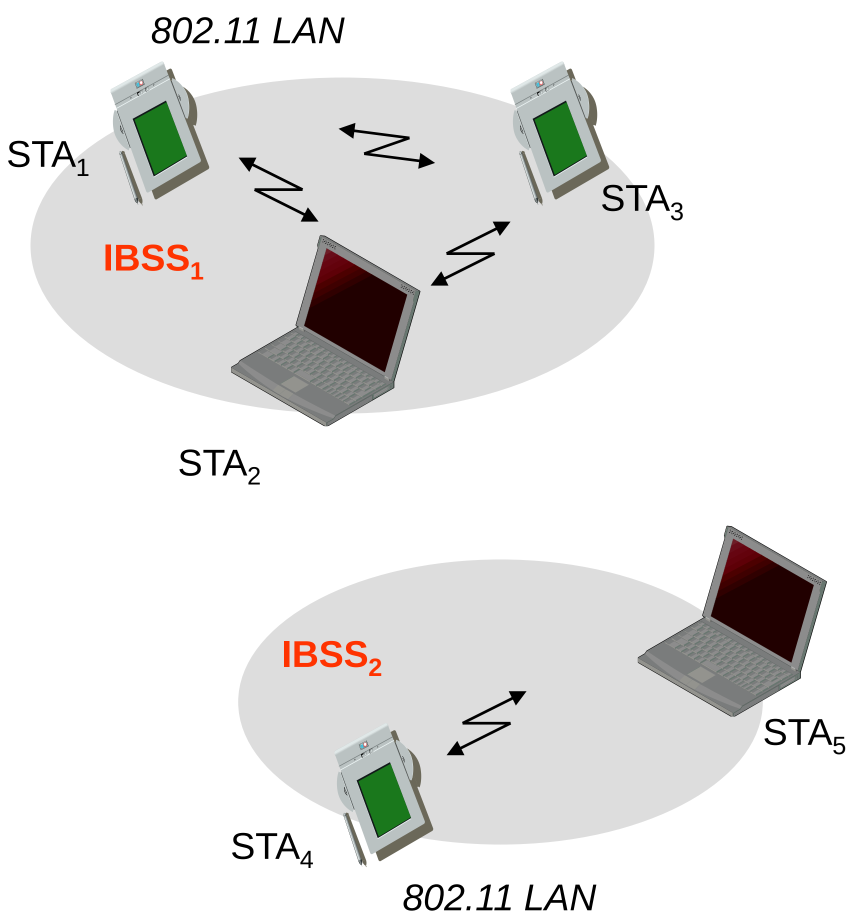


IEEE 802.11 – Infrastructure Network



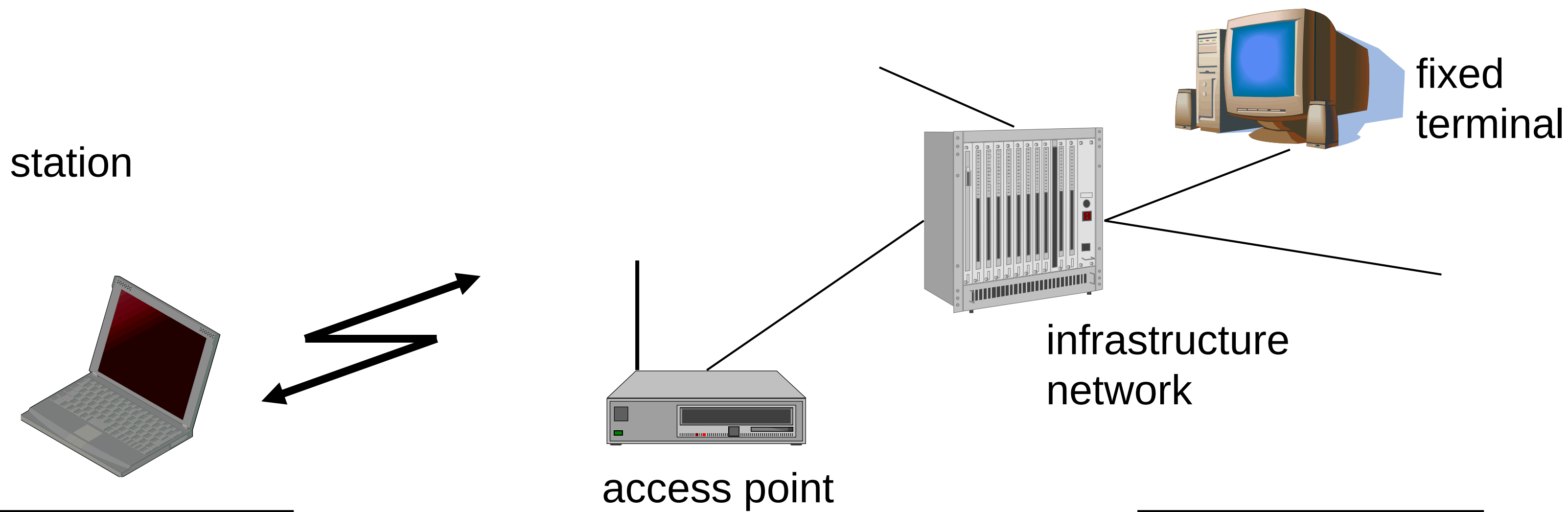
- Station
  - Terminal with radio access
- Basic Service Set (BSS)
  - Set of stations in the same channel
- Access Point (AP)
  - Interconnects LAN to wired network
  - Provides access to stations
- Stations communicate with AP
- Portal → bridge to other networks
- Distribution System
  - Interconnection network
  - Logical network
    - EES, Extended Service Set
    - Based on BSSs

IEEE 802.11 –Ad-Hoc Network



- Direct communication between stations
- Independent Basic Service Set, IBSS
  - » Set of stations working in the same channel
- IBSS and BSS are virtual networks
  - » multiple (I)BSS may co-exist
    in same channel and same space

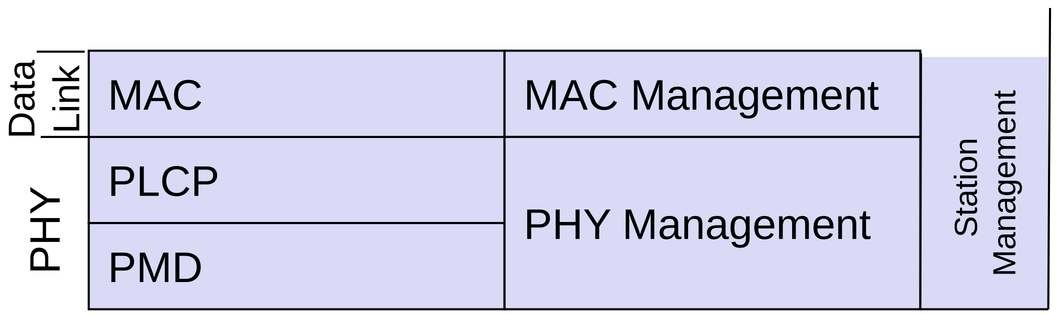
IEEE 802.11 – Protocol Stack



application			application
TCP			TCP
IP			IP
LLC	LLC		LLC
802.11 MAC	802.11 MAC	802.3 MAC	802.3 MAC
802.11 PHY	802.11 PHY	802.3 PHY	802.3 PHY

802.11 – Layers and Functionalities

- Data plane
  - MAC - medium access, fragmentation, encryption
  - PLCP - Physical Layer Convergence Protocol → convergence, carrier detection
  - PMD - Physical Medium Dependent → modulation, codes
- Management plane
  - PHY Management - channel selection, MIB
  - MAC Management - synchronization, association, mobility, power, MIB
  - Station Management - coordination of management functions



MAC Layer – Access Methods

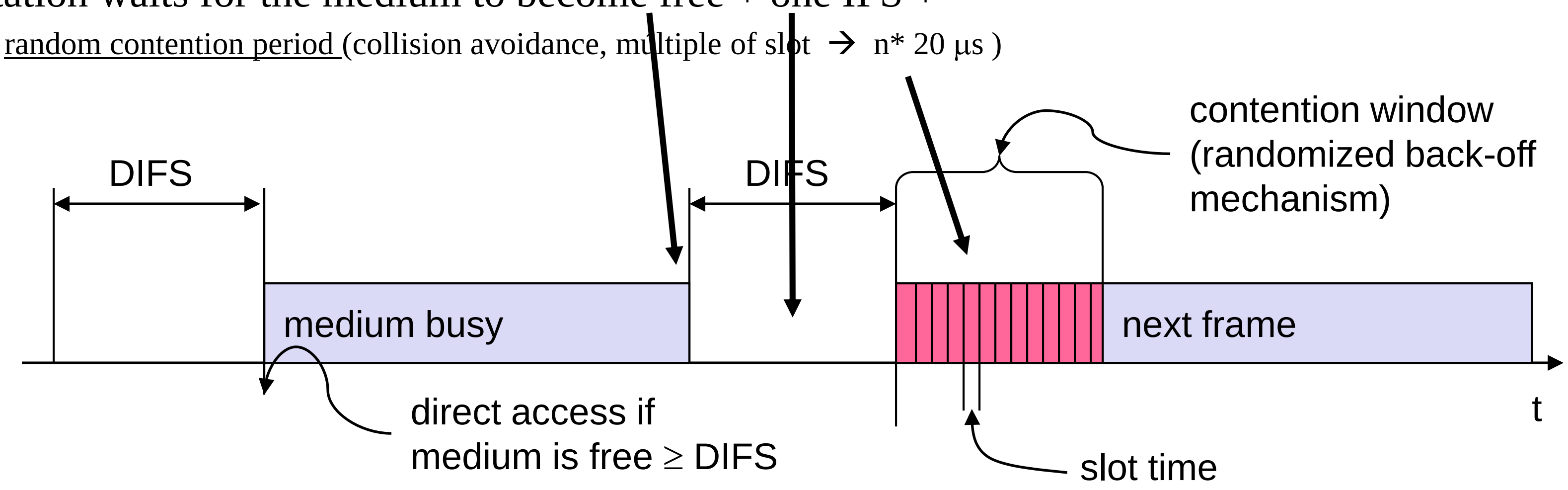
- MAC-DCF: CSMA/CA
  - Carrier sense, collision avoidance using back-off mechanism
  - ACK packet required for confirmations (except for broadcast packets)
  - Mandatory
- MAC-DCF with RTS+CTS
  - Used to avoid hidden terminal problem
  - Typically used before the transmission of long packets
  - Optional
- MAC- PCF
  - Polling
  - Access Point controls order of transmission
  - Optional (rarely used)

DCF – Distributed Coordination Function
PCF - Point Coordination Function

MAC-DCF CSMA/CA

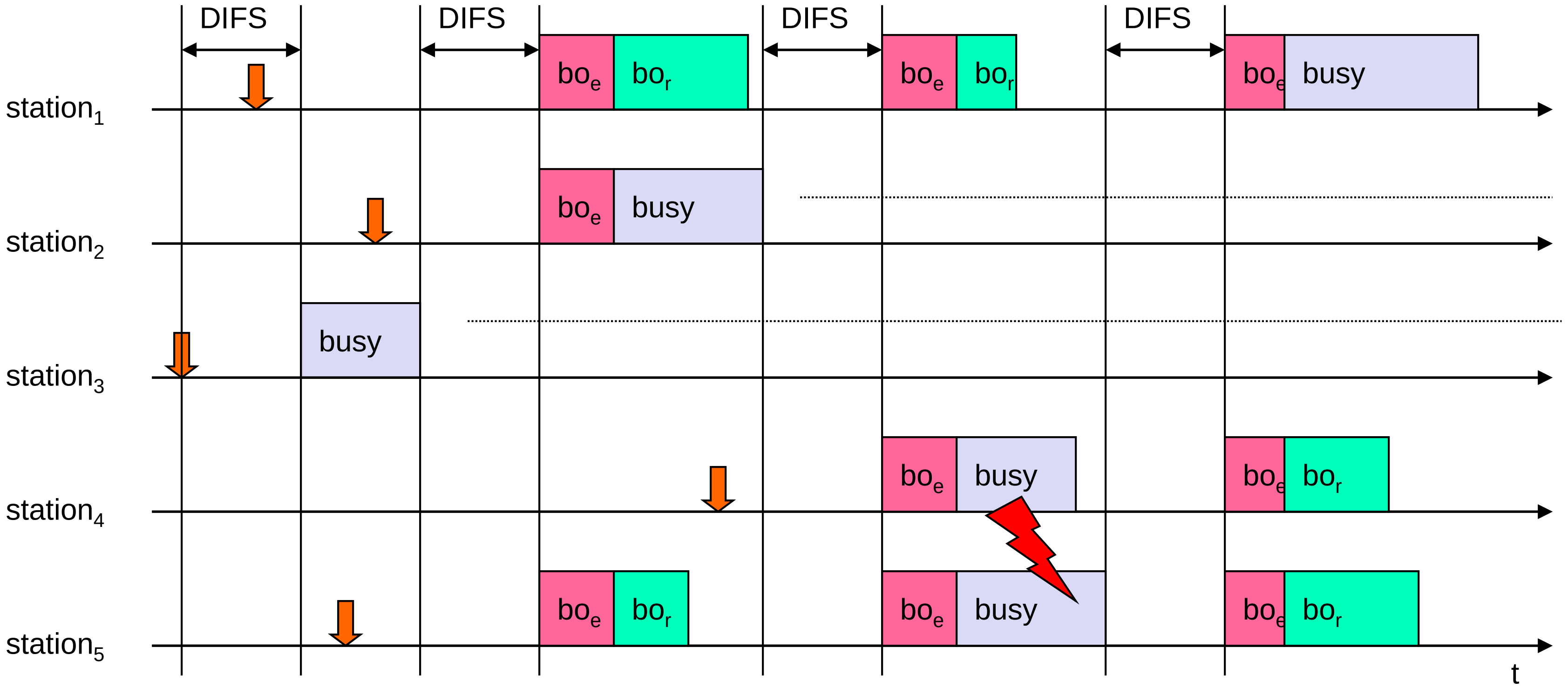
- Station having a packet to transmit senses the medium
- If the medium is free during one Inter-Frame Space (IFS)
  - » Station starts sending the frame
- If medium is busy
  - » Station waits for the medium to become free + one IFS +

    <u>random contention period</u> (collision avoidance, multiple of slot → n* 20 μs)



- If other station accesses to the medium during the contention time
  - » <u>Waiting timer is suspended</u>

MAC-DCF CSMA/CA – Concurrent Stations



busy medium not idle (frame, ack etc.)

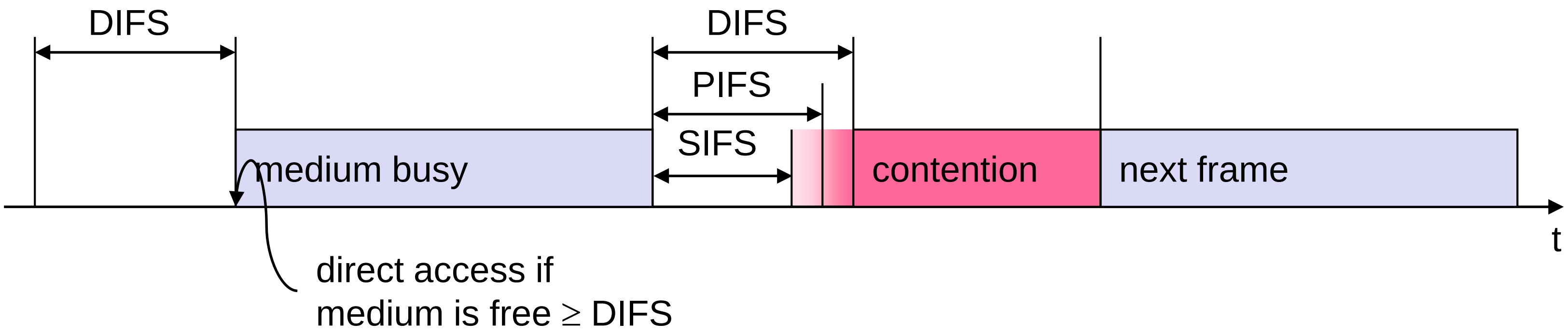
packet arrival at MAC

bo_e elapsed backoff time

bo_r residual backoff time

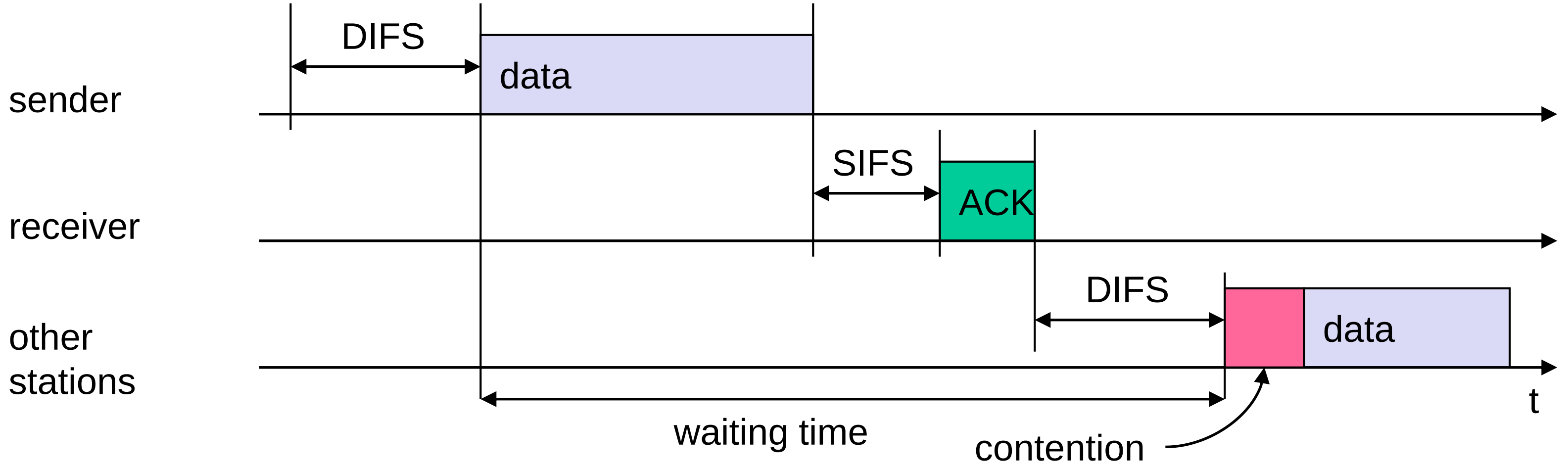
MAC Layer – Guard Time Intervals

- » DIFS (DCF IFS)
  - – Lowest priority, used for asynchronous data
- » PIFS (PCF IFS)
  - – Medium priority, used for real time traffic /QoS
- » SIFS (Short Inter Frame Spacing)
  - – Maximum priority→ used for signalling: ACK, CTS, answers to polling



MAC-DCF CSMA/CA

- Sending a frame in unicast
  - Station waits DIFS before sending the packet
  - If packet is correctly received (no errors in CRC)
    - Receiver confirms reception immediatly, using ACK, after waiting SIFS
  - In case of errors, frame is re-transmitted
  - In case of retransmission
    - Maximum value for the contention window duplicates
    - Contention window has minimum and maximum values (eg.: 7 and 255)



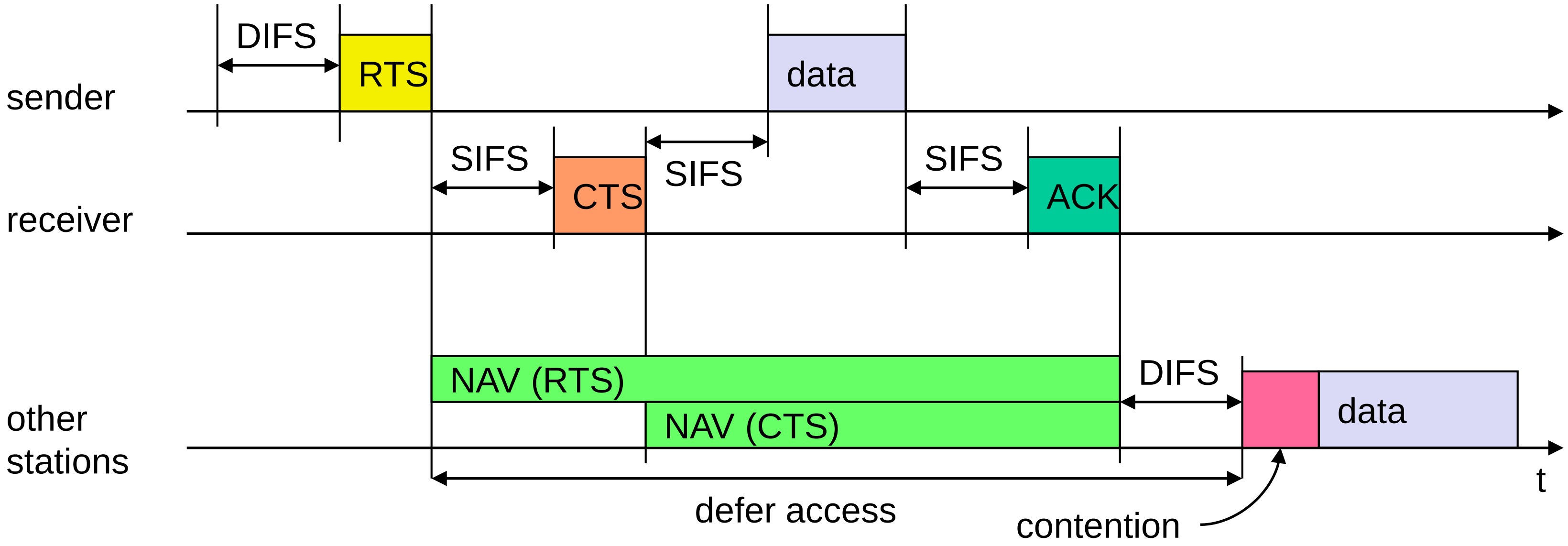
Virtual Carrier Sensing – Network Allocation Vector

- How does a station know if the medium is free?
  - » Usually, by *listening* the carrier

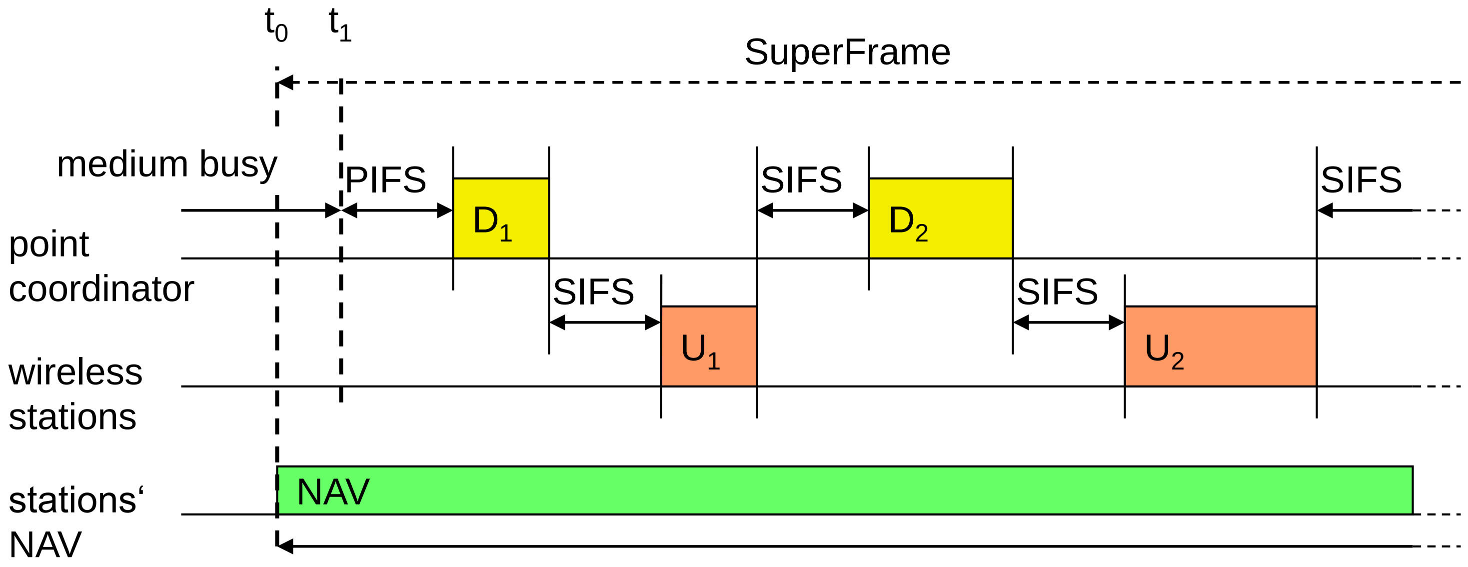
- IEEE 802.11 also uses *Network Allocation Vector* (NAV)
  - » 802.11 frames contain a duration field; used to reserve the medium
  - » Stations have a timer ***NAV***
    - – Updated with the values seen in the frames
    - – Decremented in real-time
    - – If != zero ➔ medium not free

MAC DCF with RTS+CTS

- Sending a frame in unicast
  - Station sends RTS with a reserve parameter, after waiting DIFS
    - Reserve time includes RTS+SIFS+CTS+SIFS+DATA+SIFS+ACK
  - Receiver confirms with CTS, after waiting SIFS
  - Transmitter sends frame, after waiting SIFS. Confirmation with ACK
  - Other stations become aware of reserved time by listening RTS and CTS

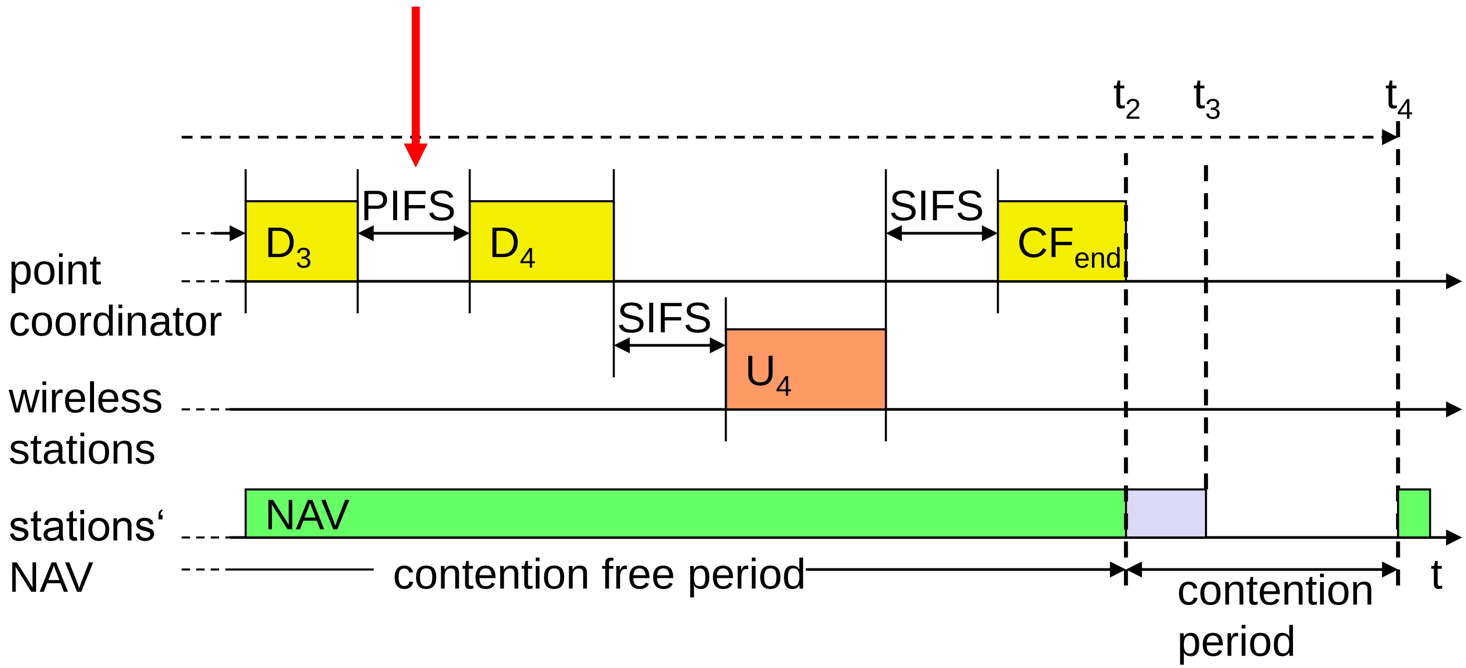


MAC- PCF (./..)



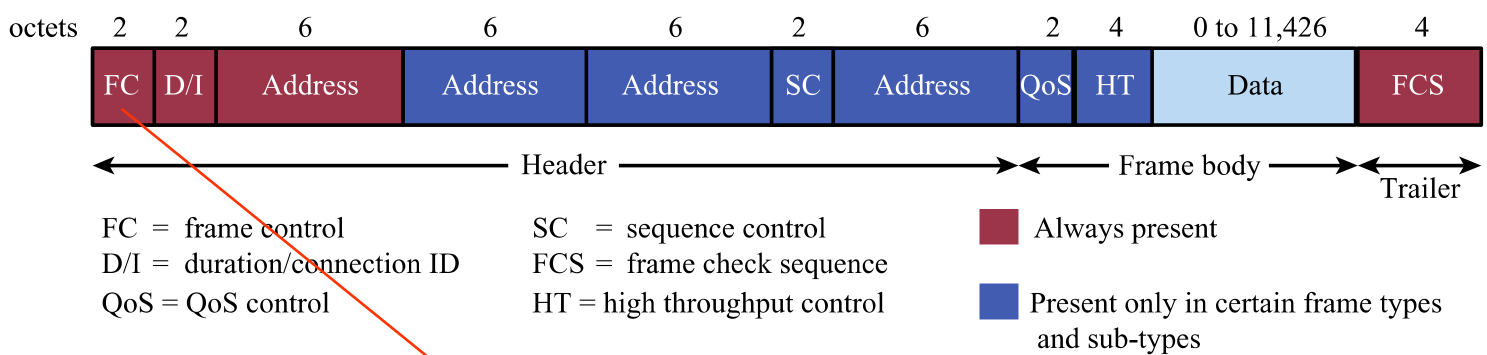
t_0
t_1
SuperFrame
medium busy
PIFS
D_1
SIFS
D_2
SIFS
point coordinator
SIFS
U_1
SIFS
U_2
wireless stations
stations‘ NAV
NAV

MAC-PCF II (../..)

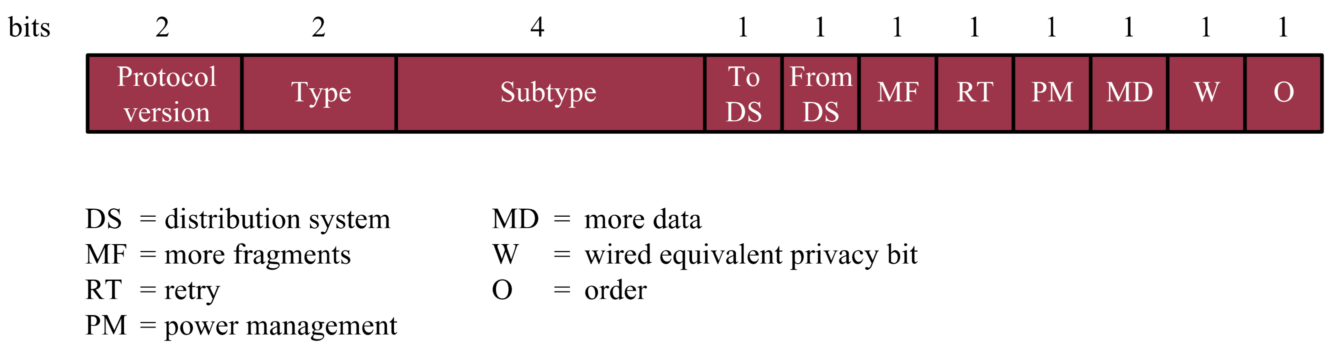


t2
t3
t4
PIFS
SIFS
D3
D4
CFend
point
coordinator
SIFS
U4
wireless
stations
NAV
stations'
NAV
contention free period
contention
period
t

IEEE 802.11 MAC Frame Format



(a) MAC frame



(b) Frame control field

Addresses in MAC

scenario	**to DS**	**from DS**	**address 1**	**address 2**	**address 3**	**address 4**
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Basic Service Set Identifier
RA: Receiver Address
TA: Transmitter Address

Special Frames- *ACK, RTS, CTS*

- Acknowledgement

ACK

bytes	2	2	6	4
	Frame Control	Duration	Receiver Address	CRC

- Request To Send

RTS

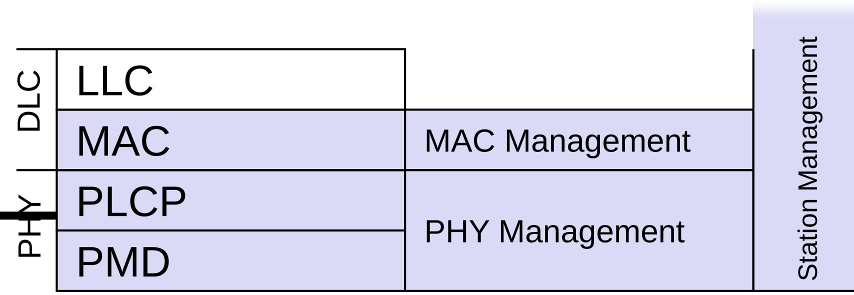
bytes	2	2	6	6	4
	Frame Control	Duration	Receiver Address	Transmitter Address	CRC

- Clear To Send

CTS

bytes	2	2	6	4
	Frame Control	Duration	Receiver Address	CRC

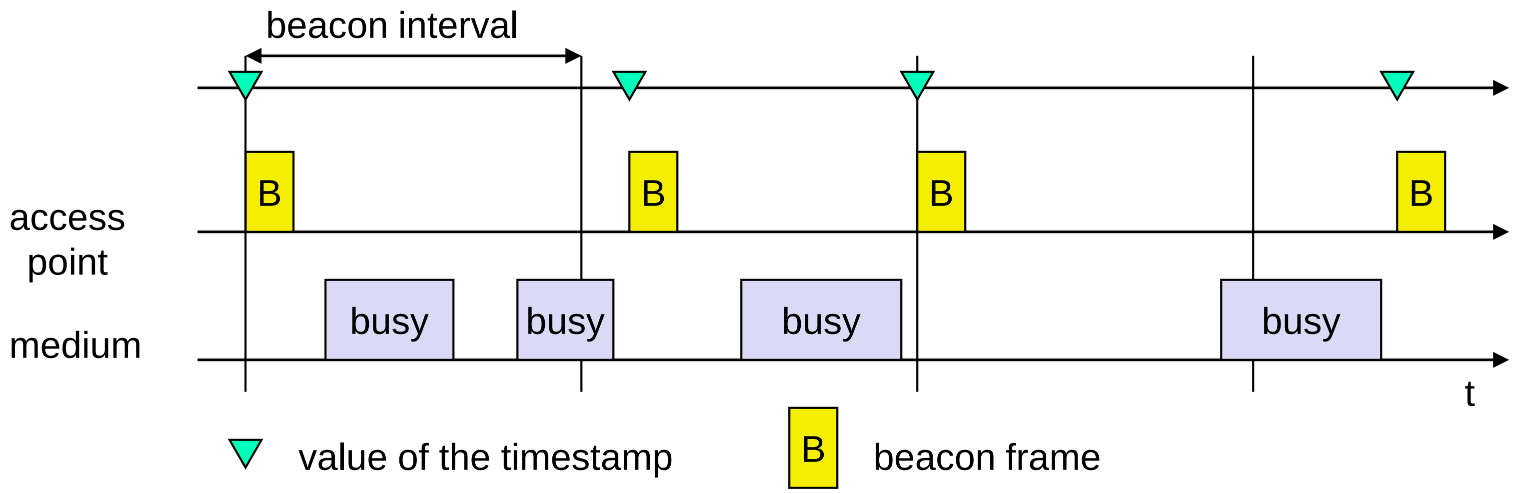
MAC Management



- Synchronization and association
  - Beacons are generated
  - Station discovers a BSS; station associates to an AP
  - Stations synchronize clocks
- Power management
  - Save terminal’s power → terminal enters *sleep* mode
    - Periodically
    - No frame loss; frames are stored
- MIB - Management Information Base

Synchronization by Beacon – Infrastructure Network

- Stations must be synchronized, e.g.
  - To preview PCF cycles
  - To change state: sleep ←→ wake
- Infrastructure networks
  - Access Point sends (almost) periodically a *Beacon* with *timestamp* e *BSSid* (sometimes medium is busy)
  - Timestamp sent is the correct
  - Other stations adjust their clocks when they receive the beacon

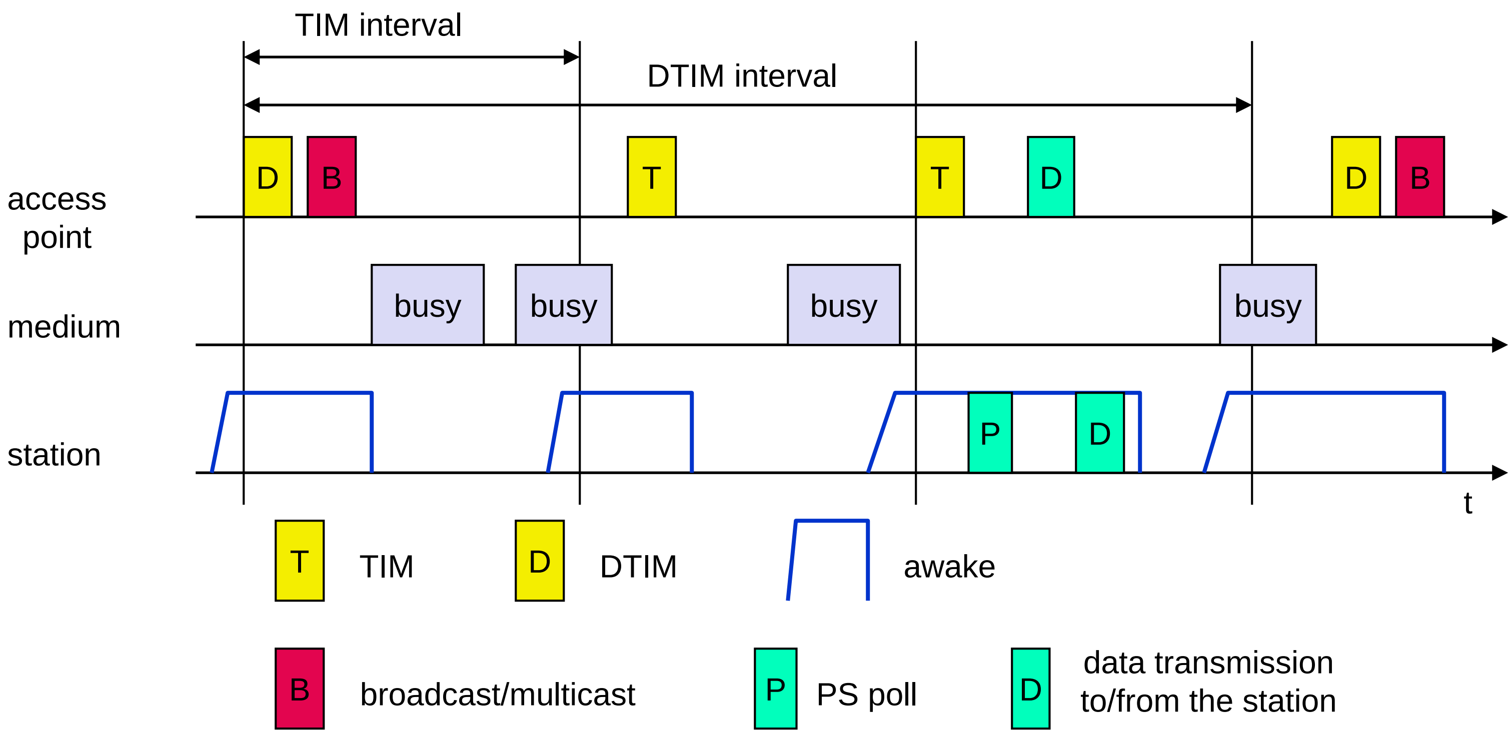


Power Management

- Objective
  - If transceiver not in use → go to sleep mode
- Station in 2 states: *sleep*, *wake*
- Infrastructure network
  - Stations wake periodically and simultaneously
  - They listen beacon to know if there are packets to receive
  - If a station has packets to receive → remains awake until it receives them
    - If not, goes sleep after sending its packets
- Ad-hoc network, a station
  - Listens/sends the beacon
  - Informs other stations it has packets for them
  - Receives and sends packets
  - Sleeps again

Power Management – Infrastructure Network

- Infrastructure network → traffic information sent **in the *beacon***
  - » *Traffic Indication Map – TIM:* list of unicast receivers
  - » *Delivery Traffic Indication Map - DTIM:* list broadcast/multicast receivers



802.11 – Physical Layer

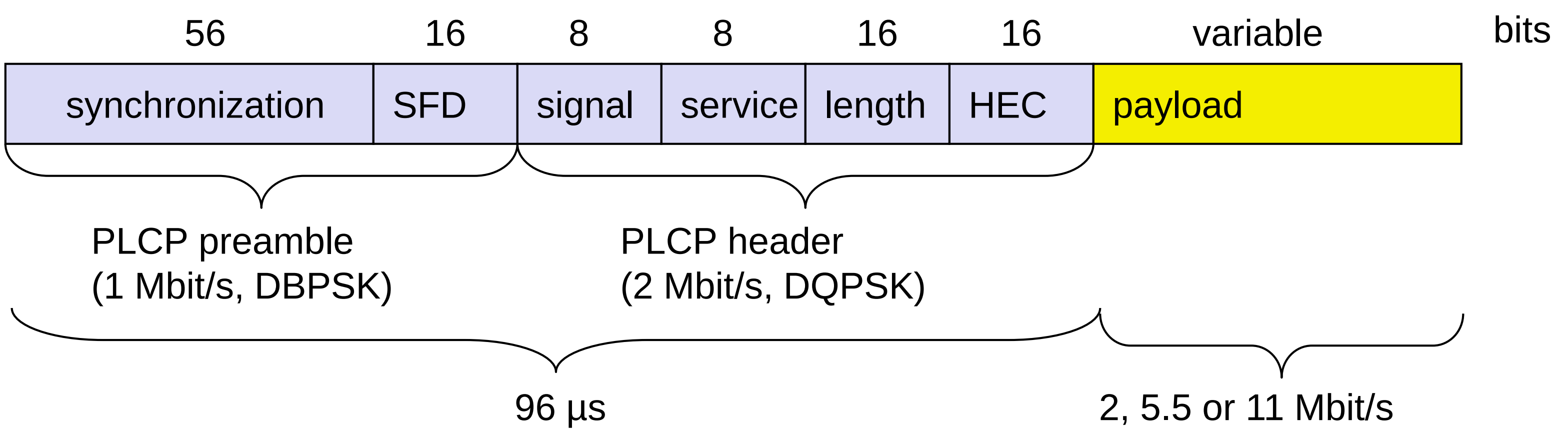
Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ad
Year introduced	1999	1999	2003	~~2000~~ 2009	2012	2014
Maximum data transfer speed	54 Mbps	11 Mbps	54 Mbps	65 to 600 Mbps	78 Mbps to 3.2 Gbps	6.76 Gbps
Frequency band	5 GHz	2.4 GHz	2.4 GHz	2.4 or 5 GHz	5 GHz	60 GHz
Channel bandwidth	20 MHz	20 MHz	20 MHz	20, 40 MHz	40, 80, 160 MHz	2160 MHz
Highest order modulation	64 QAM	11 CCK	64 QAM	64 QAM	256 QAM	64 QAM
Spectrum usage	OFDM	DSSS	DSSS, OFDM	OFDM	SC-OFDM	SC, OFDM
Antenna configuration	1×1 SISO	1×1 SISO	1×1 SISO	Up to 4×4 MIMO	Up to 8×8 MIMO, MU-MIMO	1×1 SISO

IEEE 802.11b

- DSSS (Spread Spectrum)
- Bitrates: 2, 5.5 and 11 Mbit/s
- First standard to make Wi-Fi become popular

Original Frame DSSS PHY (802.11)

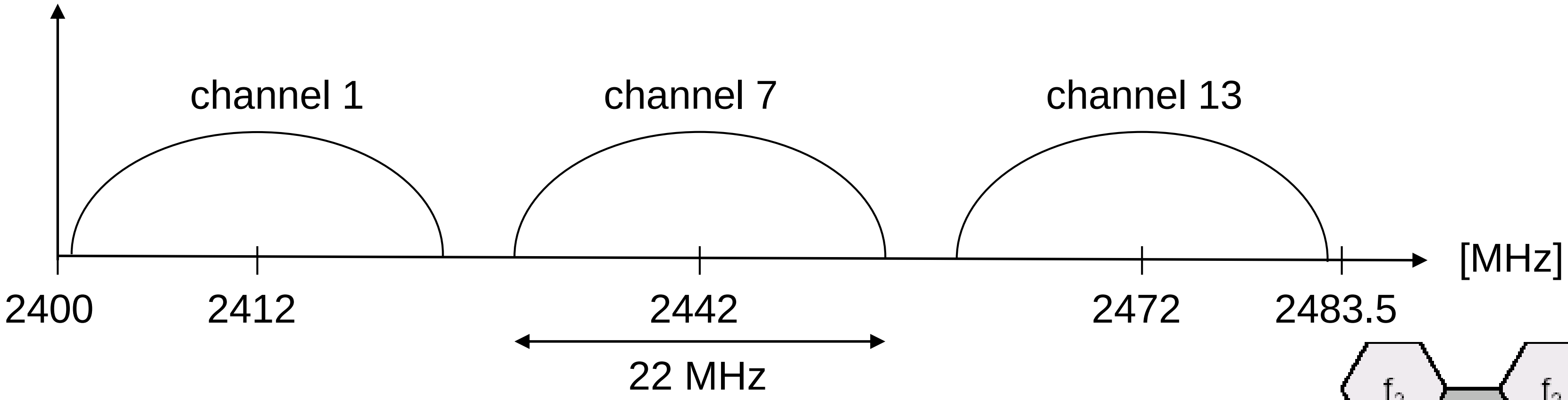
- » Barker sequence of 11 chips → +1,-1,+1,+1,-1,+1,+1,+1,-1,-1,-1
- » Synchronization
- » SFD (Start Frame Delimiter → 1111001110100000
- » Signal → Payload bitrate
- » Service → reserved, 00 = according to 802.11
- » Length → Payload length **<u>in us</u>**
- » HEC (Header Error Check)
  - – Protection of sinal, service and length, using $x^{16}+x^{12}+x^{5}+1$
- » Data (payload) MAC → scrambled with $z^{7}+z^{4}+1$

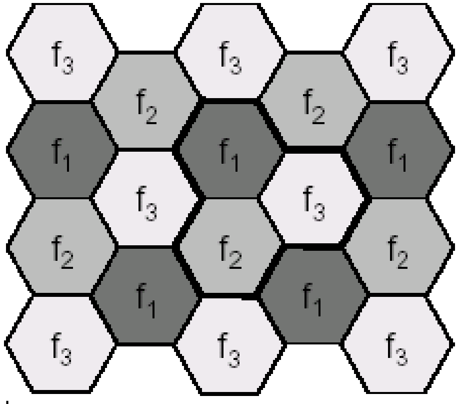


Channel Selection

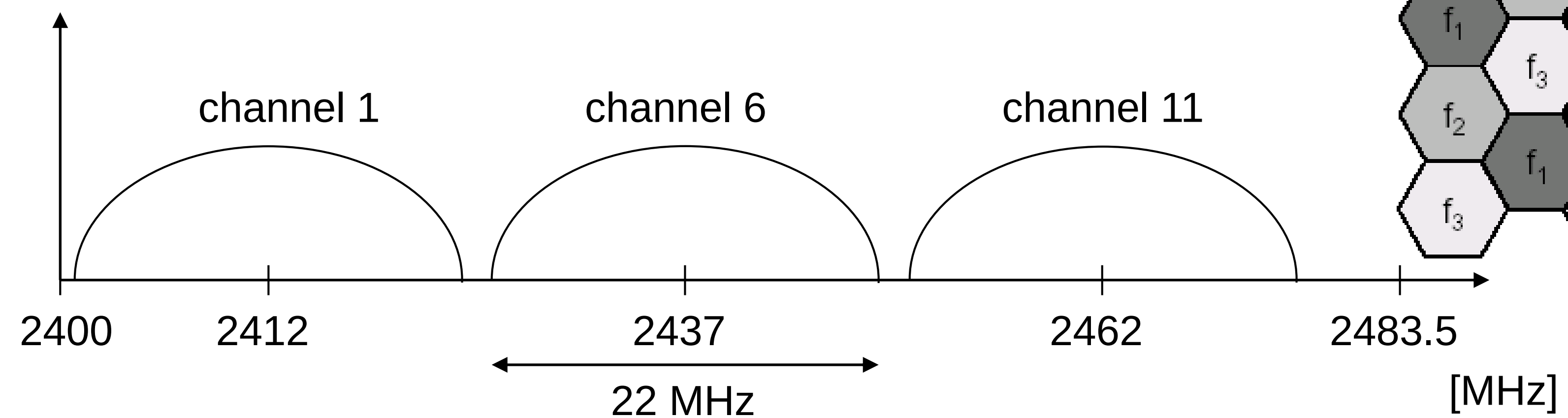
channel i = 2412MHz + (i-1)*5MHz
There are 14 channels of 5MHz
In 801.11b only 3 non-overlap channels can be used

Europe (ETSI)





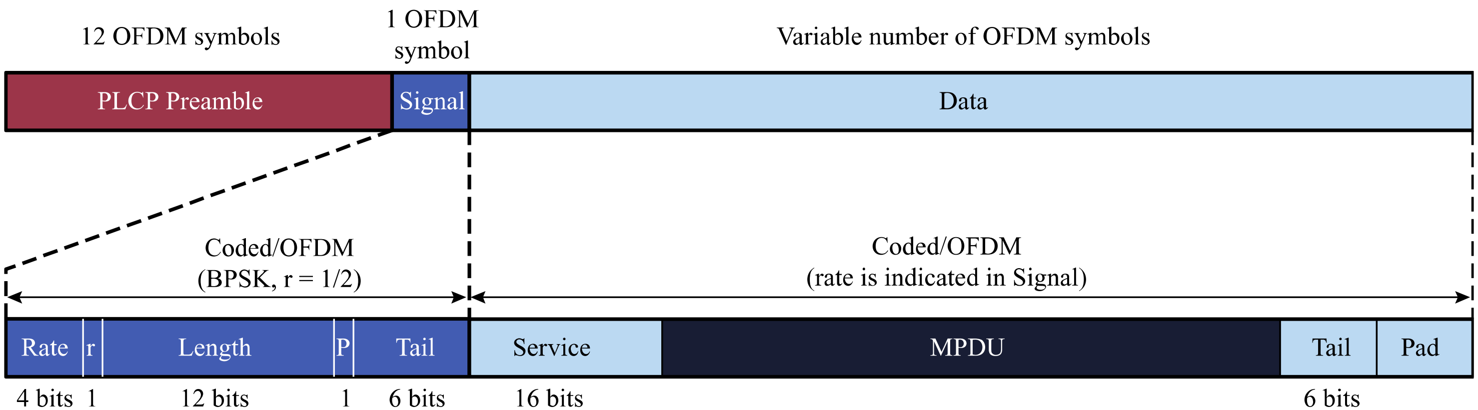
US (FCC)/Canada (IC)



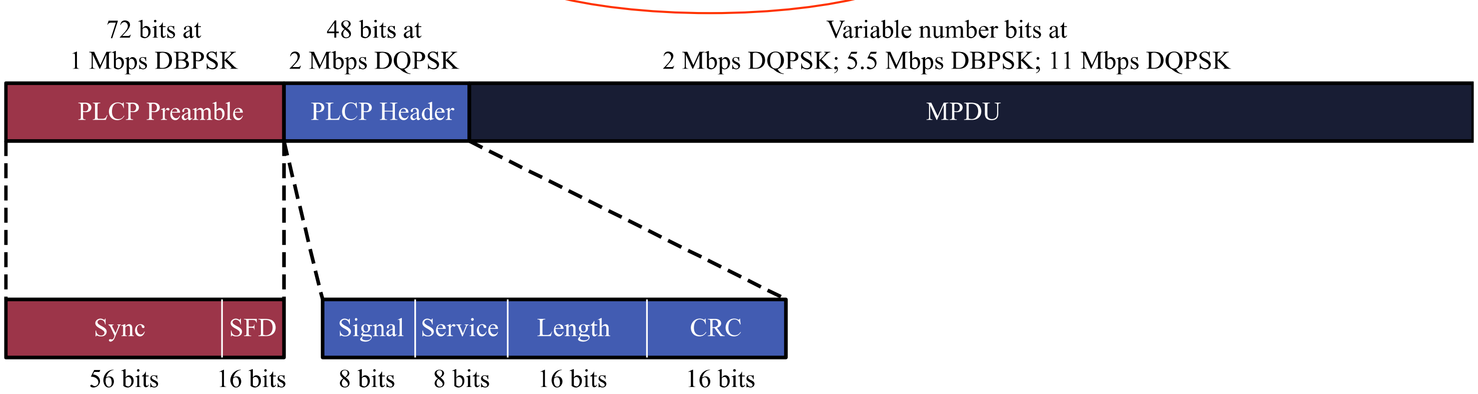
IEEE 802.11a

- Makes use of 5-GHz band
  - 5.15-5.35,   5.47-5.725 GHz   (Europe)
- Provides bitrates of 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s
  - Mandatory: 6, 12, 24 Mbit/s
- Uses Orthogonal Frequency Division Multiplexing (OFDM)
- Modulations: using BPSK, QPSK, 16-QAM, 64-QAM

IEEE 802.11a – PHY Frame

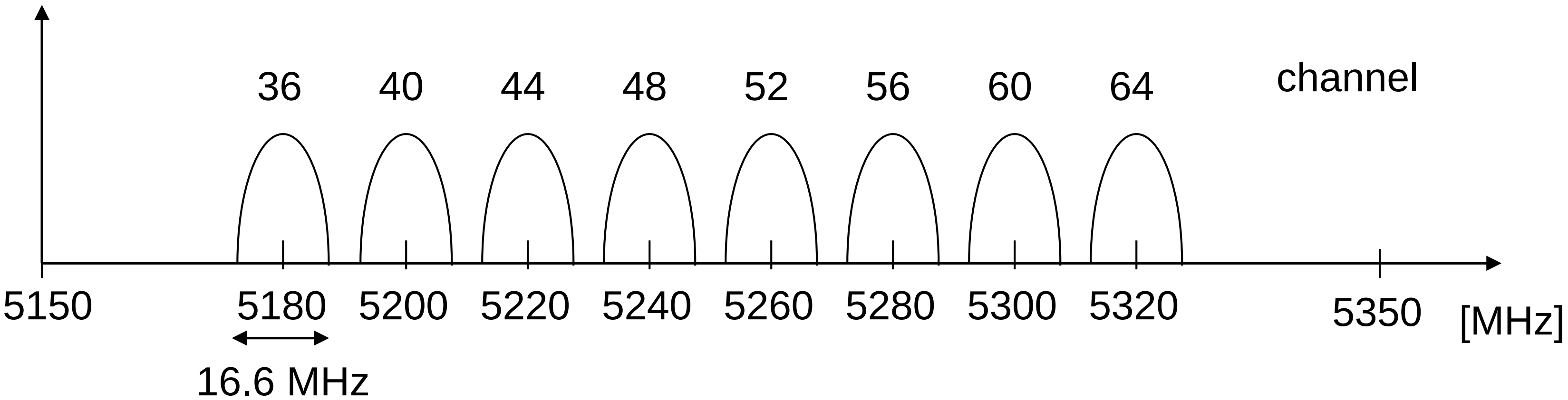


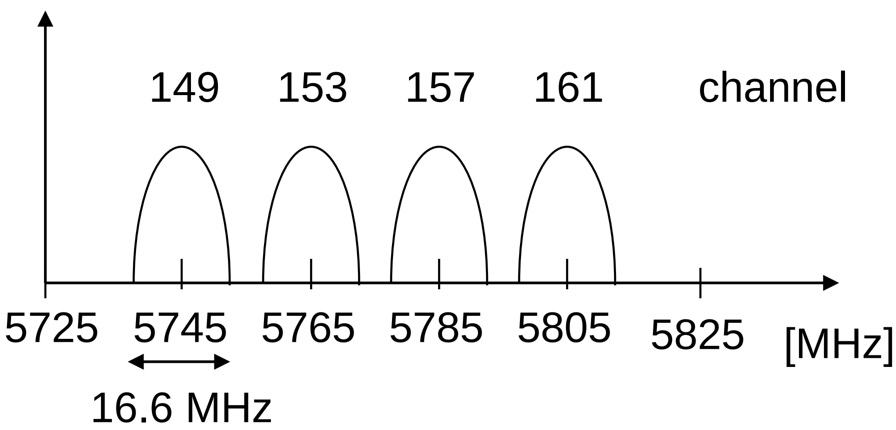
(a) IEEE 802.11a physical PDU



(b) IEEE 802.11b physical PDU

Operating channels for 802.11a / US U-NII

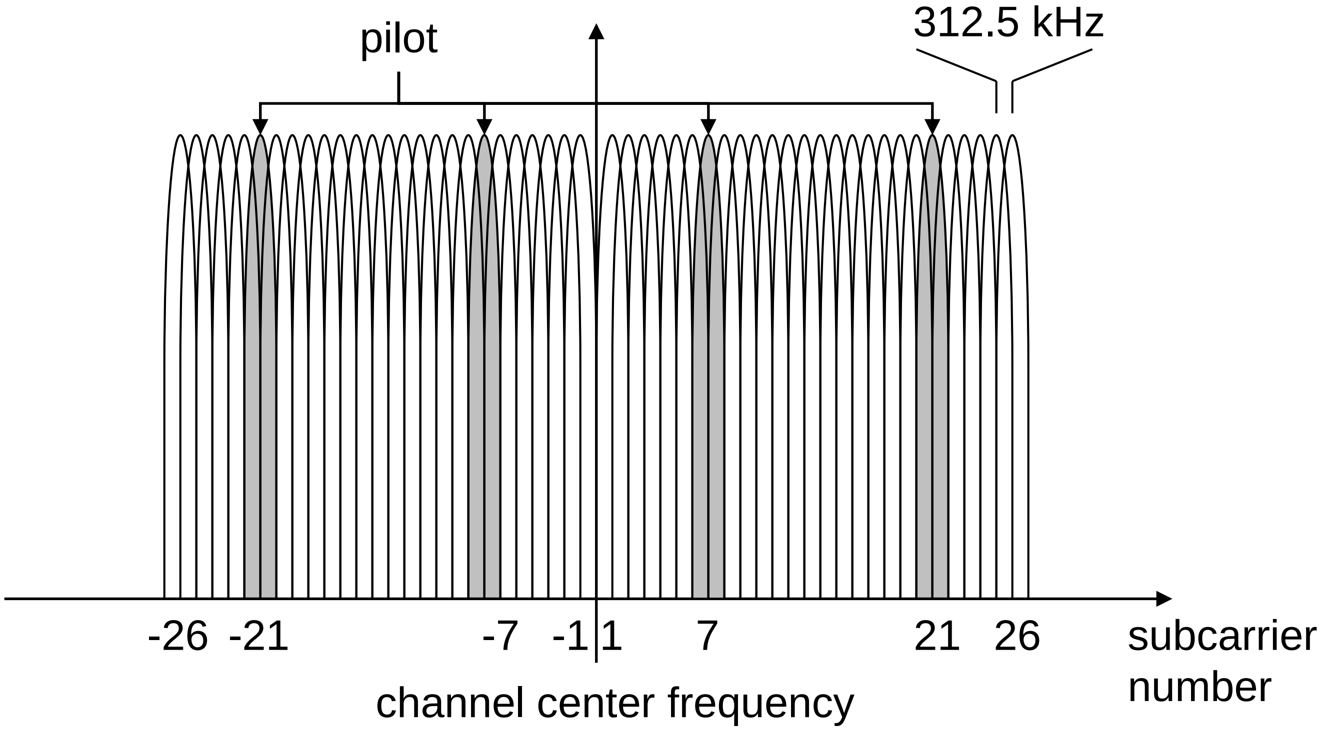




center frequency =
5000 + 5*channel number [MHz]

OFDM in IEEE 802.11a

- OFDM with 52 used subcarriers
- 48 data + 4 pilot
- 312.5 kHz spacing



802.11a – Rate Dependent Parameters

Data rate (Mbits/s)	Modulation	Coding rate (R)	Coded bits per subcarrier (N_{BPSC})	Coded bits per OFDM symbol (N_{CBPS})	Data bits per OFDM symbol (N_{DBPS})
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

% of useful information

250 kSymbol/s

IEEE 802.11g

- Extended rates up to 54 Mbit/s in 2.4 GHz band
- Continued and extended 802.11b
- Also used OFDM for rates up to 54 Mbps

IEEE 802.11n

- Operates in 2.4 GHz and 5GHz bands
- Radio transmission schemes
  - May combine two 20 MHz channels
  - Shorter 400 ns guard band
  - Higher coding rate of 5/6
  - 150 Mbit/s per 40 MHz, 600 Mbit/s for 4 parallel spatial streams
- Space Division Multiplexing
  - MIMO: Multiple parallel spatial streams (up to 4 × 4), beamforming, or diversity
  - Maximum number of simultaneous data streams
    - limited by the minimum number of antennas in use on both sides of the link
- MAC layer ➔ less overhead
  - Block acknowledgements: ACK confirms correct reception of multiple packets
  - Frame aggregation

Forms of Frame Aggregation

3 forms of aggregation

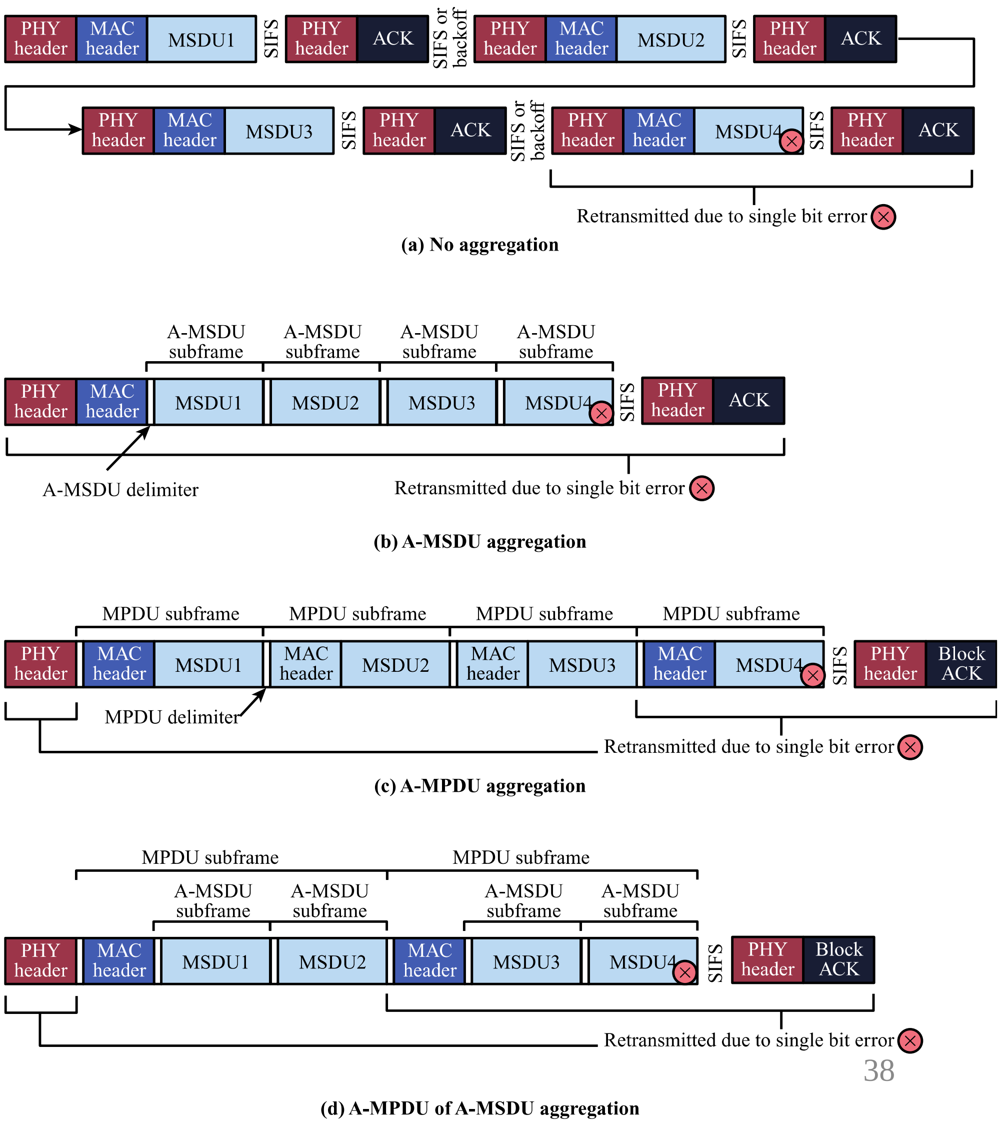
» A-MSDU aggregation: shared PHY and MAC headers and FCS

» A-MPDU aggregation: shared PHY header

– Still keep separate MAC headers, to less header reduction

– But not as much to retransmit if there is an error

» A-MPDU and A-MSDU aggregation – balances the two



- MSDU - MAC Service Data Unit comes down from the LLC layer
- MPDU – MAC Protocol Data Unit comes from the MAC layer

IEEE 802.11n - Data Rates

Spatial streams	Modulation type	Coding rate	Data rate (Mbit/s)			
			20 MHz channel		40 MHz channel	
			800 ns GI	400 ns GI	800 ns GI	400 ns GI
1	BPSK	1/2	6.50	7.20	13.50	15.00
1	QPSK	1/2	13.00	14.40	27.00	30.00
1	QPSK	3/4	19.50	21.70	40.50	45.00
1	16-QAM	1/2	26.00	28.90	54.00	60.00
1	16-QAM	3/4	39.00	43.30	81.00	90.00
1	64-QAM	2/3	52.00	57.80	108.00	120.00
1	64-QAM	3/4	58.50	65.00	121.50	135.00
1	64-QAM	5/6	65.00	72.20	135.00	150.00
2	BPSK	1/2	13.00	14.40	27.00	30.00
2	QPSK	1/2	26.00	28.90	54.00	60.00
2	QPSK	3/4	39.00	43.30	81.00	90.00
2	16-QAM	1/2	52.00	57.80	108.00	120.00
2	16-QAM	3/4	78.00	86.70	162.00	180.00
2	64-QAM	2/3	104.00	115.60	216.00	240.00
2	64-QAM	3/4	117.00	130.00	243.00	270.00
2	64-QAM	5/6	130.00	144.40	270.00	300.00
3	BPSK	1/2	19.50	21.70	40.50	45.00
3	QPSK	1/2	39.00	43.30	81.00	90.00
3	QPSK	3/4	58.50	65.00	121.50	135.00
3	16-QAM	1/2	78.00	86.70	162.00	180.00
3	16-QAM	3/4	117.00	130.70	243.00	270.00
3	64-QAM	2/3	156.00	173.30	324.00	360.00
3	64-QAM	3/4	175.50	195.00	364.50	405.00
3	64-QAM	5/6	195.00	216.70	405.00	450.00
4	…	…	…	…	…	…
4	64-QAM	5/6	260.00	288.90	540.00	600.00

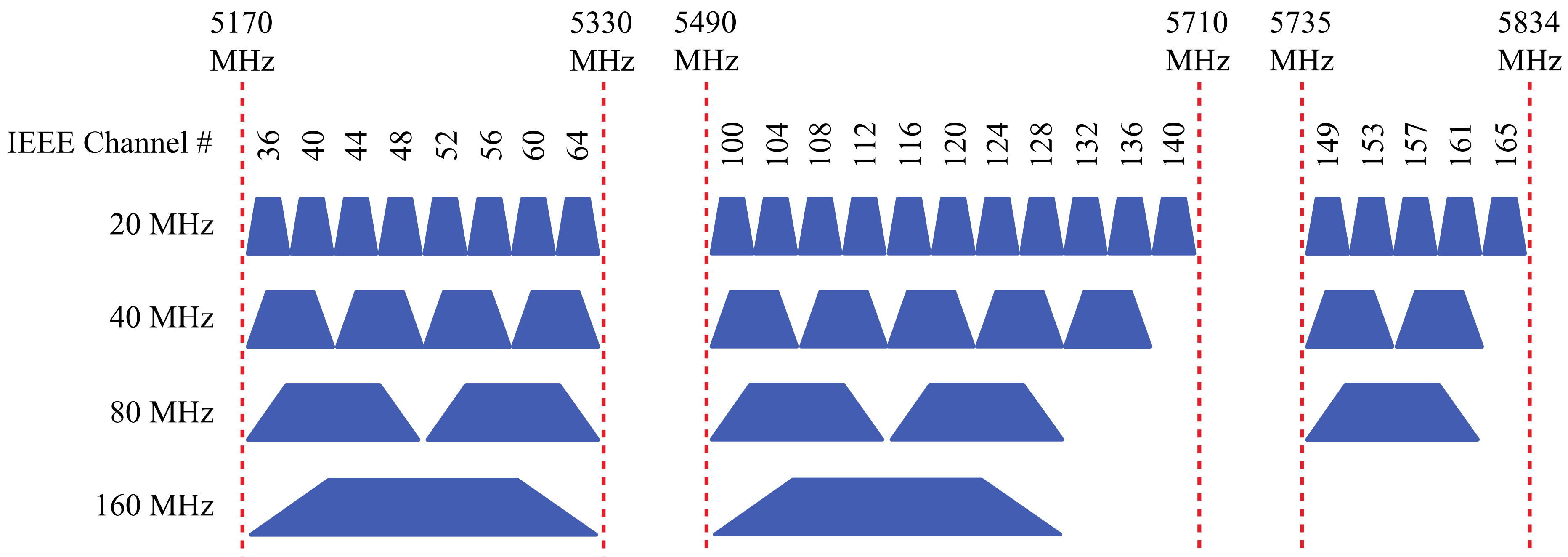
IEEE 802.11ac

- 802.11ac is an evolution from 802.11n
- 802.11ac is a multi-user form of MIMO
  - » enables an AP to send to multiple clients at the same time
- Differences between 802.11n and 802.11ac

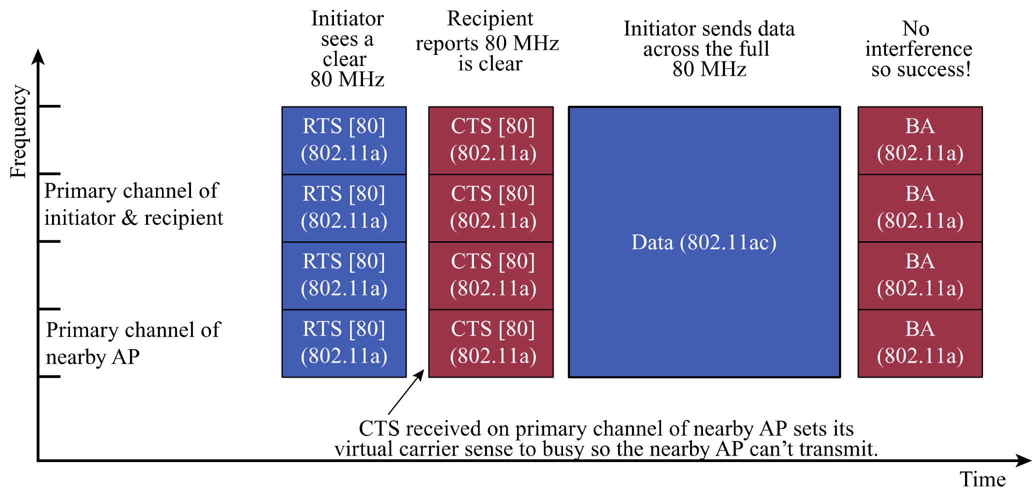
802.11n	802.11ac
Supports 20 and 40 MHz channels	Adds 80 and 160 MHz channels
Supports 2.4 GHz and 5 GHz frequency bands	Supports 5 GHz only
Supports BPSK, QPSK, 16-QAM, and 64-QAM	Adds 256-QAM
Supports many types of explicit beamforming	Supports only null data packet (NDP) explicit beamforming
Supports up to four spatial streams	Supports up to eight spatial streams (AP); client devices up to four spatial streams
Supports single-user transmission only	Adds multi-user transmission
Includes significant MAC enhancements (A-MSDU, A-MPDU)	Supports similar MAC enhancements, with extensions to accommodate high data rates

2.4 GHz	5 GHz
802.11 (direct sequence and frequency hopping)	802.11a
802.11b	802.11n
802.11g	802.11ac
802.11n	

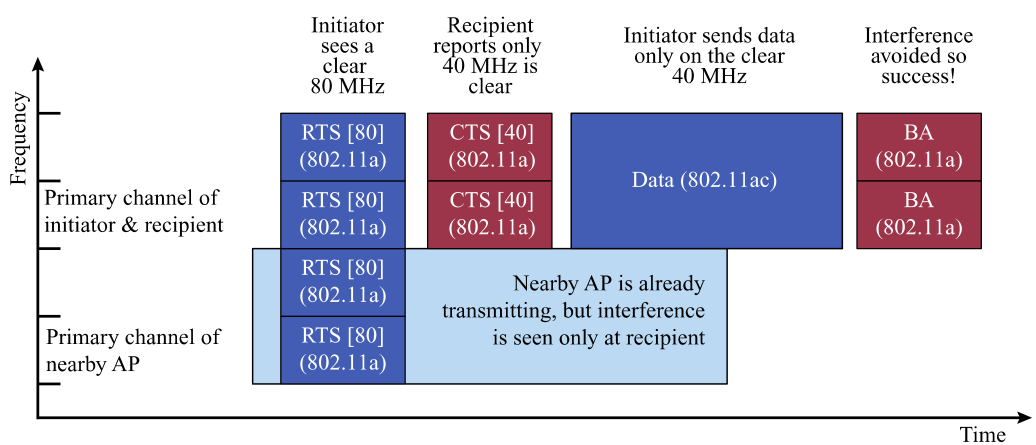
802.11ac - 5 GHz Channel Allocations



RTS/CTS Enhanced with Bandwidth Signaling



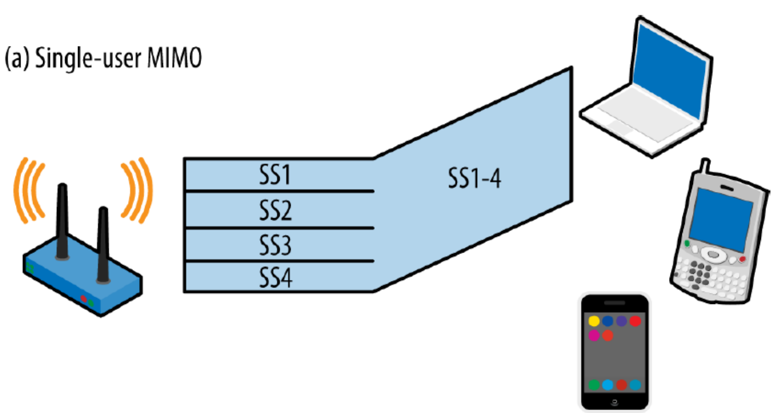
(a) No interference case



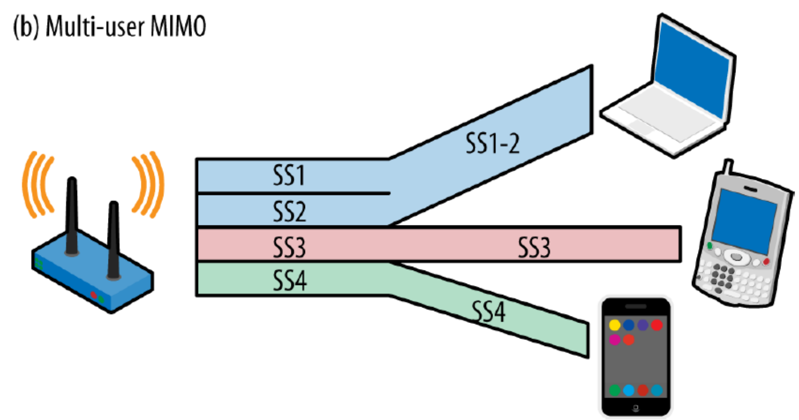
(b) Interference case

Beamforming / Multi-User MIMO (MU-MIMO)

- For receivers located in different directions
  - » beamformed transmissions may be used
  - » to send information to each of receiver, **at the same time**



802.11n



802.11ac

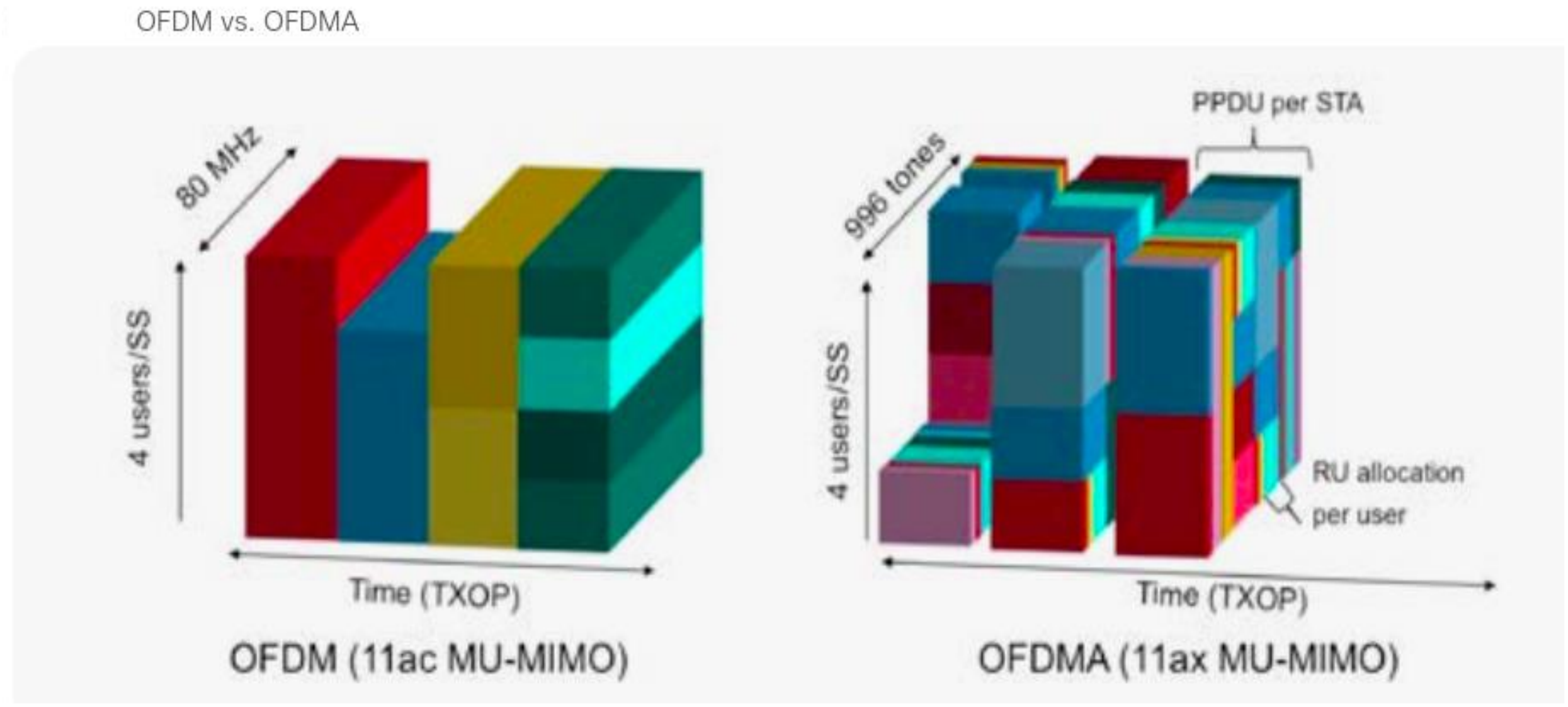
IEEE 802.11ax – Enhancements for High Efficiency WLAN

- IEEE 802.11ax (2019) built on top of IEEE 802.11ac
  - Compatibility with earlier standards
  - Provision of predictable performance for advanced applications

- Main enhancements for high efficiency
  - Denser modulation (1024-QAM)
  - OFDMA-based scheduling to reduce latency and overhead
    - OFDMA is made backward compatible with traditional CSMA

OFDM vs. OFDMA - Example

OFDMA – 3D (time, space and frequency) resource allocation



IEEE 802.11ax – Modulation and Coding Schemes

Modulation and coding schemes for single spatial stream

MCS index[a]	Modulation type	Coding rate	Data rate (in Mbit/s)[b]							
			20 MHz channels		40 MHz channels		80 MHz channels		160 MHz channels	
			1600 ns GI[c]	800 ns GI	1600 ns GI	800 ns GI	1600 ns GI	800 ns GI	1600 ns GI	800 ns GI
0	BPSK	1/2	8	8.6	16	17.2	34	36.0	68	72
1	QPSK	1/2	16	17.2	33	34.4	68	72.1	136	144
2	QPSK	3/4	24	25.8	49	51.6	102	108.1	204	216
3	16-QAM	1/2	33	34.4	65	68.8	136	144.1	272	282
4	16-QAM	3/4	49	51.6	98	103.2	204	216.2	408	432
5	64-QAM	2/3	65	68.8	130	137.6	272	288.2	544	576
6	64-QAM	3/4	73	77.4	146	154.9	306	324.4	613	649
7	64-QAM	5/6	81	86.0	163	172.1	340	360.3	681	721
8	256-QAM	3/4	98	103.2	195	206.5	408	432.4	817	865
9	256-QAM	5/6	108	114.7	217	229.4	453	480.4	907	961
10	1024-QAM	3/4	122	129.0	244	258.1	510	540.4	1021	1081
11	1024-QAM	5/6	135	143.4	271	286.8	567	600.5	1134	1201

Notes

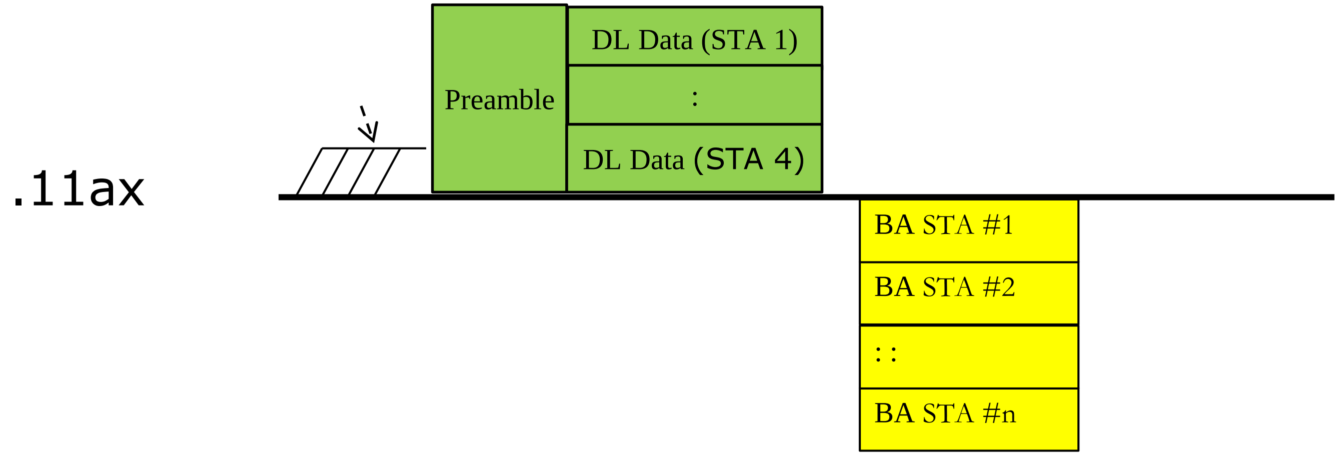
a. ^ MCS 9 is not applicable to all combinations of channel width and spatial stream count.
b. ^ A second stream doubles the theoretical data rate, a third one triples it, etc.
c. ^ *GI* stands for *guard interval*.

IEEE 802.11ax – PHY Layer Summary

- High Efficiency OFDM (HE-OFDM) / MIMO
- 2.4 / 5 GHz bands (dual band, unlike 11ac)
- Channel bandwidths: 20 / 40 / 80 / 160 MHz
- MIMO streams: up to 8
- PHY rates: up to 10.53 Gbit/s (160 MHz channels, 8 spatial streams, 1024-QAM modulation and short guard interval)
- Range: up to 30 m indoor / up to 120 m outdoor

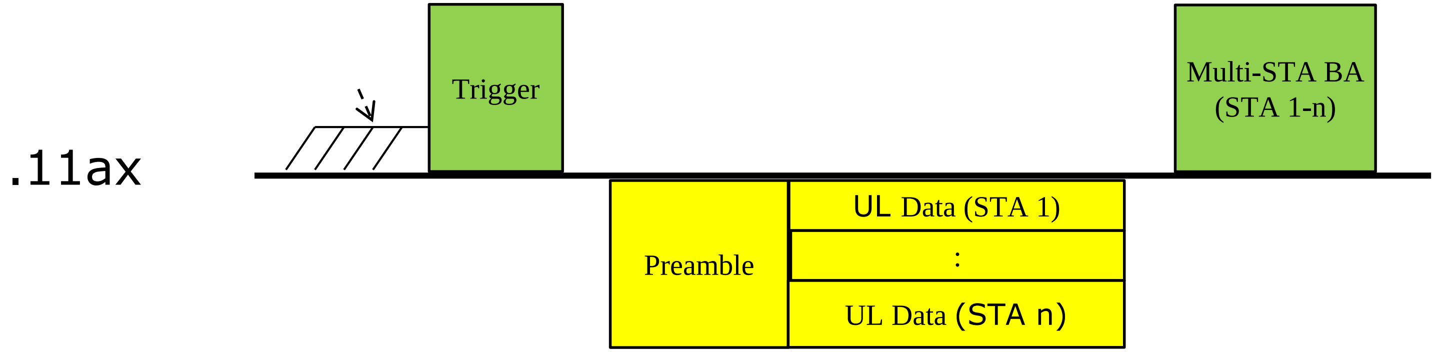
802.11ax – Multiuser DownLink

- OFDMA **DownLink** operation
  - » AP decides which STAs and size of RUs and indicates it in Preamble
  - » AP transmits DL Data to multiple STAs in their allocated RUs
  - » AP requests Block Acknowledgement from all STAs
  - » STAs send Block ACKs (BA STA#i) to AP



802.11ax – Multiuser UpLink

- OFDMA **UpLink** operation
  - » AP decides which STAs to be polled for data and which RUs to allocate
  - » AP polls data from STA with a Trigger
  - » STAs respond with UL Data
  - » AP responds with an ACK (Multi-STA BA)



IEEE 802.11ad (Gigabit WiFi)

- Uses 60-GHz bands
  - » millimeter waves (mmWave)
  - » High free space loss
  - » Poor penetration of objects
  - » Likely only useful in a single room
- Very high bandwidth: 2160 MHz
- Up to 7 Gbit/s
- Replacement of wires for video to TVs and projectors

Homework

1. Review slides

2. Read from Cory Beard and William Stallings
   » Chap. 11 - Wireless LAN Technology and the IEEE 802.11 Wireless LAN Standard

3. Answer questions at moodle