University of Antwerp
Faculty of Science

Advanced Wireless & 5G Networks

Prof. Dr. Ir. Michael Peeters — 2023–2024

Topics for today

- **4. WiFi**
  - cont.
- **5. The Specials**
- **6. AMA**

Planning

Session	Date	Topic
1	20231006	~~Introduction, history, market, industry, bands, licensed vs. unlicensed, …~~
2	20231013	~~Technology baselining (a.k.a. refreshing what you should have known): 2G, WiFi, …~~
	20231020	~~Cancelled~~
3	20231027	~~Shannon/Friis continued. 2G as a "low-complexity" example~~
~~4~~	~~20231110~~	~~L 2G~~
~~5~~	~~20231117~~	~~L 3GPP 2G-3G-4G-5G architecture evolution. 5G~~
~~6~~	~~20231124~~	~~L 5G~~
~~7~~	~~20231201-08~~	~~L 5G~~
~~8~~	~~**20231215 – 2h**~~	~~L5G and (woohoo) U IEEE Wifi Network Architecture: 802.11 abgn~~
9	**20231218 – 2h)**	U 802.11
10	**20231222 morning**	U 802.11 + other IEEE
11	**20231222 afternoon**	Remainders
(12)	TBD	Extra: Technology enablers and acronyms you need to be aware of: ADC, FEM, PA, LSA, and other key analog and digital HW blocks, mMIMO, Beam management, 802.11be, AI, 6G, THz and their implications to the network

Final schedule

Activiteitsdatums	Dag	Tijd	Tijdsduur	Naam Activiteit	zaal	Naam van Docent
6/10/2023	vr	16:00	2:00	2001WETMWN Advanced Wireless & 5G network/S01/LEC/HC01/01	M.G.005	Peeters,Michael
13/10/2023	vr	16:00	2:00	2001WETMWN Advanced Wireless & 5G network/S01/LEC/HC01/01	M.G.005	Peeters,Michael
20/10/2023	vr	16:00	2:00	2001WETMWN Advanced Wireless & 5G network/S01/LEC/HC01/01	M.G.005	Peeters,Michael
27/10/2023	vr	16:00	2:00	2001WETMWN Advanced Wireless & 5G network/S01/LEC/HC01/01	M.G.005	Peeters,Michael
10/11/2023	vr	16:00	2:00	2001WETMWN Advanced Wireless & 5G network/S01/LEC/HC01/01	M.G.005	Peeters,Michael
17/11/2023	vr	16:00	2:00	2001WETMWN Advanced Wireless & 5G network/S01/LEC/HC01/01	M.G.005	Peeters,Michael
24/11/2023	vr	16:00	2:00	2001WETMWN Advanced Wireless & 5G network/S01/LEC/HC01/01	M.G.005	Peeters,Michael
8/12/2023	vr	16:00	2:00	2001WETMWN Advanced Wireless & 5G network/S01/LEC/HC01/01	M.G.005	Peeters,Michael
15/12/2023	vr	16:00	2:00	2001WETMWN Advanced Wireless & 5G network/S01/LEC/HC01/01	M.G.005	Peeters,Michael
18/12/2023	ma	16:00	2:00	2001WETMWN Advanced Wireless & 5G network/S01/LEC/HC01/03	M.G.004	Peeters,Michael
22/12/2023	vr	8:30	2:00	2001WETMWN Advanced Wireless & 5G network/S01/LEC/HC01/02	M.G.005	Peeters,Michael
22/12/2023	vr	13:45	2:00	2001WETMWN Advanced Wireless & 5G network/S01/LEC/HC01/04	M.G.006	Peeters,Michael

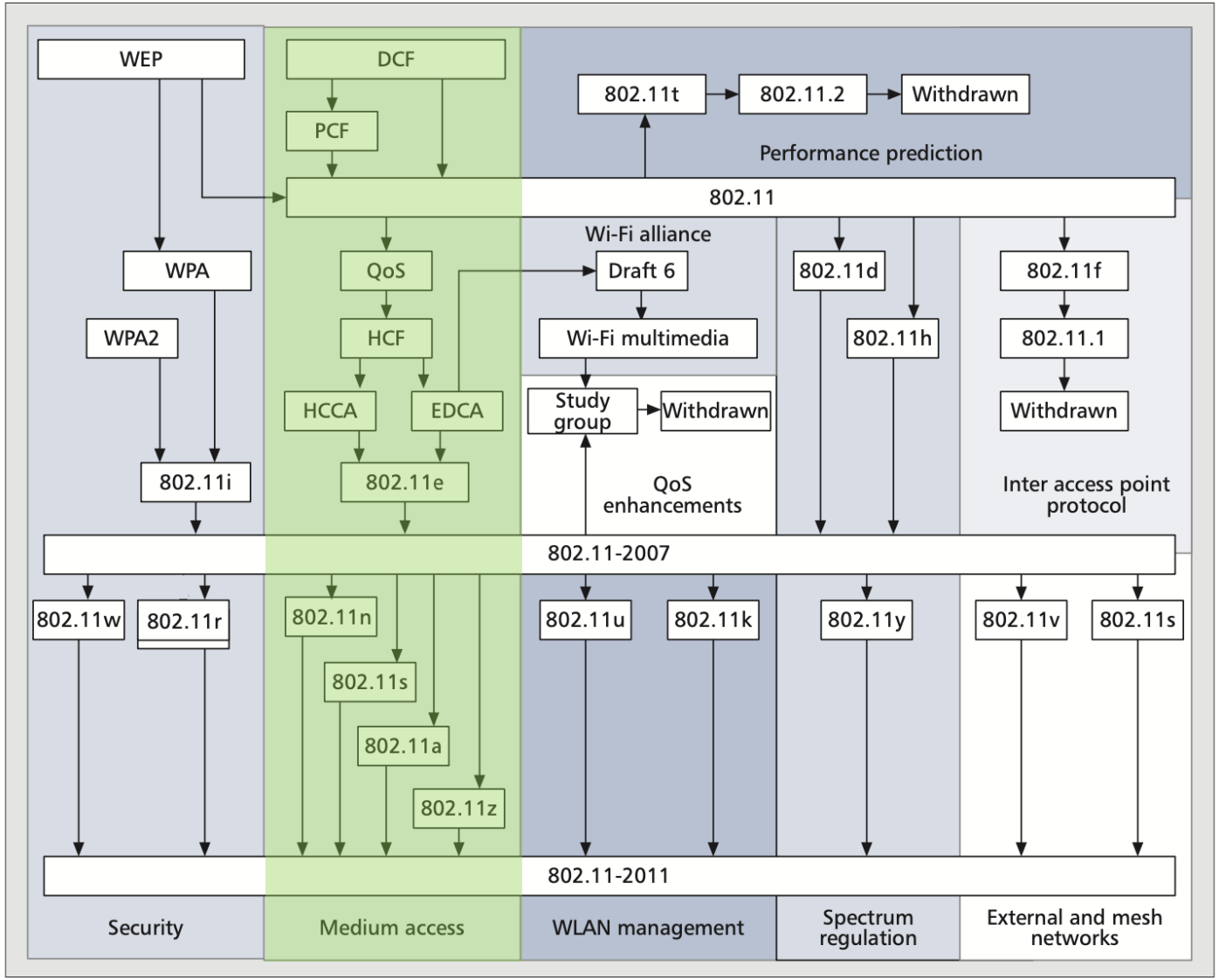
Your expectations

- ~~How it is possible that, in a world where the number of devices continue to grow, every device can get mobile wireless connectivity with the internet without saturating the network.~~
- ~~How do 4G/5G/... technologies actually work.~~
- How do you go about designing a good WiFi network, both on the physical end (devices, access point locations, ...) and on the configuration end.
- What are the technologies behind the current advancement in Cellular and Wi-Fi networks?
- ~~Be able to understand the need for improved and efficient networking technologies, and how to approach solving the drawbacks of current technologies.~~
- What are the limitations of 5G in regard to the latest trends in Ai, AR/VR and technologies that require very low latency.
- What is next?
- ~~Wifi 6 & 7 – new features.~~
- ~~Link to cloud.~~
- ~~How do modern mobile networks work and how have they changed from the previous ones?~~
- What are the main problems or limitations faced by different types of networks? If it is possible, what are the best ways to solve them?
- How will wireless and mobile networks possibly evolve in the near future?
- ~~To better understand historical challenges in wireless that companies such as blackberry faced.~~
- To better understand wireless technologies such as Zigbee and LoRaWan and their use in IOT projects.
- What role data science could have in this field?
- Can networks be perfected to the point where we don't need to keep on creating new ones or upgrade the existing ones?
- ~~Can governments stop the development of networks?~~
- ~~Will connectivity ever be available underwater or underground?~~
- Security of wireless networks.

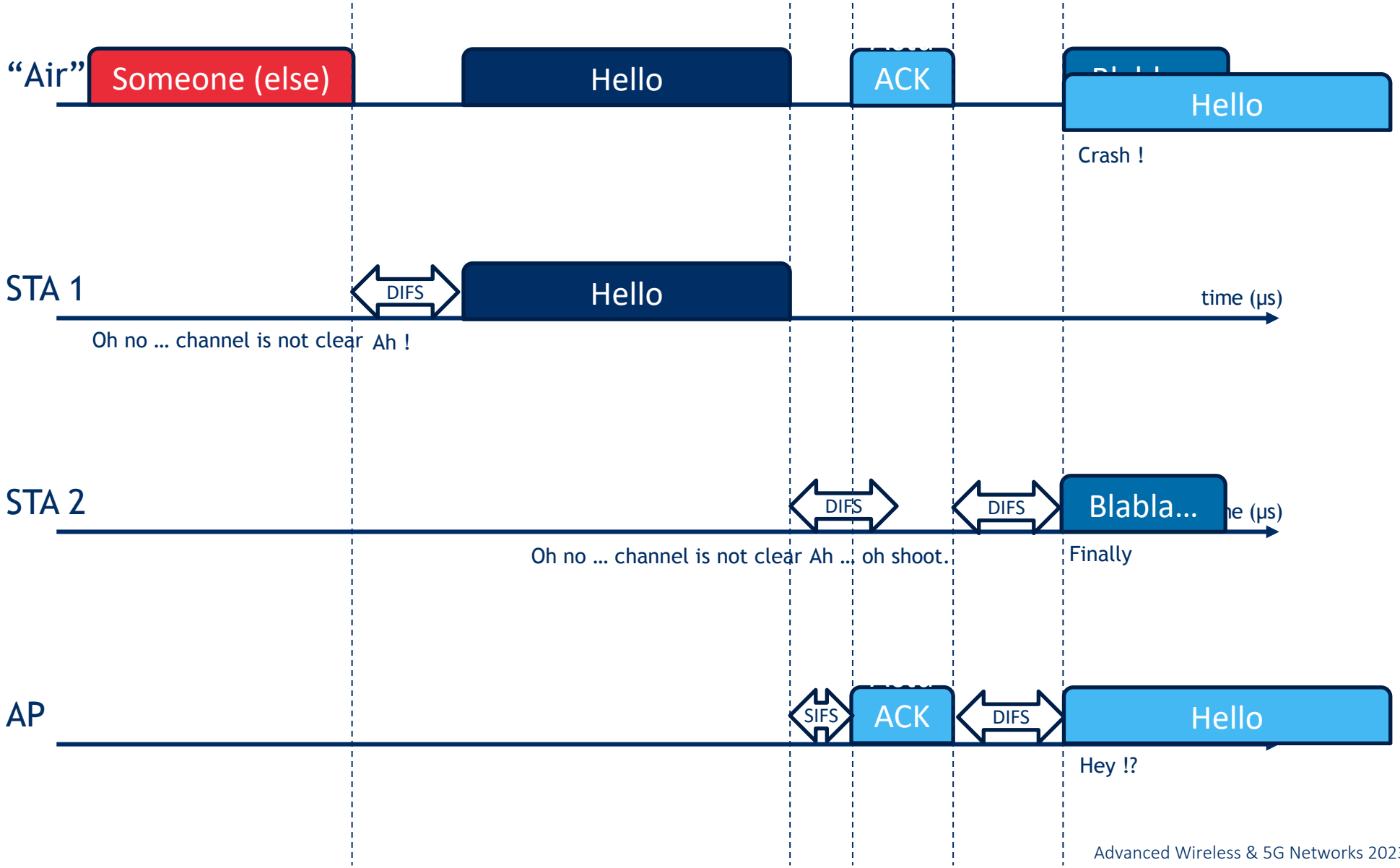
What are the steps?

1. ~~Switch on the stations (& access points)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. ~~Define how we are going to organize the bits for multiple users~~
5. ~~Listen to synchronize and get system information~~
6. Random Access
7. Get a channel (well, not exactly…)
8. Authenticate (uh, does this happen earlier?)
9. Try to send data
10. Move around

IEEE 802.11 MAC

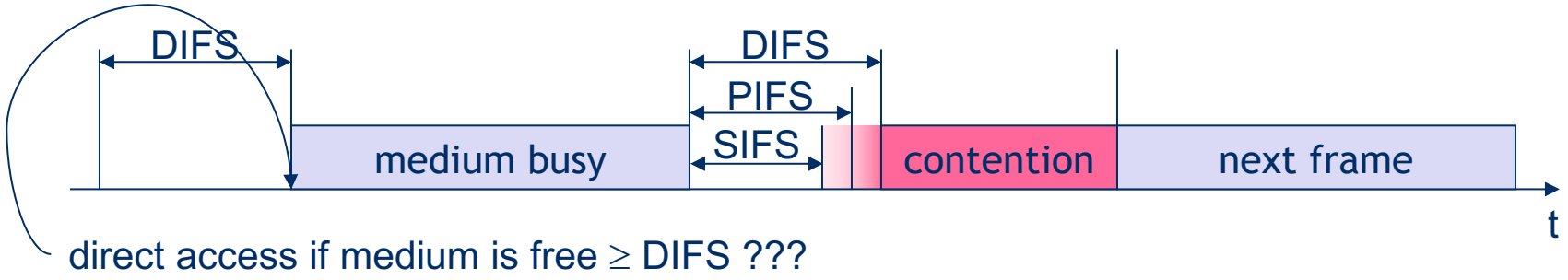


Timing chart STA1->STA2 (better, but still wrong)



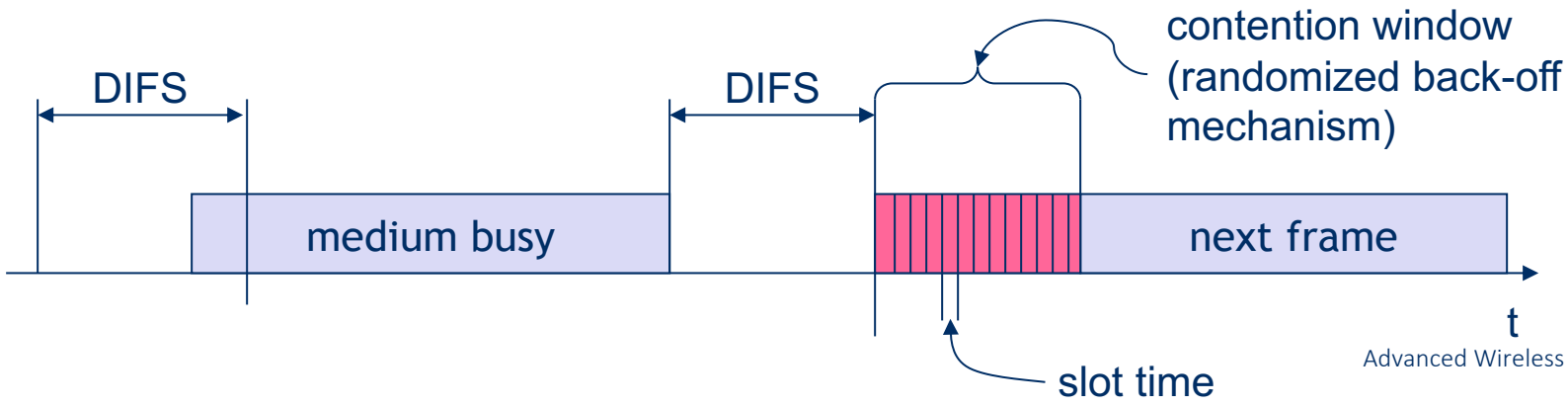
IEEE 802.11 - MAC layer - IFS

- **Priorities**
  - defined through different Inter Frame Spaces (IFS)
  - no guaranteed, hard priorities
  - SIFS (Short Inter Frame Spacing)
    - highest priority, for ACK, CTS, polling response
  - ~~PIFS (PCF IFS)~~
    - ~~medium priority, for time-bounded service using PCF~~
  - DIFS (DCF, Distributed Coordination Function IFS)
    - lowest priority, for asynchronous data service
  - EIFS (Extended IFS)
    - In case of error in decoding = longest ACK + SIFS + DIFS

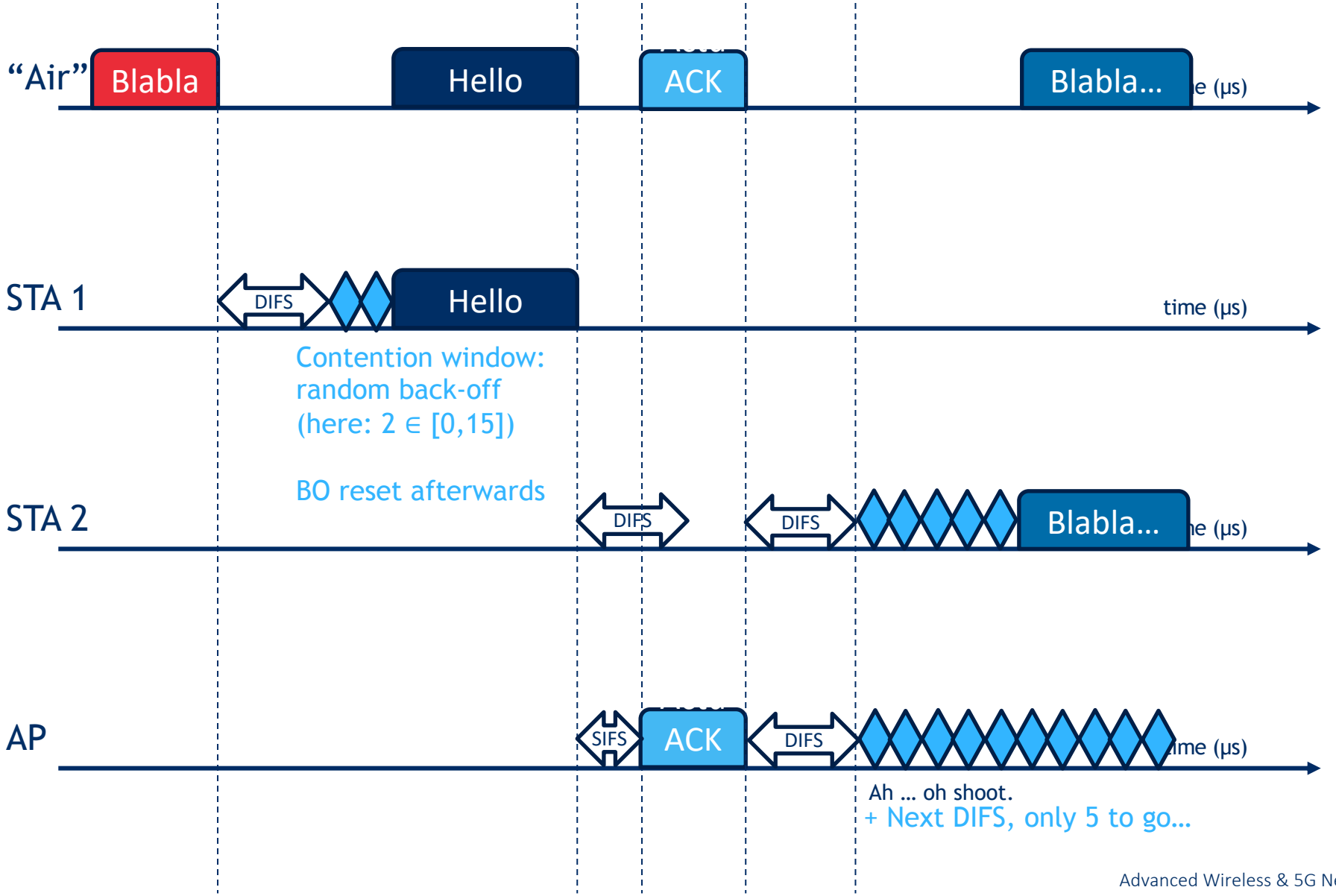


Contention Window CW

- station ready to send starts sensing the medium = **Carrier Sense based on CCA, (Clear Channel Assessment) and/or Virtual Carrier sense (we'll get there shortly)**
- if the medium is free for the duration of an Inter-Frame Space (xIFS), the station can start sending (xIFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)

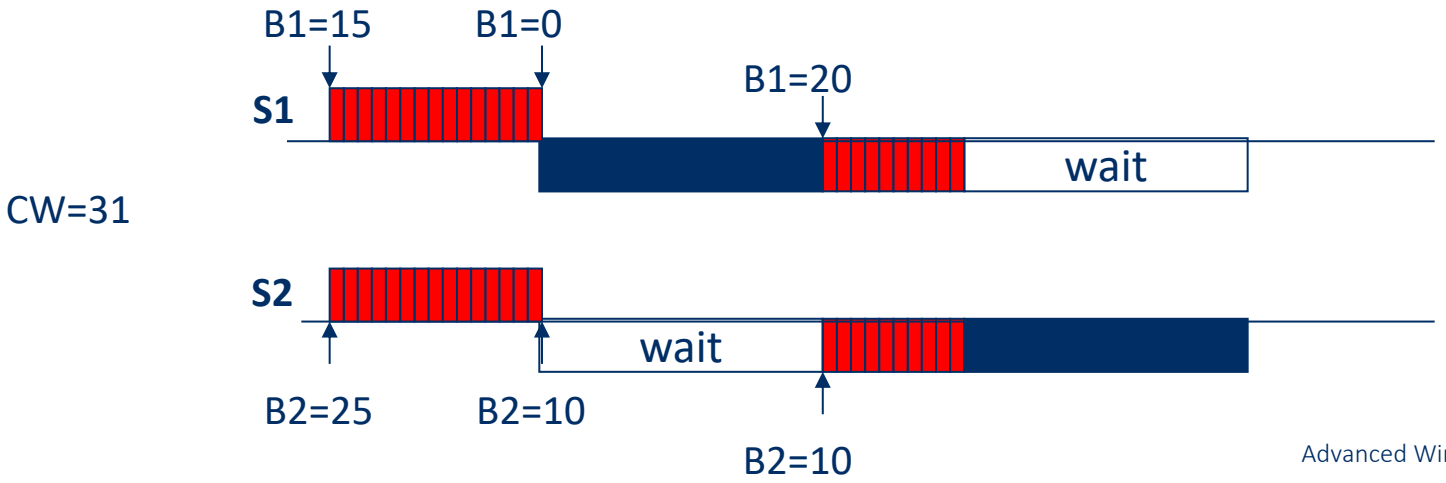


Timing chart STA1->STA2 (almost there…)

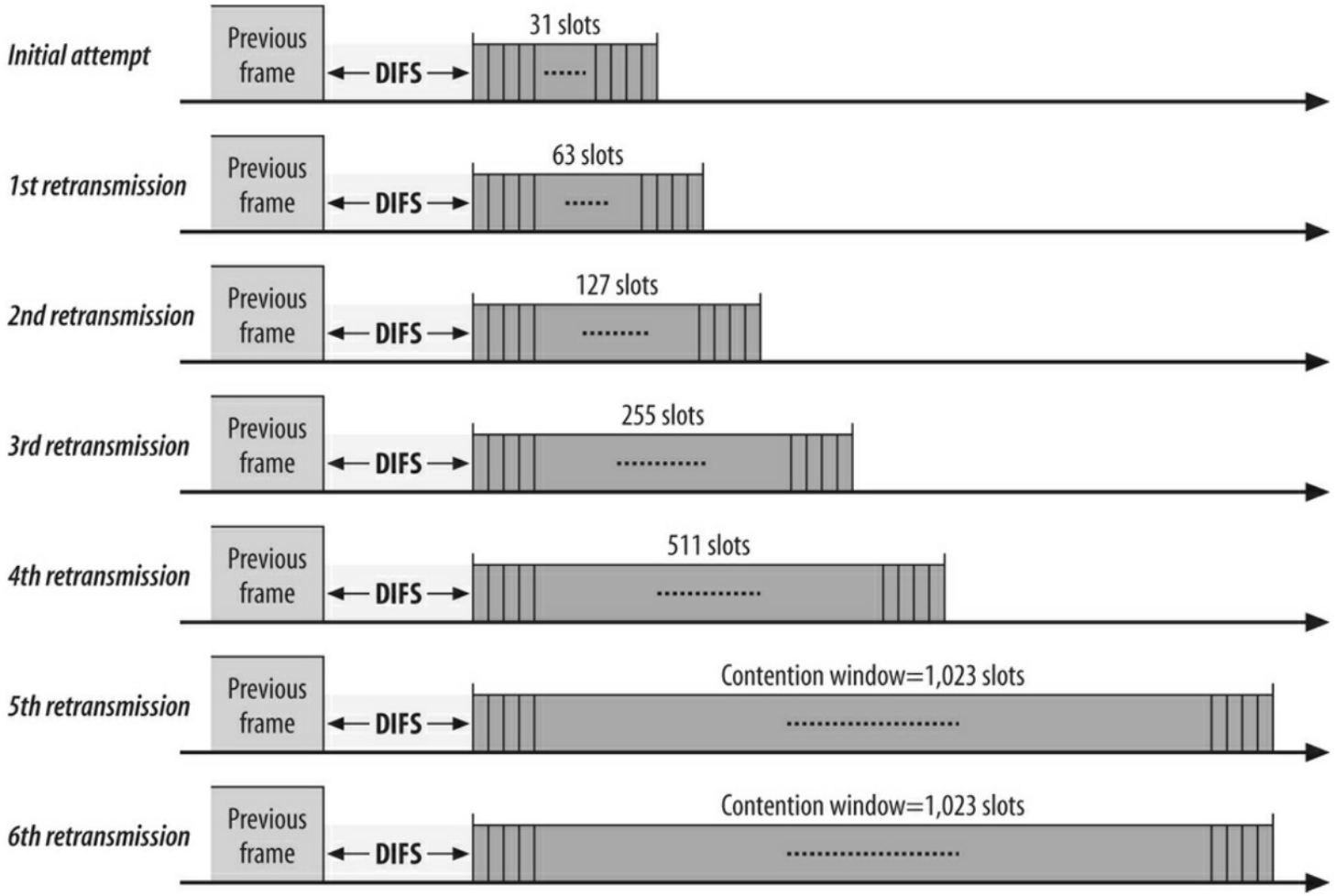


Back-off Algorithm

- **Exponential Back-off 2N-1, N ∈ [5-10]**
  - random back-off time within a contention window [0, CW]
  - contention window size N=N+1 increases with retransmission
  - back-off time = random() * slot time
  - counts down during contention window
  - random() = a pseudo random integer in [0,CW]
  - aCWmin <= CW <= acWmax, CW starts with aCWmin and increases by every retransmission upto aCWmax, and is reset after successful transmission



Contention Window Size



- Allowing long contention windows when several competing stations are attempting to gain access to the medium keeps the MAC algorithms stable even under maximum load.

CWmin and CWmax

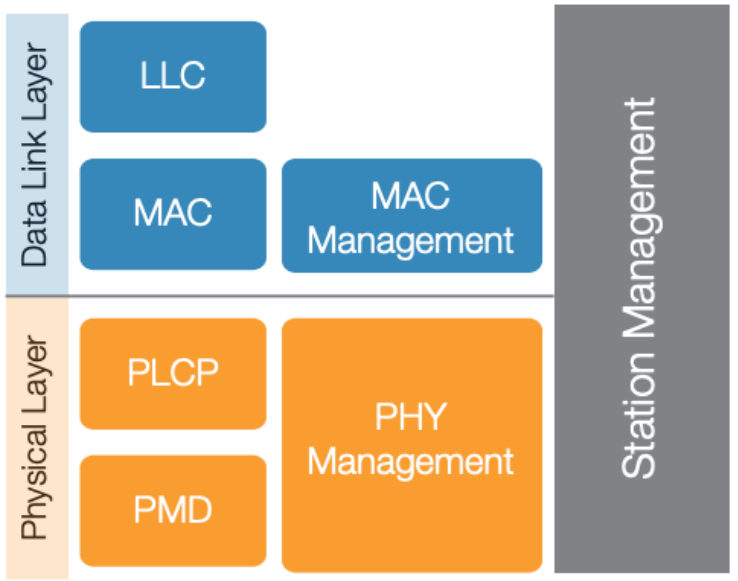
- 802.11 and 802.11b
  - Any WLAN that uses DSSS (802.11) or HR-DSSS (802.11b) technologies uses CWmin with the N-Value set to 5. This means that the CWmin value for 802.11 and 802.11b WLANs is 31. The CWmax value is 1023 (N=10)
- 802.11a/g/n/ac WLANs
  - For best effort (non-QoS) traffic: CWmin of 15 (N = 4) and a CWmax of 1023 (N = 10)
- **This is another way to differentiate QoS**

But how do you know the medium is busy?

- **Clear Channel Assessement (CCA): 2 mechanisms**
- **Physical carrier sense (the actual CCA)**
  - Energy Detection (ED): ED functionality is based upon raw RF energy. When an energy level detected in the channel crosses a certain threshold for a certain period of time, the “busy medium” indication will be triggered. Tricky to consistently calibrate, depends on Rx sensitivity, how much of a frame you detect, etc…
  - Carrier Sense (CS): more precisely, “preamble detection”—monitors and detects 802.11 preambles, which are used to trigger the CCA mechanism and indicate a busy medium.
- **Virtual Carrier Sense (using a Network Allocation Vector NAV)**

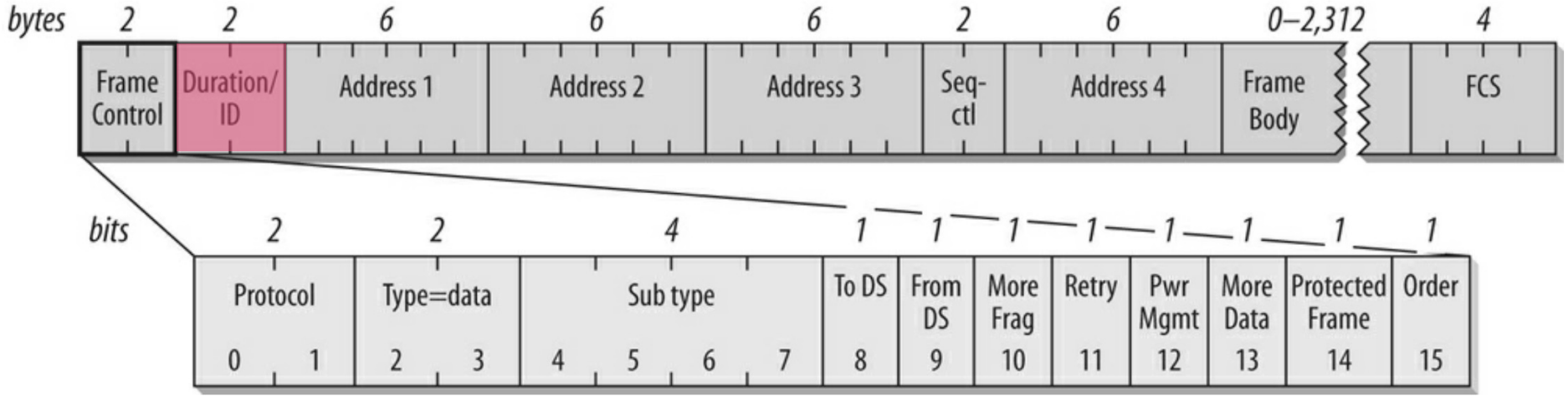
IEEE 802.11 - Layers and functions

- **MAC**
  - access mechanisms, fragmentation, encryption
- **MAC Management**
  - synchronization, roaming, MIB, power management
- **PLCP Physical Layer Convergence Protocol**
  - clear channel assessment signal (carrier sense): accomplished by detecting the presence of energy in the vicinity of the carrier
- **PMD Physical Medium Dependent**
  - modulation, coding
- **PHY Management**
  - channel selection, MIB
- **Station Management**
  - coordination of all management functions



Virtual Carrier Sense

- Uses information found in 802.11 frames to **predict the status** of the wireless medium.
- **Network Allocation Vector** (NAV = timer that is set using the duration values in the MAC header of a frame)



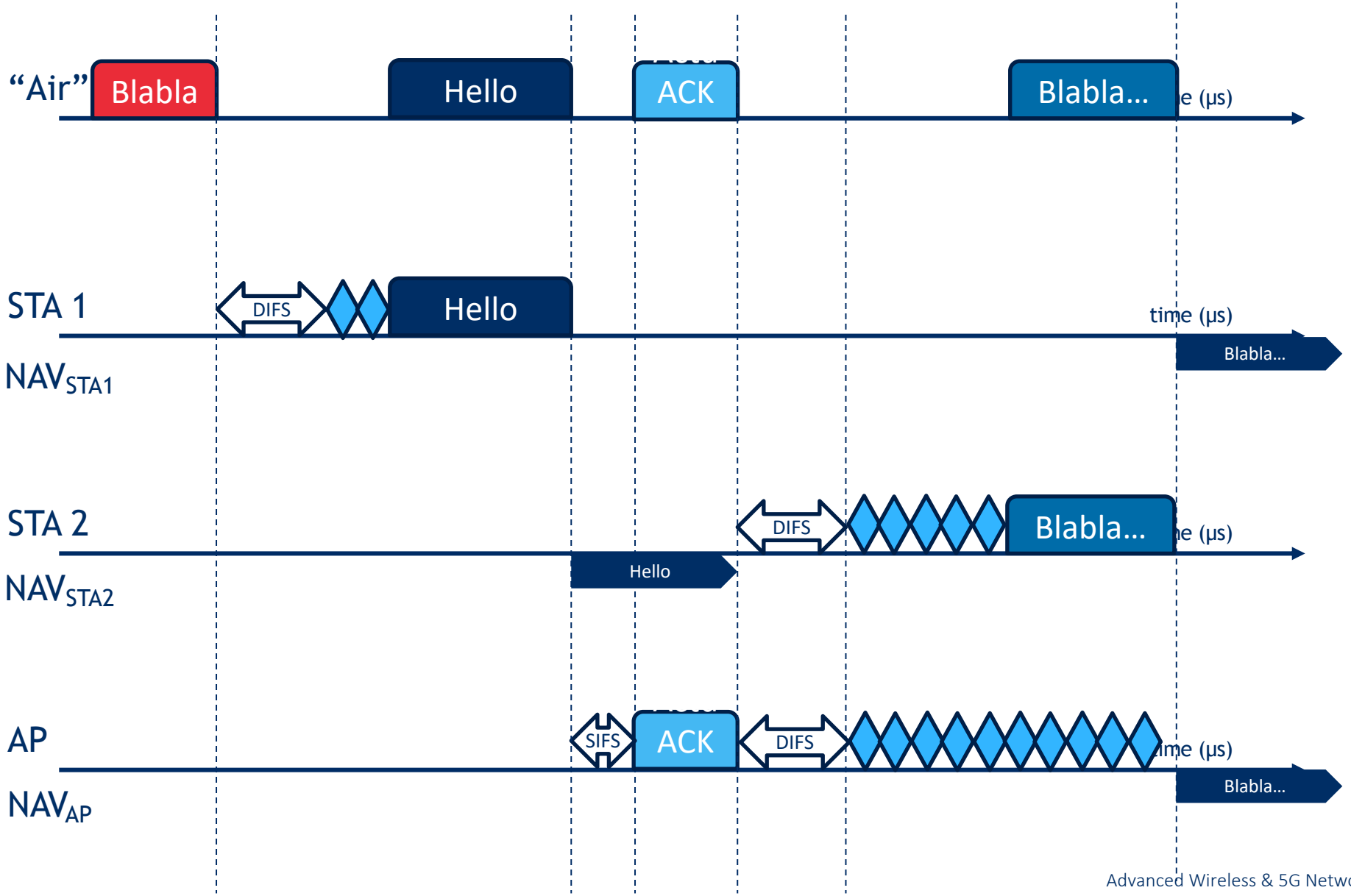
Network Allocation Vector

- All STAs attempt to process **all frames**—and a **minimum of the first** in a frame exchange (see later) —on their channel.
- The MAC header of each frame contains a **Duration** field, which indicates the amount of time necessary to complete the entire frame exchange.
  - In DCF, a transmission opportunity only allows for the transmission of one frame, thus the Duration value represents the required IFS interval and the acknowledgement frame (ACK), if one is required.
  - We will shortly see that in EDCA/HCF, this is (slightly) different

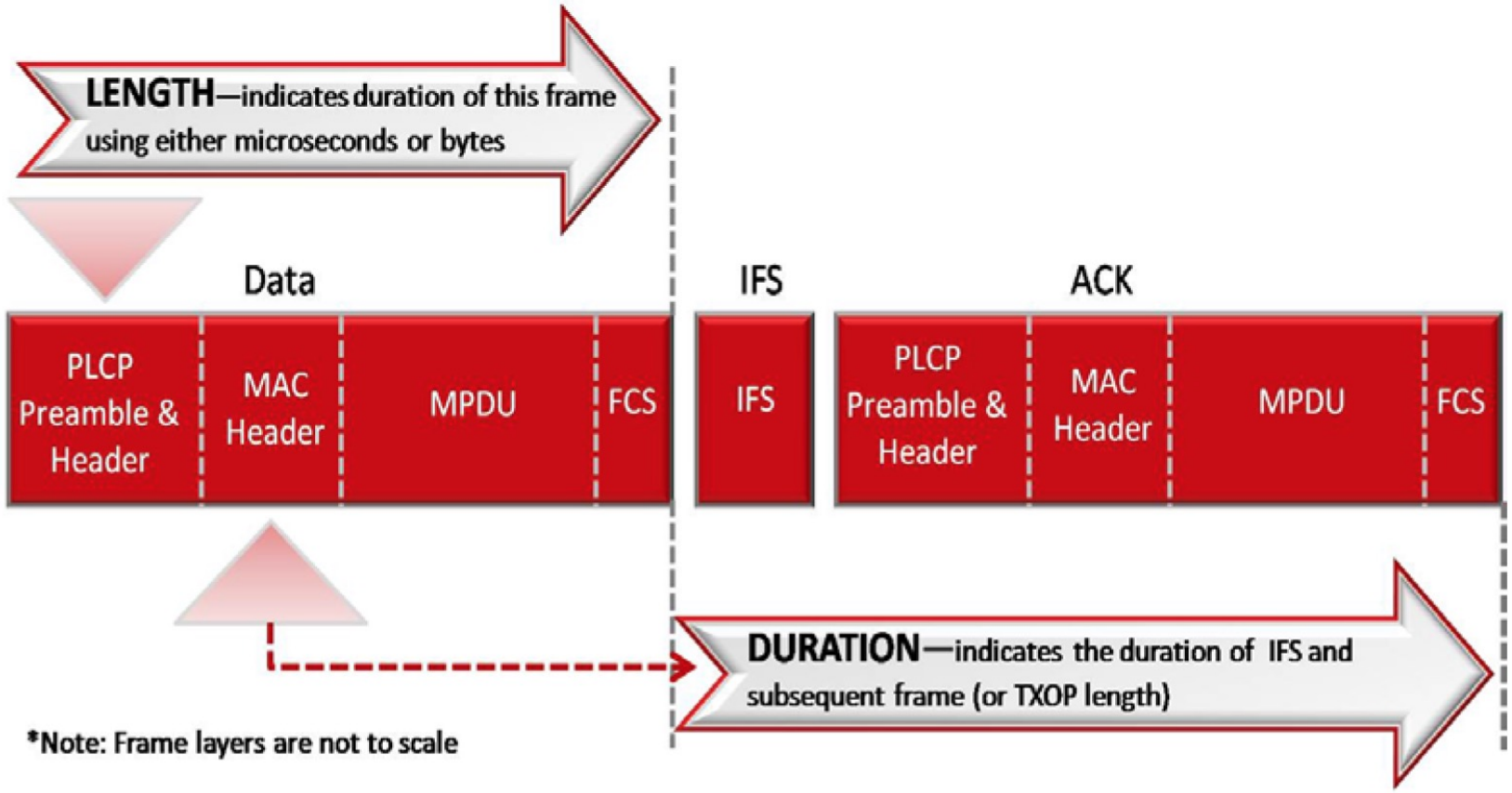
Network allocation vector

- When STAs read the Duration value in a frame, they set their **NAV timer** accordingly and **count down this duration.**
- The duration value in the MAC header indicates the time required to complete the transmission opportunity after the current—the frame in which the Duration value resides—frame if completed.
  - The duration value **does not cover the frame** in which it resides
- If a STA is counting down its NAV and it receives another frame with a **longer duration** (would increase its NAV), the **STA increases its NAV accordingly**.
- However, when a STA receives a frame with a **shorter duration** value (would decrease its NAV), the STA **ignores this value** and continues to observe the longer NAV duration.

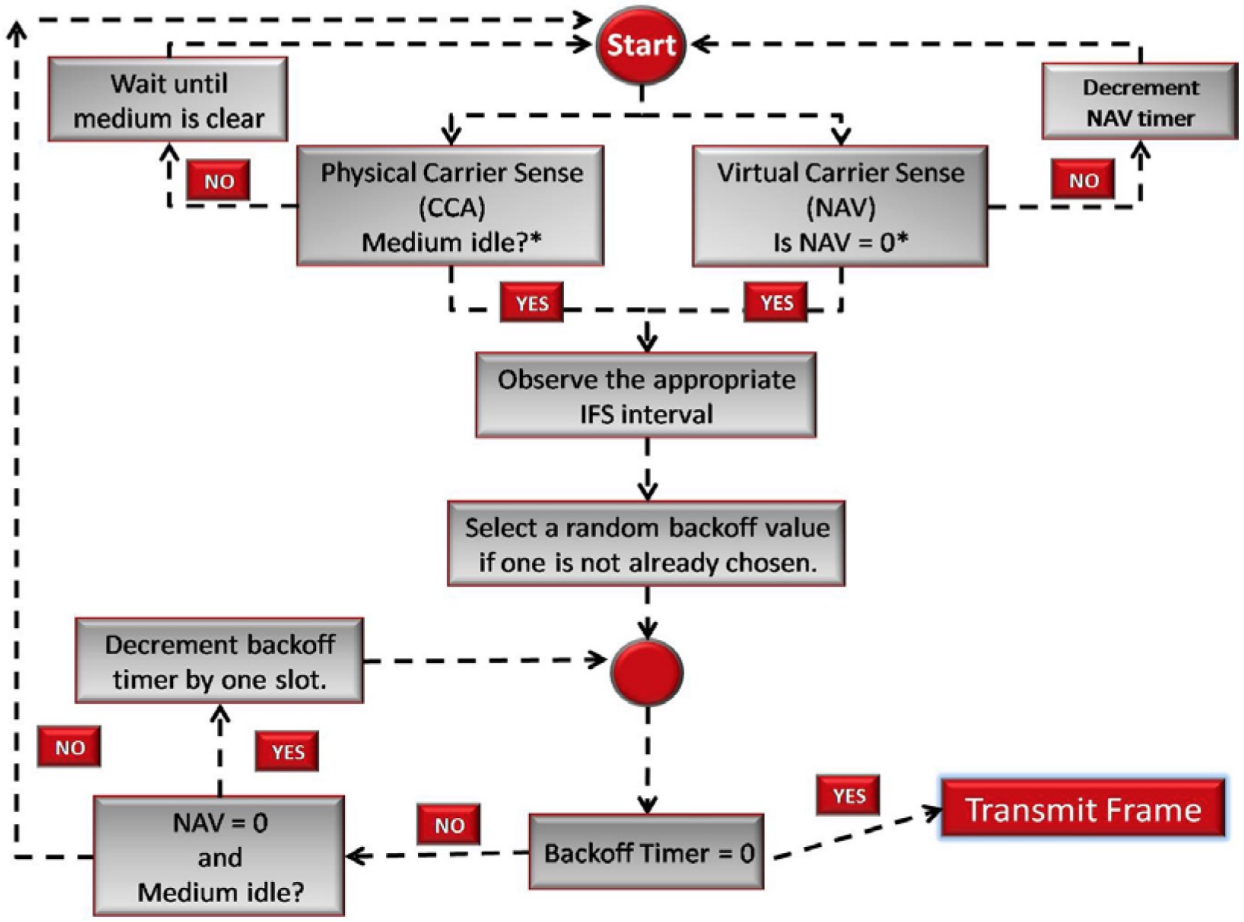
Timing chart STA1->STA2(really almost there…)



Length and Duration

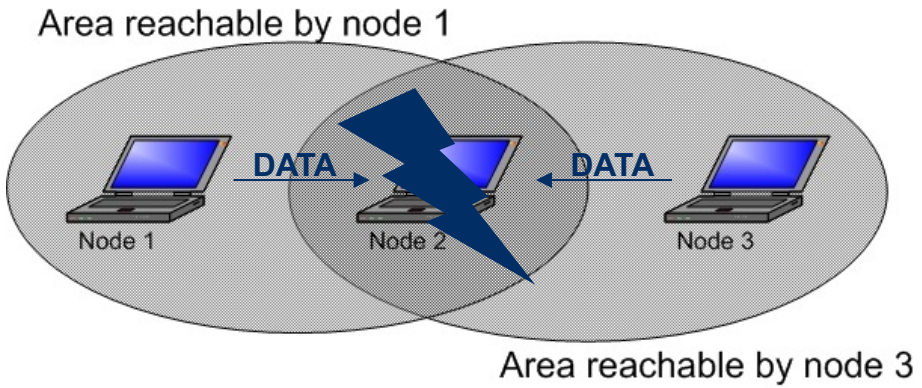


Arbitration Flowchart



* **Note** – These steps are performed continually throughout the flowchart. If either of these conditions change, the process returns to "Start"

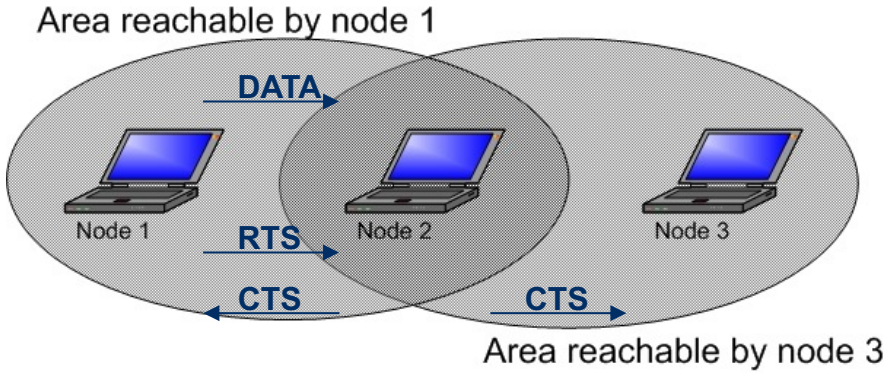
Hidden Node problem



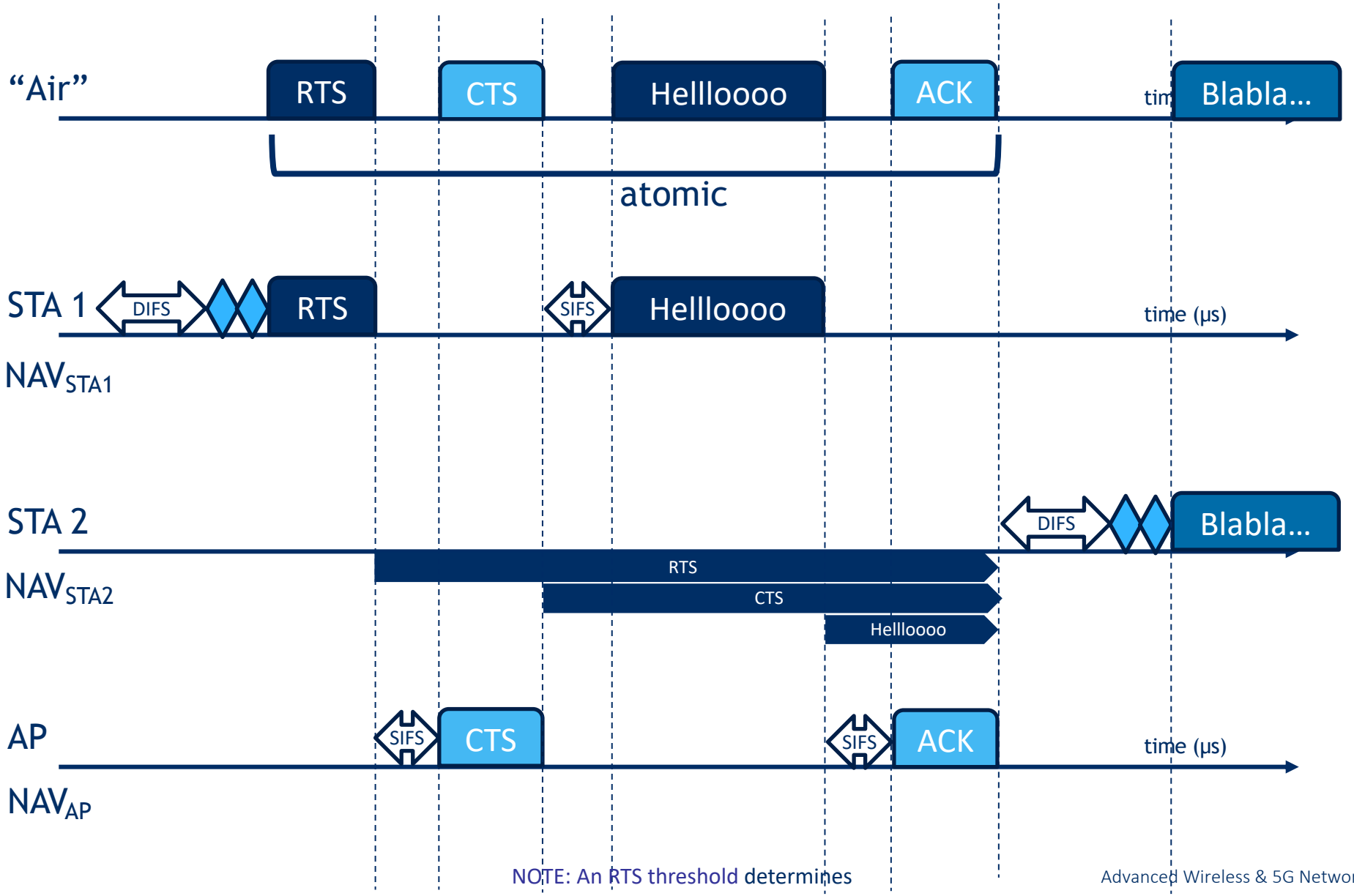
- **Scenario**
  - Node 1 is sending a data frame to node 2.
  - Node 3 cannot hear the transmission of node 1 and also sends a data frame to node 2 (CS failure).
  - Collision at receiver node 2. Node 1 and Node 3 do not notice the collision (CD failure).
  - Node 3 is “hidden” to node 1.

Hidden Node solution

- **Request To Send (RTS)/ Clear To Send (CTS) sequence**
- **Solution**
  - Node 1 first sends a RTS message to Node 2. This message instructs all the neighbors of node 1 to remain silent until the RTS/CTS procedure ends.
  - Node 2 replies with CTS message to Node 1. This message instructs all the neighbors of node 2 to remain silent during the data transfer. Node 3 overhears this CTS message.
  - Node 3 will delay its transmission until the transmission of Node 1 finishes.



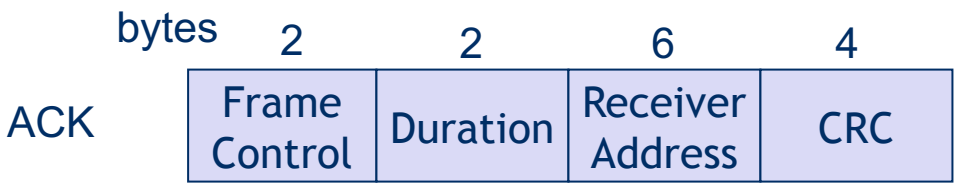
Timing chart STA1->STA2(really almost there…)



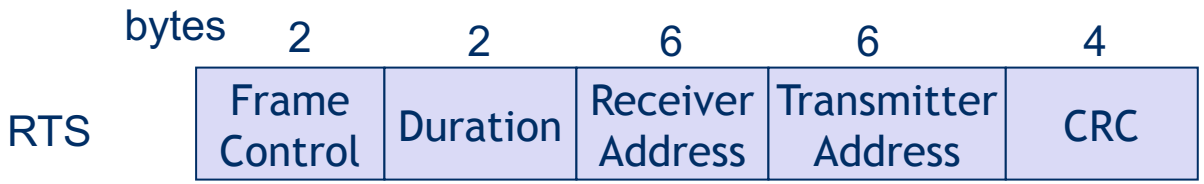
NOTE: An RTS threshold determines when to use RTS/CTS (minimal frame size)

Special Frames: ACK, RTS, CTS

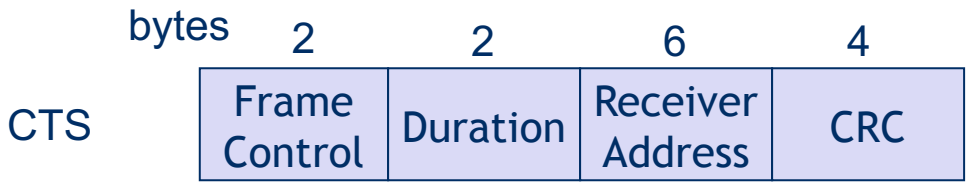
- **Acknowledgement**



- **Request To Send**

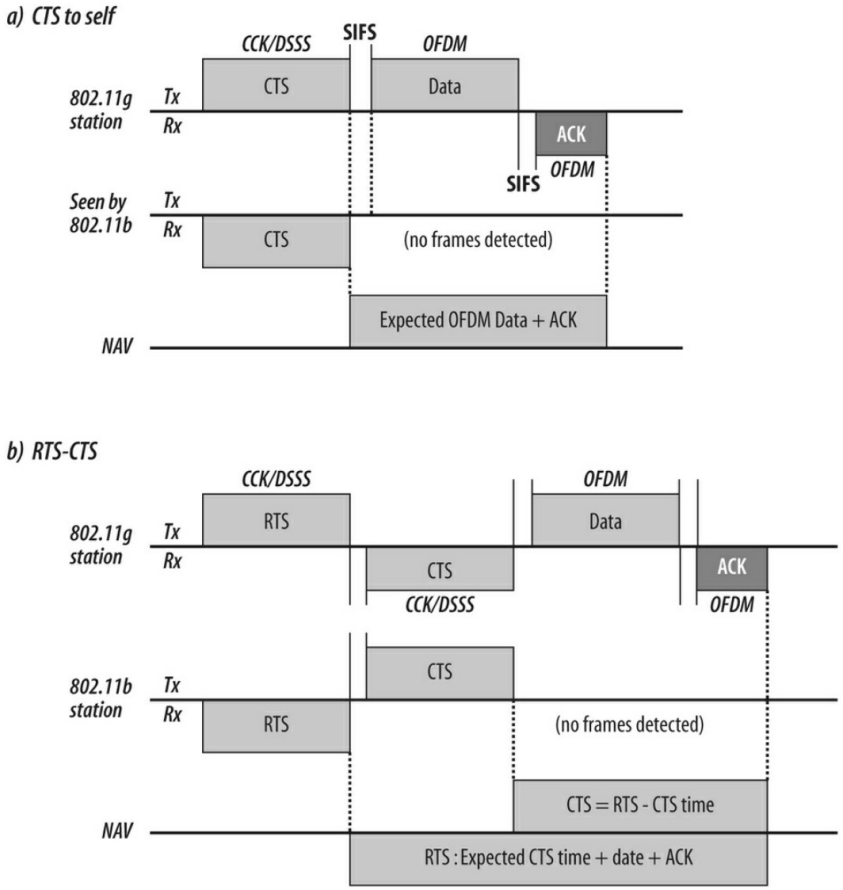


- **Clear To Send**



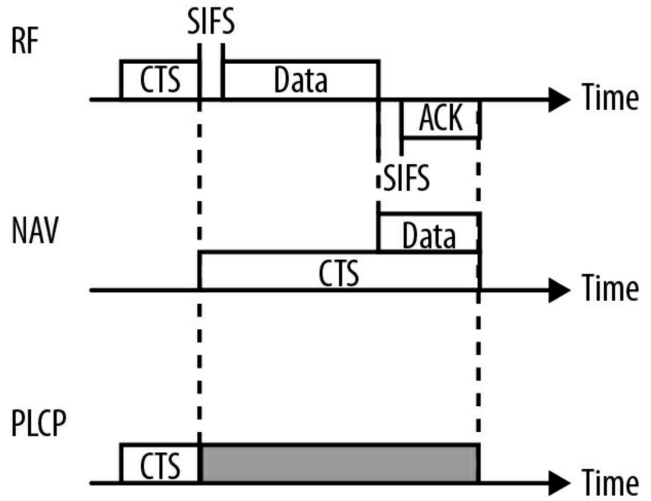
Protection Mechanisms

- **802.11g to 802.11a/b**



802.11n to a/b/g

CTS to self



QoS in IEEE 802.11

- **Two kinds of QoS**
  - Parameterized QoS:
    - Strict QoS requirement
    - Expressed quantitatively (data rate: BW of 10 Mbit/s, delay: delay bound of 10 ms, …)
    - i.e. QFI + 5QI in 5G
  - Prioritized QoS
    - Loose QoS requirement
    - Expressed in terms of relative delivery priority

QoS Support in legacy IEEE 802.11

Why is DCF not enough?

- It treats all data traffic in a FCFS, best-effort manner
- All stations contend for the wireless medium with the same priority
- No differentiation between data flows with QoS requirements

~~Why is PCF not enough?~~

- ~~Periodical appearance of DCF and PCF limiting its flexibility (because it is difficult to find a repetition period fits all flow requirements)~~
- ~~Lacking mechanism to specify traffic requirement~~

Enhanced Distributed Channel Access (EDCA)

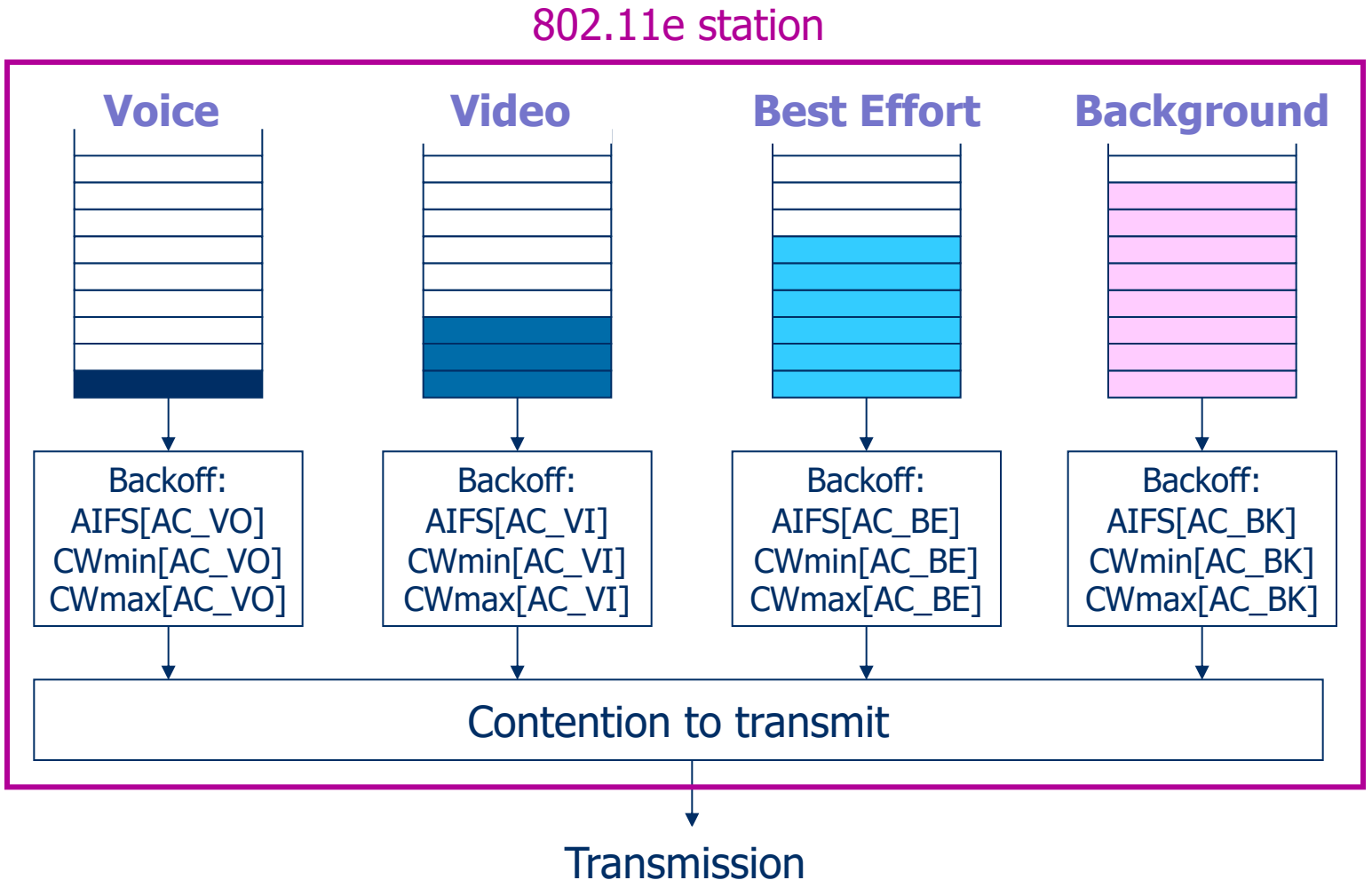
- **Differences with DCF**
  - Different **Access Classes** (AC)
    - 802.11e, synced with 802.1D
  - **Contention** between **ACs** (not between STAs)
  - **AC** contend for Transmission Opportunity (**TXOP**)
  - Inter-frame Space (IFS) per **AC**: Arbitration Inter-frame Space (**AIFS**)
  - Contention Window parameters per AC

Priorities in IEEE 802.11e

- **Access Category (AC)**
  - 4 access priorities:
    - AC_BK (Background)
    - AC_BE (Best Effort)
    - AC_VI (Video)
    - AC_VO (Voice)
- **User Priority (UP)**
  - 8 UP classes
  - Each AC contains 2 UPs, resulting in 8 classes
  - Traffic of higher UP transmitted first in one AC
    - Virtual collisions

Priority	User Priority (UP)	802.11 Access Category (AC)	802.11 AC Designation	802.1D Designation
Lowest Priority	1	AC_BK	Background	BK
	2	AC_BK	Background	--
	0	AC_BE	Best Effort	BE
	3	AC_BE	Best Effort	EE
	4	AC_VI	Video	CL
	5	AC_VI	Video	VI
Highest Priority	6	AC_VO	Voice	VO
	7	AC_VO	Voice	NC

EDCA : four access categories



Default EDCA Parameter Set

AC	CWmin	CWmax	AIFSN
AC_BK	aCWmin	aCWmax	7
AC_BE	aCWmin	aCWmax	3
AC_VI	(aCWmin-1)/2	aCWmax	2
AC_VO	(aCWmin-3)/4	(aCWmin-1)/2	2

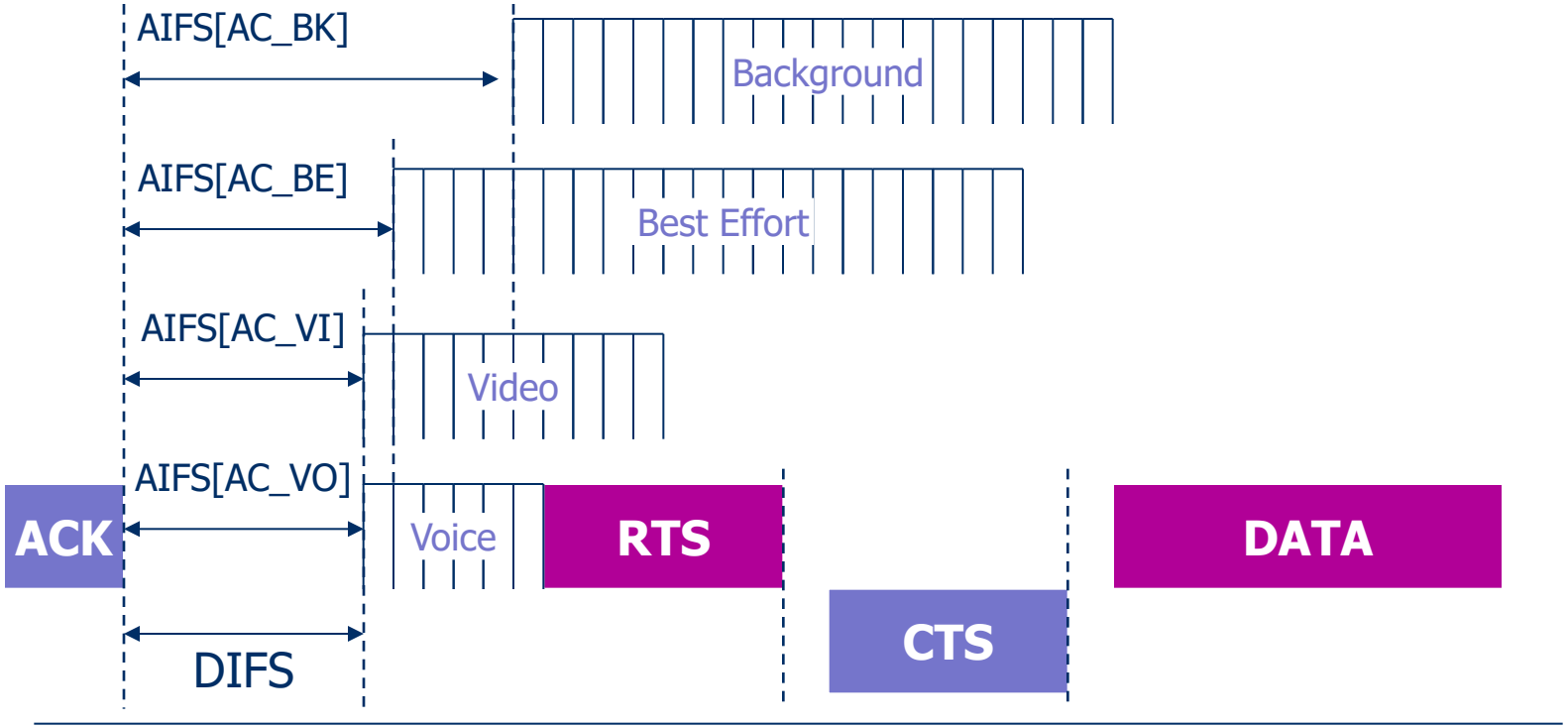
Arbitration Interframe Space Number

This is a term used in IEEE (Institute of Electrical and Electronics Engineers) 802.11 networks which are supporting the QoS (Quality of Service) enhancements originally defined in the 802.11e standard. This parameter, which is transmitted from the AP (Access Point), is used by a station in order to determine the specific AIFS (Arbitration Interframe Space) value for each of the four EDCA (Enhanced Distributed Channel Access) classes.

$$AIFS = AIFSN[AC] * ST + SIFS$$

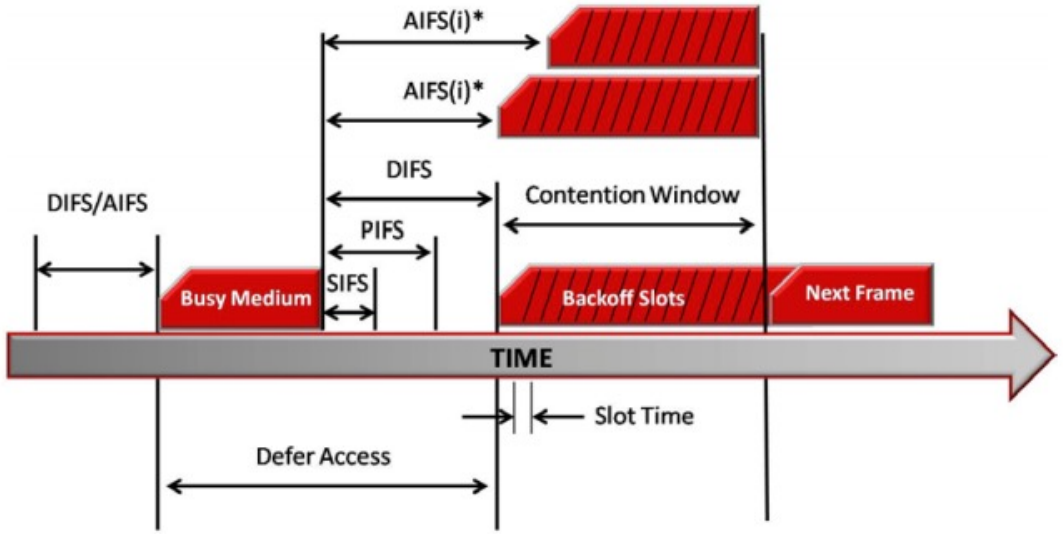
EDCA access control

- **AIFS, CWmin and CWmax can be decided by AP**



Default Arbitration IFS for different flavors

AC	AIFSN	802.11b AIFS[AC]	802.11g AIFS[AC]	802.11a AIFS[AC]	802.11n 2.4 GHz AIFS[AC]	802.11n 5 GHz AIFS[AC]
AC_BK	7	150 µs	Long = 150 µs Short = 73 µs	79 µs	Long = 150 µs Short = 73 µs	79 µs
AC_BE	3	70 µs	Long = 70 Short = 37 µs	43 µs	Long = 70 µs Short = 37 µs	43 µs
AC_VI	2	50 µs	Long = 50 µs Short = 28 µs	34 µs	Long = 50 µs Short = 28 µs	34 µs
AC_VO	2	50 µs	Long = 50 µs Short = 28 µs	34 µs	Long = 50 µs Short = 28 µs	34 µs



Arbitration Interframe Space Number

This is a term used in IEEE (Institute of Electrical and Electronics Engineers) 802.11 networks which are supporting the QoS (Quality of Service) enhancements originally defined in the 802.11e standard. This parameter, which is transmitted from the AP (Access Point), is used by a station in order to determine the specific AIFS (Arbitration Interframe Space) value for each of the four EDCA (Enhanced Distributed Channel Access) classes.

EDCA - TXOP bursting & CFB

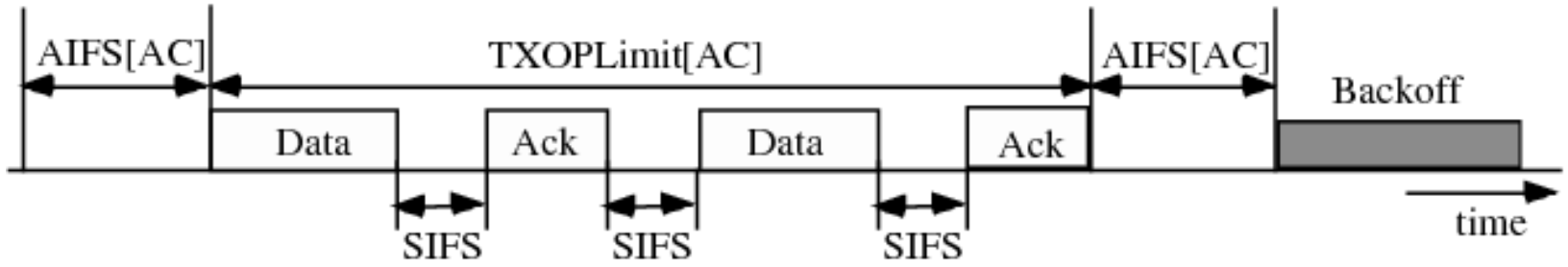


Fig. 1. IEEE 802.11e EDCA TXOP–bursting.

- EDCA introduces TXOP: a time period where one device, called TXOP holder has unfettered acccess to the channel for data transmission. The data frame transmissions within a TXOP are called a “contention free burst -CFB” During a TXOP, only the data that makes up a CFB and the ACK for that data may access the channel.

Category	AC	AIFSN	CW_min	CW_max	Default_x	TXOP (in 32 µS units)		802.11b	802.11g	802.11a	11n(2.4)	11n(5GHz)
						DSS	OFDM	AIFS [AC]	AIFS [AC]	AIFS [AC]	AIFS [AC]	AIFS [AC]
Voice	AC_VO	2	3	7	3	102	47	50 µS	L : 50 µS S : 28 µS	34 µS	L : 50 µS S : 28 µS	34 µS
Video	AC_VI	2	7	15	4	188	94	50 µS	L : 50 µS S : 28 µS	34 µS	L : 50 µS S : 28 µS	34 µS
Best Effort	AC_BE	3	15	1023	10	0	0	70 µS	L : 70 µS S : 37 µS	43 µS	L : 70 µS S : 37 µS	43 µS
Background	AC_BK	7	15	1023	10	0	0	150 µS	L : 150 µS S : 73 µS	79 µS	L : 150 µS S : 73 µS	79 µS

How long do we have the channel: TXOP

In relationship to EDCA:

- Once CCA, NAV=0, AIFS and CW all ok, the Access Categories have a different **Transmit Opportunities (TXOP).**
- The **AC_BK and AC_BE categories have a TXOP of 0.** This means they can only send 1 frame during their TXOP. Afterwards, back to CCA, NAV, AIFS, and CW (=DCF)
- The **AC_VI has a TXOP of 4.096ms (22.56ms or 16.92ms for 802.11ac devices*).** This means the video category can send as many frames it can within that time. Once its TXOP is up, it must contend for the wireless medium again if it has additional frames to send.
- Similarly, the **AC_VO has a TXOP of 2.080ms (11.28ms or 8.46ms for 802.11ac devices*)**.

Network Allocation Vector (extra)

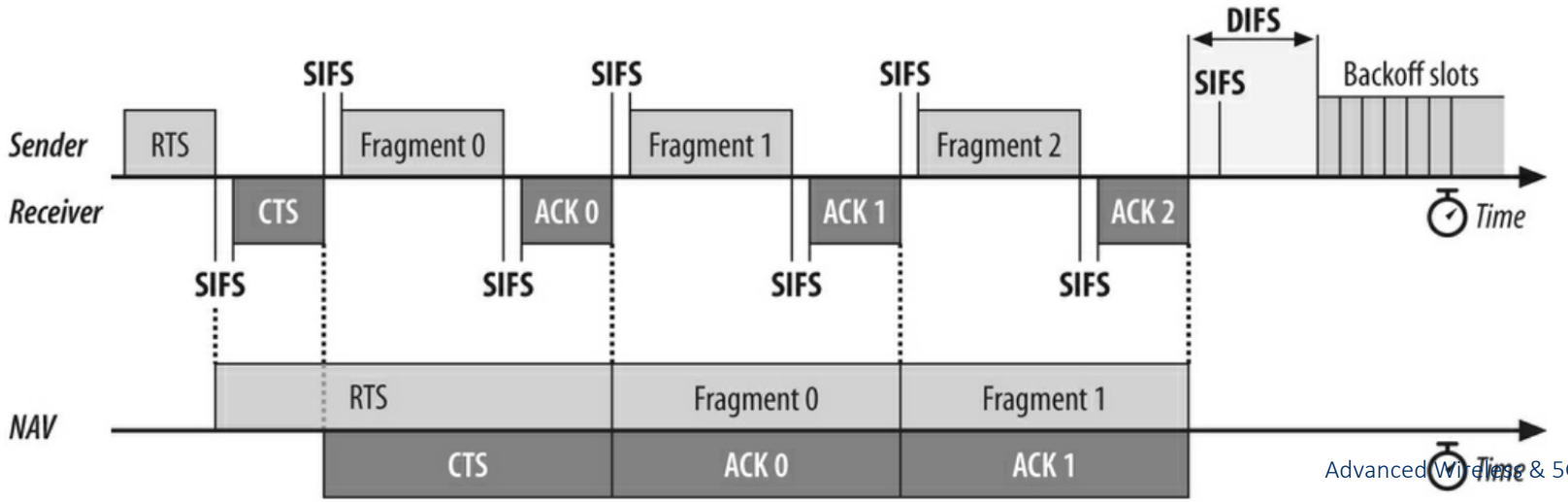
- **All STAs attempt to process all frames—and a minimum of the first in a frame exchange (see later)** —on their channel. The **first frame in a frame exchange** is significant because it can, and sometimes must, be used to determine how long a **given transmission opportunity** will occupy the medium
- The MAC header of each frame contains a **Duration field**, which indicates the amount of time necessary to complete the entire frame exchange, or the entire TXOP duration.
  - In **DCF**, a transmission opportunity only allows for the transmission of one frame, thus the Duration value represents the required IFS interval and the acknowledgement frame (ACK), if one is required.
  - The exception to this rule is for networks in which RTS/CTS or CTS-to-self protection is enabled. In this case, the transmission opportunity allows for the use of these frames.
- **In HCF, several frames may be transmitted within a transmission opportunity.** Thus, the Duration value refers to the TXOP duration. In either case, non-transmitting STAs must remain idle while the medium is reserved.

Fragmentation Mode

• **Fragmentation** in 802.11 reduces packet errors in certain situations, e.g. in a noisy environment. A larger frame has a higher chance of getting corrupted than a smaller one. The error correcting mechanism can correct some erroneous bits in a received frame, but as the bit error rate increases, it becomes less likely that it can correct all bit errors. In 802.11, a frame can be fragmented to a maximum of 16 fragments.

• Sender issues an RTS packet to reserve the medium of the first fragment; a CTS is replied; the other stations set their NAV vector for the sending of the first fragment

• The frame with the first fragment contains a duration field, reserving the medium for the transmission of the second frame. The ACK sent by the receiver also contains this duration field. The other stations set their NAV vector for the sending of fragment 2.

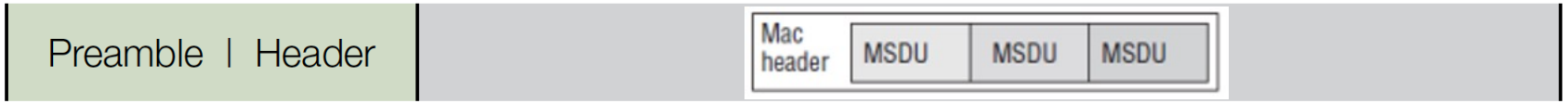


Combining multiple transmissions

More important for high-rate PHYs: nice large chunks

Hence, Frame Aggregation: 2 types

- **1. Aggregate MAC Service Data Unit (A-MSDU)**
  - At the MAC layer



- **2. Aggregate MAC Protocol Data Unit (A-MPDU)**
  - At the PLCP layer

https://mrncciew.com/2014/11/01/cwap-802-11-data-frame-aggregation/

802.11n (&ac): Frame Aggregation

FIGURE 6.8 A-MSDU frame aggregation

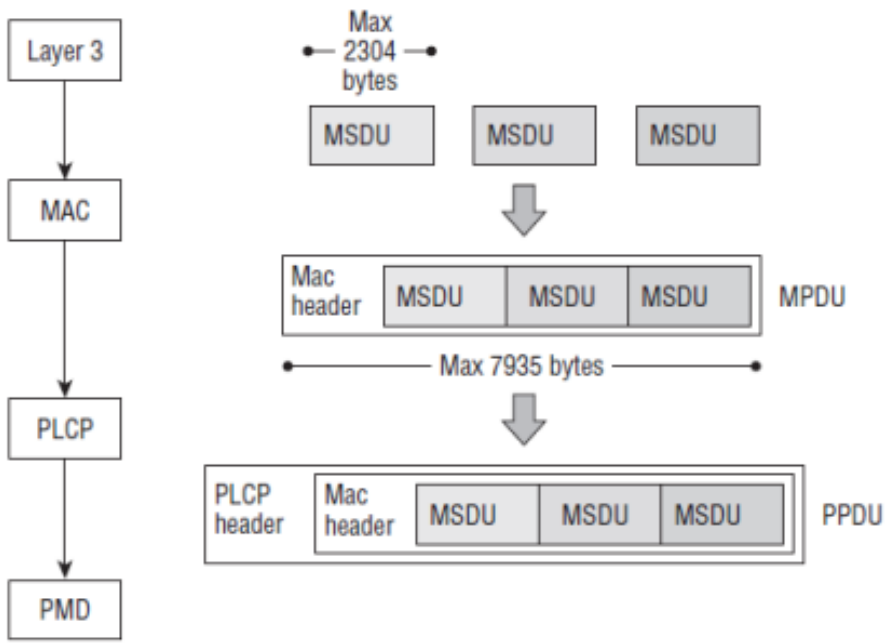
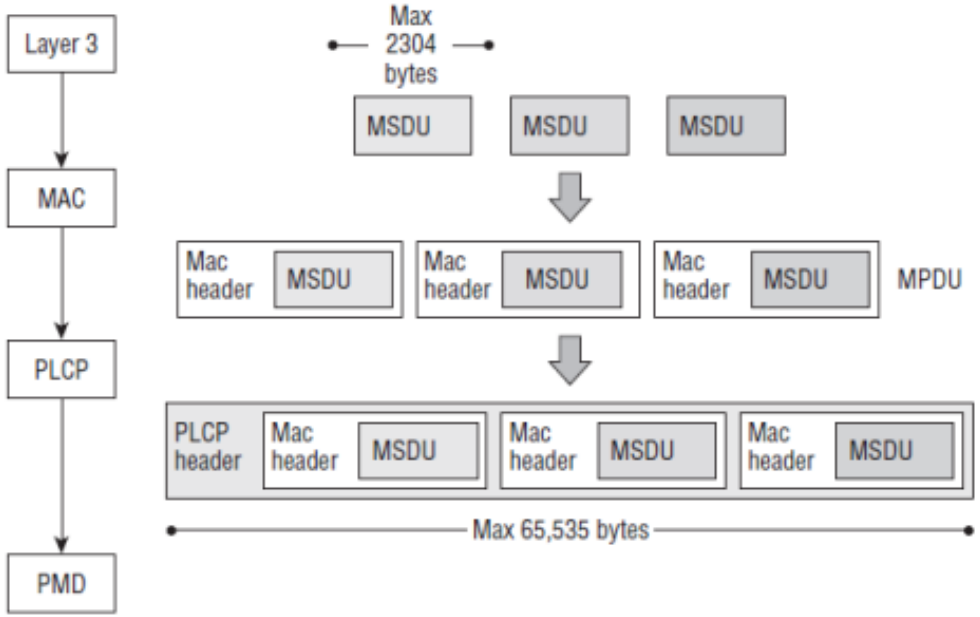
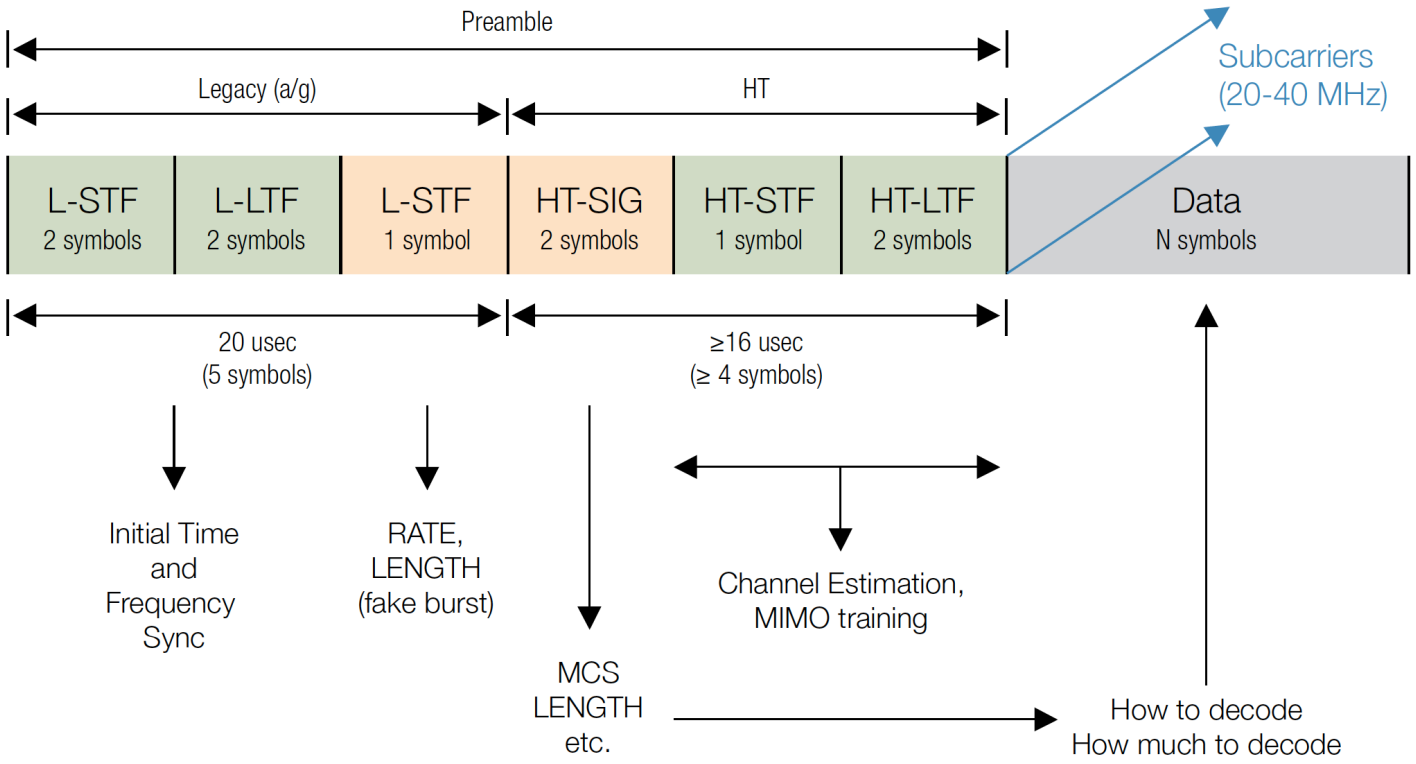


FIGURE 6.9 A-MPDU frame aggregation



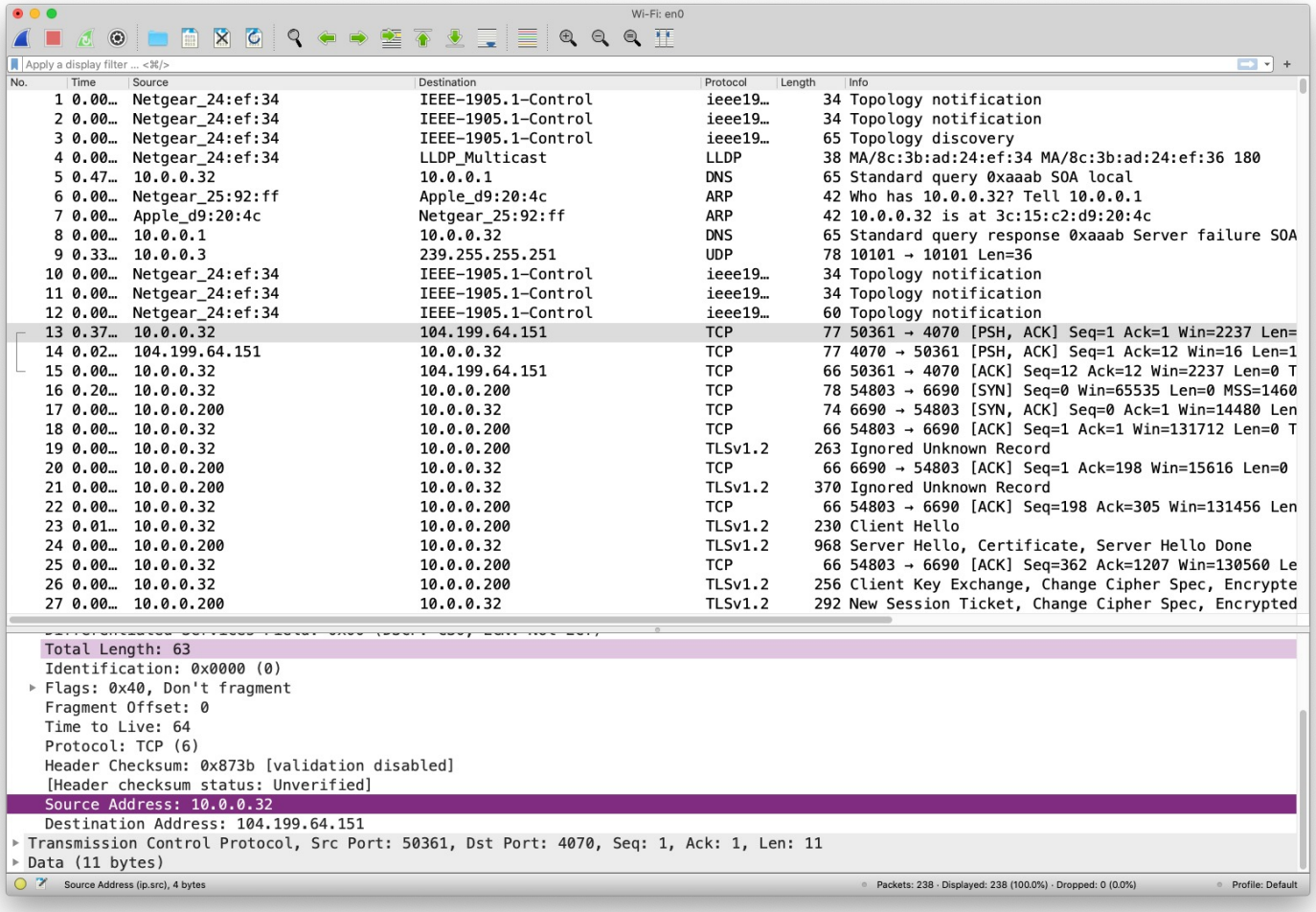
- There are constraints to A-MSDU
  - An A-MSDU shall contain only MSDUs whose DA and SA parameter values map to the same RA and TA values.
  - The constituent MSDUs of an A-MSDU shall all have the same priority parameter value.
  - An A-MSDU shall be carried, without fragmentation, within a single QoS data MPDU.
  - The Address 1 field of an MPDU carrying an A-MSDU shall be set to an individual address.
- There are constraints to A-MPDU
  - The individual MPDU within an A-MPDU must all have same receiver address.
  - The individual MPDU must all be of the same 802.11e QoS access category.
  - A-MPDU also require the use of Block Ack.
  - The Duration/ID fields in the MAC headers of all MPDUs in an A-MPDU carry the same value.

Let’s make this more concrete: 802.11n

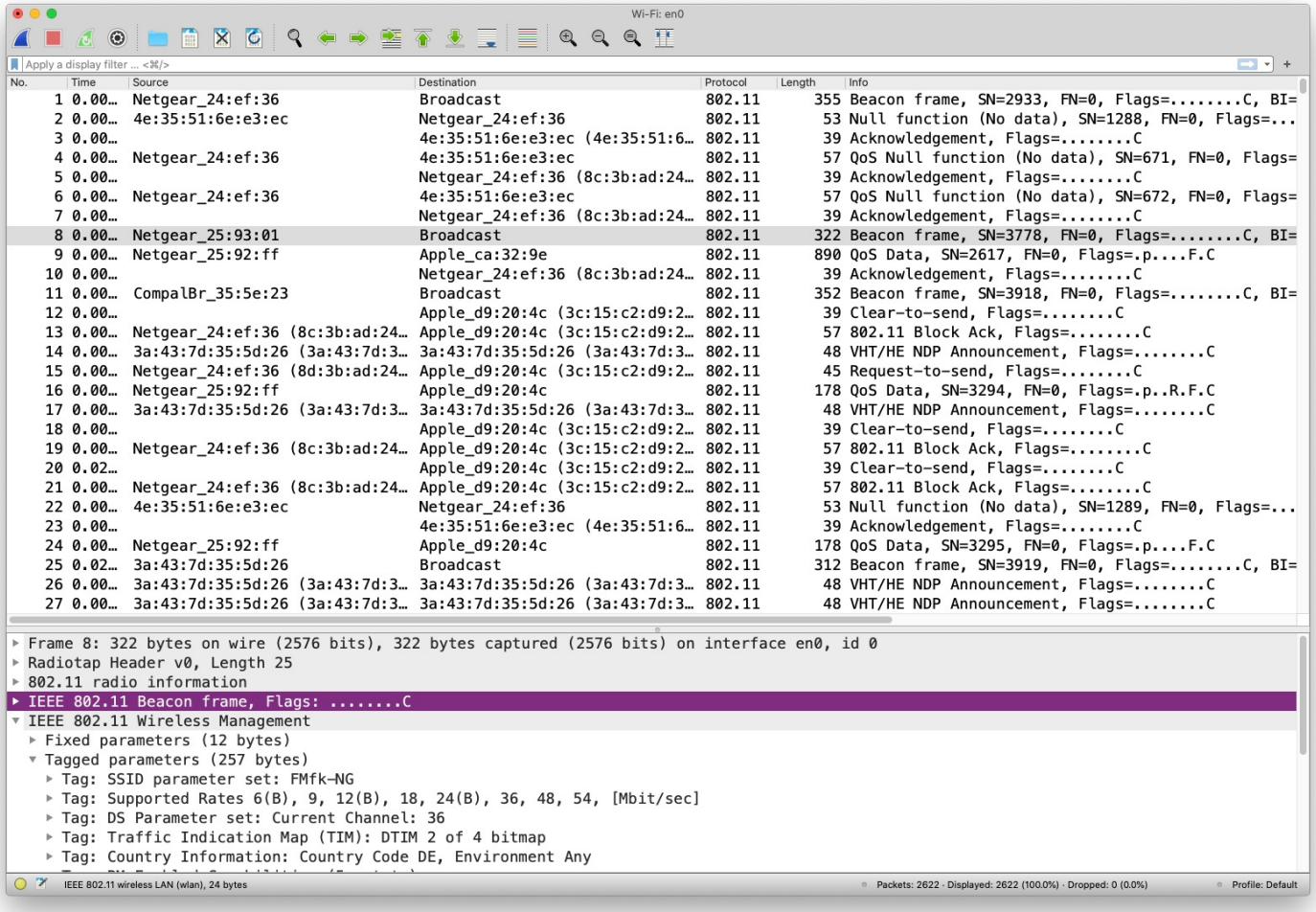


Modulation Coding Scheme and Forward Error Correction Rate for 802.11n				
MCS	Modulation	FEC Rate	Data Rate	
			20 MHz (Mbps)	40 MHz (Mbps)
0	BPSK	1/2	7.2	15.0
1	QPSK	1/2	14.4	30.0
2	QPSK	3/4	21.7	45.0
3	16QAM	1/2	28.9	60.0
4	16QAM	3/4	43.3	90.0
5	64QAM	2/3	57.8	120.0
6	64QAM	3/4	65.0	135.0
7	64QAM	5/6	72.2	150.0

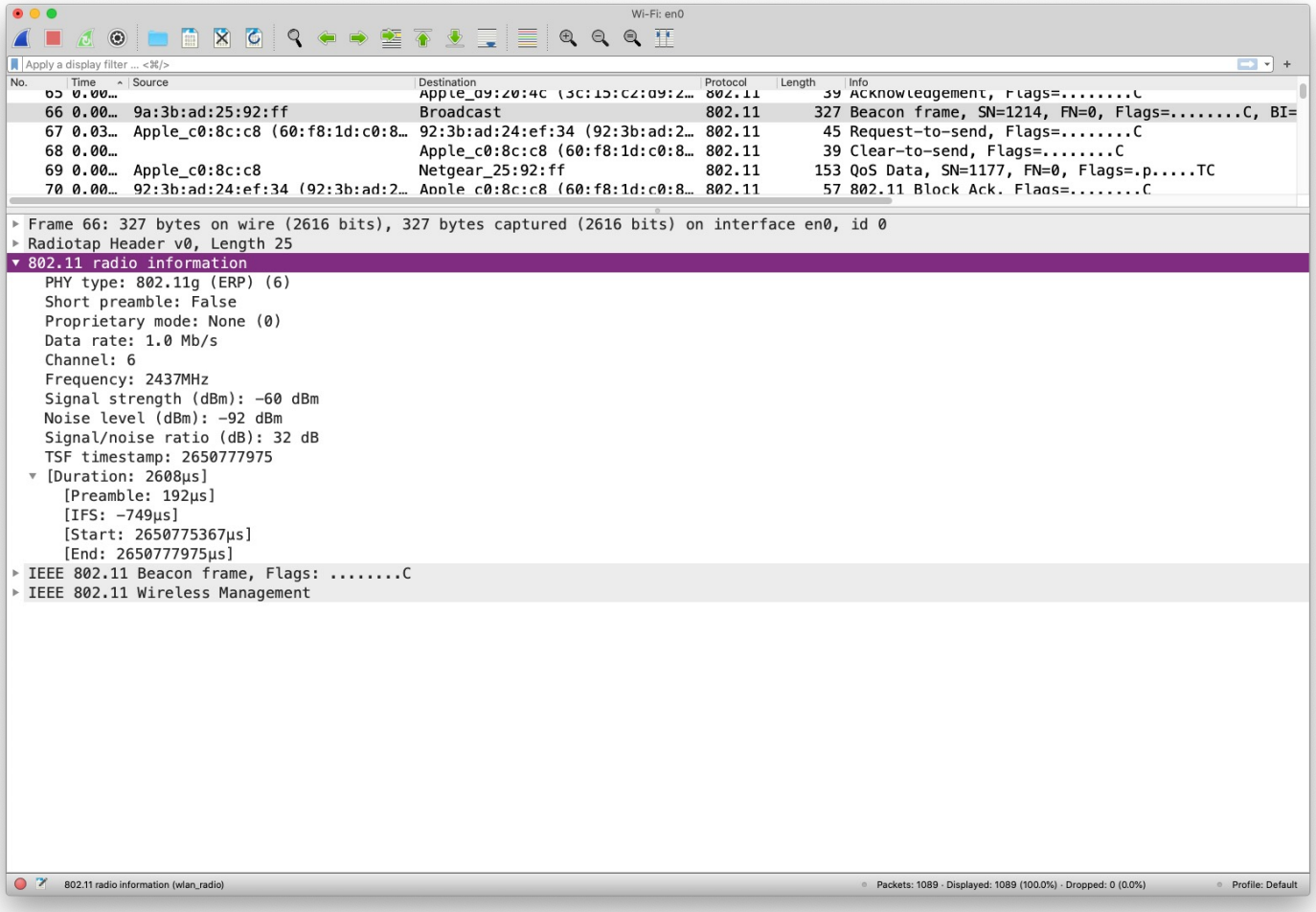
Wireshark


Wi-Fi: en0
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
1 0.00… Netgear_24:ef:34 IEEE-1905.1-Control ieee19… 34 Topology notification
2 0.00… Netgear_24:ef:34 IEEE-1905.1-Control ieee19… 34 Topology notification
3 0.00… Netgear_24:ef:34 IEEE-1905.1-Control ieee19… 65 Topology discovery
4 0.00… Netgear_24:ef:34 LLDP_Multicast LLDP 38 MA/8c:3b:ad:24:ef:34 MA/8c:3b:ad:24:ef:36 180
5 0.47… 10.0.0.32 10.0.0.1 DNS 65 Standard query 0xaaab SOA local
6 0.00… Netgear_25:92:ff Apple_d9:20:4c ARP 42 Who has 10.0.0.32? Tell 10.0.0.1
7 0.00… Apple_d9:20:4c Netgear_25:92:ff ARP 42 10.0.0.32 is at 3c:15:c2:d9:20:4c
8 0.00… 10.0.0.1 10.0.0.32 DNS 65 Standard query response 0xaaab Server failure SOA
9 0.33… 10.0.0.3 239.255.255.251 UDP 78 10101 → 10101 Len=36
10 0.00… Netgear_24:ef:34 IEEE-1905.1-Control ieee19… 34 Topology notification
11 0.00… Netgear_24:ef:34 IEEE-1905.1-Control ieee19… 34 Topology notification
12 0.00… Netgear_24:ef:34 IEEE-1905.1-Control ieee19… 60 Topology notification
13 0.37… 10.0.0.32 104.199.64.151 TCP 77 50361 → 4070 [PSH, ACK] Seq=1 Ack=1 Win=2237 Len=
14 0.02… 104.199.64.151 10.0.0.32 TCP 77 4070 → 50361 [PSH, ACK] Seq=1 Ack=12 Win=16 Len=1
15 0.00… 10.0.0.32 104.199.64.151 TCP 66 50361 → 4070 [ACK] Seq=12 Ack=12 Win=2237 Len=0 T
16 0.20… 10.0.0.32 10.0.0.200 TCP 78 54803 → 6690 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
17 0.00… 10.0.0.200 10.0.0.32 TCP 74 6690 → 54803 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len
18 0.00… 10.0.0.32 10.0.0.200 TCP 66 54803 → 6690 [ACK] Seq=1 Ack=1 Win=131712 Len=0 T
19 0.00… 10.0.0.32 10.0.0.200 TLSv1.2 263 Ignored Unknown Record
20 0.00… 10.0.0.200 10.0.0.32 TCP 66 6690 → 54803 [ACK] Seq=1 Ack=198 Win=15616 Len=0
21 0.00… 10.0.0.200 10.0.0.32 TLSv1.2 370 Ignored Unknown Record
22 0.00… 10.0.0.32 10.0.0.200 TCP 66 54803 → 6690 [ACK] Seq=198 Ack=305 Win=131456 Len
23 0.01… 10.0.0.32 10.0.0.200 TLSv1.2 230 Client Hello
24 0.00… 10.0.0.200 10.0.0.32 TLSv1.2 968 Server Hello, Certificate, Server Hello Done
25 0.00… 10.0.0.32 10.0.0.200 TCP 66 54803 → 6690 [ACK] Seq=362 Ack=1207 Win=130560 Le
26 0.00… 10.0.0.32 10.0.0.200 TLSv1.2 256 Client Key Exchange, Change Cipher Spec, Encrypte
27 0.00… 10.0.0.200 10.0.0.32 TLSv1.2 292 New Session Ticket, Change Cipher Spec, Encrypted
Total Length: 63
Identification: 0x0000 (0)
Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0x873b [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.0.0.32
Destination Address: 104.199.64.151
Transmission Control Protocol, Src Port: 50361, Dst Port: 4070, Seq: 1, Ack: 1, Len: 11
Data (11 bytes)
Source Address (ip.src), 4 bytes
Packets: 238 · Displayed: 238 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

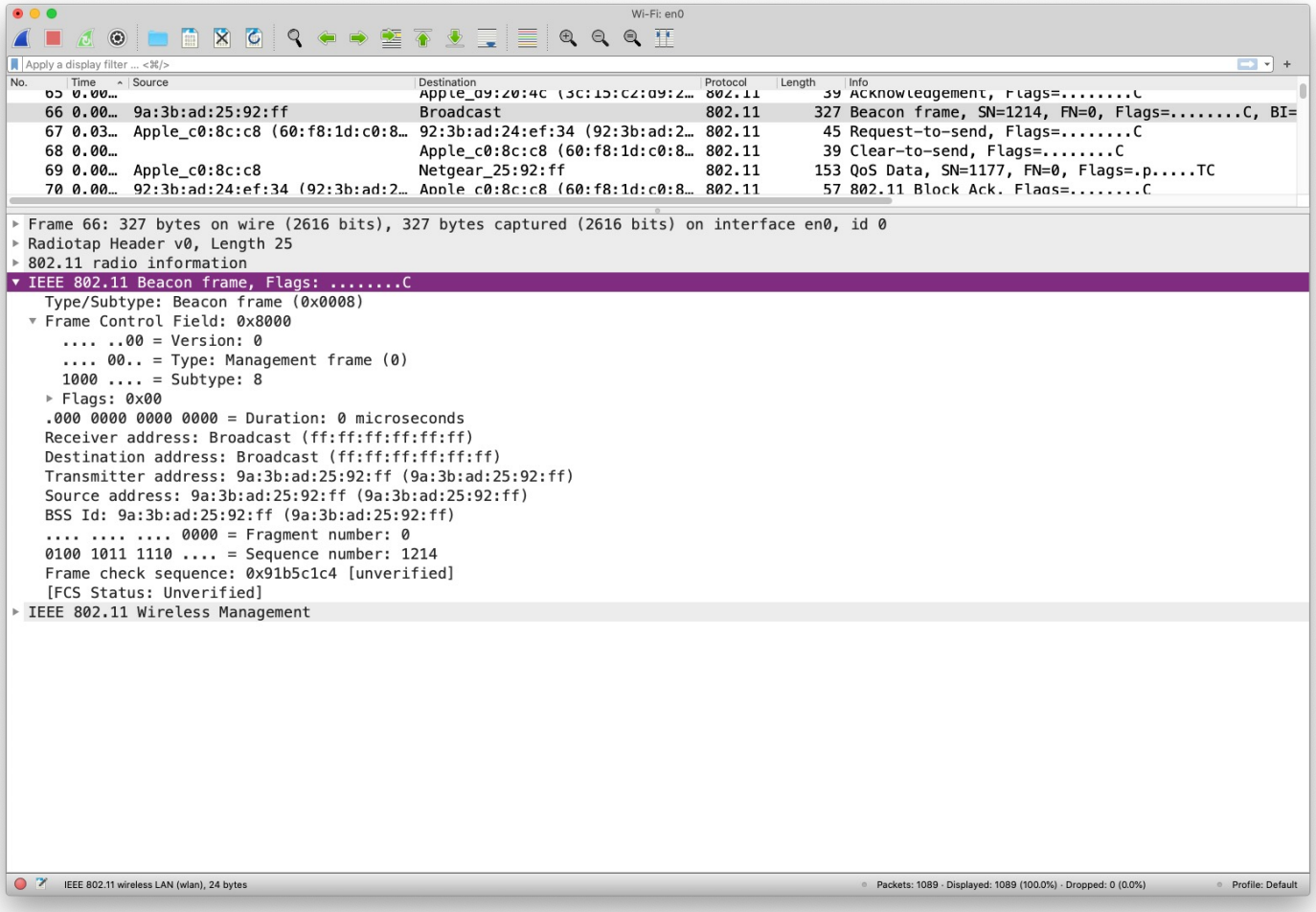
Wireshark in monitor mode



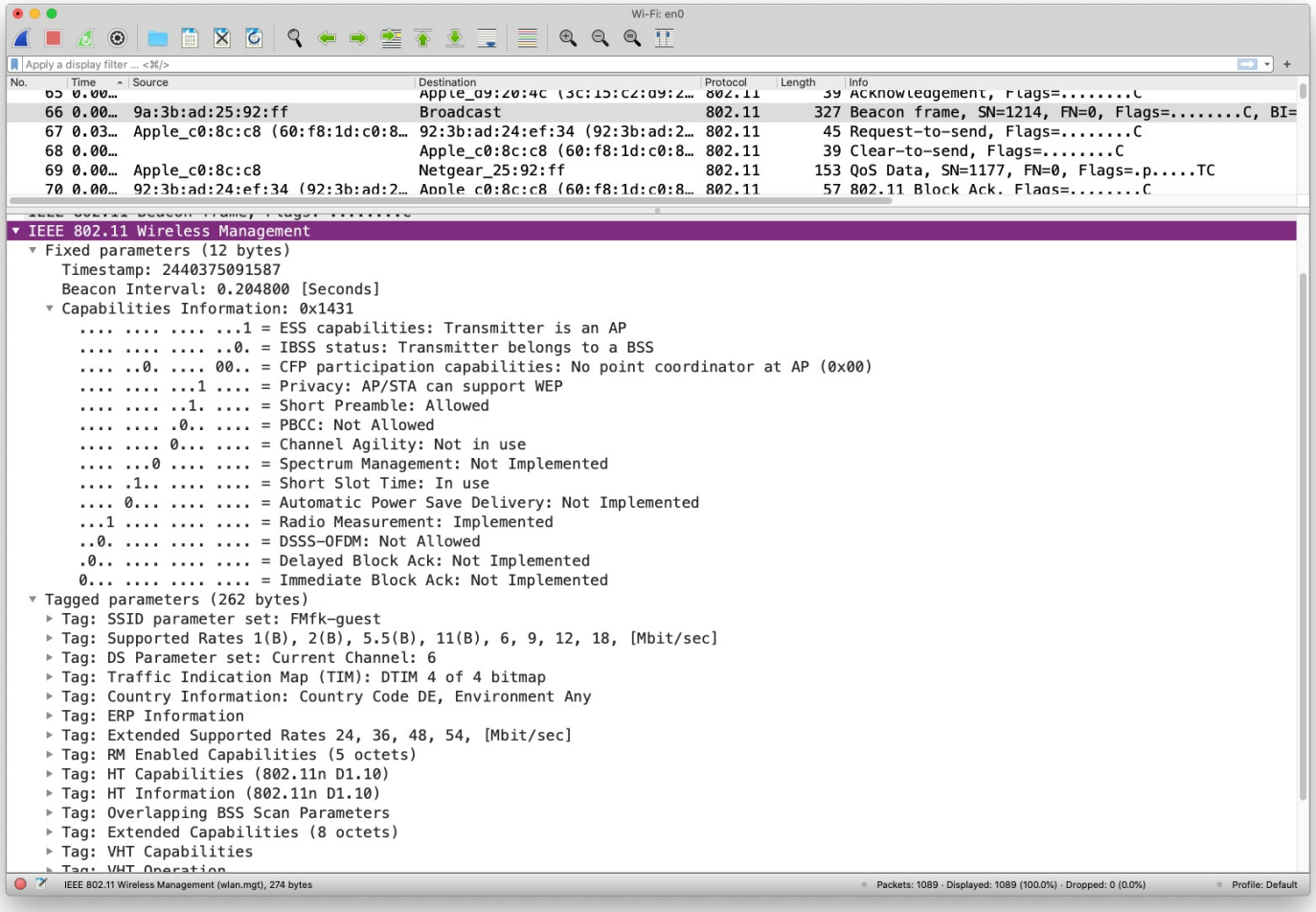
Beacon


Wi-Fi: en0
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
66 0.00… 9a:3b:ad:25:92:ff Broadcast 802.11 327 Beacon frame, SN=1214, FN=0, Flags=........C, BI=
67 0.03… Apple_c0:8c:c8 (60:f8:1d:c0:8… 92:3b:ad:24:ef:34 (92:3b:ad:2… 802.11 45 Request-to-send, Flags=........C
68 0.00… Apple_c0:8c:c8 (60:f8:1d:c0:8… 802.11 39 Clear-to-send, Flags=........C
69 0.00… Apple_c0:8c:c8 Netgear_25:92:ff 802.11 153 QoS Data, SN=1177, FN=0, Flags=.p.....TC
Frame 66: 327 bytes on wire (2616 bits), 327 bytes captured (2616 bits) on interface en0, id 0
Radiotap Header v0, Length 25
802.11 radio information
PHY type: 802.11g (ERP) (6)
Short preamble: False
Proprietary mode: None (0)
Data rate: 1.0 Mb/s
Channel: 6
Frequency: 2437MHz
Signal strength (dBm): -60 dBm
Noise level (dBm): -92 dBm
Signal/noise ratio (dB): 32 dB
TSF timestamp: 2650777975
[Duration: 2608µs]
[Preamble: 192µs]
[IFS: -749µs]
[Start: 2650775367µs]
[End: 2650777975µs]
IEEE 802.11 Beacon frame, Flags: C
IEEE 802.11 Wireless Management
802.11 radio information (wlan_radio)
Packets: 1089 · Displayed: 1089 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

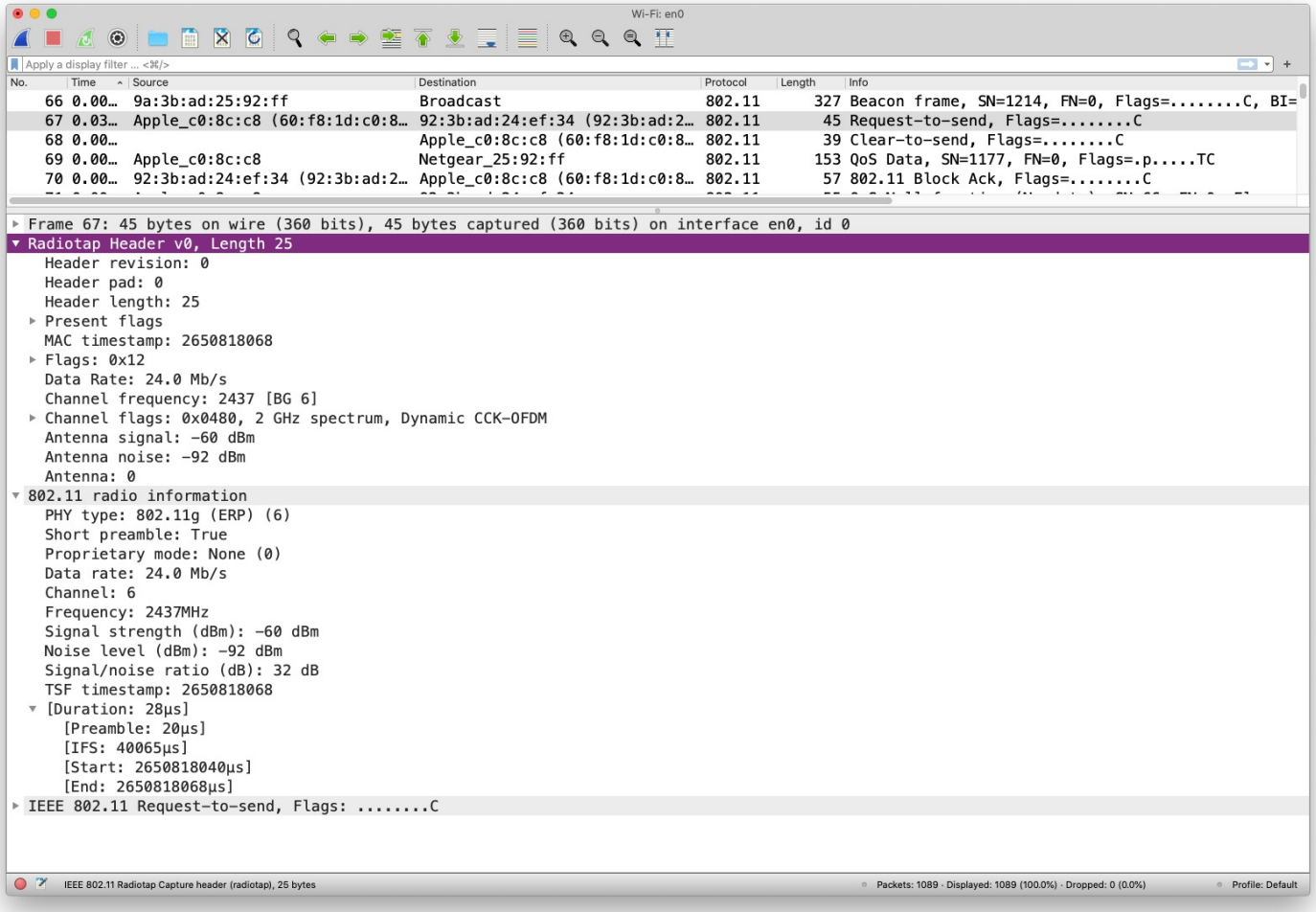
Beacon


Wi-Fi: en0
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
66 0.00… 9a:3b:ad:25:92:ff Broadcast 802.11 327 Beacon frame, SN=1214, FN=0, Flags=.....C, BI=
67 0.03… Apple_c0:8c:c8 (60:f8:1d:c0:8… 92:3b:ad:24:ef:34 (92:3b:ad:2… 802.11 45 Request-to-send, Flags=.....C
68 0.00… Apple_c0:8c:c8 (60:f8:1d:c0:8… 802.11 39 Clear-to-send, Flags=.....C
69 0.00… Apple_c0:8c:c8 Netgear_25:92:ff 802.11 153 QoS Data, SN=1177, FN=0, Flags=.p....TC
Frame 66: 327 bytes on wire (2616 bits), 327 bytes captured (2616 bits) on interface en0, id 0
Radiotap Header v0, Length 25
802.11 radio information
IEEE 802.11 Beacon frame, Flags: C
Type/Subtype: Beacon frame (0x0008)
Frame Control Field: 0x8000
.... ..00 = Version: 0
.... 00.. = Type: Management frame (0)
1000 .... = Subtype: 8
Flags: 0x00
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Transmitter address: 9a:3b:ad:25:92:ff (9a:3b:ad:25:92:ff)
Source address: 9a:3b:ad:25:92:ff (9a:3b:ad:25:92:ff)
BSS Id: 9a:3b:ad:25:92:ff (9a:3b:ad:25:92:ff)
.... 0000 = Fragment number: 0
0100 1011 1110 .... = Sequence number: 1214
Frame check sequence: 0x91b5c1c4 [unverified]
[FCS Status: Unverified]
IEEE 802.11 Wireless Management
IEEE 802.11 wireless LAN (wlan), 24 bytes
Packets: 1089 · Displayed: 1089 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

Beacon

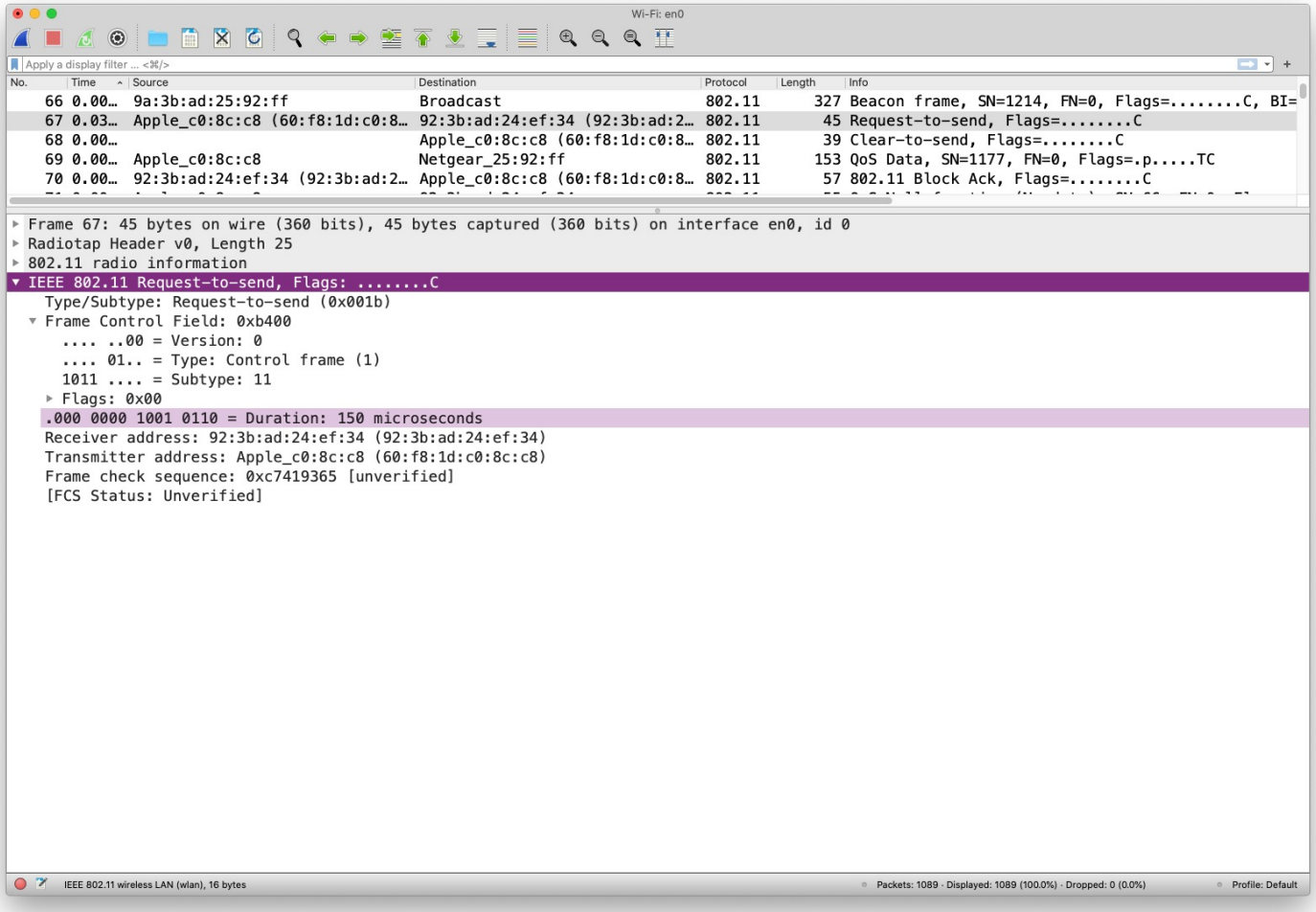

Wi-Fi: en0
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
66 0.00… 9a:3b:ad:25:92:ff Broadcast 802.11 327 Beacon frame, SN=1214, FN=0, Flags=........C, BI=
67 0.03… Apple_c0:8c:c8 (60:f8:1d:c0:8… 92:3b:ad:24:ef:34 (92:3b:ad:2… 802.11 45 Request-to-send, Flags=........C
68 0.00… Apple_c0:8c:c8 (60:f8:1d:c0:8… 802.11 39 Clear-to-send, Flags=........C
69 0.00… Apple_c0:8c:c8 Netgear_25:92:ff 802.11 153 QoS Data, SN=1177, FN=0, Flags=.p.....TC
70 0.00… 92:3b:ad:24:ef:34 (92:3b:ad:2… Apple_c0:8c:c8 (60:f8:1d:c0:8… 802.11 57 802.11 Block Ack, Flags=........C
IEEE 802.11 Wireless Management
Fixed parameters (12 bytes)
Timestamp: 2440375091587
Beacon Interval: 0.204800 [Seconds]
Capabilities Information: 0x1431
....1 = ESS capabilities: Transmitter is an AP
....0. = IBSS status: Transmitter belongs to a BSS
.... ..0. .... 00.. = CFP participation capabilities: No point coordinator at AP (0x00)
....1 .... = Privacy: AP/STA can support WEP
....1. .... = Short Preamble: Allowed
.... .0.. .... = PBCC: Not Allowed
.... 0... .... = Channel Agility: Not in use
....0 .... = Spectrum Management: Not Implemented
.... .1.. .... = Short Slot Time: In use
.... 0... .... = Automatic Power Save Delivery: Not Implemented
...1 .... = Radio Measurement: Implemented
..0. .... = DSSS-OFDM: Not Allowed
.0.. .... = Delayed Block Ack: Not Implemented
0... .... = Immediate Block Ack: Not Implemented
Tagged parameters (262 bytes)
Tag: SSID parameter set: FMfk-guest
Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
Tag: DS Parameter set: Current Channel: 6
Tag: Traffic Indication Map (TIM): DTIM 4 of 4 bitmap
Tag: Country Information: Country Code DE, Environment Any
Tag: ERP Information
Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
Tag: RM Enabled Capabilities (5 octets)
Tag: HT Capabilities (802.11n D1.10)
Tag: HT Information (802.11n D1.10)
Tag: Overlapping BSS Scan Parameters
Tag: Extended Capabilities (8 octets)
Tag: VHT Capabilities
IEEE 802.11 Wireless Management (wlan.mgt), 274 bytes
Packets: 1089 · Displayed: 1089 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

RTS

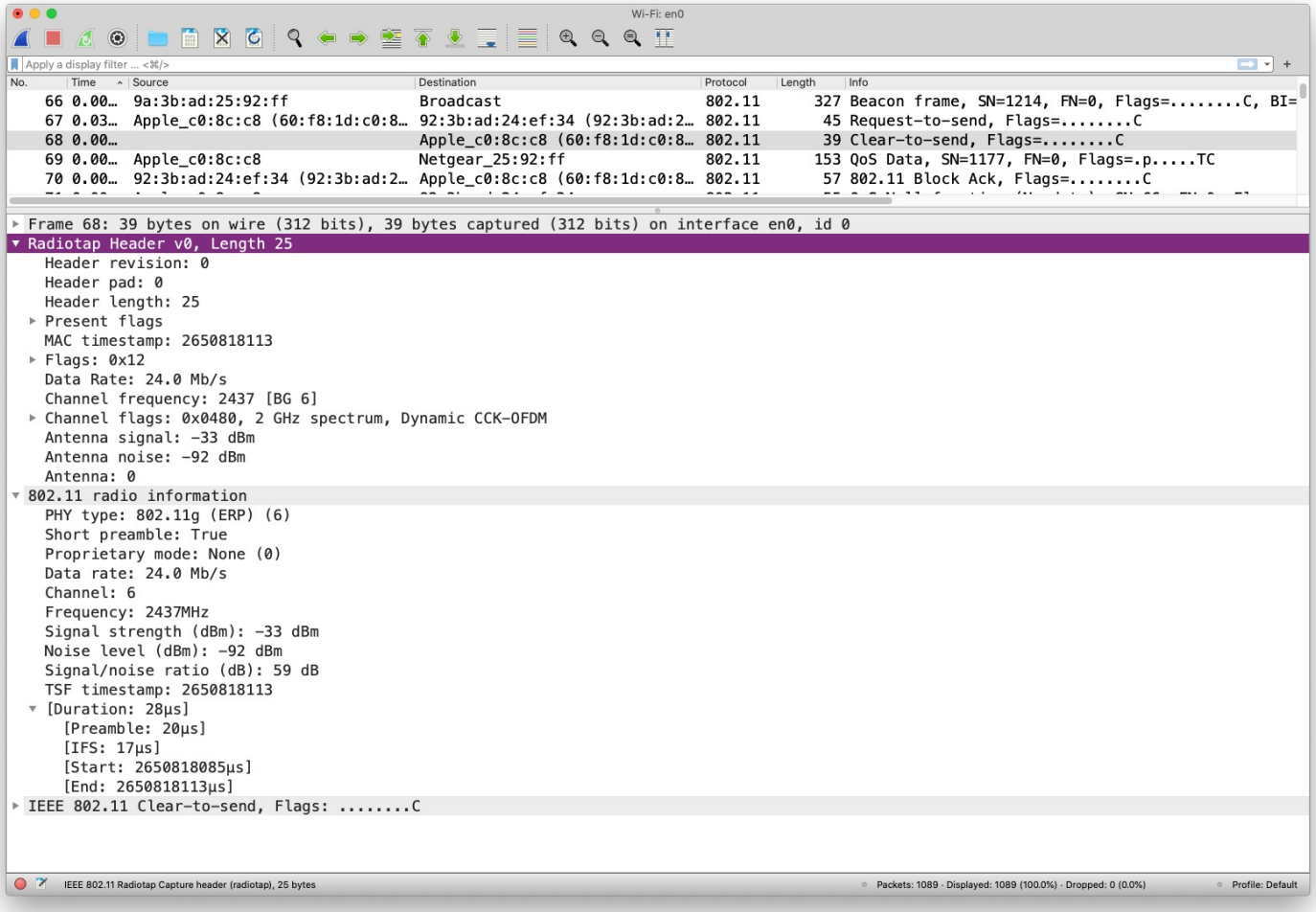


(**C**omplimentary **C**ode **K**eying/**O**rthogonal **FDM**) A hybrid spread spectrum coding method that transmits the header in a single radio frequency (CCK) and the payload in multiple frequencies (OFDM). CCK/OFDM is an option in the 802.11g wireless LAN standard that is designed to avoid collisions with 802.11b (CCK) systems. Since both header (CCK) and payload (OFDM) transmit in the 2.4 GHz range, the CCK header alerts the 802.11b node of a pending transmission. See 802.11, CCK and OFDM.

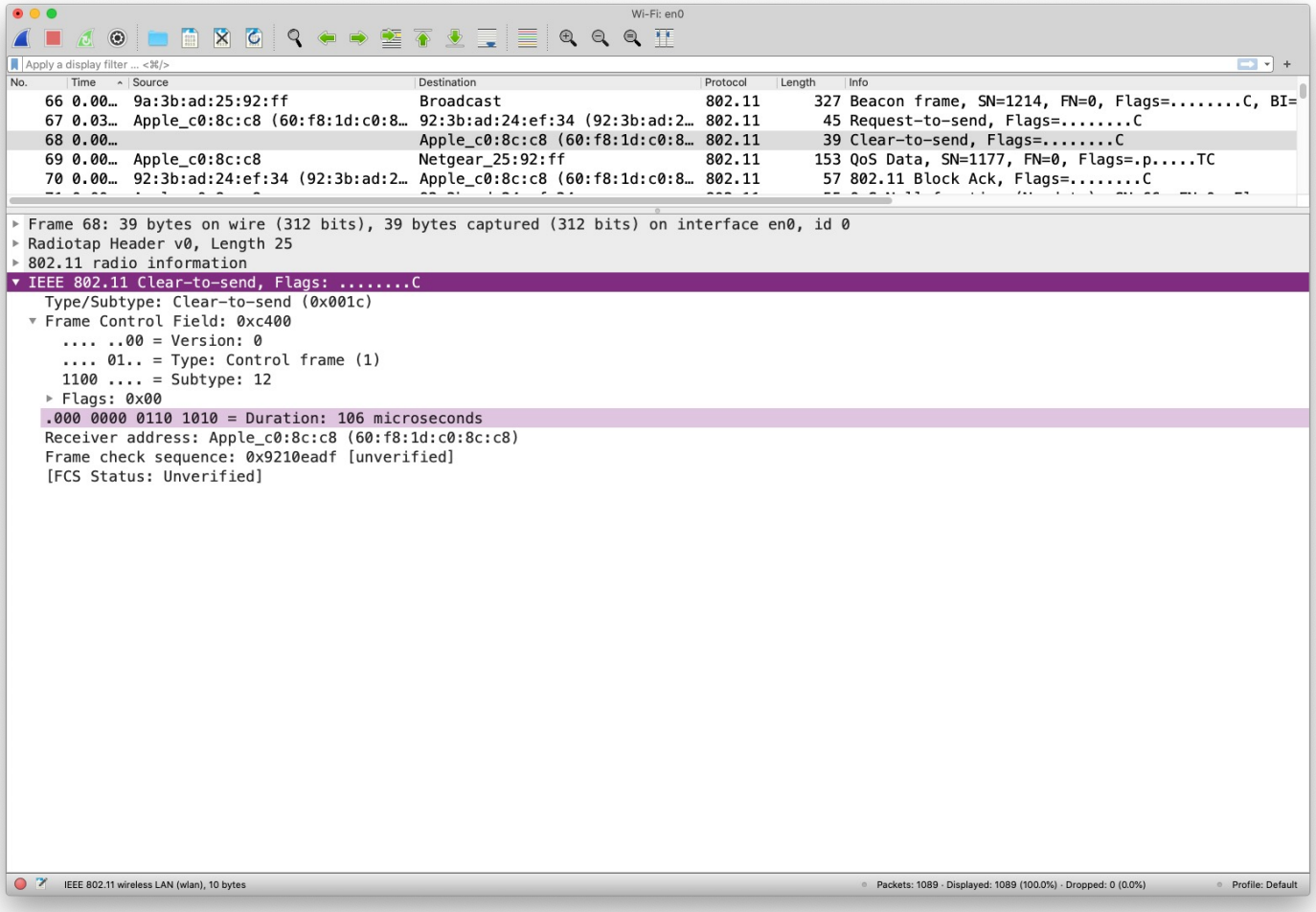
RTS: I need 150 µs (after I am done)



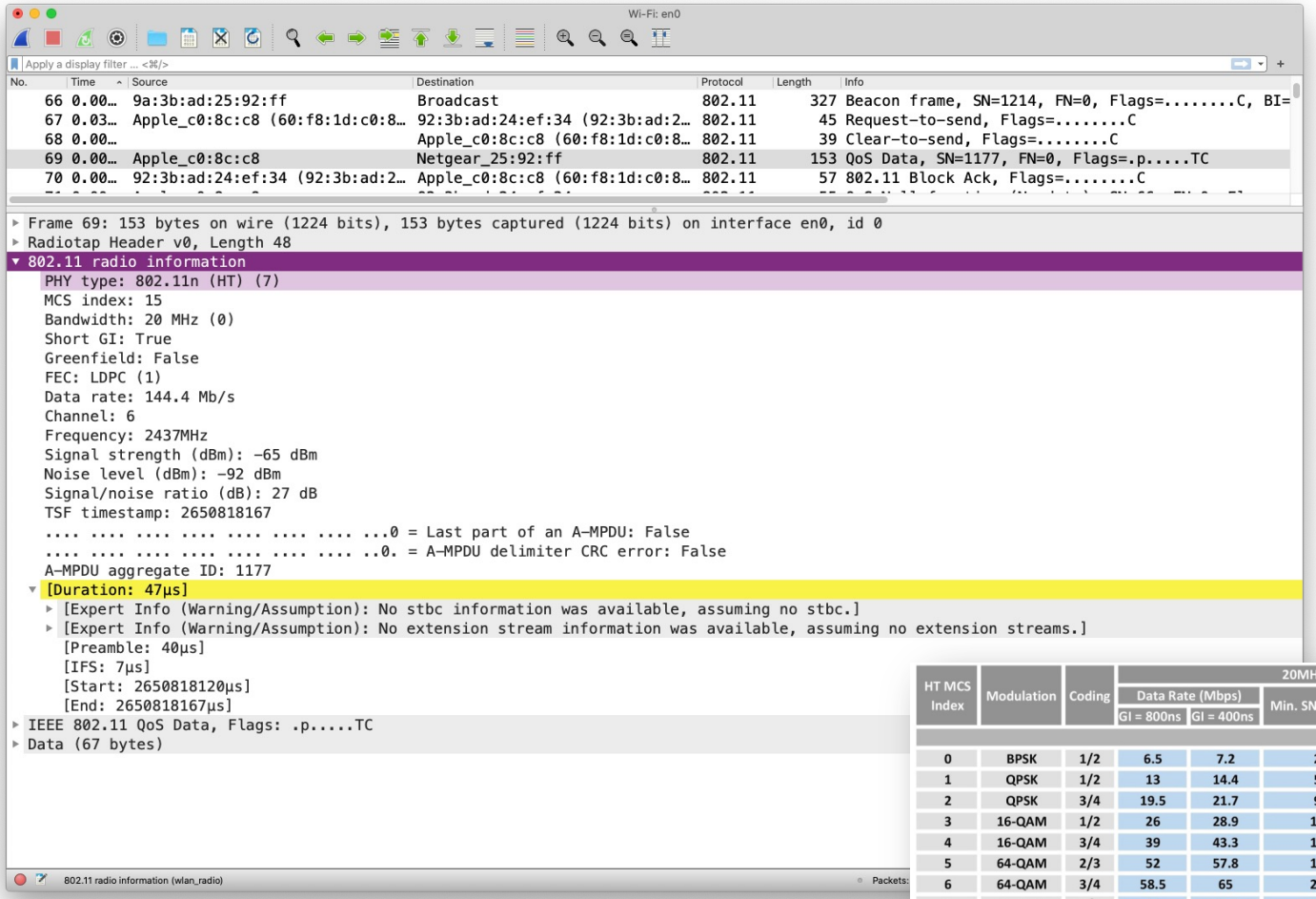
CTS


Wi-Fi: en0
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
66 0.00… 9a:3b:ad:25:92:ff Broadcast 802.11 327 Beacon frame, SN=1214, FN=0, Flags=........C, BI=
67 0.03… Apple_c0:8c:c8 (60:f8:1d:c0:8… 92:3b:ad:24:ef:34 (92:3b:ad:2… 802.11 45 Request-to-send, Flags=........C
68 0.00… Apple_c0:8c:c8 (60:f8:1d:c0:8… 802.11 39 Clear-to-send, Flags=........C
69 0.00… Apple_c0:8c:c8 Netgear_25:92:ff 802.11 153 QoS Data, SN=1177, FN=0, Flags=.p.....TC
70 0.00… 92:3b:ad:24:ef:34 (92:3b:ad:2… Apple_c0:8c:c8 (60:f8:1d:c0:8… 802.11 57 802.11 Block Ack, Flags=........C
Frame 68: 39 bytes on wire (312 bits), 39 bytes captured (312 bits) on interface en0, id 0
Radiotap Header v0, Length 25
Header revision: 0
Header pad: 0
Header length: 25
Present flags
MAC timestamp: 2650818113
Flags: 0x12
Data Rate: 24.0 Mb/s
Channel frequency: 2437 [BG 6]
Channel flags: 0x0480, 2 GHz spectrum, Dynamic CCK-OFDM
Antenna signal: -33 dBm
Antenna noise: -92 dBm
Antenna: 0
802.11 radio information
PHY type: 802.11g (ERP) (6)
Short preamble: True
Proprietary mode: None (0)
Data rate: 24.0 Mb/s
Channel: 6
Frequency: 2437MHz
Signal strength (dBm): -33 dBm
Noise level (dBm): -92 dBm
Signal/noise ratio (dB): 59 dB
TSF timestamp: 2650818113
[Duration: 28µs]
[Preamble: 20µs]
[IFS: 17µs]
[Start: 2650818085µs]
[End: 2650818113µs]
IEEE 802.11 Clear-to-send, Flags: C
IEEE 802.11 Radiotap Capture header (radiotap), 25 bytes
Packets: 1089 · Displayed: 1089 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

CTS: I still need 106 µs

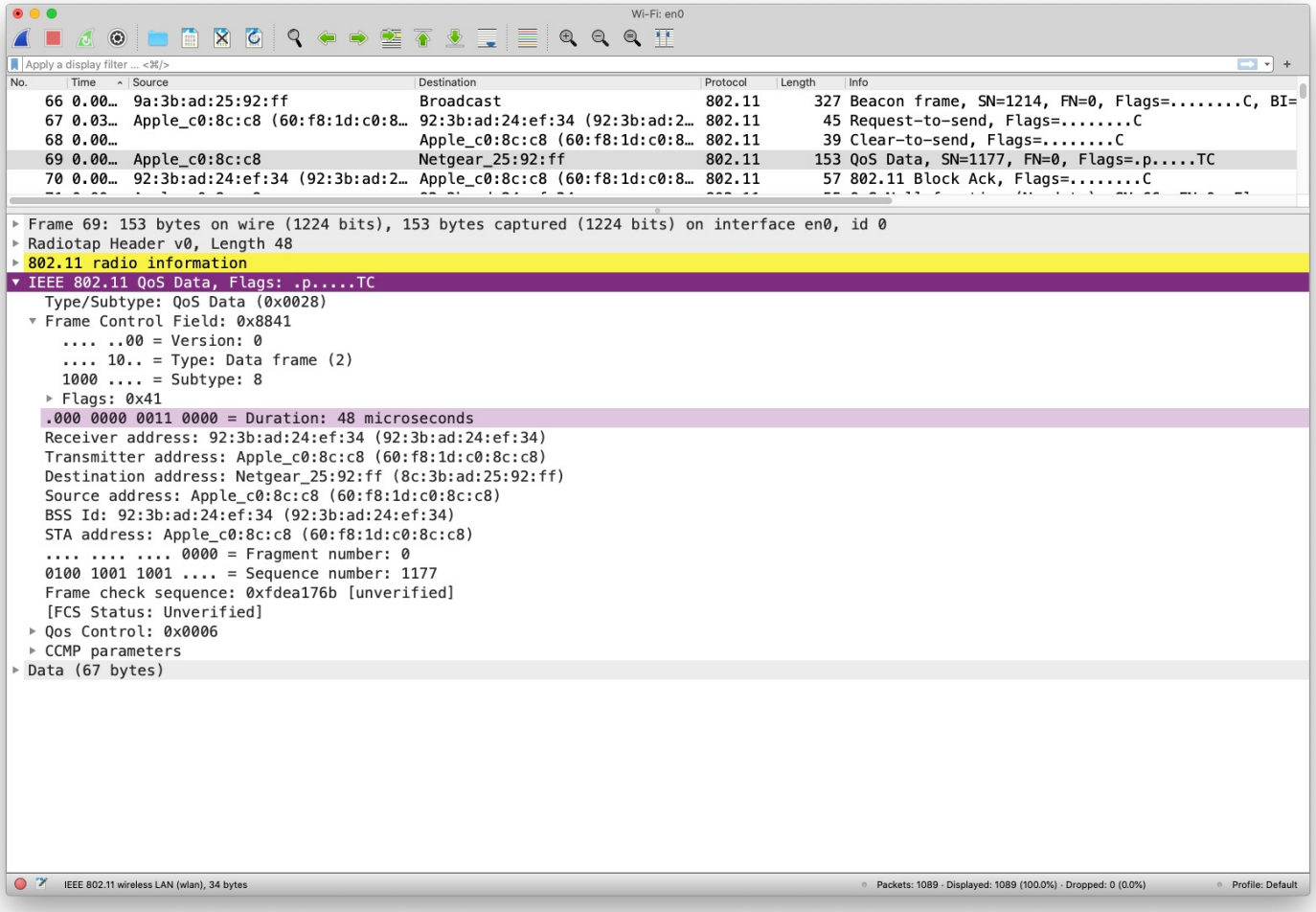


QoS Data

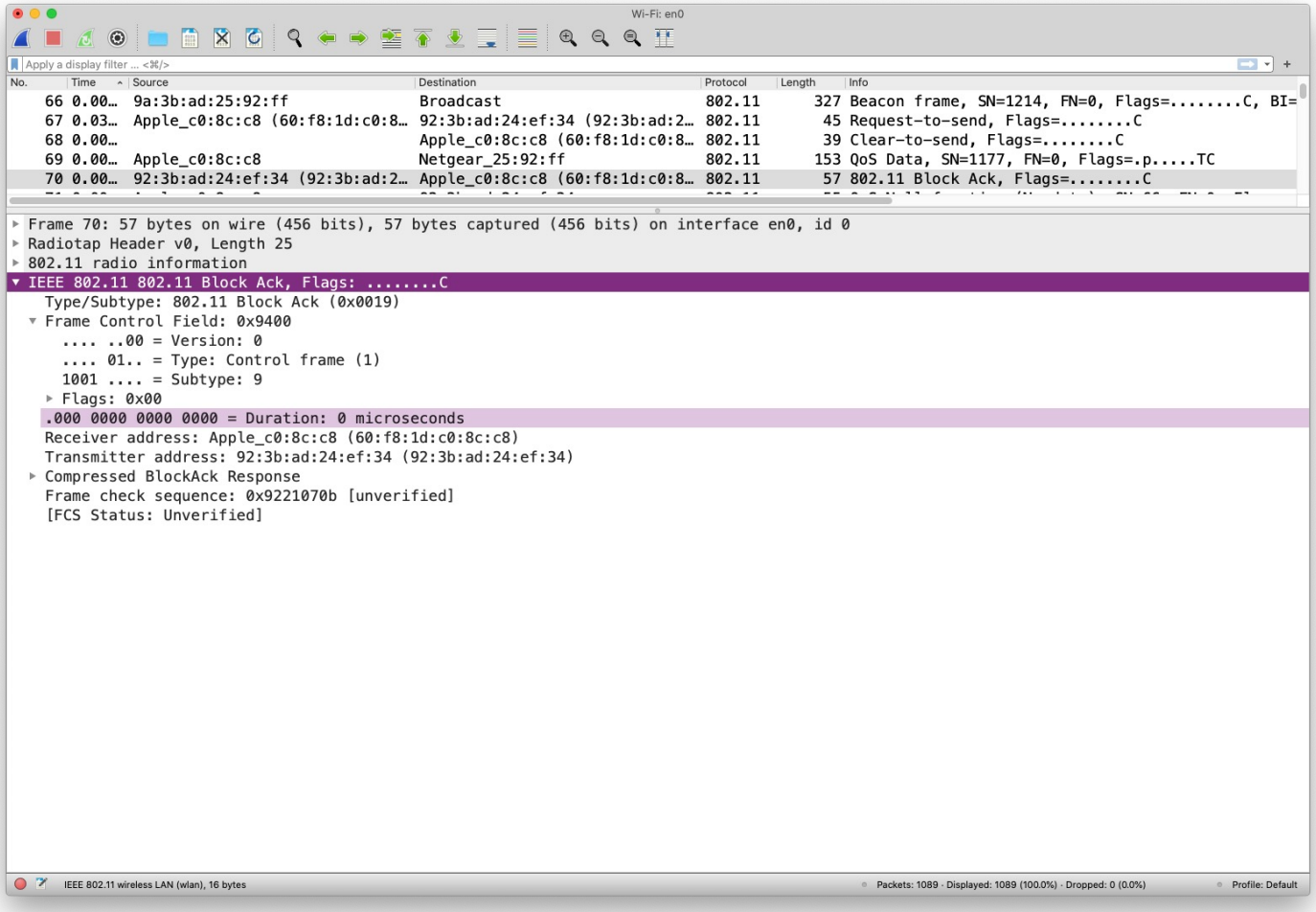


HT MCS Index	Modulation	Coding	20MHz				40MHz			
			Data Rate (Mbps)		Min. SNR (dBm)	Receive Sensitivity (RSSI)	Data Rate (Mbps)		Min. SNR (dBm)	Receive Sensitivity (RSSI)
			GI = 800ns	GI = 400ns			GI = 800ns	GI = 400ns		
1 Spatial Stream										
0	BPSK	1/2	6.5	7.2	2	-82	13.5	15	5	-79
1	QPSK	1/2	13	14.4	5	-79	27	30	8	-76
2	QPSK	3/4	19.5	21.7	9	-77	40.5	45	12	-74
3	16-QAM	1/2	26	28.9	11	-74	54	60	14	-71
4	16-QAM	3/4	39	43.3	15	-70	81	90	18	-67
5	64-QAM	2/3	52	57.8	18	-66	108	120	21	-63
6	64-QAM	3/4	58.5	65	20	-65	121.5	135	23	-62
7	64-QAM	5/6	65	72.2	25	-64	135	150	28	-61
2 Spatial Streams										
8	BPSK	1/2	13	14.4	2	-82	27	30	5	-79
9	QPSK	1/2	26	28.9	5	-79	54	60	8	-76
10	QPSK	3/4	39	43.3	9	-77	81	90	12	-74
11	16-QAM	1/2	52	57.8	11	-74	108	120	14	-71
12	16-QAM	3/4	78	86.7	15	-70	162	180	18	-67
13	64-QAM	2/3	104	115.6	18	-66	216	240	21	-63
14	64-QAM	3/4	117	130.3	20	-65	243	270	23	-62
15	64-QAM	5/6	130	144.4	25	-64	270	300	28	-61

QoS Data: I still need 48µs



Block ACK: all done



IEEE 802.11 Multi-rate capability

- 802.11 PHY supports **1, 2 Mbps**
- 802.11b PHY supports **1,2,5.5 and 11 Mbps**
- 802.11a/g PHY support 6,9,12,18,24,36,48 and 54 Mbps
- **802.11n PHY supports various rates** depending on the channel (20 or 40 MHz), the Guard Interval (400 or 800 ns), the modulation type, the number of streams (1 or 4) (see following slides)
- …

Rate Adaptation Mechanisms

- **Selection of optimal PHY data rate** according to **varying** wireless Channel conditions
- No **specifications** in 802.11 standard: implementation manufacturer specific
- **Statistics Based Mechanisms**
  - Decision at sender
  - Estimators : frame errors, throughput calculation
  - Examples: **ARF** (Auto Rate Fallback), **AARF** (Adaptive ARF)
- **SNR Based Mechanisms**
  - Decision at receiver (BUT NOT STANDARD COMPATIBLE i.e. not implemented)
  - Estimators: SNR (=10 log10(Psignal/Pnoise)), RSSI (received signal strength indication)
  - Examples: RBAR (Receiver Based Auto Rate)

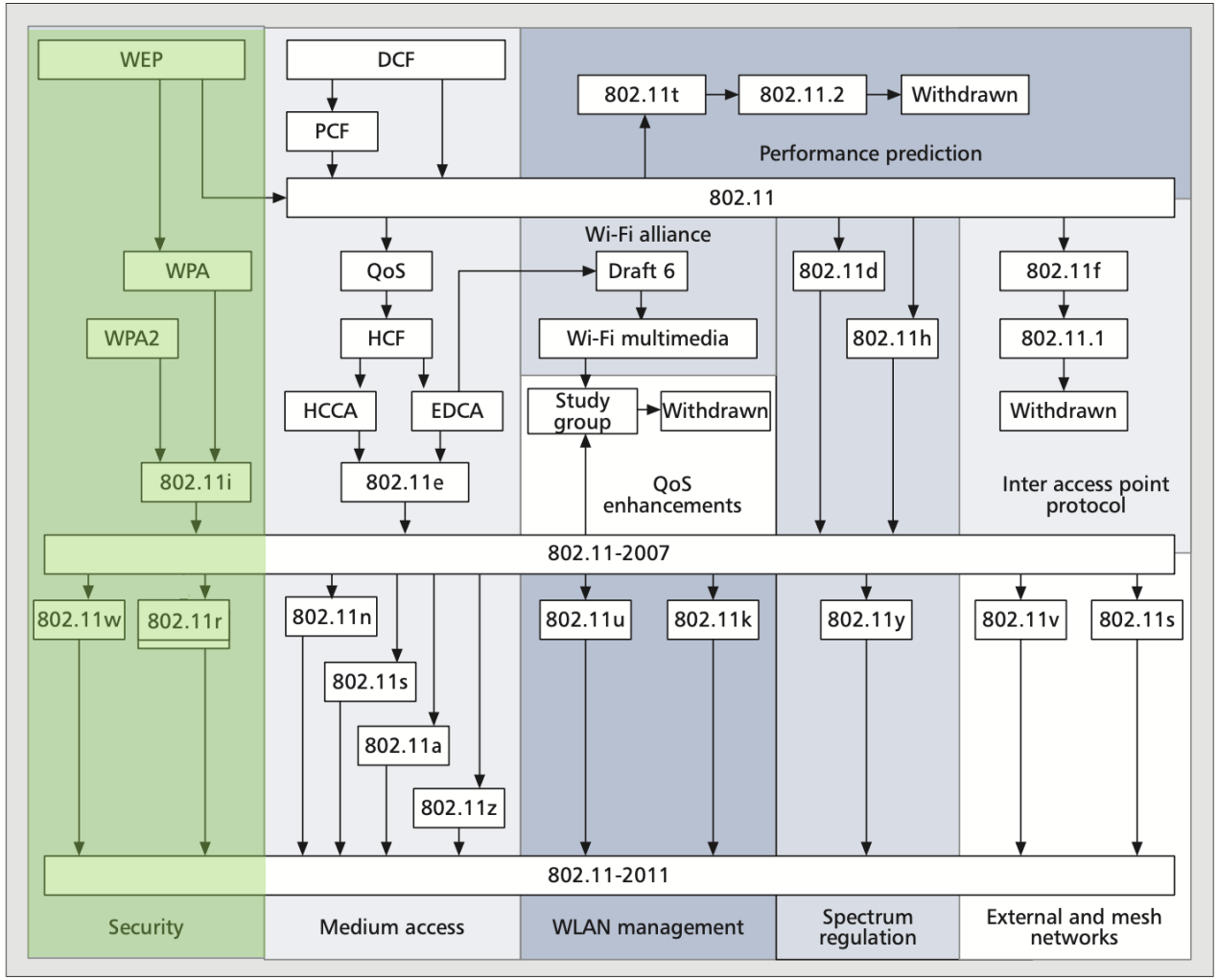
Auto Rate Fallback (ARF)

- If **two consecutive ACK frames are not received correctly**, the second retry and subsequent transmissions are done at a lower rate and a timer is started.
- When the number of **successfully received ACKs reaches 10** or the timer goes off, a probe frame is sent at the next higher rate.
- If no ACK is received for this frame, the rate is lowered back and the timer is restarted.
- **Adaptive ARF**: when the probe frame fails, not only the rate is lowered but also the number of successfully received ACKs is doubled

What are the steps?

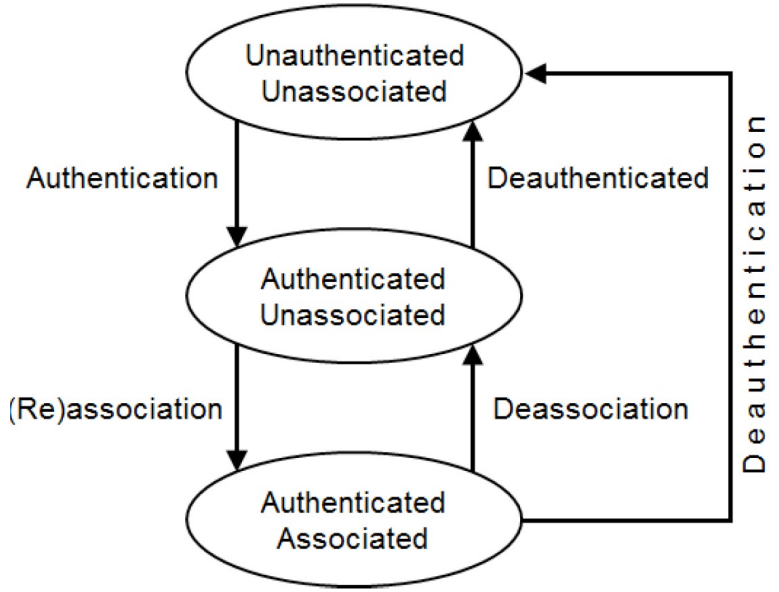
1. ~~Switch on the stations (& access points)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. ~~Define how we are going to organize the bits for multiple users~~
5. ~~Listen to synchronize and get system information~~
6. ~~Random Access~~
7. ~~Get a channel (well, not exactly…)~~
8. Authenticate (uh, does this happen earlier?)
9. Try to send data
10. Move around

IEEE 802.11 Association and Security



Joining a network

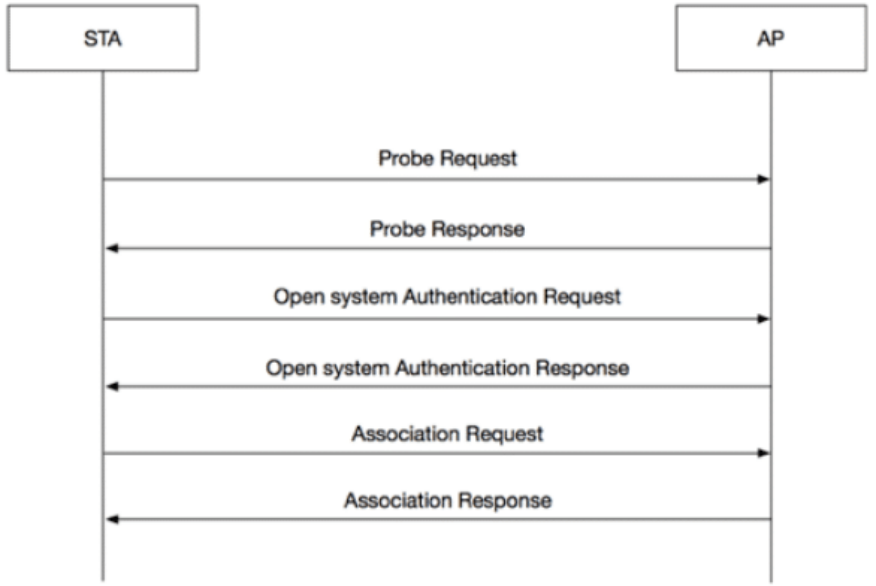
- For a station to successfully **join a WiFi network**, a series of frame exchanges must occur which make up the **Authentication and Association process**, the 802.11 State Machine. The frames part of this transaction are as follows:
  - Probe Request
  - Probe Response
  - Authentication Request
  - Authentication Response
  - Association Request
  - Association Response



802.11 “Authentication”

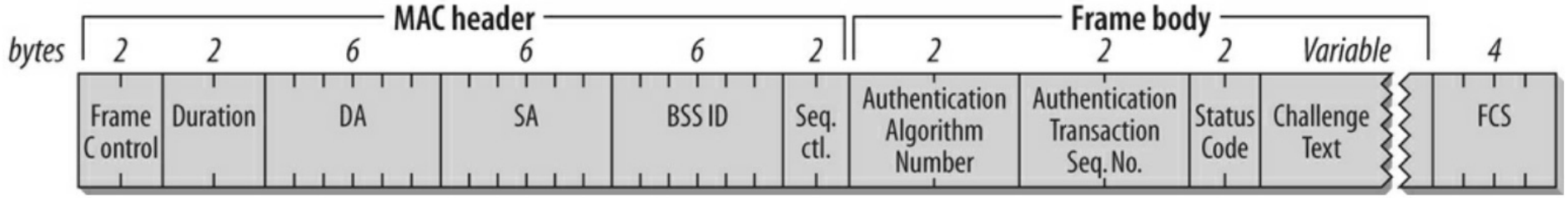
- 802.11 requires that **a station establish its identity before sending frames**. However, there are **no cryptographic secrets** that are passed around or validated. Authentication is an initial step in the handshake process that a station uses to attach to the network, and **one that identifies the station to the network.**
- The **network is under no obligation to authenticate**; the authentication process is not mutual.
- The method is called “Open-system authentication”

Association



Open System authentication is a null authentication algorithm. Any station can request Open System authentication and be authenticated if the receiver has the authentication algorithm set to true, which is usually the case.

Authentication frame



- **At the beginning of 802.11 networking**, stations authenticated using a **shared key**, and exchanged Authentication frames.
- With 802.11i, shared key authentication was kept in the standard, but made **incompatible** with the new security mechanisms.
- If a station uses shared key authentication, it will not be allowed to use the strong security protocols
  - Open system: authentication algo = 0
  - Shared key: authentication algo = 1

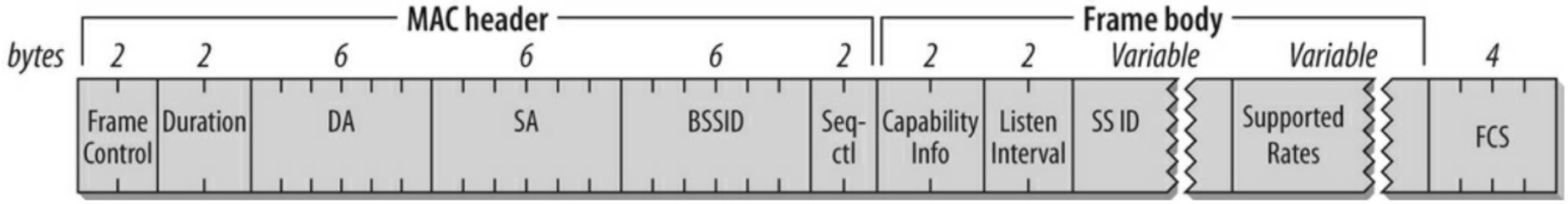
Wired Equivalent Privacy (WEP)

- Used to protect the data of authorized users from tampering during transmission on a WLAN. **WEP uses the RC4 algorithm** to encrypt data using a 64-bit, 128-bit, or 152-bit encryption key.
- **WEP uses a static encryption key. That is, all STAs associating with the same SSID use the same key to connect to the wireless network.**
- WEP security policy defines a link authentication mechanism and a data encryption mechanism.
- If open system authentication is used, data is not encrypted during link authentication. After a user goes online, service data can be encrypted by WEP or not, depending on the configuration.
- If shared key authentication is used, the WLAN client and server complete key negotiation during link authentication. After a user goes online, service data is encrypted using the negotiated key.
- **WEP encryption users the static shared key. The same WEP key is used for encrypting different users, bringing security risks.**
  - Trivial to attack due to flaw in RC4 keystream

WEP Flaws

- **Authentication is one-way only**
- **The same shared secret key is used for authentication and encryption**
  - weaknesses in any of the two protocol can be used to break the key
  - different keys for different functions are desirable
- **No session key is established during authentication**
  - access control is not continuous
  - once a STA has authenticated and associated to the AP, an attacker send messages using the MAC address of STA
  - correctly encrypted messages cannot be produced by the attacker, but replay of STA messages is still possible

Association request



- **Capability Information field** is used to indicate the type of network the mobile station wants to join.
- Before AP accepts, it verifies that the Capability Information, SSID, and (Extended) Supported Rates **all match the parameters** of the network.
- Stations supporting security will have the **RSN (Robust Security Network)** information element!

Draft 802.11i

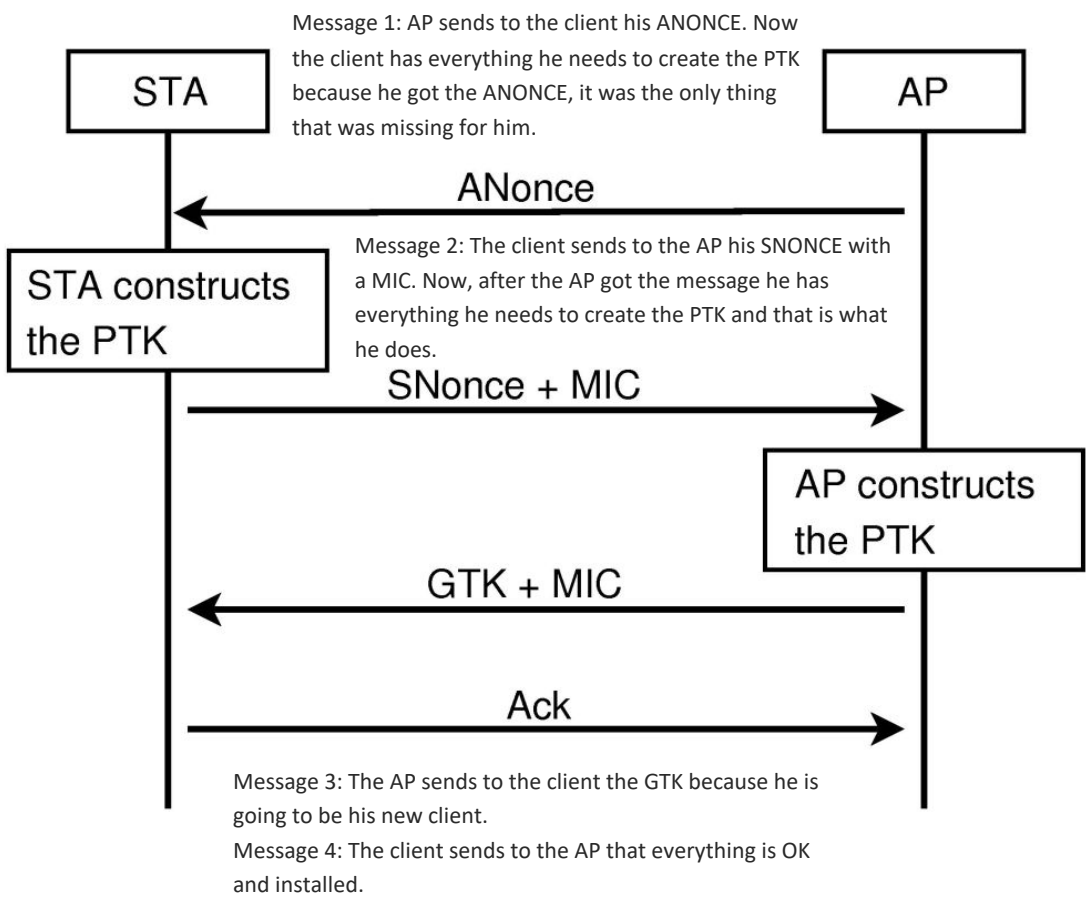
Enter Wi-Fi Protected Access (WPA)

- **Wi-Fi Alliance developed Wi-Fi Protected Access (WPA) to overcome the shortcomings of WEP**
- **WPA still uses the RC4 algorithm, but it uses an 802.1X authentication framework**
  - Supports Extensible Authentication Protocol-Protected Extensible Authentication Protocol (EAP-PEAP)
  - Supports EAP-Transport Layer Security (EAP-TLS) authentication
  - Defines the Temporal Key Integrity Protocol (TKIP) encryption algorithm (built on top of WEP
  - Link Authentication is always open system
- **WPA had an enterprise edition and a personal edition.**
  - enterprise uses a RADIUS server and the EAP protocol for authentication. Users provide authentication information, including the user name and password, and are authenticated by an authentication server (generally a RADIUS server).
  - personal provides a simplified authentication mode: pre-shared key authentication (WPA-PSK). A WLAN client can access the WLAN if its pre-shared key is the same as that configured on the WLAN server. The PSK is not used for encryption; therefore, it does not pose security risks like the 802.11 shared key authentication.

WPA2 Key element: 4-way handshake

- **The initial authentication process is carried out either using a pre-shared key (PSK), or following an EAP exchange through 802.1X (known as EAPOL, which requires the presence of an authentication server)**
  - This process ensures that the client station (STA) is authenticated with the access point (AP).
- **Afterwards, a shared secret key is generated, called the Pairwise Master Key (PMK).**
  - In PSK authentication, the PMK is typically derived from the WiFi password by putting it through a key derivation function that uses SHA-1 as the cryptographic hash function.
  - If an 802.1X EAP exchange was carried out, the PMK is derived from the EAP parameters provided by the authentication server.

WPA2 Key element: 4-way handshake



PMK- Pairwise Master Key = 256bit version of the Pre-Shared Key

- In WPA/WPA2/personal the PMK is the PSK.
- Both the machines have the PMK in assumed the the client knows the password for the WI-FI.

GMK- Group Master Key:

- The GMK is used in this action to create the GTK, the GTK is generated on every AP and shared with the devices that are connected with him.

PTK — Pairwise Transit Key:

- The PTK is encryption for uni-cast traffic. In this example between the client and the AP.To get this encryption the client and the AP needs several parameters.
- PTK = PMK + ANONCE + SNONCE + MAC(AA) + MAC(SA)

GTK- Group Temporal Key:

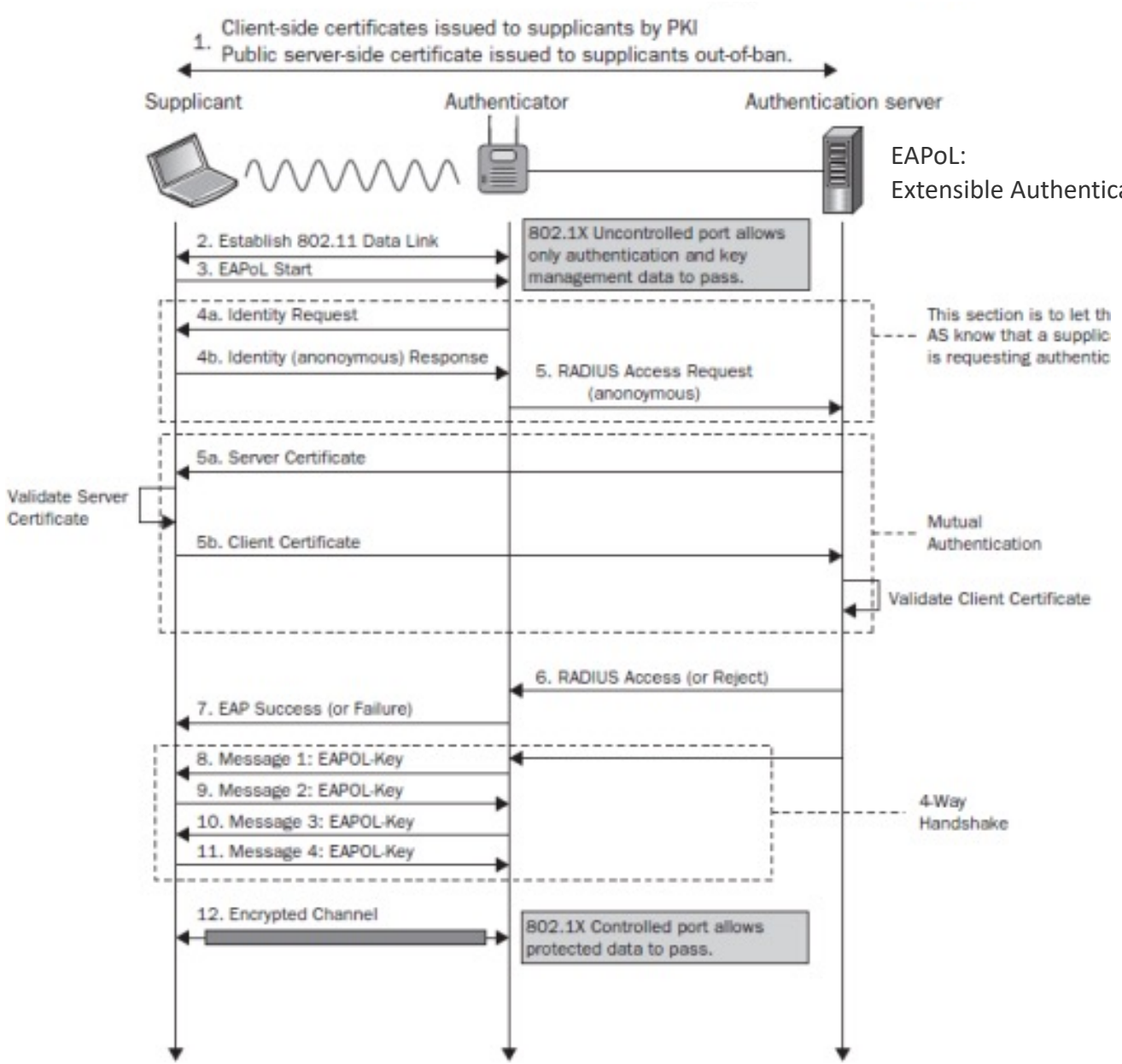
- The GTK is the encryption for broadcast and multicast for the traffic between one AP to his clients.
- For every different AP there is a different GTK to secure the traffic in the “air” that belongs to the same network.
- All the clients that connect to the same AP have the same GTK.

MIC = Message Integrity Code

- the MIC is mainly for the AP to recognize that this message is realy from this client, its like a signature (a high level algorithm signature).

https://mrncciew.com/2014/08/26/cwsp-eap-tls/

EAP-TLS 802.1X example



EAPoL:
Extensible Authentication Protocol over LAN

To summarize for your home network

- **Open (risky): Open Wi-Fi networks have no passphrase. You shouldn't set up an open Wi-Fi network—seriously, you could have your door busted down by police.**
- WEP 64 (risky): The old WEP protocol standard is vulnerable and you really shouldn't use it.
- WEP 128 (risky): This is WEP, but with a larger encryption key size. It isn't really any less vulnerable than WEP 64.
- WPA-PSK (TKIP): This uses the original version of the WPA protocol (essentially WPA1). It has been superseded by WPA2 and isn't secure.
- WPA-PSK (AES): This uses the original WPA protocol, but replaces TKIP with the more modern AES encryption. It's offered as a stopgap, but devices that support AES will almost always support WPA2, while devices that require WPA will almost never support AES encryption. So, this option makes little sense.
- WPA2-PSK (TKIP): This uses the modern WPA2 standard with older TKIP encryption. This isn't secure, and is only a good idea if you have older devices that can't connect to a WPA2-PSK (AES) network.
- **WPA2-PSK (AES): This is the most secure option. It uses WPA2, the latest Wi-Fi encryption standard, and the latest AES encryption protocol. You should be using this option. On some devices, you'll just see the option "WPA2" or "WPA2-PSK." If you do, it will probably just use AES, as that's a common-sense choice.**
- WPAWPA2-PSK (TKIP/AES): Some devices offer—and even recommend—this mixed-mode option. This option enables both WPA and WPA2, with both TKIP and AES. This provides maximum compatibility with any ancient devices you might have, but also allows an attacker to breach your network by cracking the more vulnerable WPA and TKIP protocols.
- **Better approach: set up separate SSID for older devices**

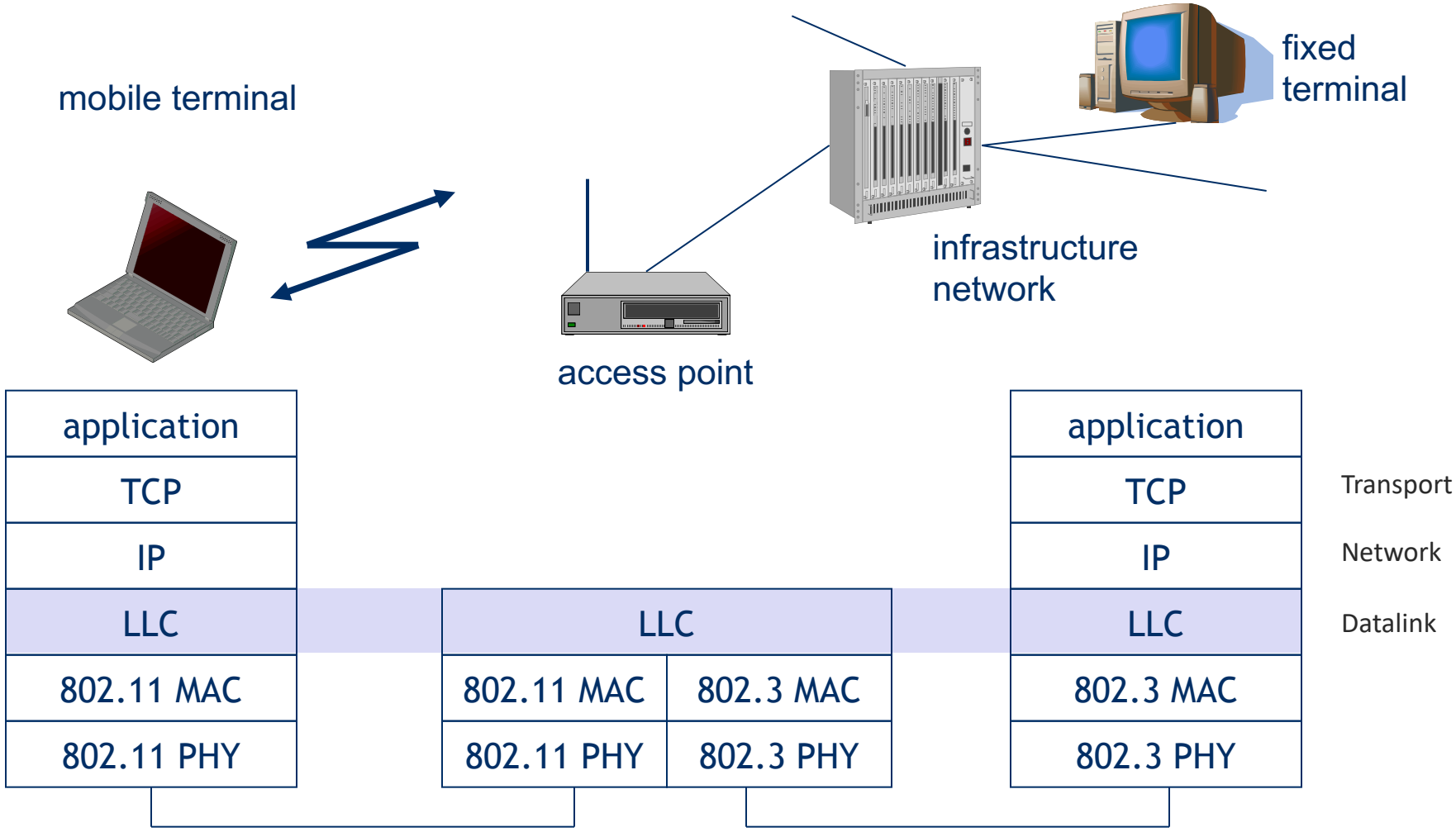
What are the steps?

1. ~~Switch on the stations (& access points)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. ~~Define how we are going to organize the bits for multiple users~~
5. ~~Listen to synchronize and get system information~~
6. ~~Random Access~~
7. ~~Get a channel (well, not exactly…)~~
8. ~~Authenticate (uh, does this happen earlier?)~~
9. Try to send data
10. Move around

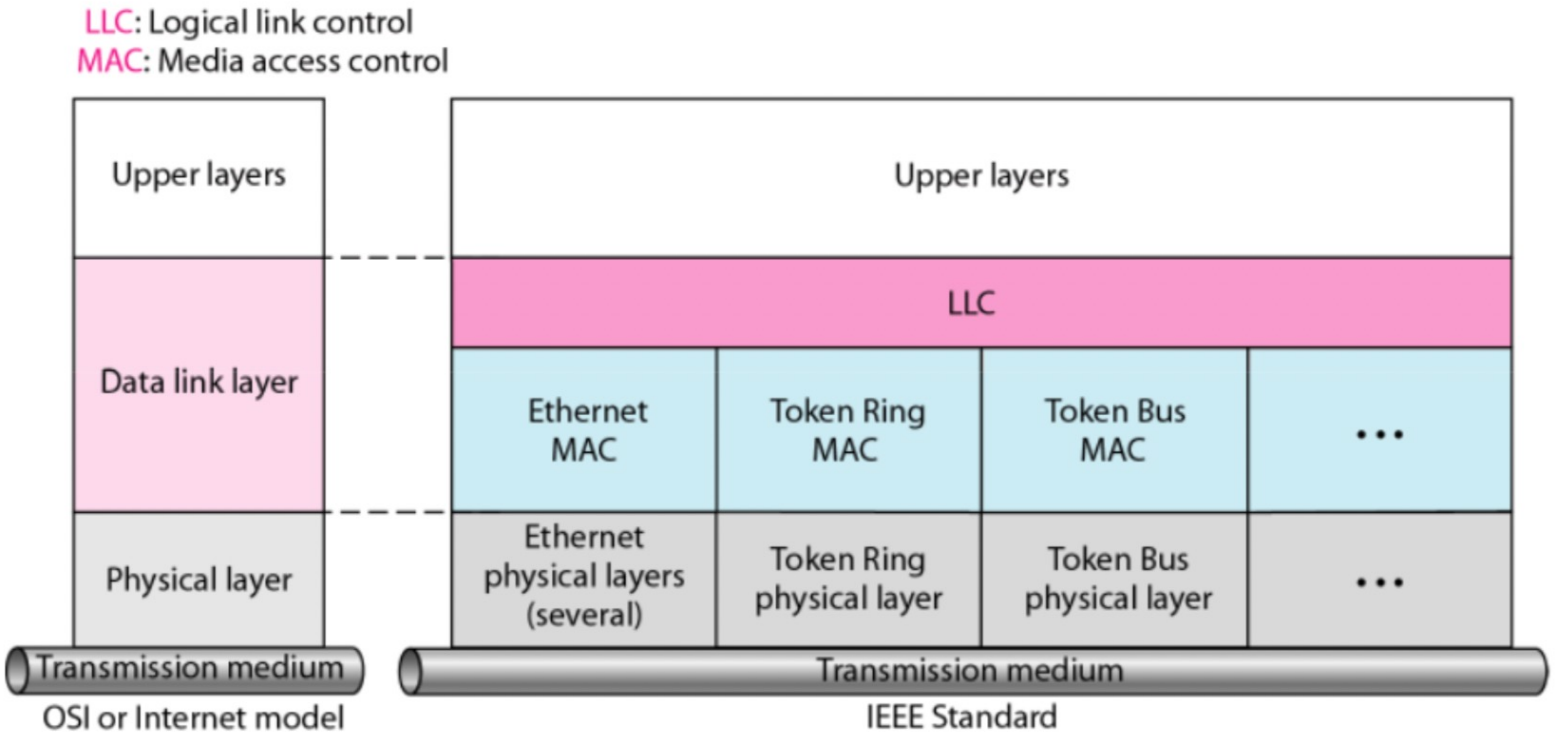
ESS = link layer domain= layer 2

- 802.11 supplies **link-layer mobility** within an ESS, but only if the backbone network appears to be a single link-layer domain. This important **constraint** on mobility is often a major factor in the way that wireless LANs are deployed, and one of the major ways that vendors differentiate their products.
- Early access points required that the backbone network be a single hub or VLAN, but newer products can interface directly with the backbone. Many can support multiple VLANs simultaneously with 802.1Q tags, and some can even dynamically instantiate VLANs based on authentication information.

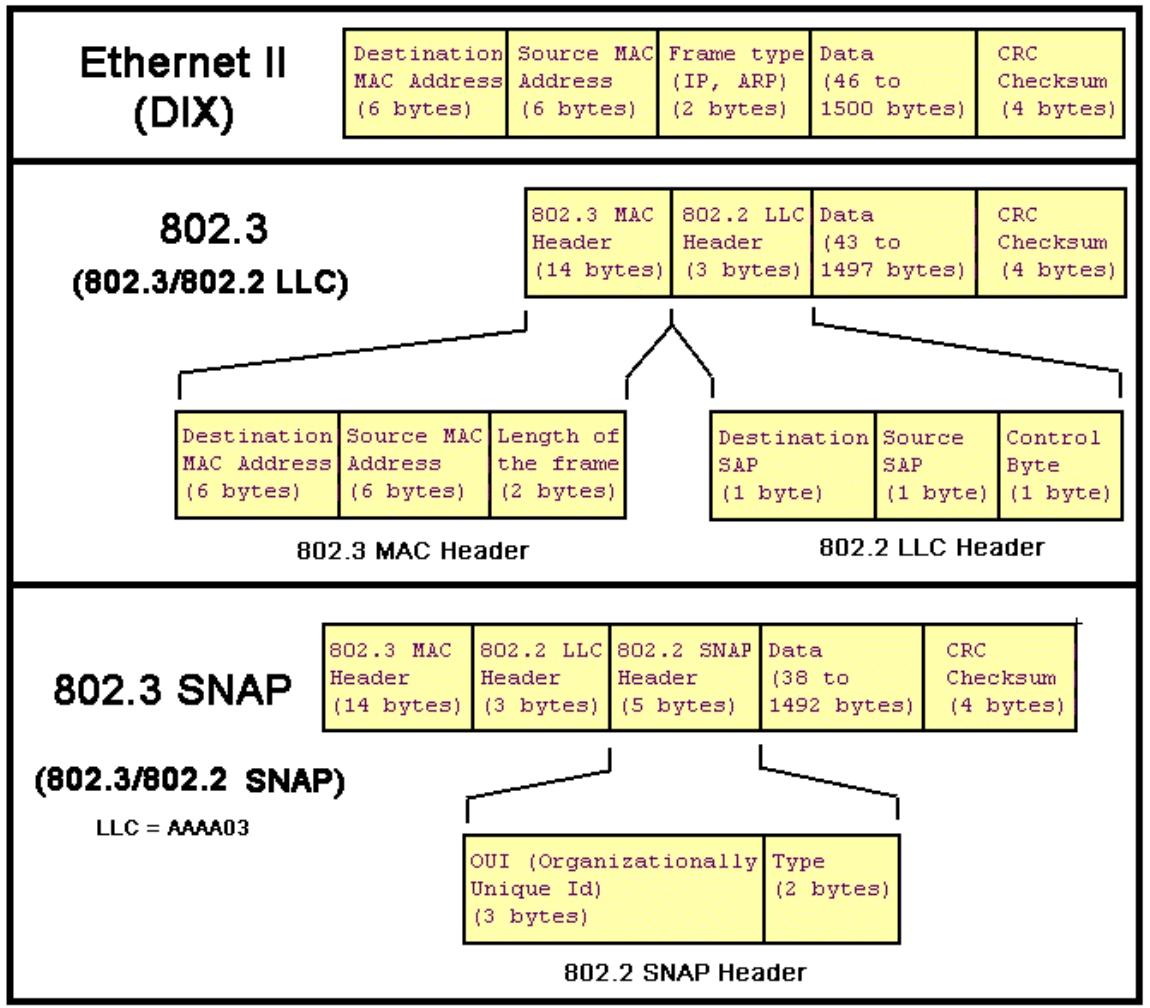
IEEE 802.11 Protocol Stack



LLC – why?


LLC: Logical link control
MAC: Media access control
Upper layers
Data link layer
Physical layer
Transmission medium
OSI or Internet model
Upper layers
LLC
Ethernet MAC
Token Ring MAC
Token Bus MAC
...
Ethernet physical layers (several)
Token Ring physical layer
Token Bus physical layer
...
Transmission medium
IEEE Standard

LLC and SNAP



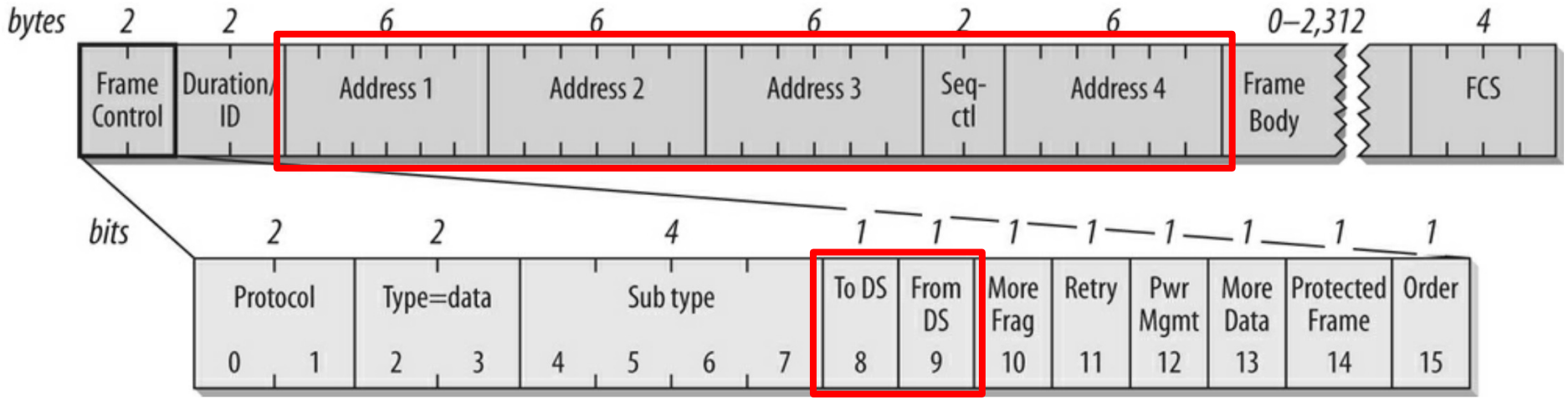
Logical Link Control => multiplexing multiple network protocols
Subnetwork Access Protocol => extension
SAP => Service Access Point

Transmission in a Wifi network

Always via the AP (in infrastructure mode):

- To DS=0, From DS=0
  - All management and control frames (directly sent to the AP and not the DS).
  - ~~All frames sent between two stations inside ad-hoc network.~~
- **To DS=0, From DS=1**
  - A frame exiting the DS for a station.
- **To DS=1, From DS=0**
  - A frame sent by a station for an AP (can be for STA or **other host on DS**)
- To DS=1,From DS=1
  - Only frame using all four addresses fields. Seen in Wireless DS (mesh, repeater, …) where an AP sends a frame to another AP, it is exiting the DS and destined to the DS at the same time in that situation.

802.11 Payload = PSDU



- Duration; to set NAV (used by RTS/CTS and in fragmentation mode)
  - Network Allocation Vector
- Sequence numbers: important against duplicated frames due to lost ACKs
- **To DS, From DS and Addresses**
- Retry: set to 1 if frame is re-transmission
- Power management: bit is set to 1 if station goes in power-save mode
- More data: used by AP to indicate STA in power-save mode that more data is buffered or by STA to indicate AP that more polling is needed
- Order: set to 1 if frames must be processed in strict order

MAC address format

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

Address1: physical receiver

Address 2: physical transmitter

Address 3,4: logical addresses

DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Basic Service Set Identifier uniquely identifies a BSS
- In infrastructure mode BSSID is the MAC address of the wireless interface of the AP that is creating the BSS
- In case of ad-hoc mode BSSID is a 48-bit number in the MAC address format, which is composed of 46-bit randomly generated number

RA: Receiver Address (MAC address of receiving AP)
TA: Transmitter Address (MAC address of sending AP)

Wireline to wireless (802.2)

- The access point first checks that a received frame should be processed further by checking that the **destination address** belongs to a **station currently associated with the AP**
- The SNAP header is prepended to the data in the Ethernet frame. The higher-level packet is encapsulated within a SNAP header whose Type code is copied from the Ethernet type code. If the Ethernet frame uses SNAP as well, the entire SNAP header can be copied.
- The frame is scheduled for transmission.
  - (lots of fun in case of fragmentation and protection)
- The 802.11 MAC header is constructed from the Ethernet MAC header. The Ethernet destination address is copied to the Address 1 field of the 802.11 MAC header. The BSSID is placed in the Address 2 field of the MAC header, as the sender of the frame on the wireless medium. The source address of the frame is copied to the Address 3 field of the MAC header.
- The new frame is transmitted on the 802.11 interface.

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

Wireline and Wireless

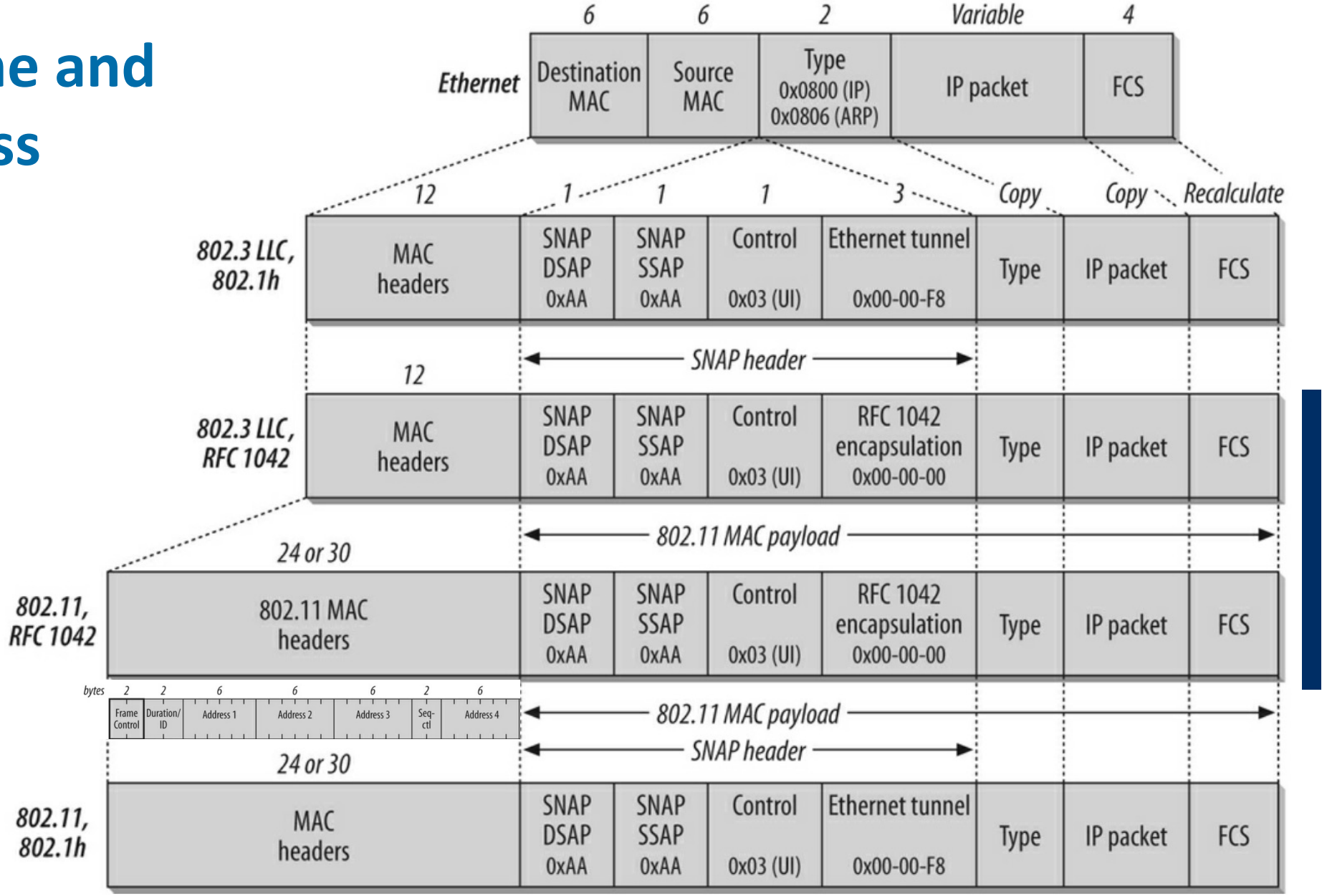
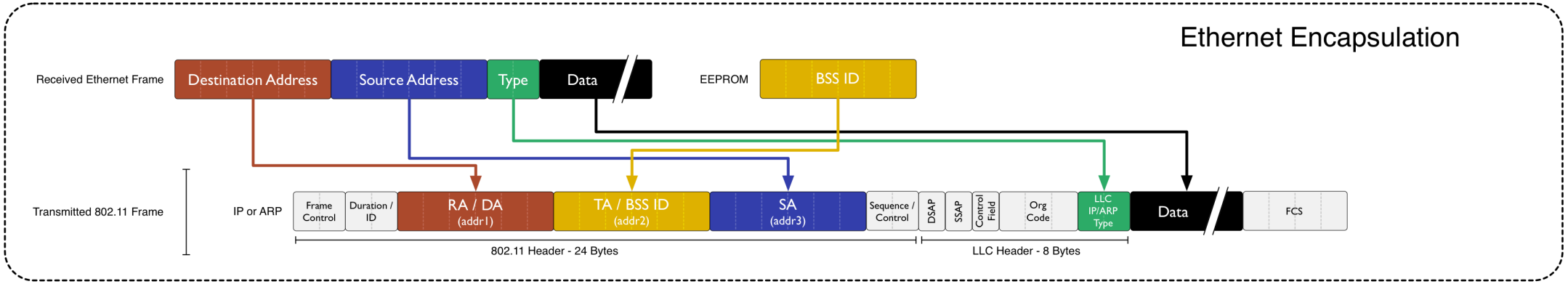
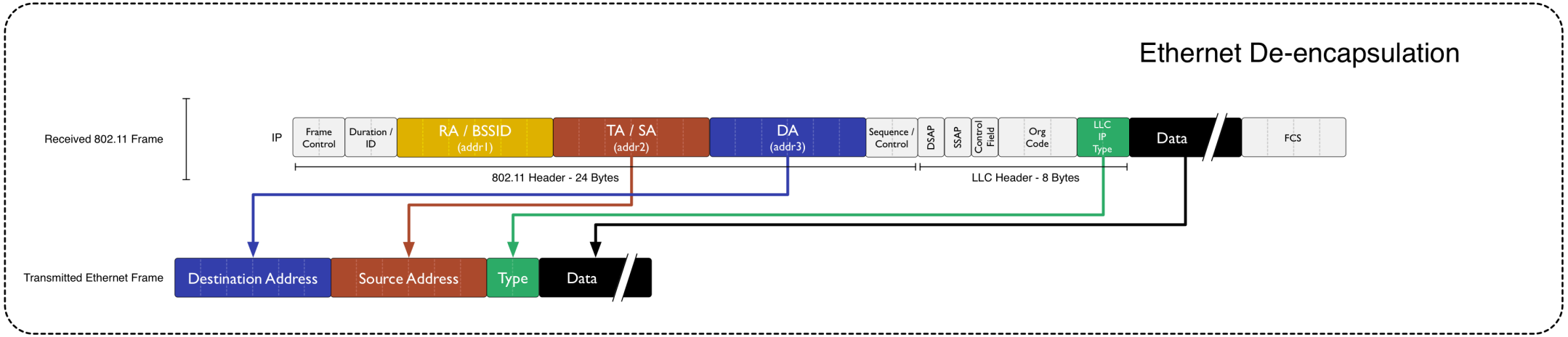


Figure 3-13. IP encapsulation in 802.11

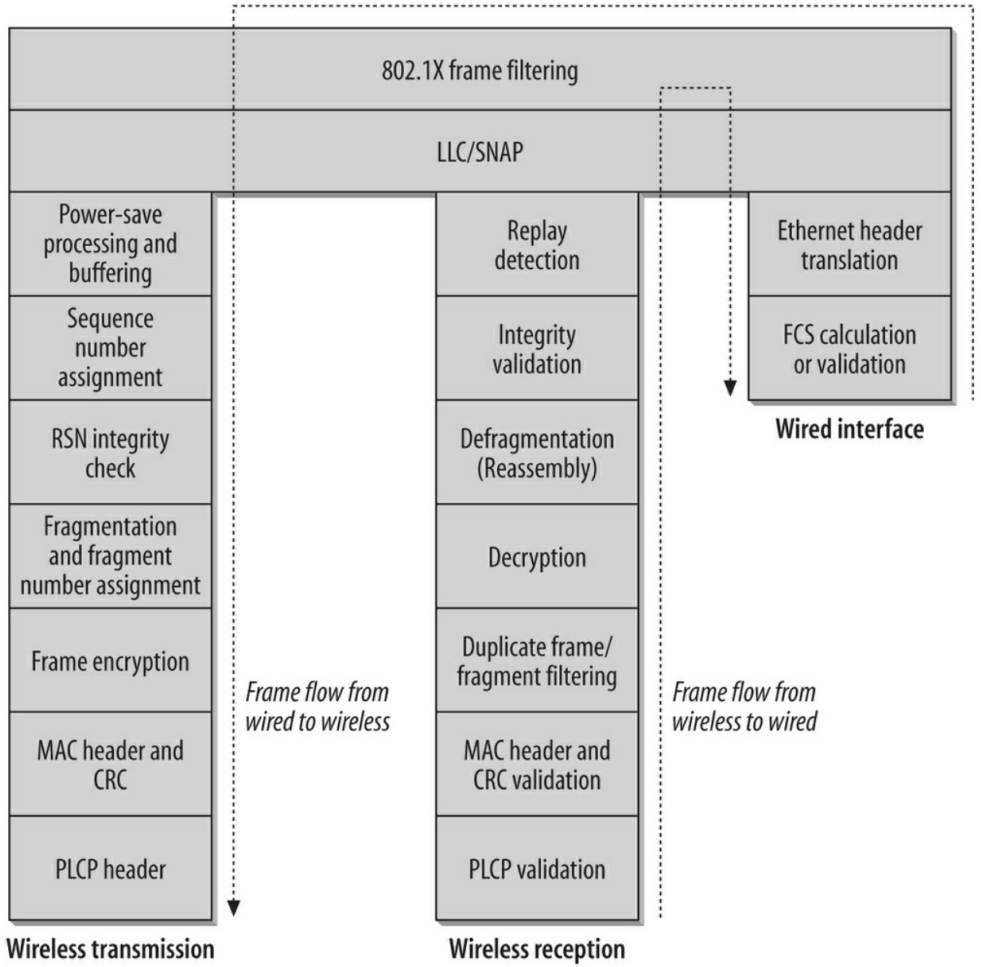
From and to the wire (DS)

Access Point





Note: there is a bunch of other stuff that happens…



What are the steps?

1. ~~Switch on the stations (& access points)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. ~~Define how we are going to organize the bits for multiple users~~
5. ~~Listen to synchronize and get system information~~
6. ~~Random Access~~
7. ~~Get a channel (well, not exactly…)~~
8. ~~Authenticate (uh, does this happen earlier?)~~
9. ~~Try to send data~~
10. Move around

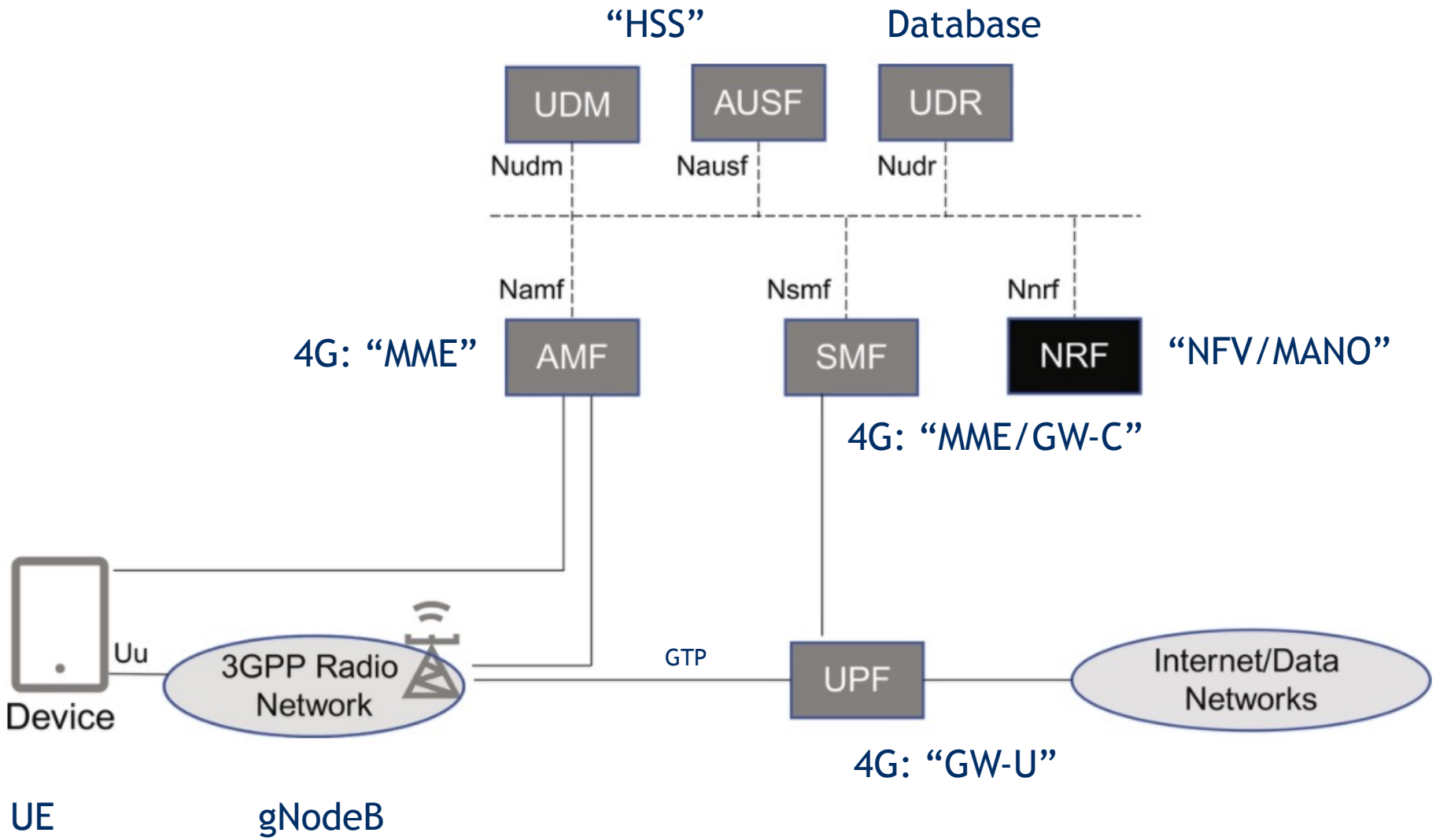
IEEE 802.11 – Mobility & Roaming

- **No or bad connection? Then perform:**
- **Scanning**
  - scan the environment, i.e., listen into the medium for beacon signals or send probes into the medium and wait for an answer
  - Active or Passive scanning
- **Association Request**
  - station sends a request to one or several AP(s)
- **Association Response**
  - success: AP has answered, station can now participate
  - failure: continue scanning
- **AP accepts Association Request**
  - signal the new station to the distribution system
  - the distribution system updates its data base (i.e., location information)
  - typically, the distribution system now informs the old AP so it can release resources (→ sometimes incompatible proprietary solutions)
  - IEEE 802.11f (Inter Access Point Protocol IAPP) solves this problem – BUT IT WAS NEVER STANDARDIZED

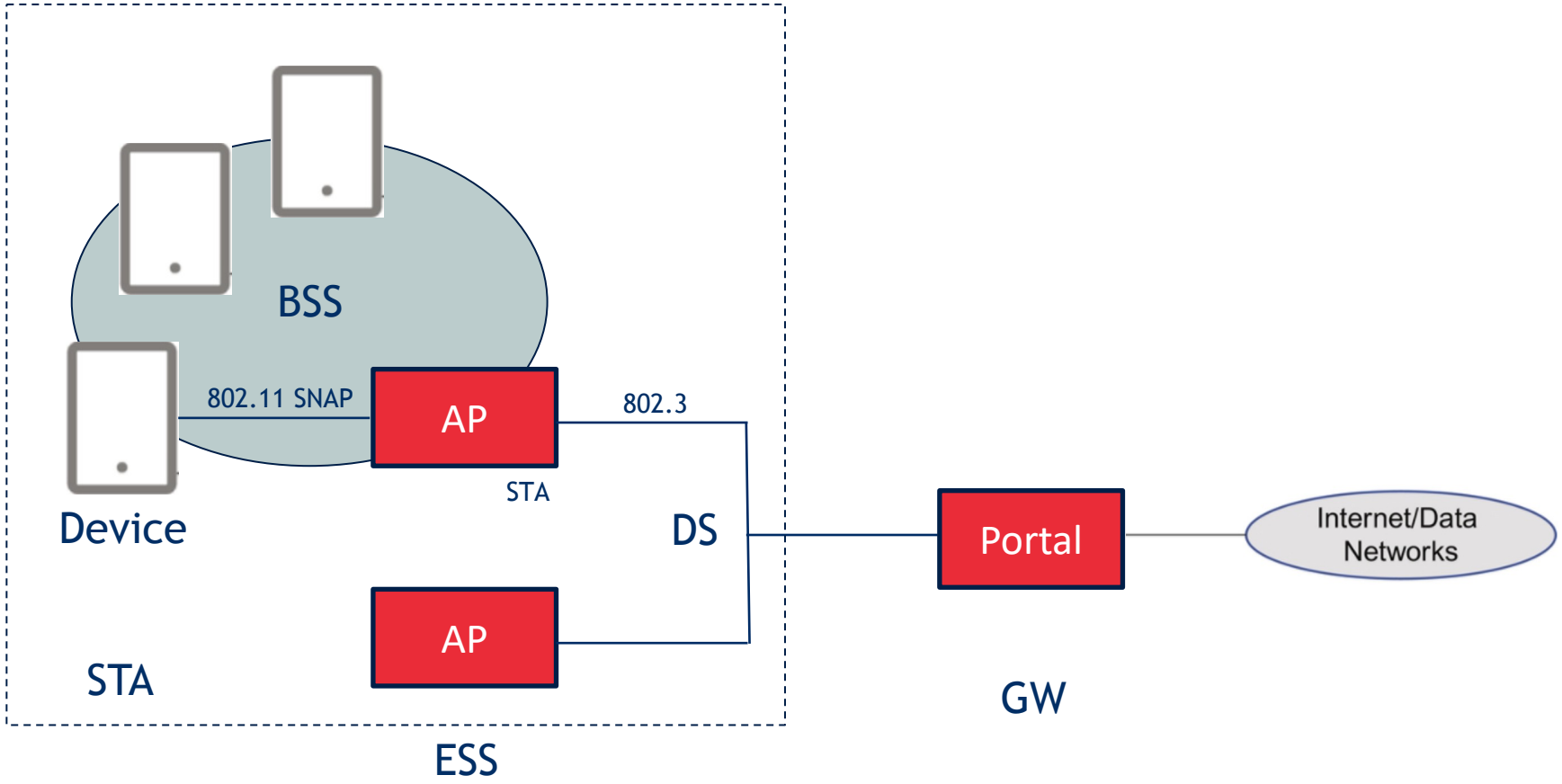
TL; DR;

- **2 main approaches, mainly depending on**
  - Market and ecosystem
  - Spectrum allocation strategy
- **5G (NR)**
  - Cellular, centralized scheduling
  - Licensed
- **Wifi (6)**
  - Distributed scheduling
  - Unlicensed

5G CN: the core of the core



WiFi: the infrastructure network



Things you should ask yourself

1. What is the equipment needed?
2. Which frequencies?
3. How do we send bits?
4. How are the bits organized?
5. How do we figure out what to connect to?
6. How do we get connected the first time?
7. How do we set up a connection?
8. How do we authenticate?
9. How do we send packets e2e?
10. What happens when we move?

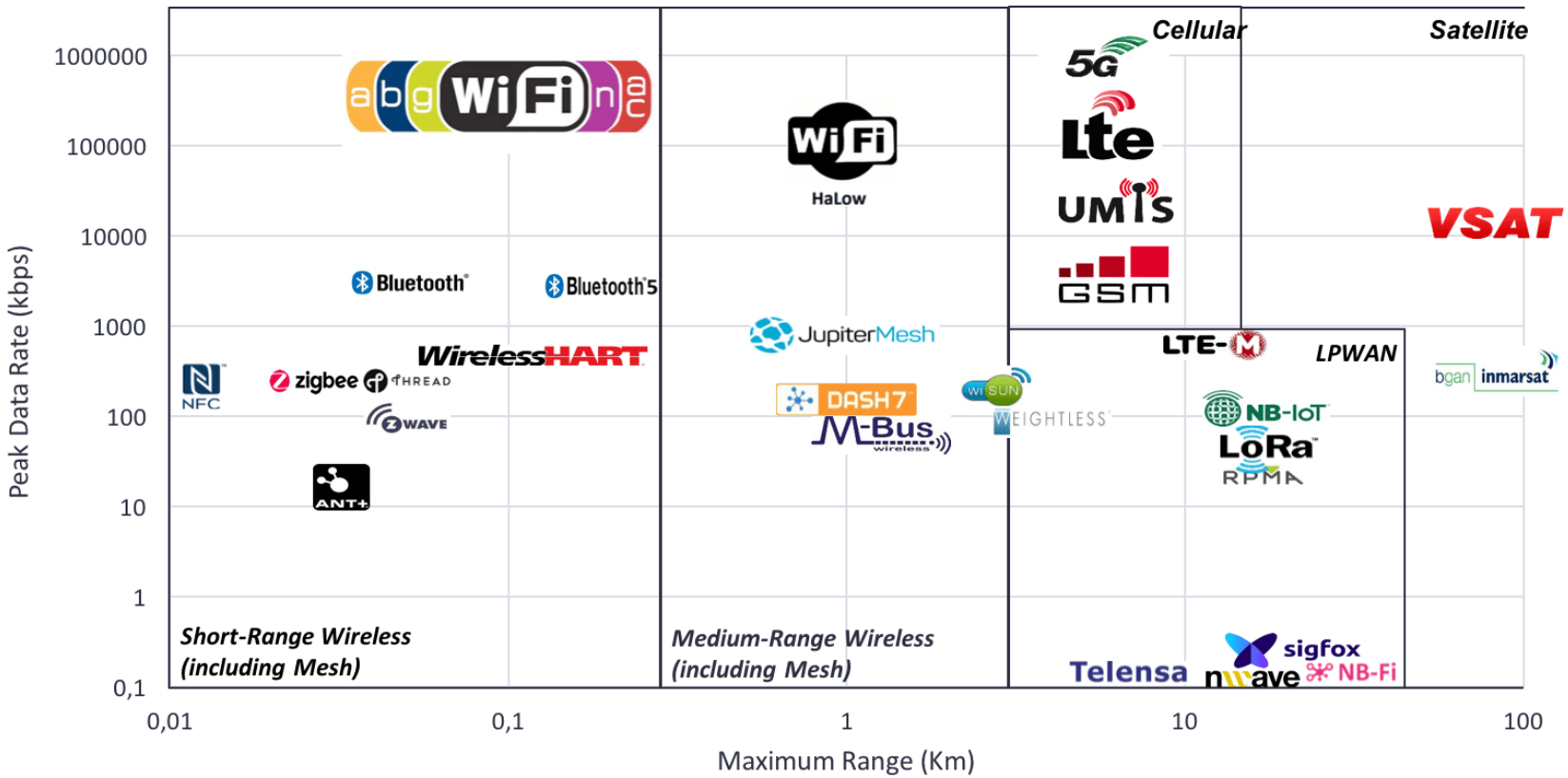
5. The Specials

(but wait, there is more)

So many choices

Comparison Wireless technologies

Peak Data Rate vs Maximum Range



Please note that this chart is meant to show the maximum theoretical range and data rate for each technology, but this does not mean that the two can be achieved at the same time. On the contrary, no wireless technology can achieve the maximum range while transmitting at its peak data rate, but rather the higher is the used data rate, the lower is the achievable communication range.

https://iot-analytics.com/iot-segments/iot-connectivity/

The specials => dedicated usecases

- **Until now, typically networks for broadband**
- **Range from a few meters to a few kms**
- **Wide standards**
  - With addition for specific cases e.g. URLLC in 5G, 802.11ah flavor of Wi-Fi
- **But there are others**
  - Dedicated “standards”
  - A couple of important ones
    - V2V
    - Shared spectrum
    - Personal Area Networks: shorter range
    - Low Power Wide Area Networks: longer range
    - Body Area Networks (recent)

Automotive

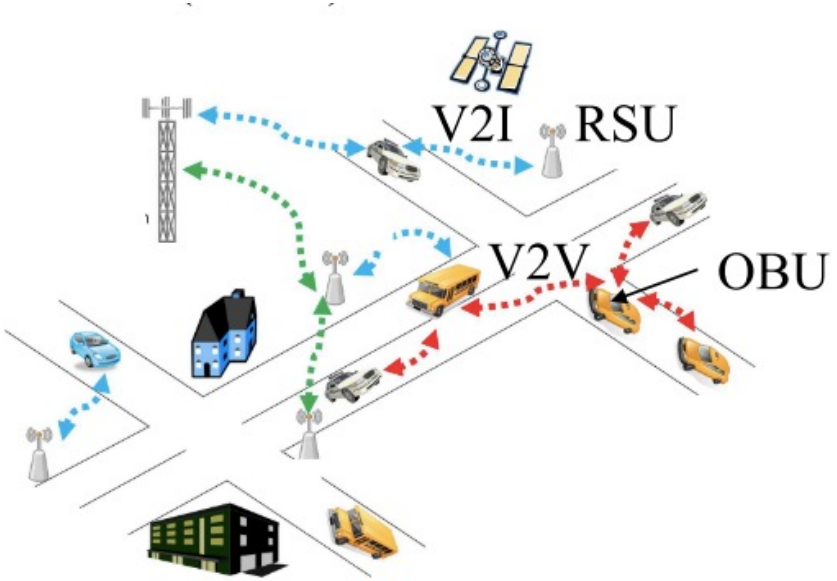
Vehicular networks

- **Applications**

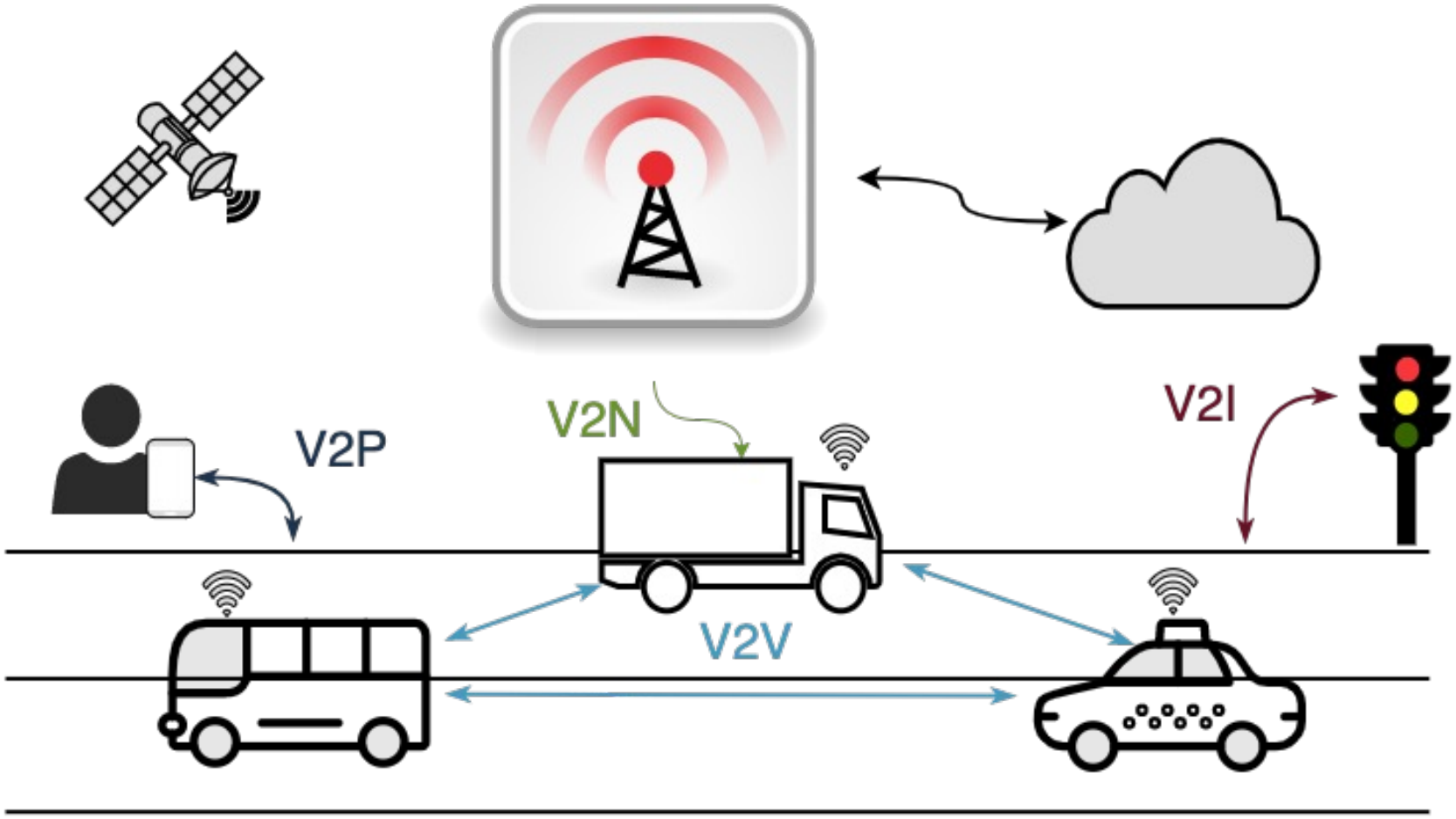
Vehicular networks

What is different

- **VANET**
- High **speed** and large doppler
- Fast **changing** network topology
- Geographically **constrained** and predictable mobility
- High **unstable** communication environment



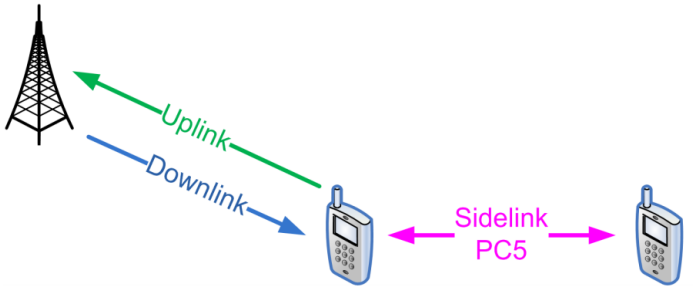
V2V, V2X

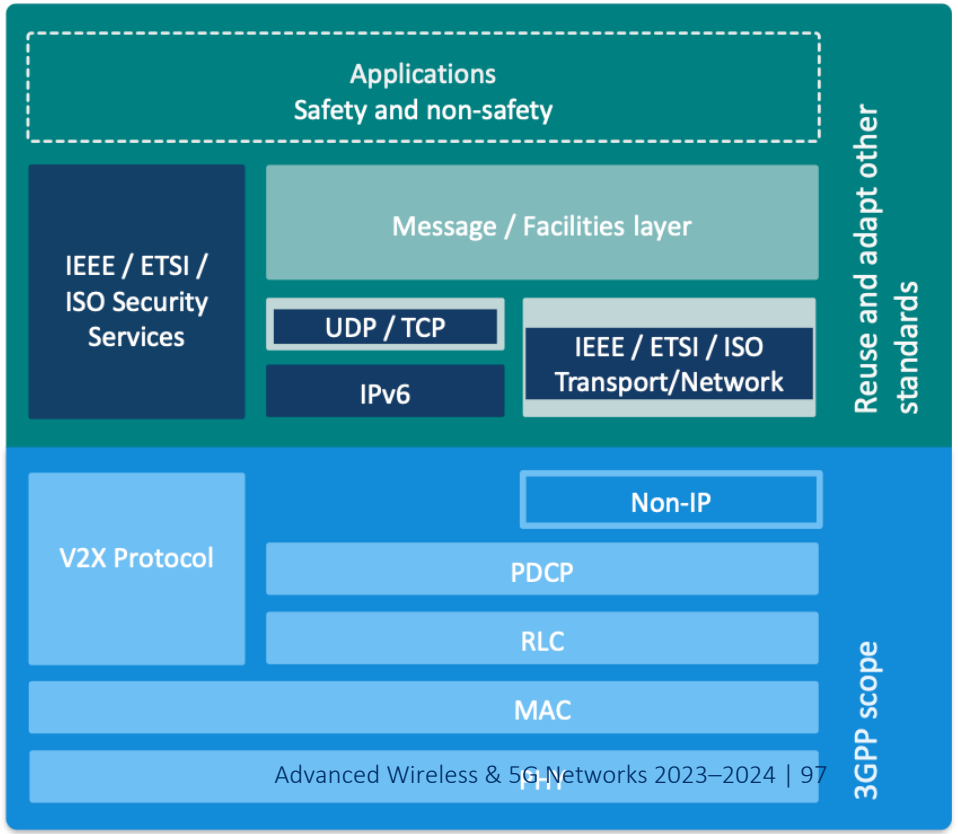


https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_application/application_notes/1ma264/1MA264_0e_D2DComm.pdf
https://arxiv.org/pdf/2102.04538.pdf
https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/c-v2x_its_stack.pdf

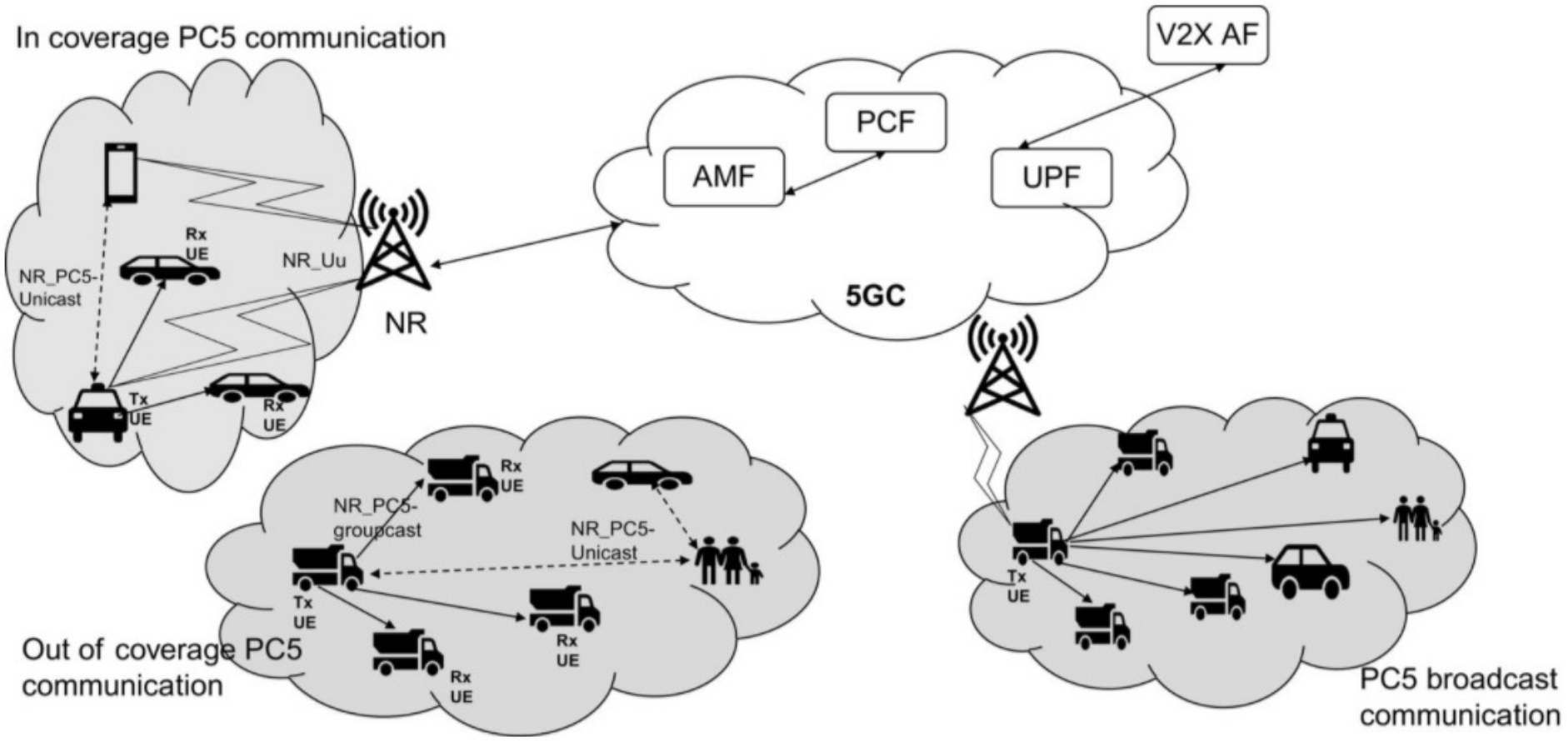
Sidelink

- Key concept in LTE & 5G **over PC5 interface**
- The services rely on the broadcast transmission of small awareness messages such as CAMs (Cooperative Awareness Messages)
- C-V2X Reuses Upper Layers Defined by the Automotive Industry
- Central to sidelink transmission and reception is the concept of Resouce Pools (RP). A resource pool is a set of resources assigned to the sidelink operation. It consists of the subframes and the resource blocks within.
- In R12: D2D ProSe, Mode 1 & 2
- In R15-16: Mode 3 and 4 for V2V with much lower latency (but less efficient as well)
  - Mode 3: eNB- or gNB-controlled channel access (centralized control)
  - Mode 4: Sensing, with semi-persistent transmission (before knowing the packet size, decentralized control)
- Synchronization via GNSS (Global Navigation Satellite System)





V2X in NR (R16)


In coverage PC5 communication
V2X AF
PCF
AMF
UPF
5GC
NR
NR_Uu
NR_PC5-
Unicast
Rx
UE
Tx
UE
Rx
UE
NR_PC5-
groupcast
NR_PC5-
Unicast
Tx
UE
Rx
UE
Rx
UE
Rx
UE
Out of coverage PC5
communication
Tx
UE
PC5 broadcast
communication

V2X Improvements

ENHANCEMENT OF 3GPP SUPPORT FOR V2X SCENARIOS (R15)

- **Vehicle Platooning** - Vehicles platooning enables the vehicles to dynamically form a group travelling together. All the vehicles in the platoon receive periodic data from the leading vehicle, in order to carry on platoon operations, allowing the distance between vehicles to become extremely small, i.e., the gap distance translated to time can be very low (sub second).
- **Advanced Driving** - Advanced Driving enables semi-automated or fully-automated driving. Longer inter-vehicle distance is assumed. Each vehicle and/or RSU shares data obtained from its local sensors with vehicles in proximity, thus allowing vehicles to coordinate their trajectories or manoeuvres. In addition, each vehicle shares its driving intention with vehicles in proximity. The benefits of this use case group are safer travelling, collision avoidance, and improved traffic efficiency.

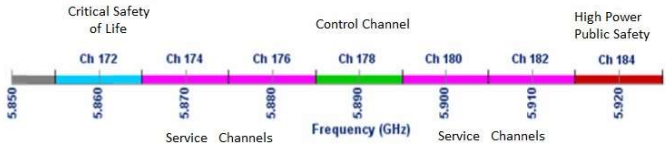
V2X Improvements

ENHANCEMENT OF 3GPP SUPPORT FOR V2X SCENARIOS

- **Extended Sensors** - Extended Sensors enables the exchange of raw or processed data gathered through local sensors or live video data among vehicles, RSUs, devices of pedestrians and V2X application servers. The vehicles can enhance the perception of their environment beyond what their own sensors can detect and have a more holistic view of the local situation.
- **Remote Driving** - Remote Driving enables a remote driver or a V2X application to operate a remote vehicle for those passengers who cannot drive themselves or a remote vehicle located in dangerous environments. For a case where variation is limited and routes are predictable, such as public transportation, driving based on cloud computing can be used. In addition, access to cloud-based back-end service platform can be considered for this use case group.

https://www.igi-global.com/gateway/chapter/71835

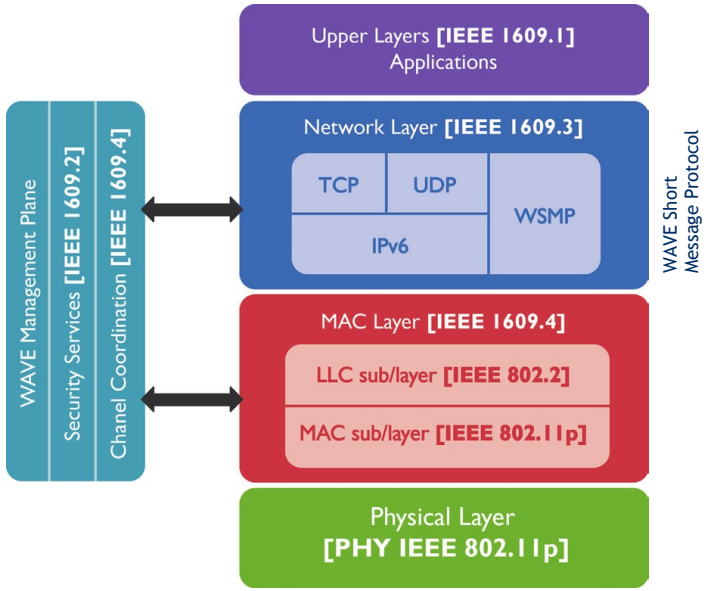
802.11p

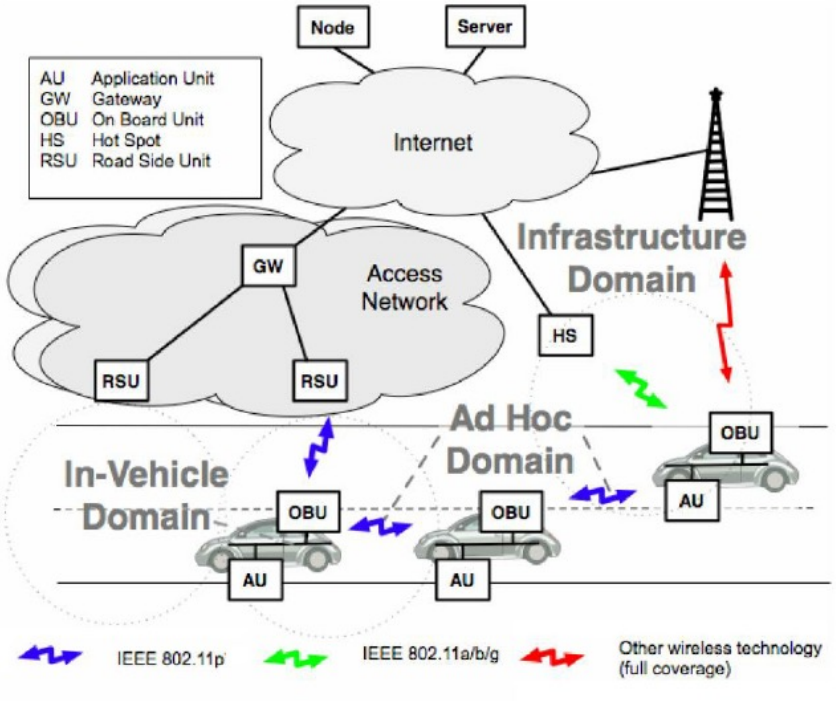


802.11p WAVE frequency spectrum

IEEE 802.11p is an approved amendment to the IEEE 802.11 standard to add wireless access in vehicular environments (WAVE), a vehicular communication system. It defines enhancements to 802.11 (the basis of products marketed as Wi-Fi) required to support Intelligent Transportation Systems (ITS) applications. Also: DSRC

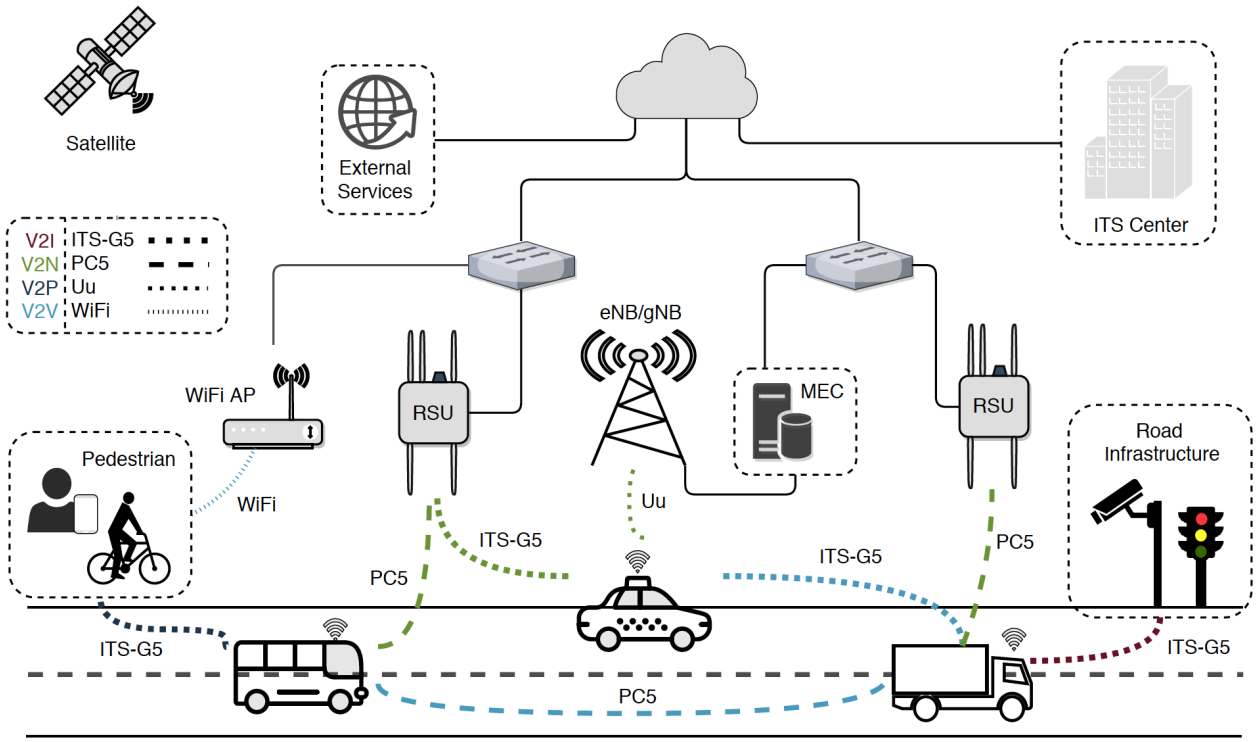
Dedicated Short-Range Communications





The future will be heterogeneous

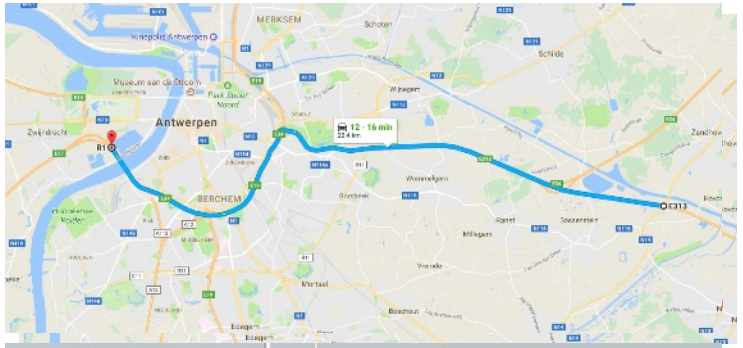
- **And includes MEC and SDVN**



Imec/UA's V2X testbed – "smart highway"

- For validated & reliable V2X communication

Real life, real time, large scale…



… testing and validating

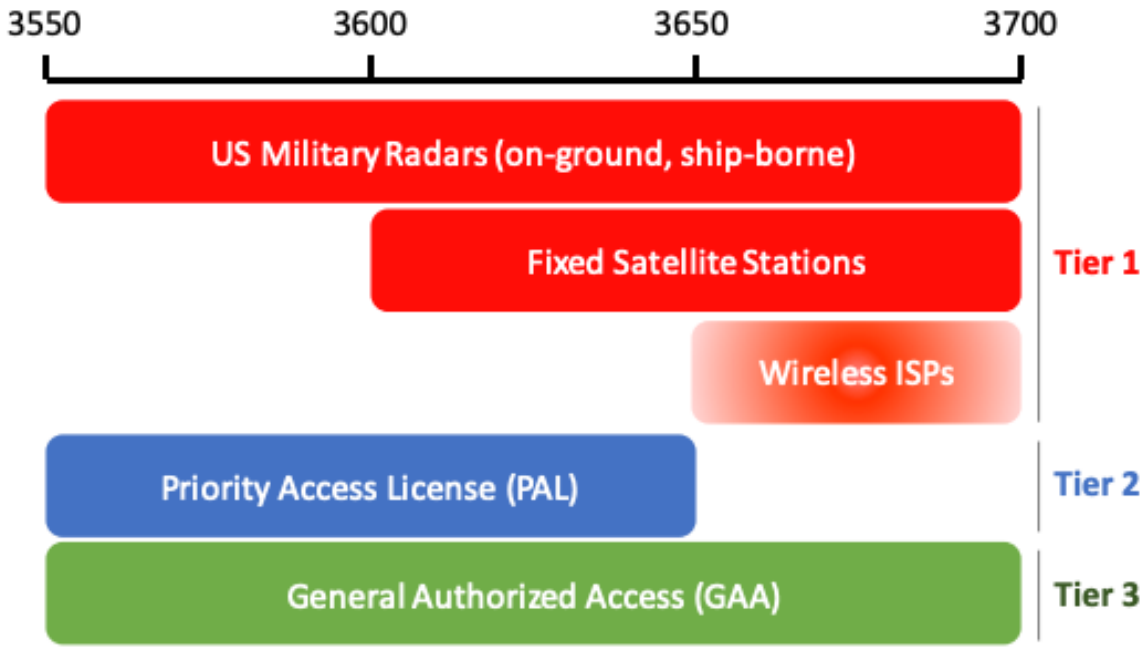
1. Ultra-fast **connectivity**
   - Vehicle-to-vehicle & vehicle-to-infrastructure communication
   - Minimal latency (10-15 ms)
2. Extensive **computing power**
   - In the vehicle & at the roadside
   - Supporting data-intensive applications, e.g. using artificial intelligence
3. Precise **positioning**
   - GPS combined with other techniques for optimized accuracy
   - In the order of 1-10 cm

Different ways to use spectrum

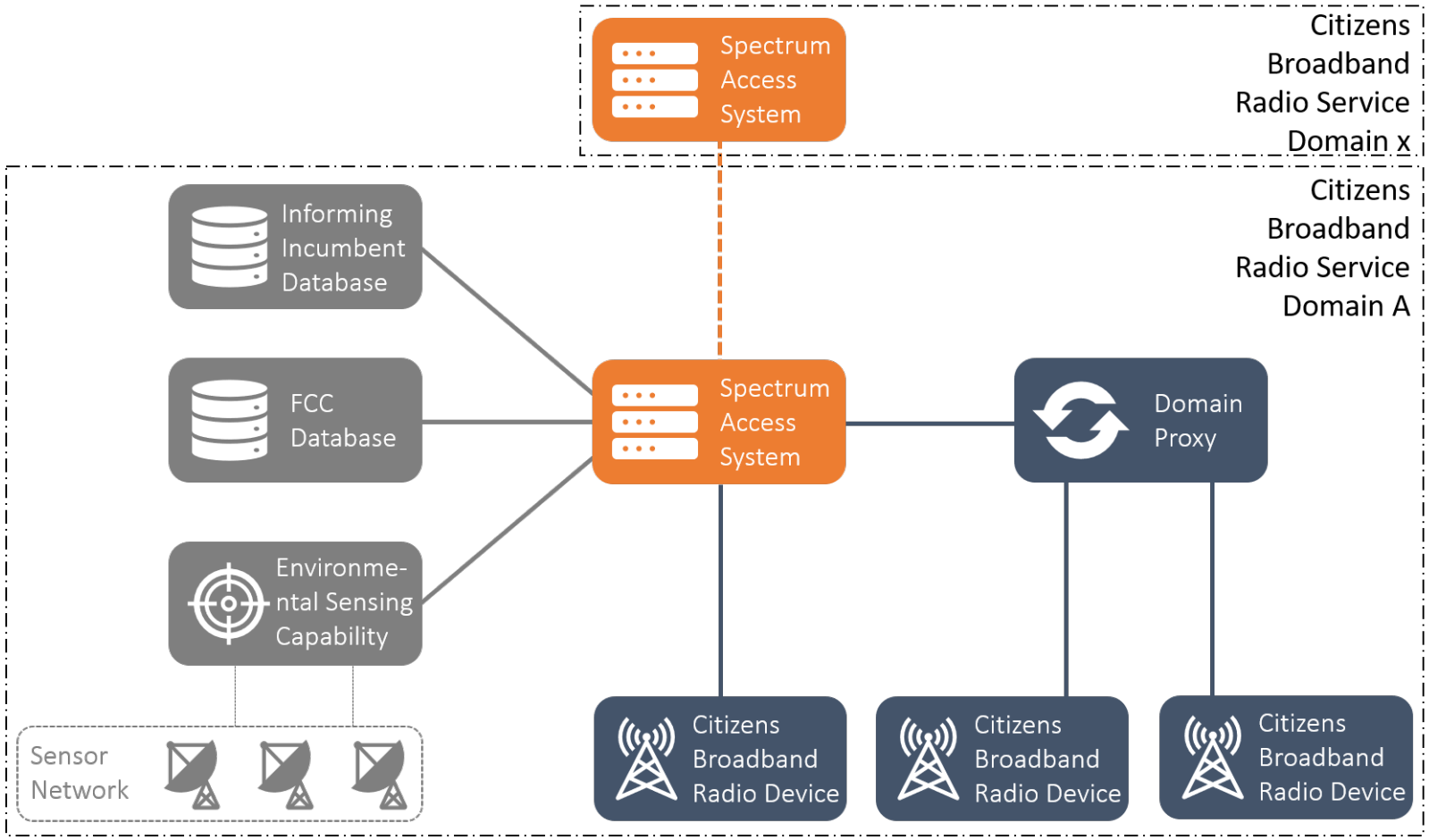
Spectrum licensing: 3 models

CBRS (Brand: OnGo)

- There is never enough spectrum – and some of it is not well utilized. => Citizens Broadband Radio Service
- 150 MHz of underutilized spectrum: B48 (US specific)
- 3 tiers



CBRS architecture

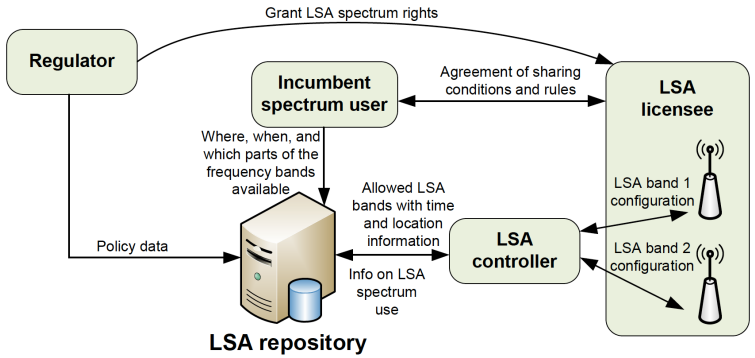


Can allow stand-alone or paired used with licensed spectrum

https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/spectrum-sharing-lsa-sas-paper.pdf

LSA

- Similarly, in Europe, there are chunks of spectrum un(der)used. Enter Licensed Shared Access (2.3 GHz)



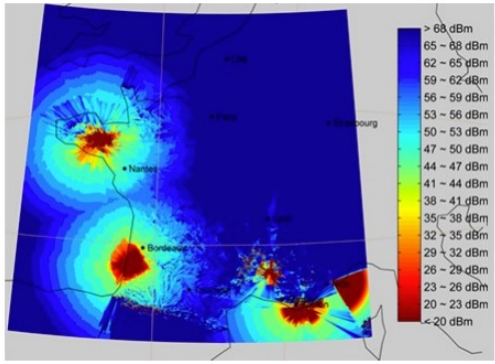


Figure 8: LSA Spectrum Availability in France [17].

- LSA provides a licensed sharing of frequencies that are already assigned to the so-called incumbents in return for compensation. LSA can thereby increase the utilization of bands in a controlled way, specifying the use for given location and time in an LSA repository.
- Note: in Europe, mostly Supplementary Downlink, no stand-alone use.