University of Antwerp
Faculty of Science

Advanced Wireless & 5G Networks

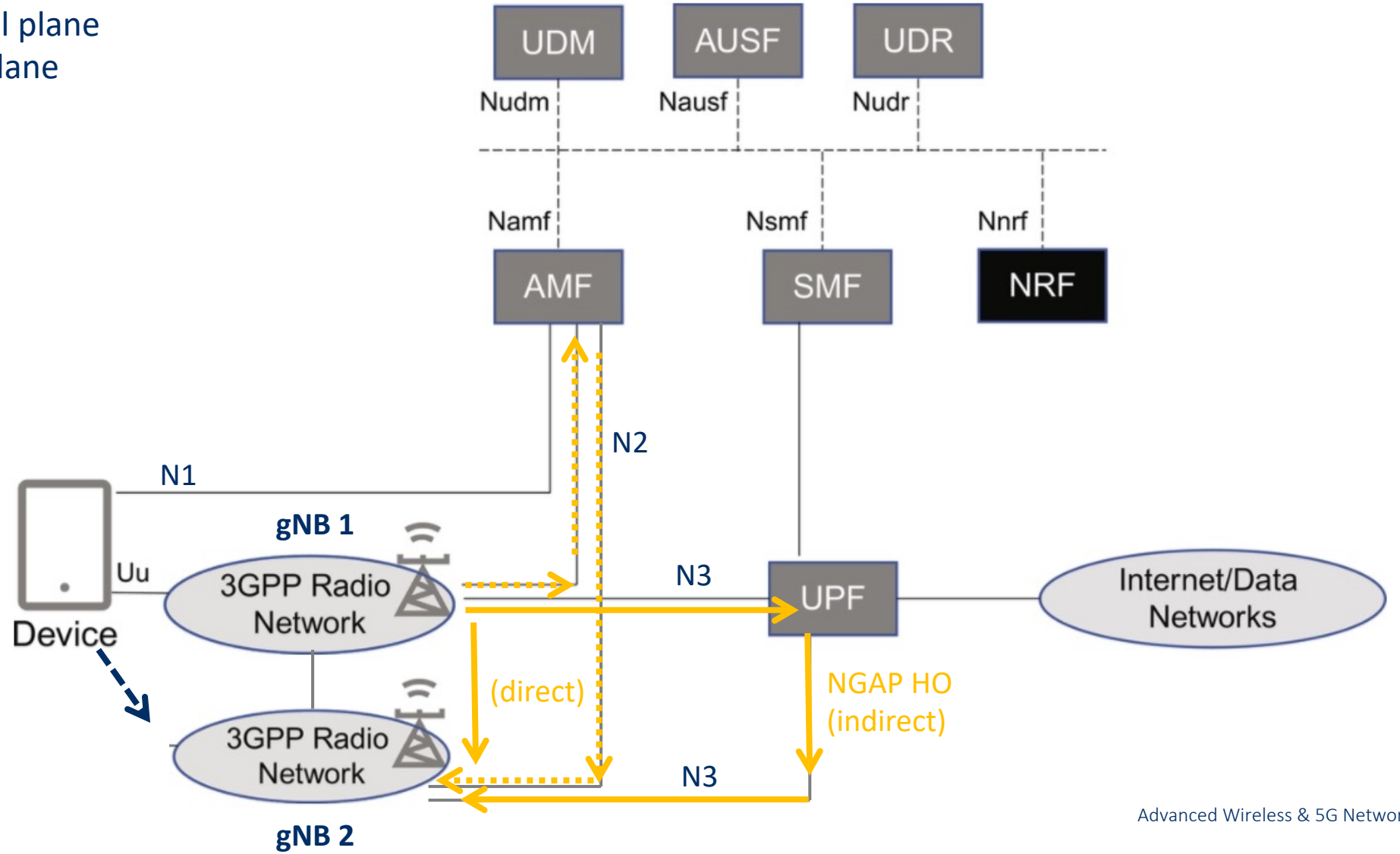
Prof. Dr. Ir. Michael Peeters — 2023–2024

Topics for today

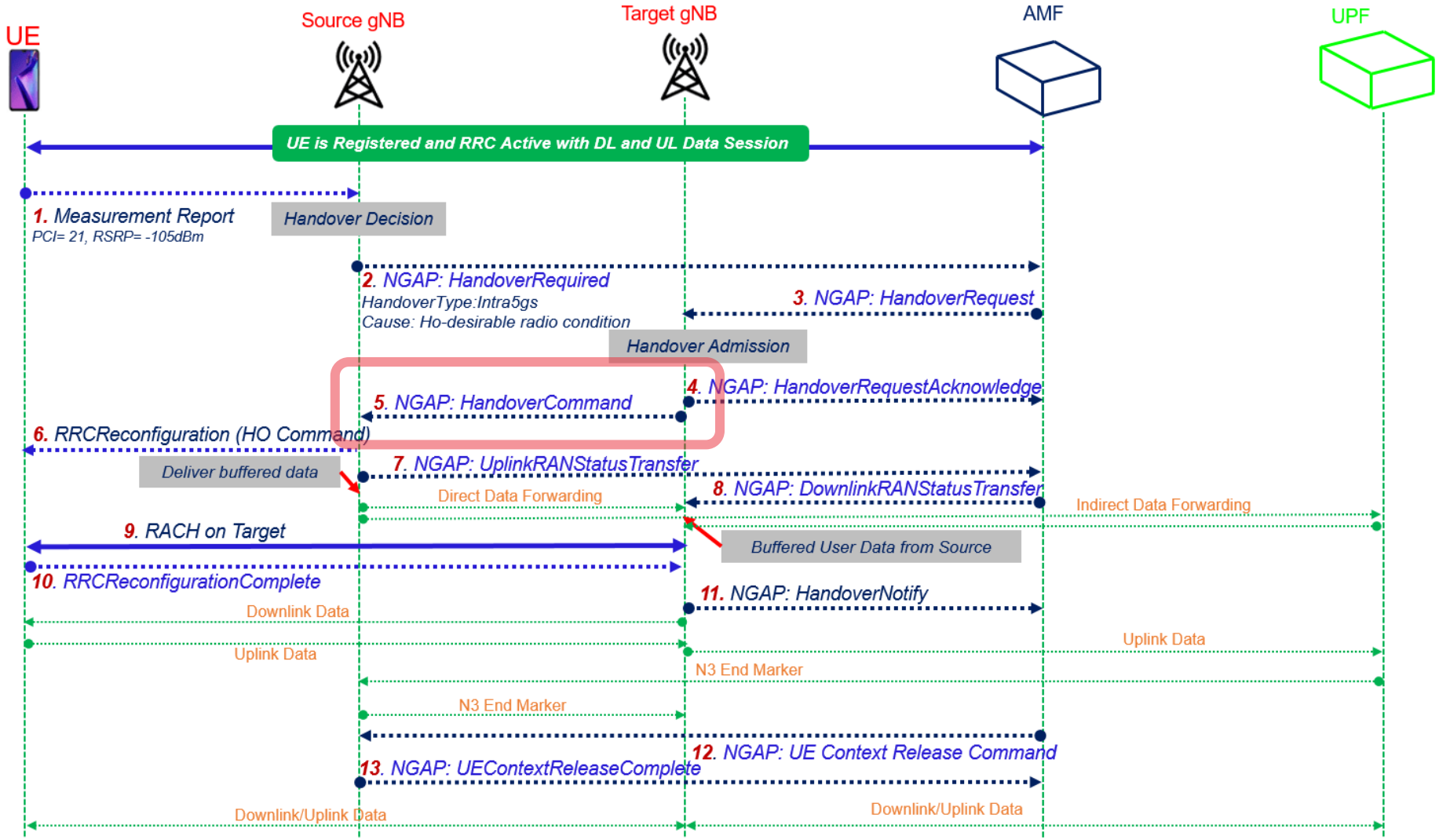
- **Open question**
  - N2 HO
- **4. WiFi**
  - cont.

N2/NGAP HO

Control plane
User plane

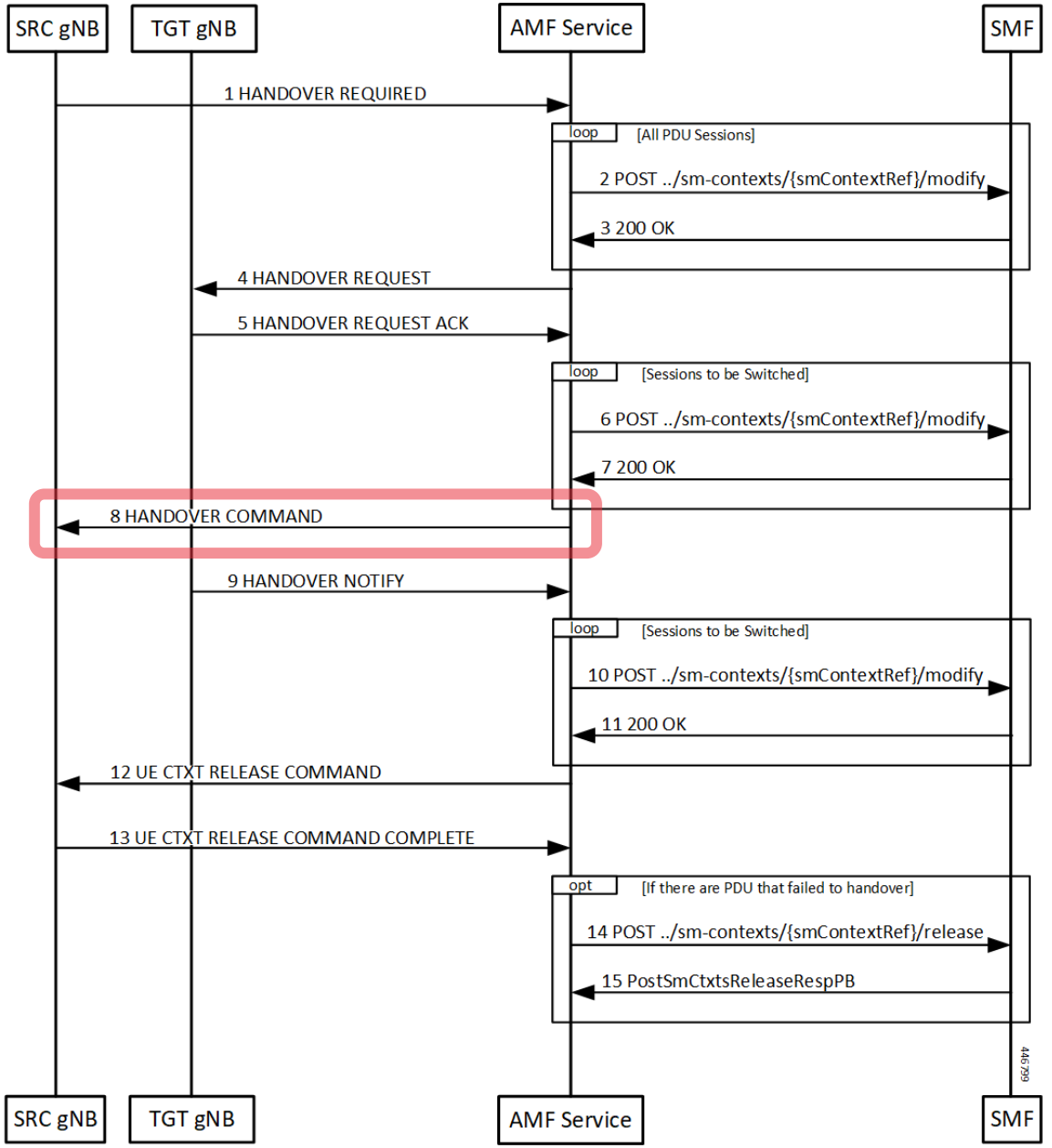


N2 or NGAP Handover

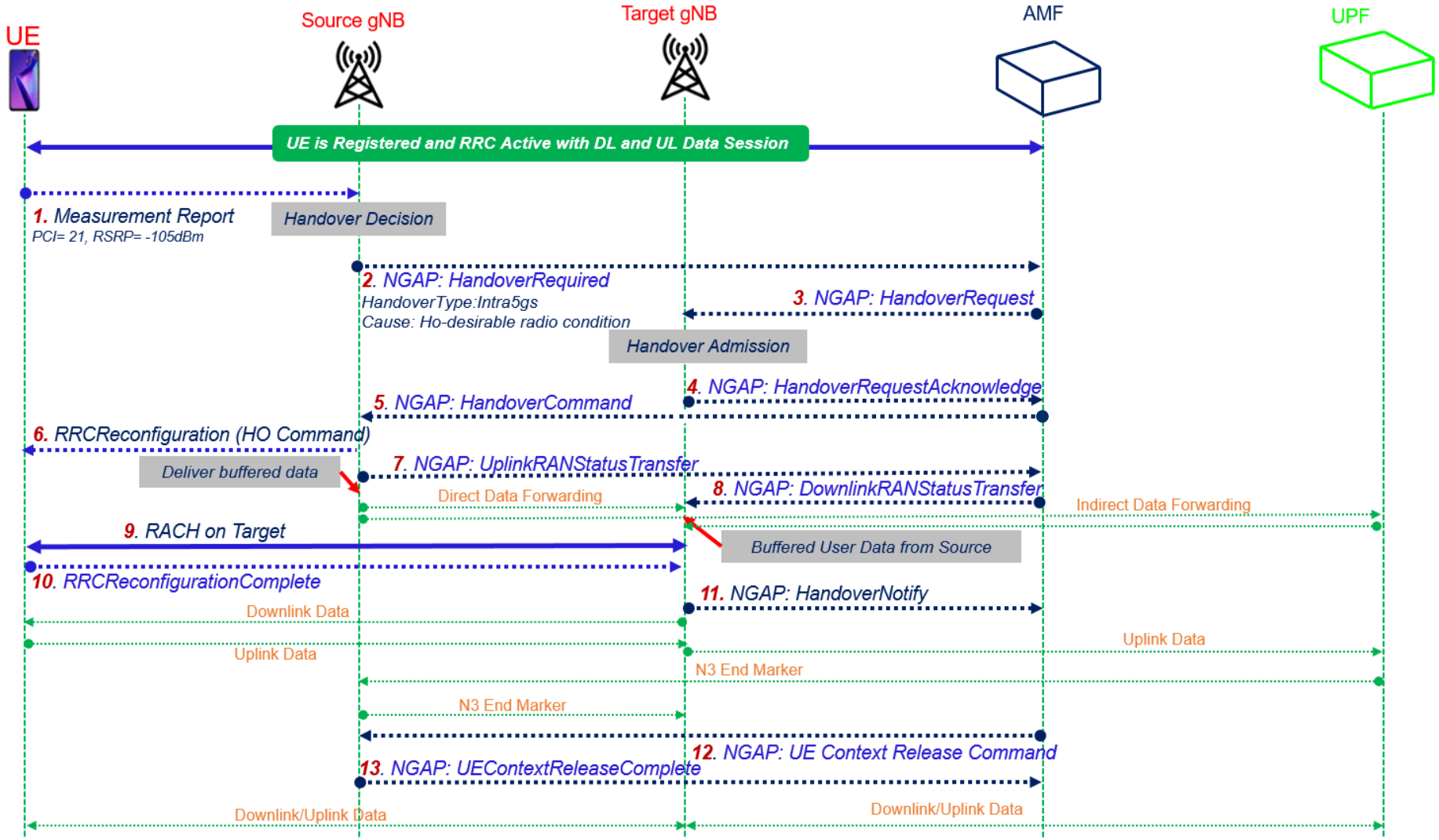


N2 with less cruft

Step	Description
1	With signaling from the UE, the source gNB starts the handover procedure by sending a HANDOVER REQUIRED message to the AMF.
2	The AMF finds a gNB that can support the signaled TargetId from the gNB. AMF rejects the message when it can't find gNB. The AMF creates a ModificationRequest and sends it to the SMF.
3	The SMF analyzes the TargetID and takes appropriate actions. The SMF then responds.
4	The AMF finds the gNB corresponding to the Target ID, and the NGAP EP that serves that gNB. The AMF then sends a handover required message to the target gNB.
5	Target gNB sets up the resources required for the handover and responds with an ACK message. This ACK message contains the PDU resources that failed to setup as well.
6	The AMF constructs a Sm Context Modify message to update the target gNB tunnel endpoint IDs to the SMF. The AMF starts a guard timer and forwards the message to the SMF.
7	The SMF updates the information in associated UPFs and responds to the AMF.
8	The AMF builds a HandoverCommand message and sends it to the source gNB.
9	The UE now completes the handover at the target gNB. The target gNB sends a HANDOVER NOTIFY message to the AMF.
10	The AMF constructs a Sm Context Modify request to inform the SMF that the handover is complete.
11	SMF responds to the update.
12	The Handover procedure ends. The source gNB receives a UE context release command.
13	If there are PDU sessions that fail to setup at the target gNB are now released at the SMF.



N2 or NGAP Handover



But what about Direct Data Forwarding?

- **TS 23.503:** The availability of a direct forwarding path is determined in the source NG-RAN and indicated to the SMFs. If IP connectivity is available between the source and target NG-RAN and security association(s) is in place between them, a direct forwarding path is available.
  - i.e. this is IP Forwarding, not Xn-U forwarding. The Xn User plane (Xn-U) interface is defined between two NG-RAN nodes. The transport network layer is built on IP transport and GTP-U is used on top of UDP/IP to carry the user plane PDUs.
- **See also:** https://www.ericsson.com/en/blog/2020/4/indirect-direct-data-forwarding-5g-3gpp

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 evening**	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

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.

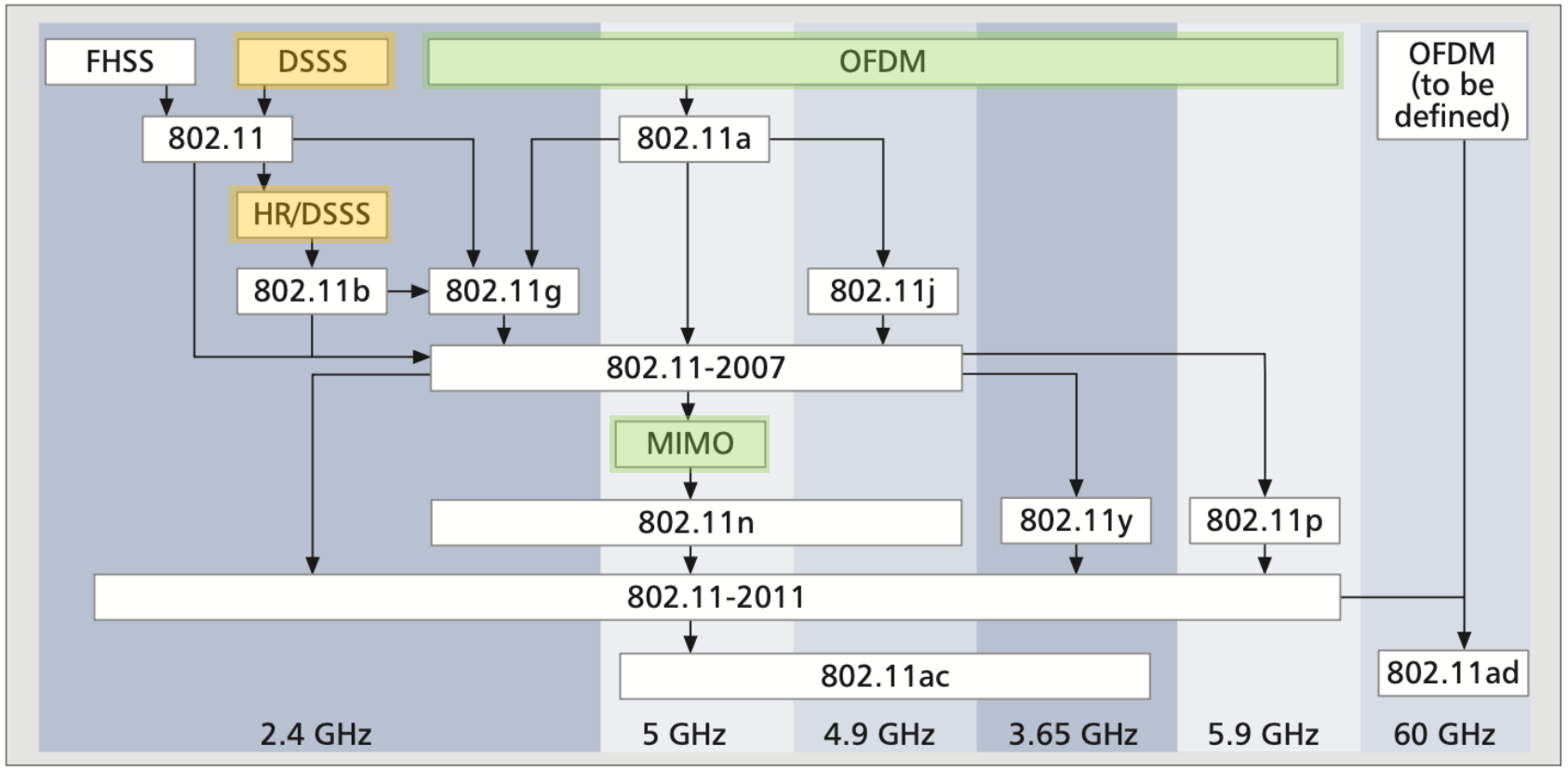
4. Wi-Fi, the 802.11 family

(from licensed to unlicensed)

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

Only 2 ways that are really different.



FHSS: Frequency Hopping Spread Spectrum
DSSS: Direct Sequence Spread Spectrum
HR: High Rate
OFDM: Orthogonal Frequency Division Multiplexing
MIMO: Multiple Input/Multiple Output

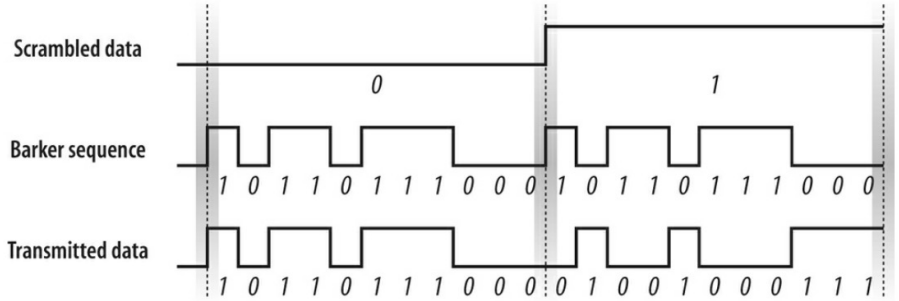
Today, grouped in IEEE 802.11-2016
MIMO = multiple-input, multiple-output = capacity increasing, on top of OFDM (last session)

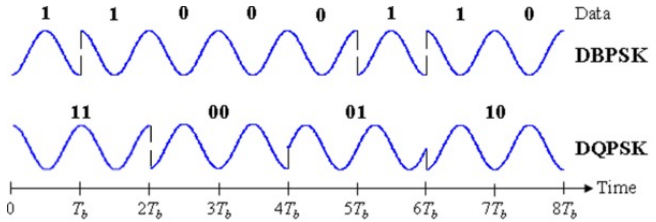
Legacy IEEE 802.11 - Physical layer

- **3 versions: 2 radio (typical 2.4 GHz), 1 IR: data rates 1 or 2 Mbit/s**
- **FHSS (Frequency Hopping Spread Spectrum) – Google Hedy Lamarr**
  - spreading, de-spreading, signal strength, typical 1 Mbit/s
  - min. 2.5 frequency hops/s (USA), two-level GFSK modulation
- **DSSS (Direct Sequence Spread Spectrum)**
  - DBPSK modulation for 1 Mbit/s (Differential Binary Phase Shift Keying), DQPSK for 2 Mbit/s (Differential Quadrature PSK)
  - preamble and header of a frame is always transmitted with 1 Mbit/s, rest of transmission 1 or 2 Mbit/s
  - chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
  - max. radiated power 1 W (USA), 100 mW (EU), min. 1mW
- **Infrared**
  - 850-950 nm, diffuse light, typical 10 m range
  - carrier detection, energy detection, synchronization

Direct Sequence Spread Spectrum

- **DSSS**
  - Spreading is achieved by the use of codes
  - Spreading using 11-chip Baker sequence:
    - Symbol rate is 1 MHz resulting in 11 MHz chipping rate
  - Implementation more complex than FHSS
  - Robust against interference and insensitivity to multipath propagation
  - Modulation scheme:
    - 1 Mbit/s: Differential Binary Phase Shift Keying (DBPSK)
    - 2 Mbit/s: Differential Quadrature Phase Shift Keying (DQPSK)



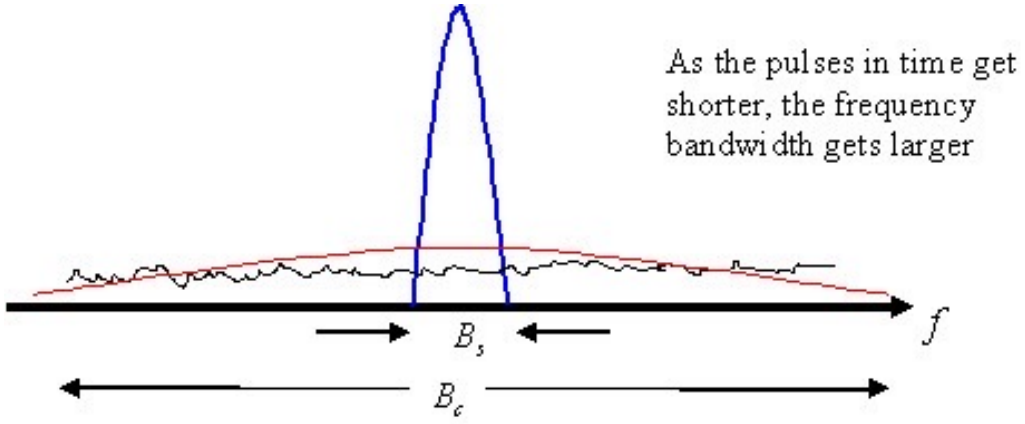


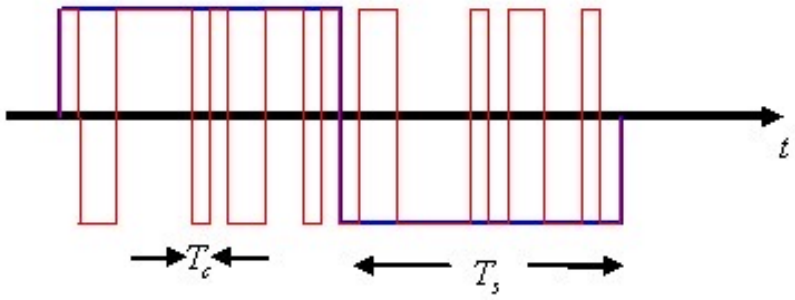
Note: first the chipping, then the BPSK

https://www.ni.com/ru-ru/innovations/white-papers/06/understanding-spread-spectrum-for-communications.html

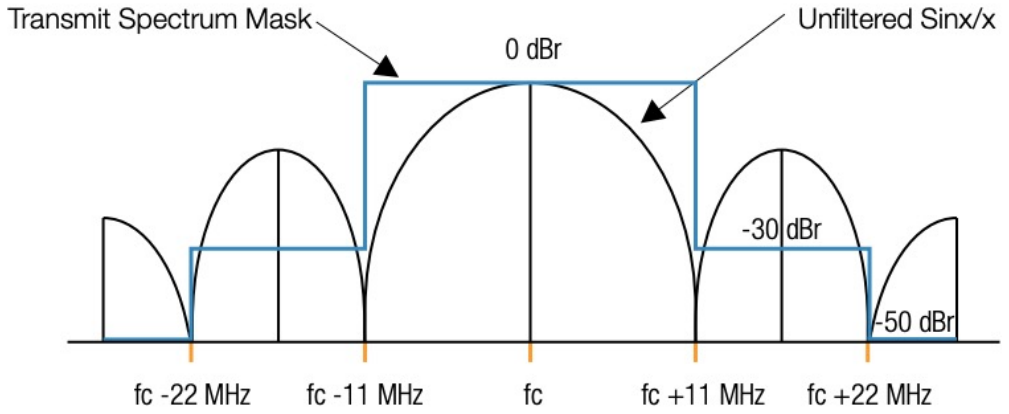
DSSS

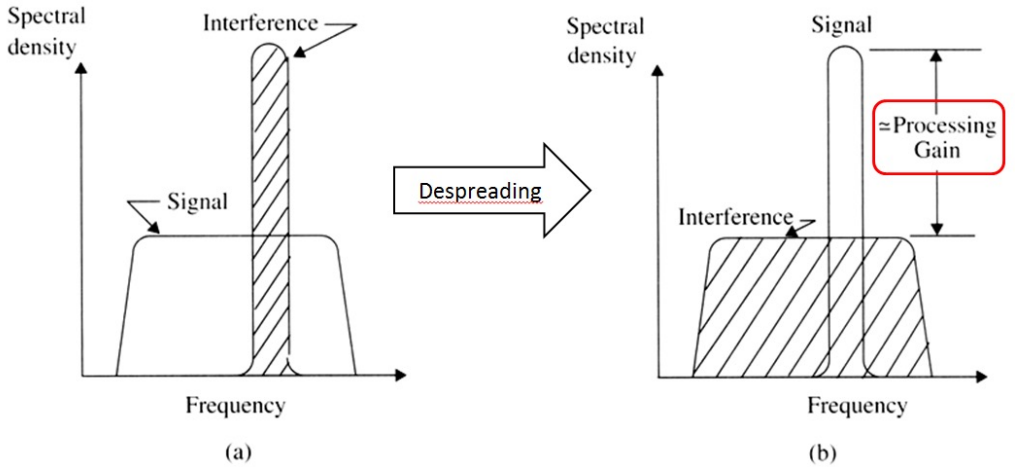
Shorter pulses = wider bandwidth





Needs to fit into mask, so additional filter is needed





Despreading mitigates narrowband noise

IEEE 802.11b: HR-DSSS

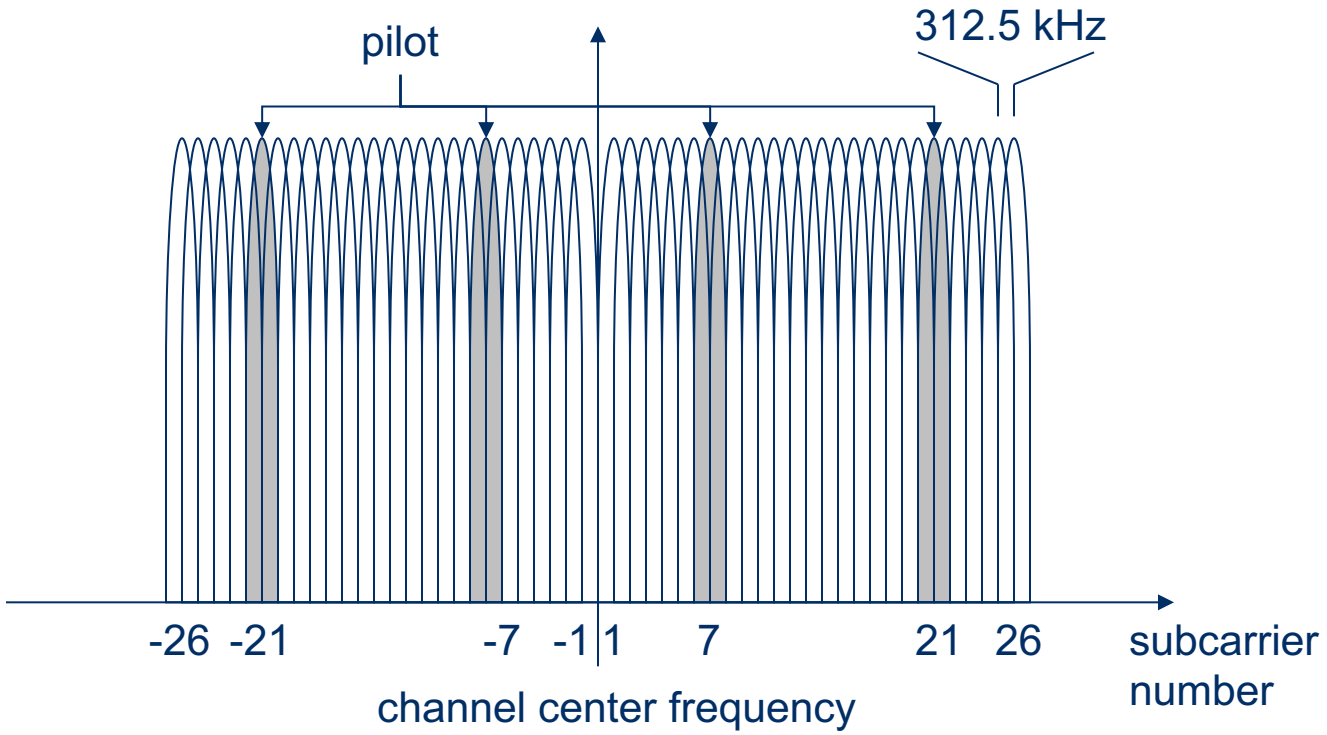
- **Data rate**
  - 1, 2, 5.5, 11 Mbit/s, depending on SNR, User data rate max. 6 Mbit/s
- **DSSS**
  - 1,2 Mbit/s: 11-chip Baker code
  - 5.5, 11 Mbit/s: 8-chip code using Complementary Code Keying (CCK)
    - 4,8 bit symbols at 1.375 Msym/s
  - Still 22 MHz BW
- **Transmission range**
  - 300m outdoor, 30m indoor
  - Max. data rate ~10m indoor
  - Free 2.4 GHz ISM-band
- **Security**
  - Limited, WEP Wired Equivalent Protection) insecure
- **Connection set-up time**
  - Connectionless/always on
- **Quality of Service**
  - Typ. Best effort, no guarantees (unless polling is used, limited support in products)
  - **Slot duration 20µs (!)**
- **Manageability**
  - Limited (no automated key distribution, sym. Encryption)
- **Special Advantages/Disadvantages**
  - Advantage: many installed systems, lot of experience, available worldwide, free ISM-band, many vendors, integrated in laptops, simple system
  - Disadvantage: heavy interference on ISM-band, no service guarantees, slow relative speed only

IEEE 802.11a: OFDM at 5GHz

- **Data rate**
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, depending on SNR
  - User throughput (1500 byte packets): 5.3 (6), 18 (24), 24 (36), 32 (54)
  - 6, 12, 24 Mbit/s mandatory
- **Transmission range**
  - 100m outdoor, 10m indoor
    - E.g., 54 Mbit/s up to 5 m, 48 up to 12 m, 36 up to 25 m, 24 up to 30m, 18 up to 40 m, 12 up to 60 m
- **Frequency**
  - Free 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz ISM-band
- **Security**
  - Limited, WEP insecure
- **Connection set-up time**
  - Connectionless/always on
- **Quality of Service**
  - Typ. best effort, no guarantees (same as all 802.11 products)
- **Manageability**
  - Limited (no automated key distribution, sym. Encryption)
- **Special Advantages/Disadvantages**
  - Advantage: fits into 802.x standards, free ISM-band, available, simple system, uses less crowded 5 GHz band
  - Disadvantage: stronger shading due to higher frequency, data rates may drop fast with distance, no QoS

OFDM in IEEE 802.11a

- OFDM with 52 used subcarriers (64 = 2^6 in total)
- 48 data + 4 pilot (plus 12 virtual subcarriers)
- 312.5 kHz spacing = >16.6MHz



IEEE 802.11g: OFDM at 2.4GHz

Extended Rate PHY (ERP): flavors

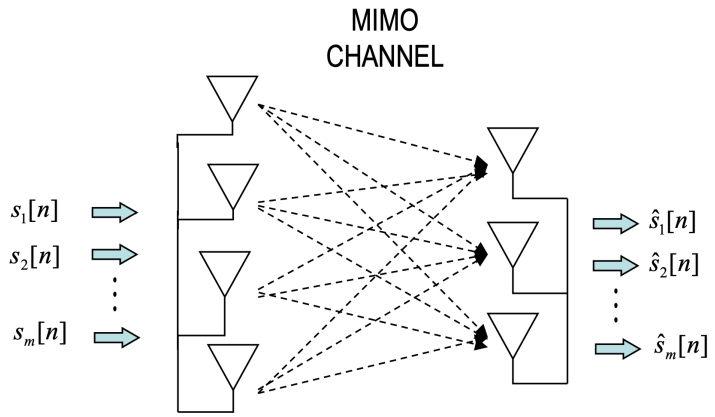
- **ERP-DSSS** and ERP-CCK These modes are backwards compatible with the original direct sequence specification (1 Mbps and 2 Mbps) as well as the 802.11b enhancements (5.5 Mbps and 11 Mbps)
- **ERP-OFDM** This is the major mode of 802.11g. It is essentially running 802.11a in the ISM frequency band (2.4 GHz), with a few minor changes to provide backwards compatibility. It supports the same speeds as 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. Speeds of 6, 12, and 24 Mbps are mandatory.
- ERP-PBCC and DSSS-OFDM: not widely used

IEEE802.11n: OFDM

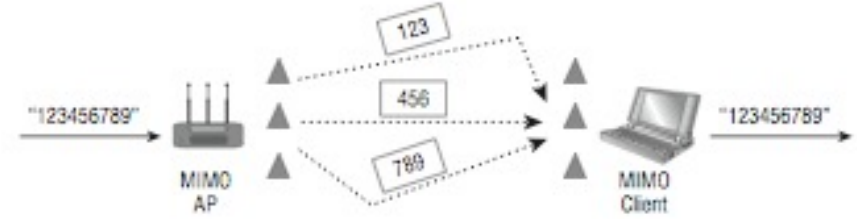
- **IEEE802.11a and 802.11g use OFDM**
  - 20 MHZ OFDM channels
  - Each channel: 52 subcarriers (48 subcarriers + 4 pilot tones)
- **IEEE802.11n uses OFDM**
  - 20 MHz OFDM channels and 40 MHz OFDM channels
    - 20 MHz OFDM channels have 56 subcarriers (52 subcarriers + 4 pilot tones)
    - 40 MHz OFDM channels have 112 subcarriers (108 subcarriers + 4 pilot tones)
    - 40 MHz channels by bonding two 20 MHz channels

IEEE 802.11n: Spatial Multiplexing, MIMO

- **MIMO** radios transmit multiple radio signals at the same time (= spatial streams)
- Each individual radio signal is transmitted by unique radio and antenna
- Each **individual stream can contain different data** and travels a different path (at least half-wave-length space between the antennas of MIMO system)
- Following different paths is called **spatial diversity**
- Multiple independent streams + spatial diversity = **spatial multiplexing**
- Spatial multiplexing drastically increases the throughput



An $n_R \times n_T$ MIMO channel with i.i.d. entries has a spatial multiplexing gain of $r = \min(n_R, n_T)$



IEEE802.11n: MIMO Diversity

- **Multipath** produces multiple copies of the same signal arriving at the receiver with different amplitudes
- **Switched diversity**: chose the signal with the best amplitude; when transmitting, select the antenna where the best amplitude was received
- **Maximal radio combining** (MRC): combine multiple signals (e.g. when client is non-MIMO and AP is MIMO)
- IEEE802.11n uses switched diversity and MRC

IEEE802.11n: Transmit Beamforming

- **TxBF**: allows MIMO transmitter to focus the transmission of the multiples antennas in a coordinated way (= smart antenna)
- When multiples copies of the same signal are sent to the receiver, the phase is adjusted such that the signals arrive in-phase

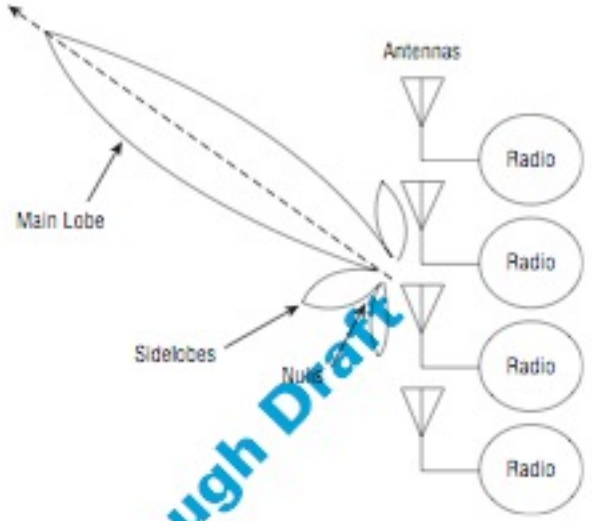


FIGURE 18.5 Transmit beamforming data

IEEE 802.11n: summary

- **MIMO (Multi-input Multi-Output):**
  n×m:k => n transmitters, m receivers, k streams
  k is the number parallel radio chains inside < # of Antennas => k times more throughput
  E.g., 2×2:2, 2×3:2, 3×2:2, 4×4:4
- **Diversity**: More receive antennas than the number of streams. Select the best subset of antennas.
- **Beam Forming**: Focus the beam directly on the target antenna
- **MIMO Power Save**: Use multiple antennas only when needed
- **Frame Aggregation**: Transmit multiple frames on each transmit opportunity => Less overhead => More throughput

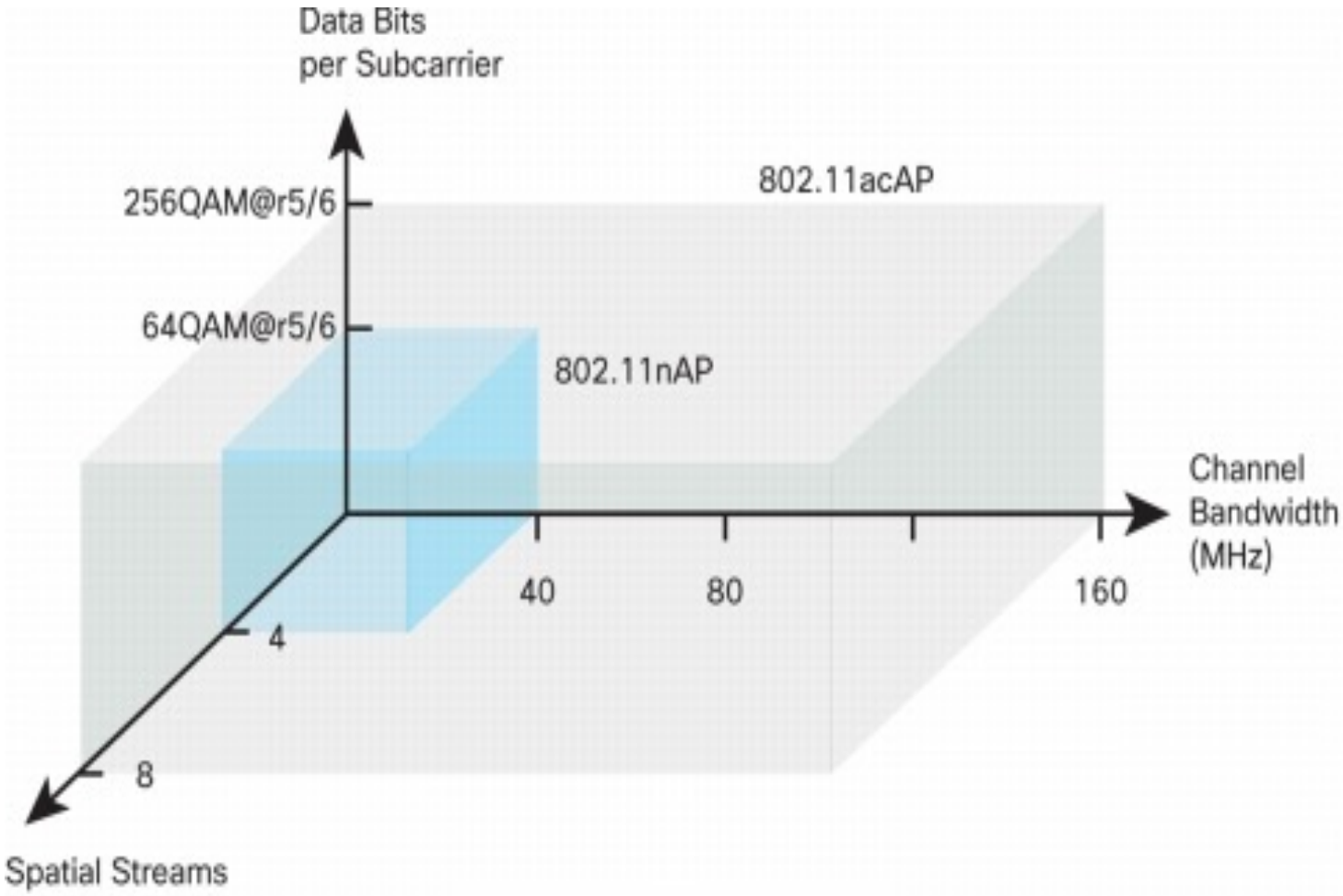
IEEE 802.11n: summary

- Lower FEC (**forward error correction**) Overhead: 5/6 instead of 3⁄4
- Reduced **Guard Interval**: 400 ns instead of 800 ns
- Reduced **Inter-Frame Spacing** (SIFS=2 µs, instead of 10 µs)
- Greenfield Mode: Optionally **eliminate support for a/b/g** (shorter and higher rate preamble)
- Dual Band: **2.4 and 5.8 GHz**
- Channel **Bonding**: Use two adjacent 20 MHz channels
- **More subcarriers**: 52+4 instead of 48+4 with 20 MHz, 108+6 with 40MHz
- Data rate: 4 Streams × 64-QAM × 5/6 FEC × 40 MHz and short interval 400 ns => **600 Mbps**

IEEE 802.11ac

- Improvements of 802.11n air interface:
  - **Wider bandwidth** (from 40MHz in 802.11n to 80 MHZ and even to 160 MHz)
  - **Up to 8 MIMO spatial streams**
  - High-density modulation scheme (from **64-QAM** in 802.11n up to **256-QAM**)
- First-wave 802.11ac products: 80 MHz, up to 433 Mbps (low end), 867 Mbps (midtier), or 1.3 Gbps (high end) at the physical layer.
- 2nd-generation products: **up to 3.47 Gbps.**

From 802.11n to 802.11ac



To summarize

IEEE 802.11 PHY Standards						
Release Date	Standard	Frequency Band (GHz)	Bandwidth (MHz)	Modulation	Advanced Antenna Technologies	Maximum Data Rate
1997	802.11	2.4 GHz	20 MHz	DSSS, FHSS	N/A	2 Mbits/s
1999	802.11b	2.4 GHz	20 MHz	DSSS	N/A	11 Mbits/s
1999	802.11a	5 GHz	20 MHz	OFDM	N/A	54 Mbits/s
2003	802.11g	2.4 GHz	20 MHz	DSSS, OFDM	N/A	542 Mbits/s
2009	802.11n	2.4 GHz, 5 GHz	20 MHz, 40 MHz	OFDM	MIMO, up to 4 spatial streams	600 Mbits/s
2013	802.11ac	5 GHz	40 MHz, 80 MHz, 160 MHz	OFDM	MIMO, MU-MIMO, up to 8 spatial streams	6.93 Gbits/s

IEEE 802.11 ax

- Efforts on **throughput enhancements** (e.g., 802.11n/ac/ad) focus **on theoretical peak throughput** in a single BSS environment.
- Increasingly more APs are deployed in crowded areas leading to overlapping BSSs in which inter-BSS **interference and collisions become more severe.**
- **IEEE 802.11ax aims to improve efficiency of spectrum usage by enhancing the area throughput** (bits/sec/m2) and average throughput per-user in both indoor and outdoor highly-dense deployment scenarios in multiple BSS environments.

	802.11ac	802.11ax
BANDS	5 GHz	**2.4 GHz** and 5 GHz
CHANNEL BANDWIDTH	20 MHz, 40 MHz, 80 MHz, 80+80 MHz & 160 MHz	20 MHz, 40 MHz, 80 MHz, 80+80 MHz & 160 MHz
FFT SIZES	64, 128, 256, 512	256, 512, 1024, 2048
SUBCARRIER SPACING	312.5 kHz	**78.125 kHz**
OFDM SYMBOL DURATION	3.2 us + 0.8/0.4 us CP	**12.8 us + 0.8/1.6/3.2 us CP**
HIGHEST MODULATION	256-QAM	**1024-QAM**
DATA RATES	433 Mbps (80 MHz, 1 SS) 6933 Mbps (160 MHz, 8 SS)	600.4 Mbps (80 MHz, 1 SS) 9607.8 Mbps (160 MHz, 8 SS)

802.11be under construction

TABLE 2. Main Innovations of IEEE 802.11be and Candidate Features.

Innovation \ Target	Nominal Throughput	Interference Mitigation	Spectrum Effeciency	Real-Time Applications
EHT PHY	4096 QAM, 320 MHz, 16x16 MU-MIMO		EHT Preamble	
EDCA with 802 TSN Features				IEEE 802 TSN, Faster Backoff, New Access Categories, TXOP capturing
Enhanced OFDMA		Preamble puncturing	Multi-RU, Direct links	Enhanced UORA
Multi-link Operation	Multi-link Architecture	Synchronous Channel Access	Virtual BSS	Asynchronous Channel Access, Packet Duplication, Queue Management, Dynamic Link Switching
Channel Sounding Optimization			Implicit Sounding, Explicit Feadback, Channel Estimation	
Advanced PHY	Full Duplex		HARQ, NOMA / SOMA	
Multi-AP Cooperation		Null steering, Co-OFDMA, CSR	Distributed MU-MIMO, Multi-AP Sounding	Joint Reception

Starting to look ever more like 5G NR

What are the steps?

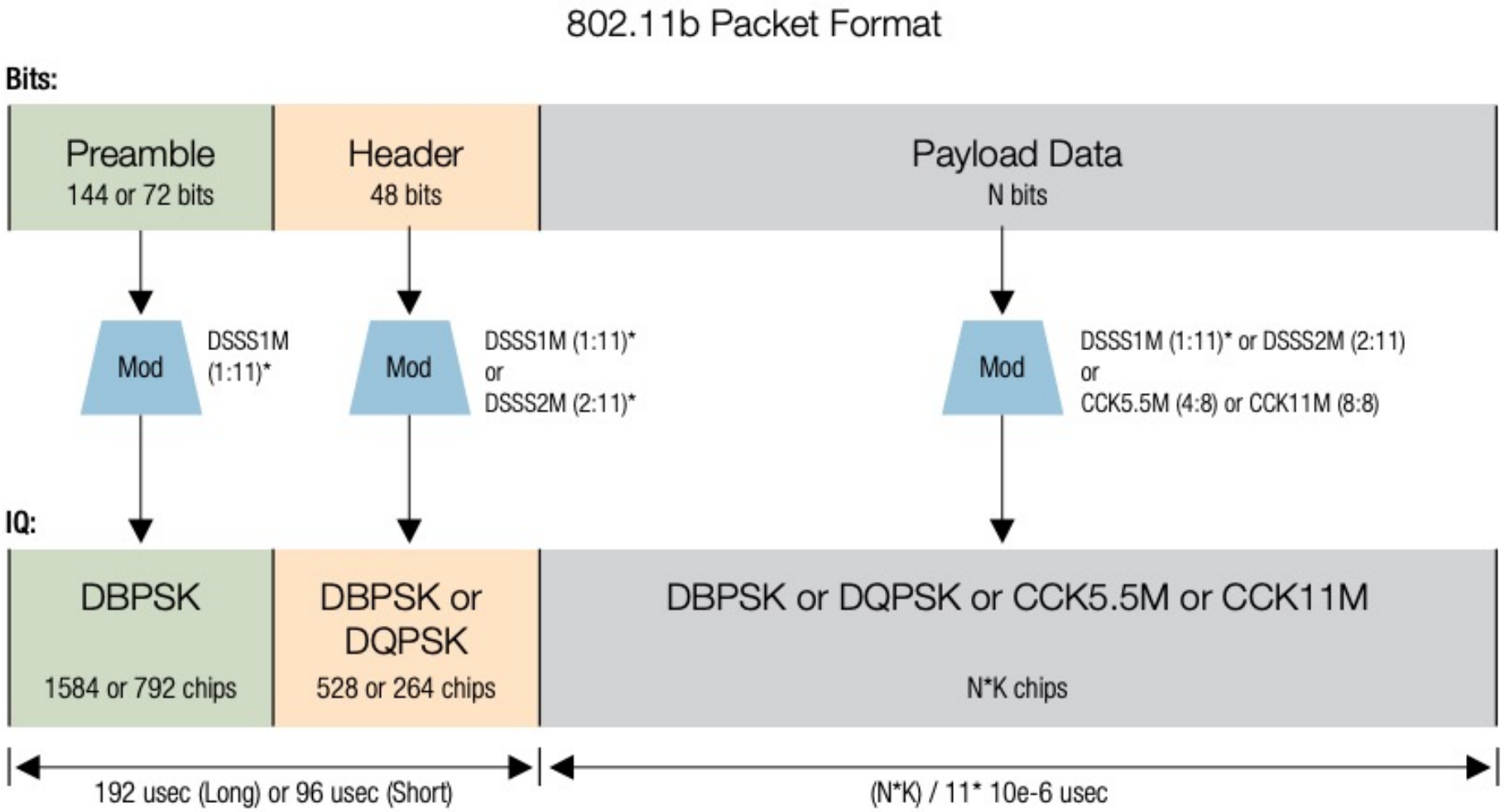
1. ~~Switch on the stations (& access points)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. Define how we are going to organize the bits for multiple users
5. Listen to synchronize and get system information
6. Random Access
7. Get a channel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

802.11 PHY Frame structure

- **The 802.11 Physical Layer uses bursted transmissions or packets. Each packet contains a Preamble, Header and Payload data. Each packet is for one user/station.**
  - The Preamble allows the receiver to obtain time and frequency synchronization and estimate channel characteristics for equalization. It is a bit sequence that receivers watch for to lock onto the rest of the transmission.
  - The Header provides information about the packet configuration, such as format, data rates, etc.
  - The Payload Data contains the user's payload data beingtransported.
- **The 802.11 standards define "frame" types for use in transmission of data as well as management and control of wireless links. At the top level these frames are divided into three functions:**
  - Management Frames
  - Control Frames
  - Data Frames.
- **Each frame consists of an MAC header, payload (some may not contain this) and frame check sequence (FCS).**
- **This of this as "self-contained" transmissions. Much as 5G NR now has. There is no constant broadcast of system information as in 3GPP**

https://www.cnrood.com/en/media/solutions/Wi-Fi_Overview_of_the_802.11_Physical_Layer.pdf

802.11b (and legacy) packet format



https://www.cnrood.com/en/media/solutions/Wi-Fi_Overview_of_the_802.11_Physical_Layer.pdf

802.11b (and legacy) packet format

802.11b Packet Format

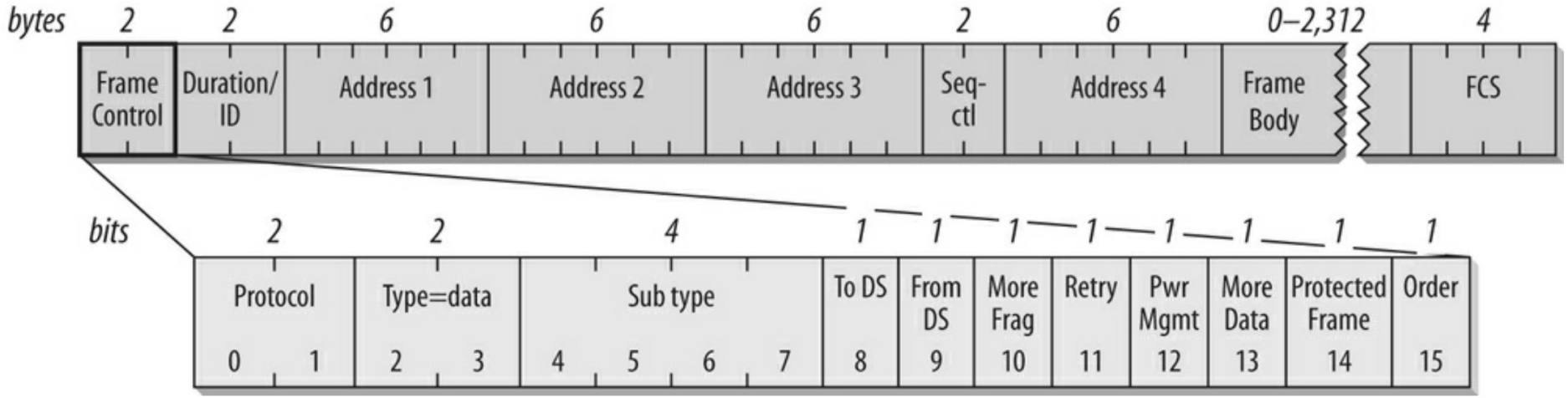
Bits:

802.11b Packet Format (refer to figure below)	
Preamble and Header	**Long** (required in original) **Short** (optional in "b")
Preamble	Always uses DSS1M Long Preamble contains 144 bits (128 scrambled 1's + 16 SFD marker bits) Short Preamble contains 72 bits (56 scrambled 0's + 16 SFD marker bits)
Header	Long Header uses DSSS1M, Short Header uses DSSS2M Contains 48 bits indicating configuration: SIGNAL (8 bits): indicates payload data rate (1, 2, 5.5 or 11 Mbps) SERVICE (8 bits): additional HR configuration bits LENGTH (16 bits): length of data Payload in microseconds CRC (16 bits): Protects header data contents
Payload	Payload data modulated with DSSS1M, DSSS2M, CCK5.5M, or CCK11M

802.11b		
Modulation	Symbol/Chip Ratio	Data Rate (Mbps)
DBPSK	1/11	1
DQPSK	1/5	2
DQPSK	1/2	5.5
BPSK	1/2	5.5
DQPSK	1	11
QPSK	1/2	11
8PSK	1	22
8PSK	1	33

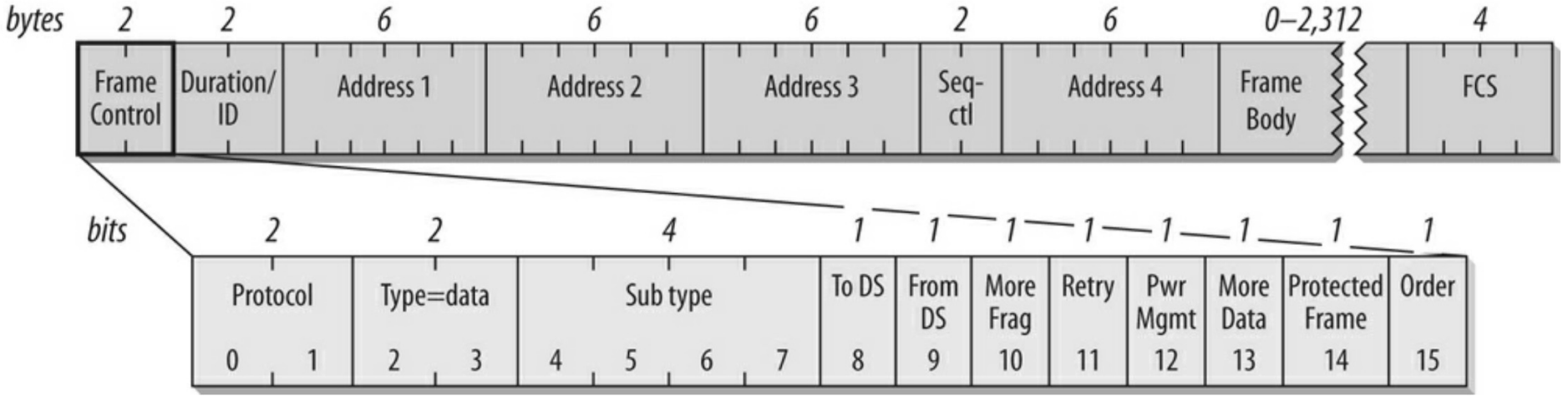
* (N:M) = (Nbits:Mchips), K= M / N

802.11 Payload = PSDU



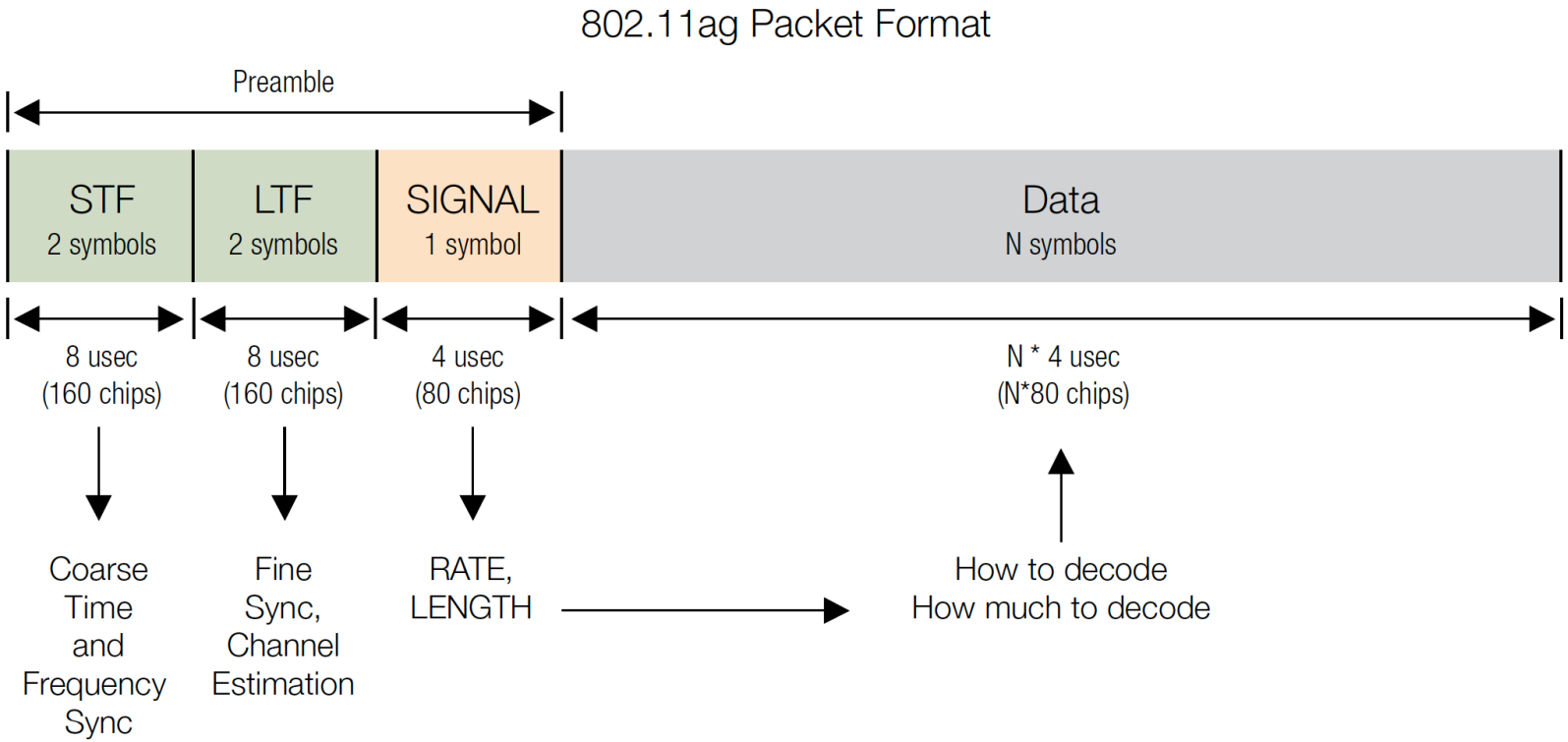
- **PLCP Service Data Unit** (Physical Layer Convergence Protocol SDU) — Generic frame contains:
  - **Protocol version**: Two bits indicate which version of the 802.11 MAC is contained in the rest of the frame. At present, only one version of the 802.11 MAC has been developed; it is assigned the protocol number 0. Other values will appear when the IEEE standardizes changes to the MAC that render it incompatible with the initial specification. So far, none of the revisions to 802.11 have required incrementing the protocol number.
  - **Type and subtype fields identify the type of frame** used. To cope with noise and unreliability, a number of management functions are incorporated into the 802.11 MAC.

802.11 Payload = PSDU



- **Duration;** to set NAV (used by RTS/CTS and in fragmentation mode)
  - Netwrok Allocation Vector – see later
- **Sequence numbers:** important against duplicated frames due to lost ACKs
- **To DS, From DS and Addresses**: see later
- 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

802.11a/g Packet Format



* (N:M) = (Nbits:Mchips), K= M / N

802.11a/g			
RATE	Modulation	FEC Rate	Data Rate (Mbps)
1101 (13)	BPSK	1/2	6
1111 (15)	BPSK	3/4	9
0101 (5)	QPSK	1/2	12
0111 (7)	QPSK	3/4	18
1001 (9)	16QAM	1/2	24
1011 (11)	16QAM	3/4	36
0001 (1)	64QAM	2/3	48
0011 (3)	64QAM	3/4	54

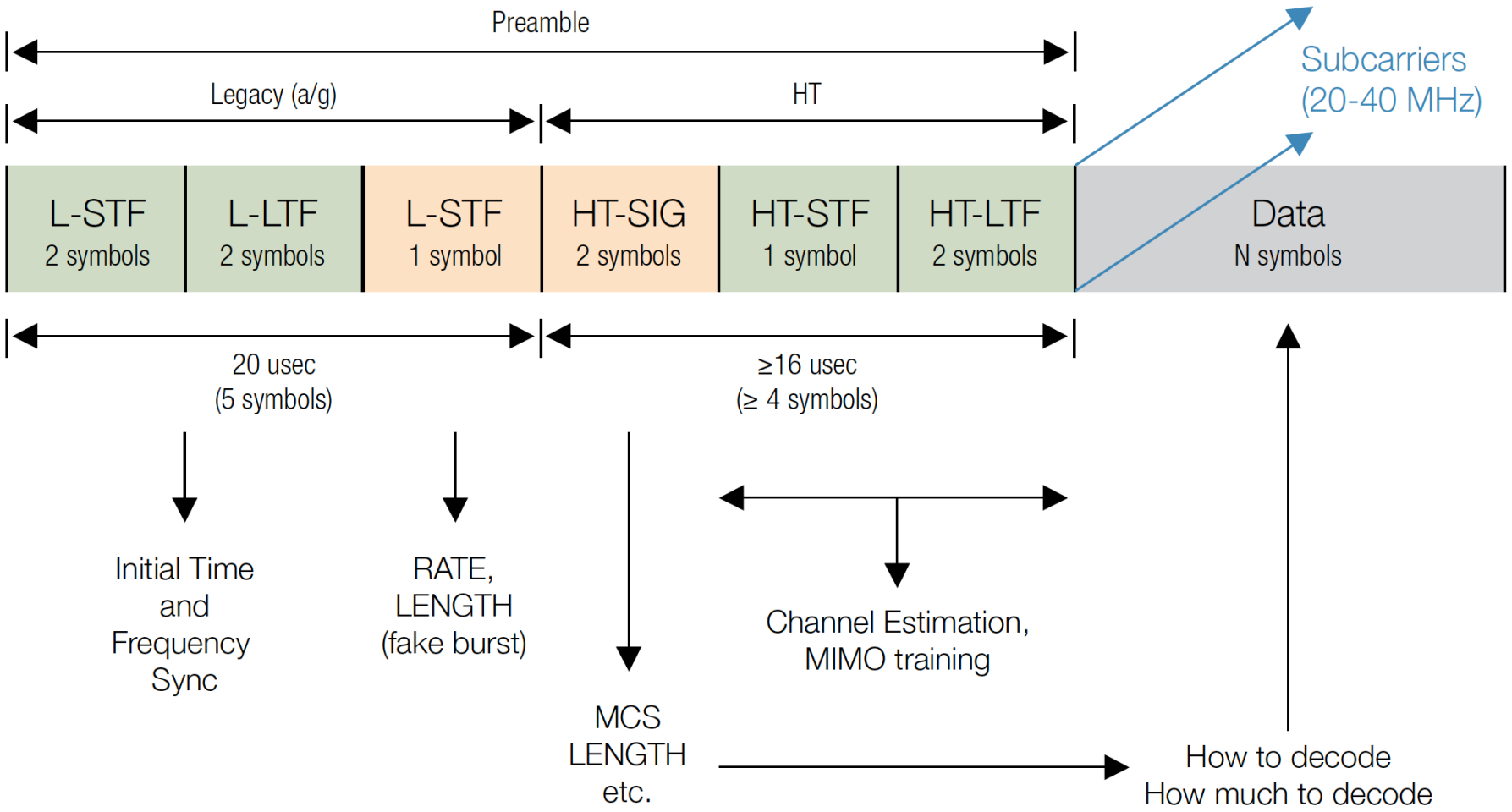
802.11a/g Packet Format

802.11a/g Packet Format (refer to figure below)	
Preamble	**STF:** Short Training Field (2 symbols) - Uses on 1/4 of subcarriers. Repeats every 16 chips. - Initial timing sync and frequency estimate. **LTF:** Long Training Field (2 symbols) - Uses all 52 subcarriers (same as Data symbols). - Fine timing and frequency sync, and channel response estimation. **SIGNAL:** (1 symbol) - Encoded similar to a Data symbol, but always uses BPSK modulation. 24 bits of configuration data. - Fields: - RATE (4 bits): Indicates Data FEC coding and modulation (8 combinations), aka "MCS" - LENGTH (12 bits): Number of octets (bytes) carried in Payload - PARITY (1 bit): Even parity-check on RATE+LENGTH data - TAIL (7 bits): Used for SIGNAL symbol FEC decoding
Payload	52 subcarriers, 48 Data + 4 Pilot Data subcarriers use BPSK, QPSK, 16QAM or 64QAM modulation. Same in all symbols Pilots subcarriers (BPSK only) are used to track frequency/phase and amplitude variations over the burst

802.11n Packet format (mixed)

Note: there is also a full non-HT AND HT mode

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

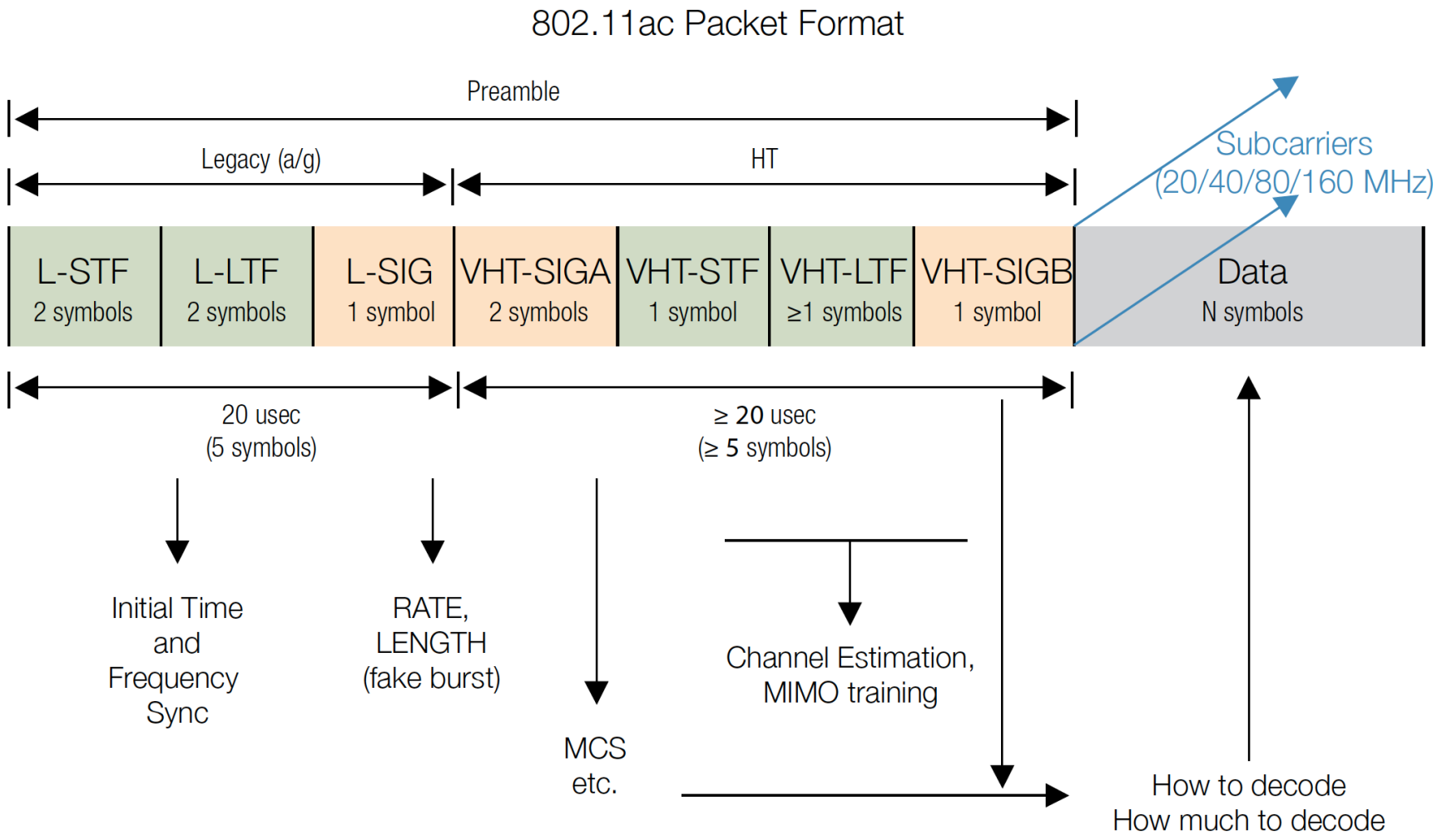


802.11n Packet format (mixed)

802.11n Packet Format (refer to figures on page 23)	
Preamble Mixed Mode	**Non-HT Legacy** L-STF, L-LTF, L-SIG are backward compatible to a/g systems L-SIG contains RATE and LENGTH values that inform Legacy systems how long to hold off next Tx attempt **HT Mixed Mode** HT-SIG (2 symbols): Indicates MCS (Modulation and Coding Scheme), Length, and other HT-specific parameters HT-STF (1 symbol), HT-LTF (≥1 symbol): Allow sync and channel estimation on HT bandwidth (more subcarriers than L-LTF). Additional HT-LTF symbols are included for MIMO modes to "sound" the multiple channels (paths)
Greenfield Mode	L-STF, L-LTF, L-SIG are dropped, HT-STF and HT-LTF replace L-STF/LTF Otherwise similar to MF Preamble - Fields: - RATE (4 bits): Indicates Data FEC coding and modulation (8 combinations), aka "MCS" - LENGTH (12 bits): Number of octets (bytes) carried in Payload - PARITY (1 bit): Even parity-check on RATE+LENGTH data - TAIL (7 bits): Used for SIGNAL symbol FEC decoding
Payload	56 (20 MHz) or 114 (40 MHz) subcarriers Data subcarriers use BPSK, QPSK, 16QAM, or 64QAM modulation. Same in all symbols Pilots subcarriers (BPSK only) are used to track frequency/phase and amplitude variations over the burst Optional Short Guard Interval can be used if multipath environment allows

The mandatory HT Mixed mode will be the most common 802.11n AP operating mode. In this mode, HT enhancements can be used simultaneously with HT Protection mechanisms that permit communication with legacy stations. HT Mixed mode provides backwards compatibility, but 802.11n devices pay significant throughput penalties as compared to Greenfield mode.

802.11ac Packet format



802.11ac Packet format

802.11ac Packet Format (refer to figure below)	
Preamble	Single Preamble format, no Greenfield type
Legacy Mode	L-STF, L-LTF, L-SIG are backward compatible to a/g systems L-SIG contains RATE and LENGTH values that inform Legacy systems how long to hold off next Tx attempt
VHT Mode	VHT-SIGA (2 symbols): Indicates MCS (Modulation and Coding Scheme), and other VHT-specific parameters VHT-STF (1 symbol), VHT-LTF (≥1 symbol): Allow sync and channel estimation on VHT bandwidth (more subcarriers than L-STF/L-LTF). Additional VHT-LTF symbols are included for MIMO configs to "sound" the multiple channels (paths) VHT-SIGB (1 symbol): Length parameters, MU-MIMO support
Payload	56/114/242/484 (20/40/80/160 MHz) subcarriers (Data + Pilot) Data subcarriers use BPSK, QPSK, 16QAM, 64QAM or 256QAM modulation. Same in all symbols Pilots subcarriers (BPSK only) are used to track frequency/phase and amplitude variations over the burst Optional Short Guard Interval can be used if multipath environment allows

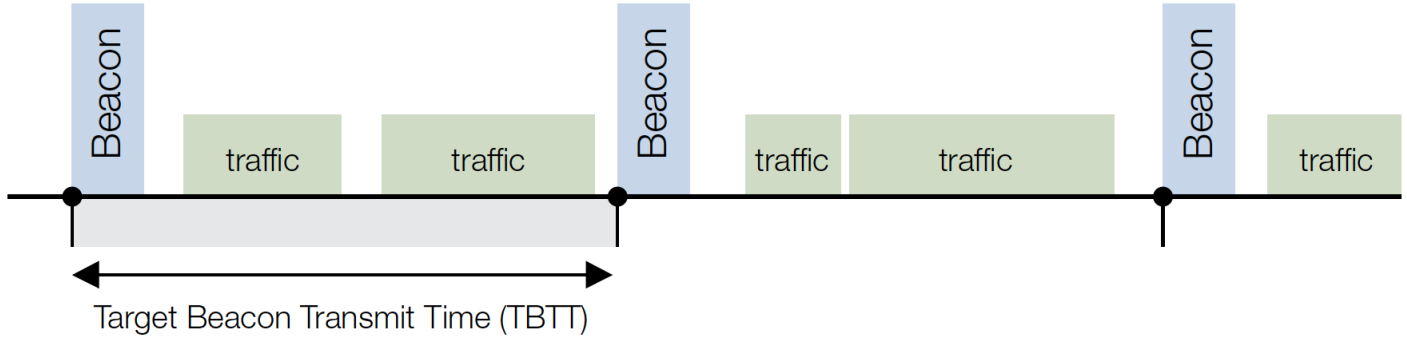
802.11ac MCS

Modulation Coding Scheme and Forward Error Correction Rate for 802.11ac						
MCS	Modulation	FEC Rate	Data Rate			
			20 MHz (Mbps)	40 MHz (Mbps)	80 MHz (Mbps)	160 MHz (Mbps)
0	BPSK	1/2	7.2	15.0	32.5	65.0
1	QPSK	1/2	14.4	30.0	65.0	130.0
2	QPSK	3/4	21.7	45.0	97.5	195.0
3	16QAM	1/2	28.9	60.0	130.0	260.0
4	16QAM	3/4	43.3	90.0	195.0	390.0
5	64QAM	2/3	57.8	120.0	260.0	525.0
6	64QAM	3/4	65.0	135.0	292.5	585.0
7	64QAM	5/6	72.2	150.0	325.0	650.0
8	256QAM	3/4	86.7	180.0	390.0	780.0
9	256QAM	5/6	N/A	200.0	433.3	866.7

What are the steps?

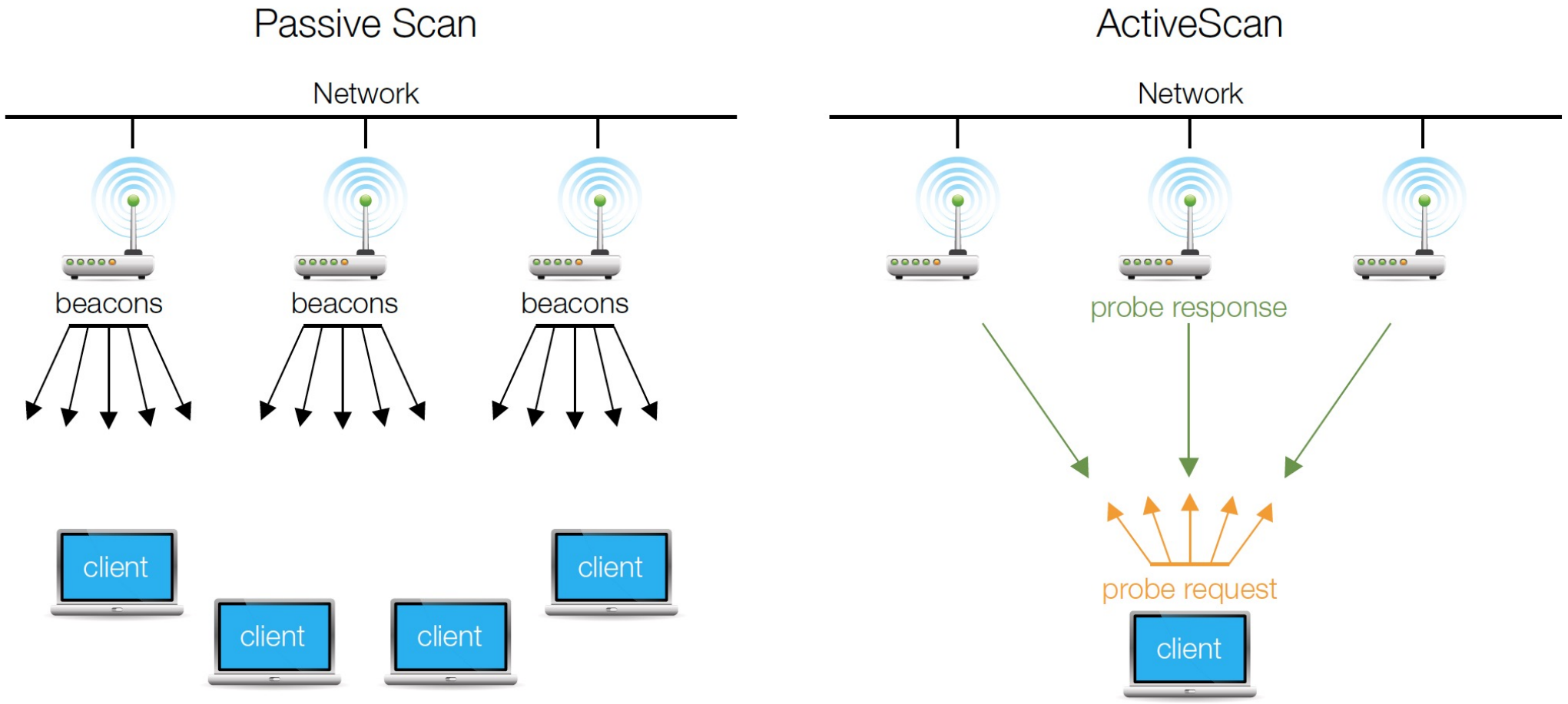
1. ~~Switch on the stations (& access points)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. ~~Define how we are going to organize the bits for multiple users~~
5. Listen to synchronize and get system information
6. Random Access
7. Get a channel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

Beacons



- **IEEE 802.11 specifies Timing Synchronization Function (TSF)**
- Power management (see later)
- **Coordination**
- **In a BSS**
  - Use of beacon
  - **Beacon contains timestamp and other mngt information (power mngt, roaming)**
  - **Used by STA to adjust its local clock**
  - Beacon not periodic (deferred when medium is busy)
- **In infrastructure mode**: AP tries to schedule beacon according to expected beacon interval (= target beacon transmission time); time stamp in the beacon is the real transmit time, not the scheduled time

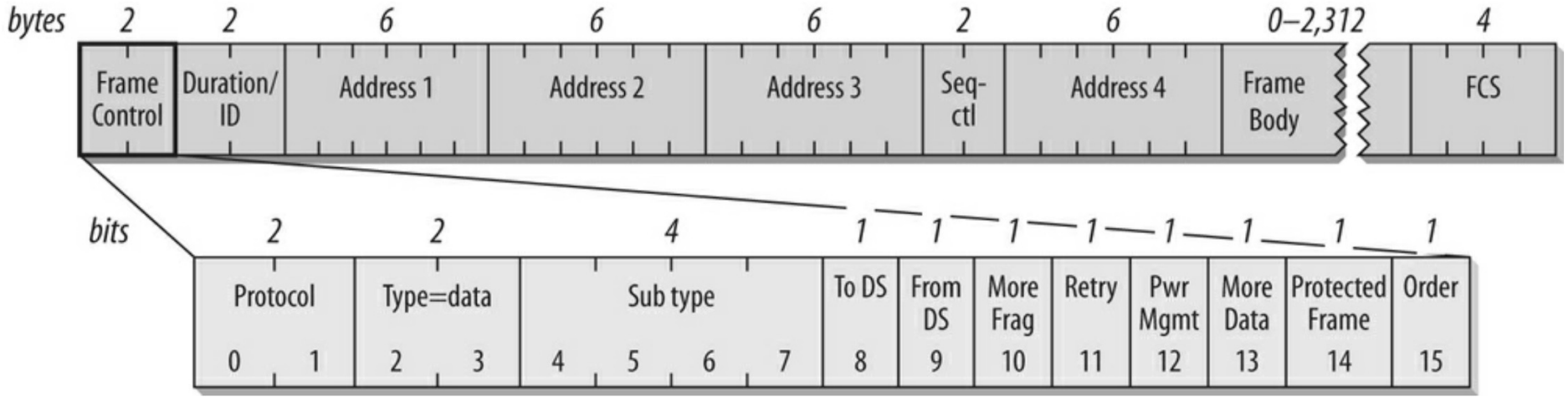
2 scanning approaches



Scanning

- **Passive Scanning uses Beacons.**
  - After selecting a channel, the scanning device listens for Beacons. In the case of passive scanning the client just waits to receive a Beacon Frame from the AP. A Beacon is transmitted from an AP and contains information about the AP along with a timing reference. Like other transmissions, they are subject to a clear channel test and so may be delayed. The device searches for a network by just listening for beacons until it finds a suitable network to join.
- **Active Scanning** sees the device trying to locate an AP by transmitting Probe Request Frames
  - Waits for Probe Response from the AP. Listening for a clear channel, the device which seeks to establish contact sends a Probe Request. The probe request frame can be a directed or a broadcast probe request. The probe response frame from the AP is similar to the beacon frame. Based on the response from the AP, the client makes a decision about connecting to the AP. **While active scanning is a faster way to establish contact, it consumes more battery power.**

802.11 Payload = PSDU



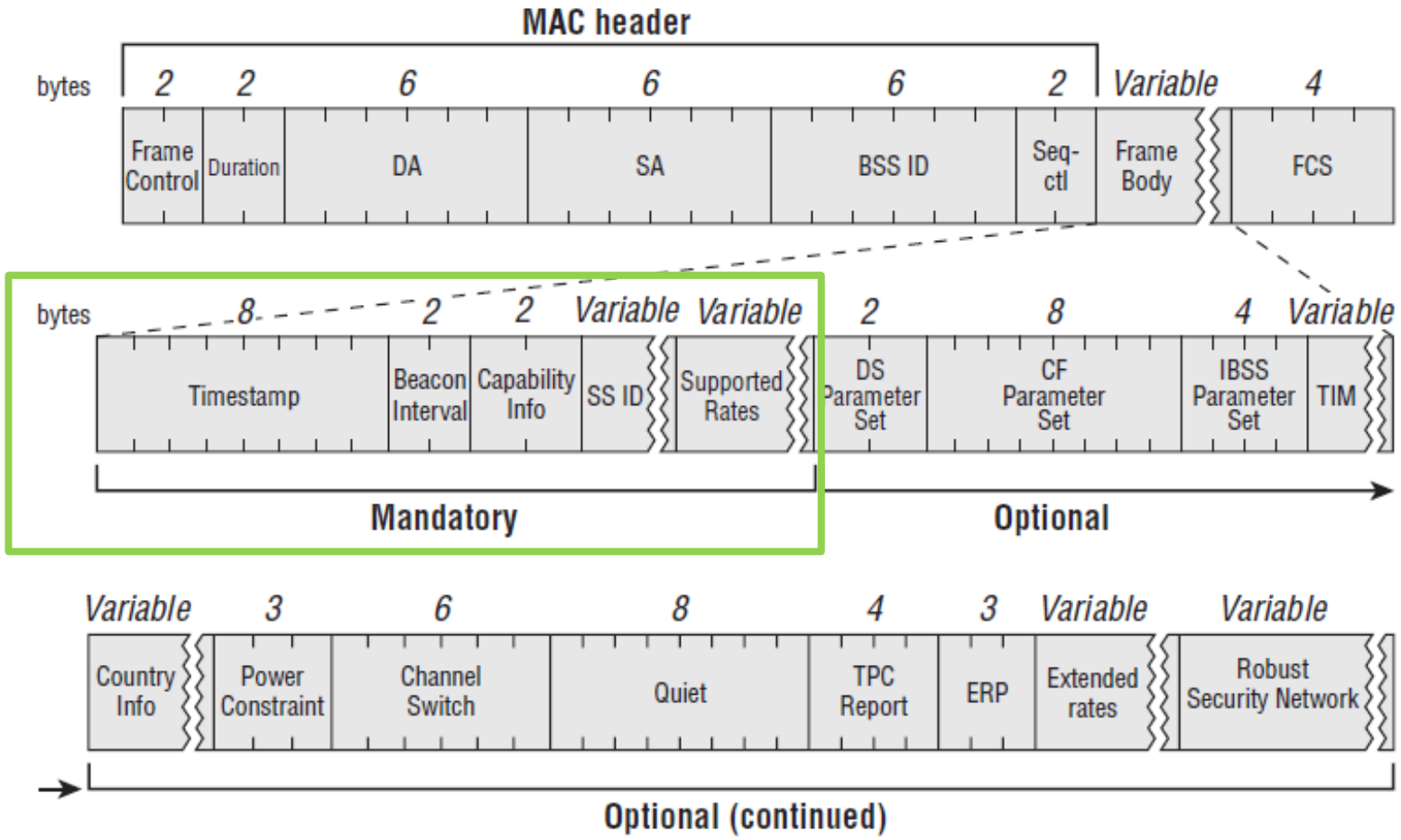
- **PLCP Service Data Unit** (Physical Layer Convergence Protocol SDU) — Generic frame contains:
  - **Protocol version**: Two bits indicate which version of the 802.11 MAC is contained in the rest of the frame. At present, only one version of the 802.11 MAC has been developed; it is assigned the protocol number 0. Other values will appear when the IEEE standardizes changes to the MAC that render it incompatible with the initial specification. So far, none of the revisions to 802.11 have required incrementing the protocol number.
  - **Type and subtype fields identify the type of frame** used. To cope with noise and unreliability, a number of management functions are incorporated into the 802.11 MAC.

Frame Control : Type and Sub-Type

- **Type**
  - 0 0 Management Frame
  - 0 1 Control Frame
  - 1 0 Data Frame
  - 1 1 Reserved
- **Sub-Type**
  - Management: Association Req, Resp; Reassociation Req, Resp; Disassociation; Probe Req, Resp; **Beacon**; ATIM; Authentication; Deauthentication
  - Control: PS Poll; RTS; CTS; ACK; CF End; CF End + CF ACK
  - Data: Data; Data + CF Ack; Data + CF Poll; Data + CF ACK + CF Poll; CF ACK; CF Poll; CF ACK + CF Poll

Beacon Frame

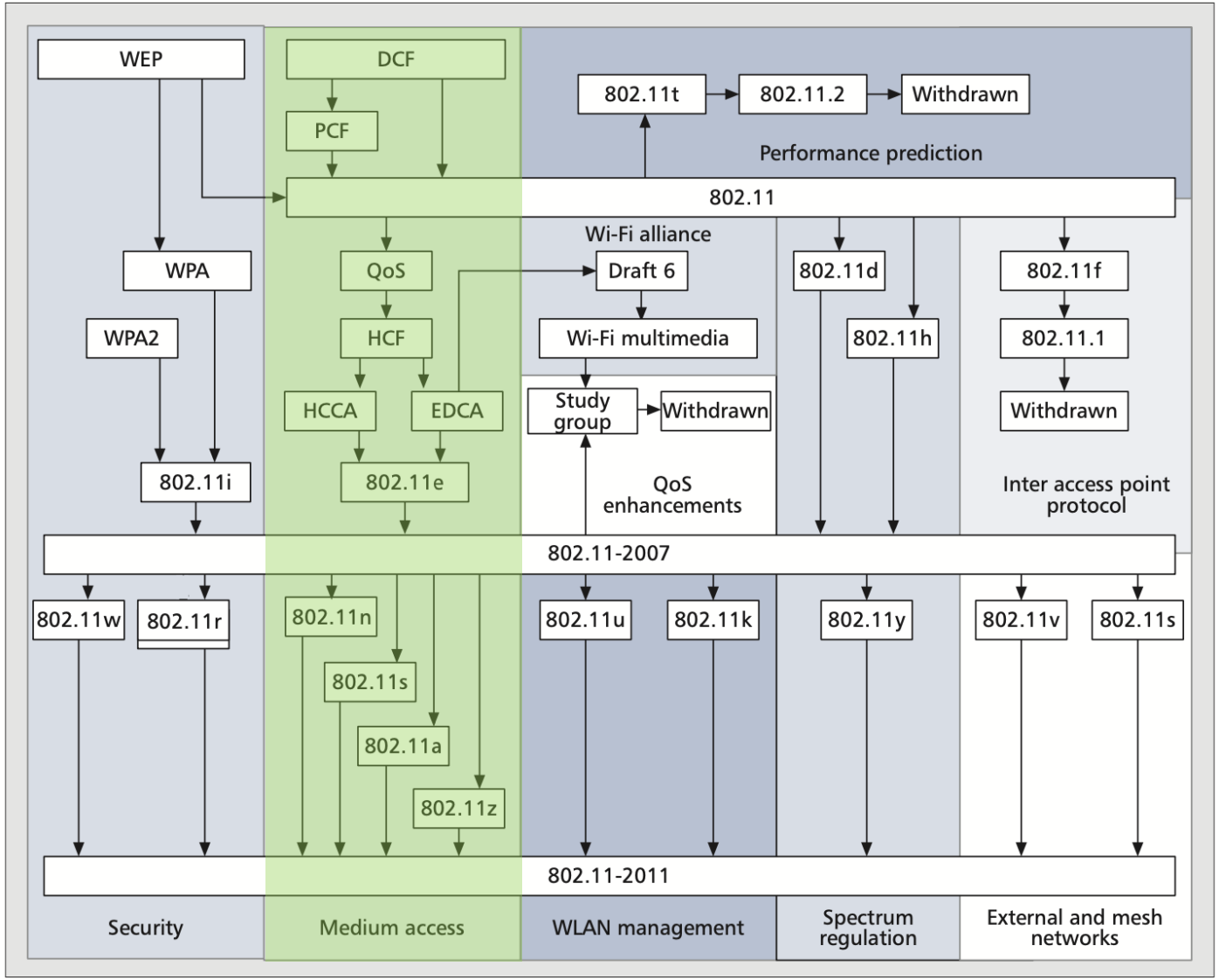
FIGURE 4.5 Beacon frame structure



What are the steps?

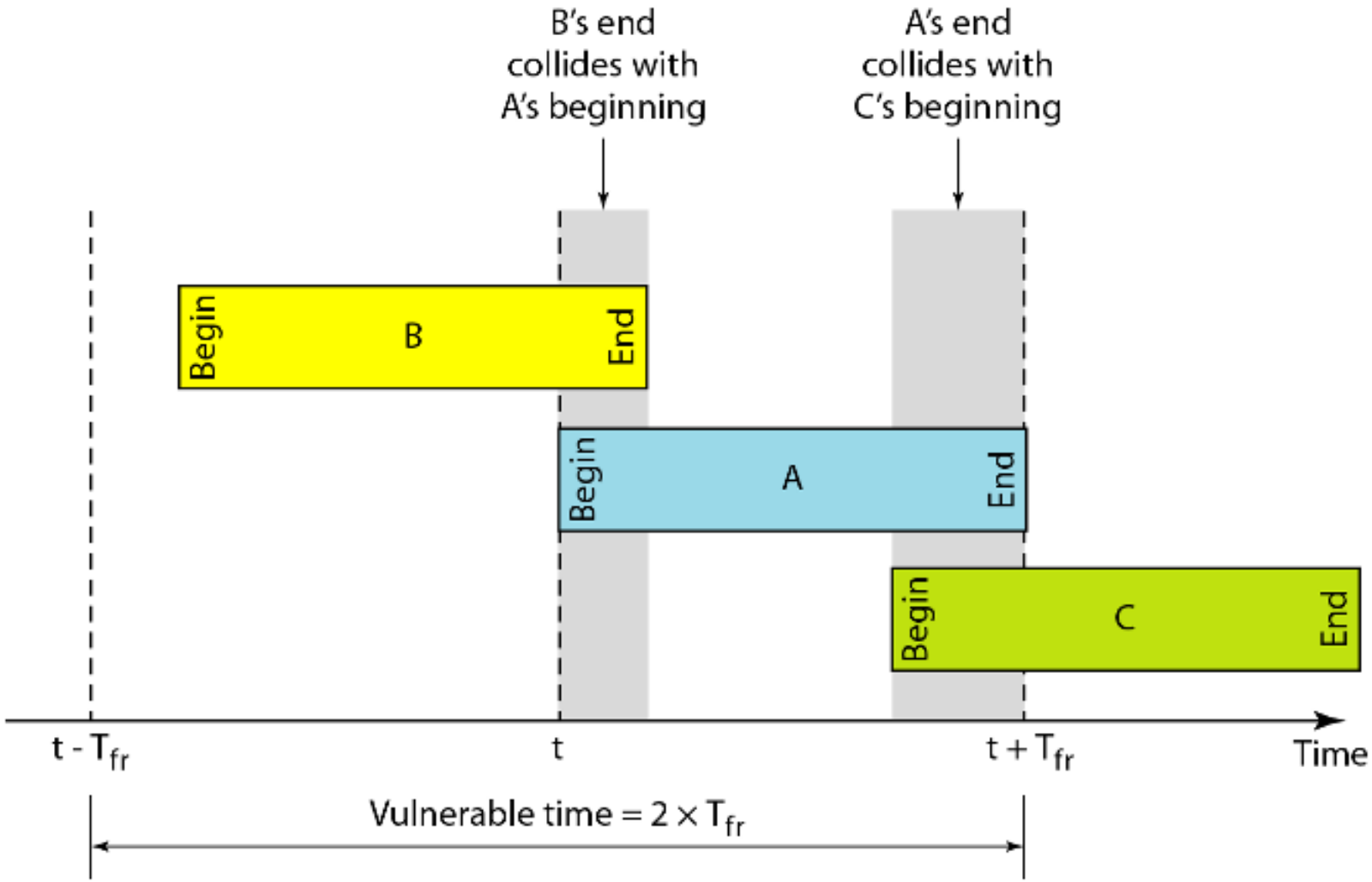
1. ~~Switch on the stations (& access points)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. ~~Define how we are going to organize the bits for multiple users~~
5. ~~Listen to synchronize and get system information~~
6. Random Access
7. Get a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

IEEE 802.11 MAC

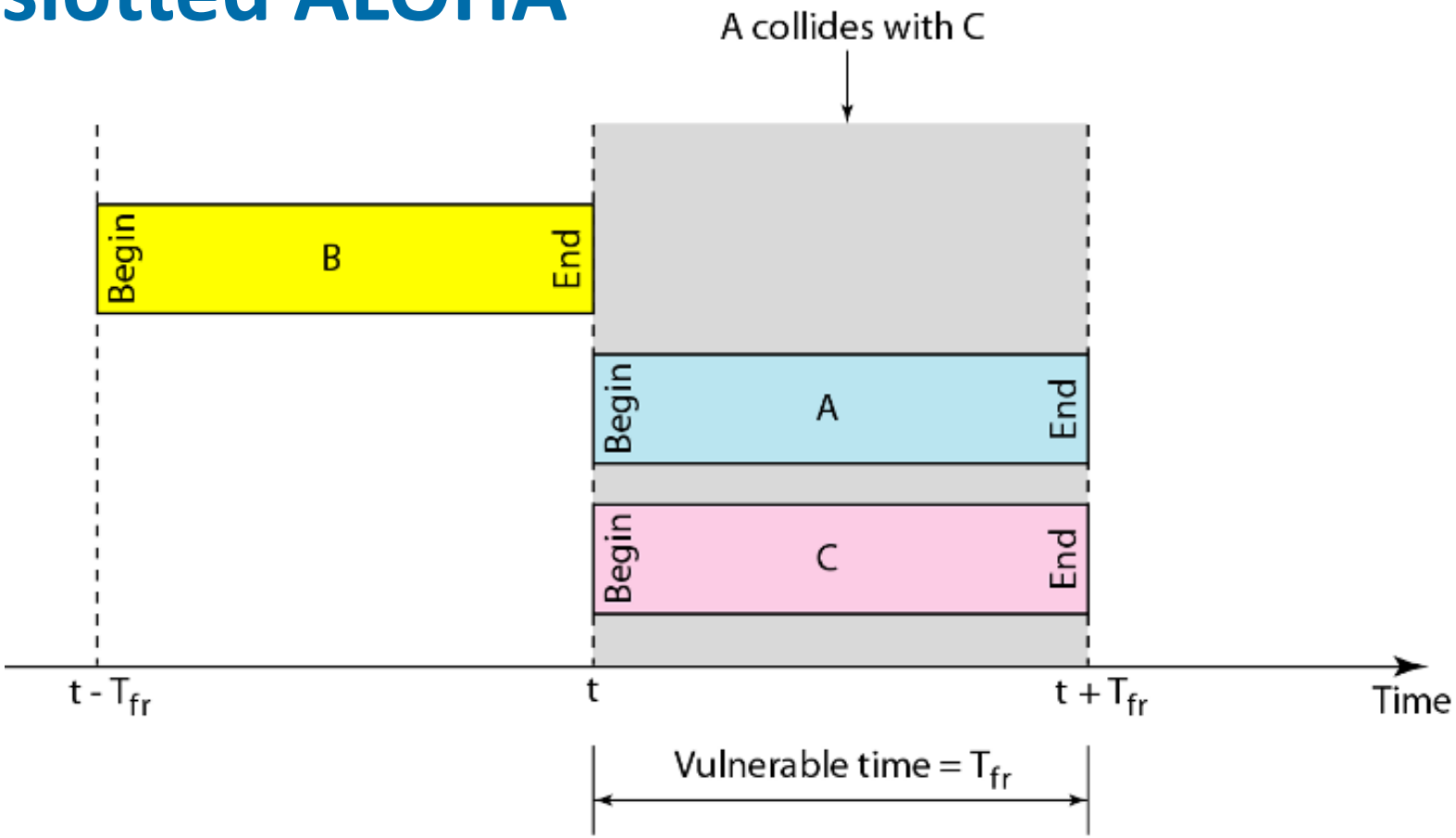


“Distributed Coordination Function”

Refresh: unslotted ALOHA

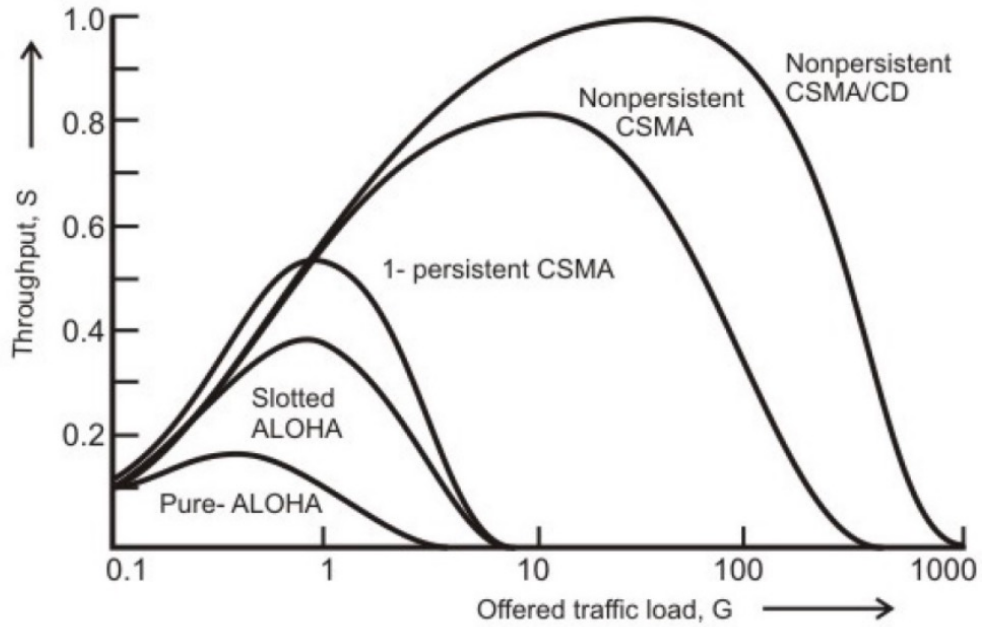


Refresh: slotted ALOHA



802.11 MAC will build on this + channel persistence to create the access mechanism (CSMA/CA). Key for now is that we use frames that can only be transmitted at certain times.

Basics CSMA/CA vs. CSMA/CD



- Carrier-sense multiple access with collision detection
  - CSMA/CD is used to improve CSMA performance by terminating transmission as soon as a collision is detected, thus shortening the time required before a retry can be attempted. 1-persistent CSMA/CD is used by Ethernet.
- Carrier-sense multiple access with collision avoidance
  - In CSMA/CA collision avoidance is used to improve the performance of CSMA. If the transmission medium is sensed busy before transmission, then the transmission is deferred for a random interval. This random interval reduces the likelihood that two or more nodes waiting to transmit will simultaneously begin transmission upon termination of the detected transmission, thus reducing the incidence of collision. CSMA/CA is used by Wi-Fi.

Calculation of throughput (1)

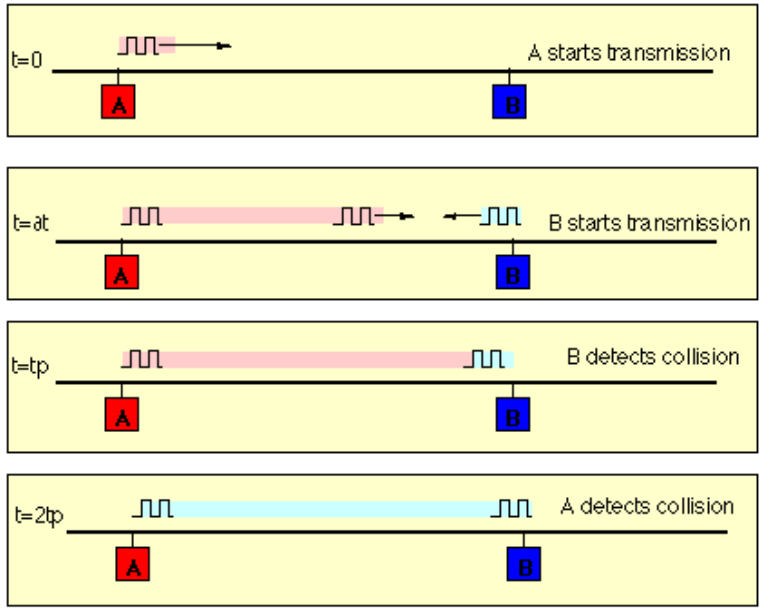
- **Assume frame duration T**
  - number of bits per frame/rate
- **Assume N frames are offered per T from an infinite number of STA**
  - Poisson distributed, average N
  - If N>1, we get collisions all the time, so we add retransmissions
- **Assume G frames + retransmissions**
  - Again Poisson, average G
  - For small G, G is approx. N
- **Throughput $S = G.P_0$**
  - with P_0 the chance of success

Calculation of throughput (2)

- **Chance that k packets are transmitted in one frame duration T**
  - $P(k) = \frac{G^k e^{-G}}{k!}$
- **Chance that no packets are transmissed in one frame duration T**
  - $P(0) = e^{-G}$
- **Chance that no packets are transmissed in two frame duration T**
  - $P(0,0) = e^{-2G}$ (as they are independent)
- **Hence, throughput**
  - Unslotted: S = G.P0 = $G.e^{-2G}$ and max is about 18%
  - Slotted: S = G.P0 = $G.e^{-G}$ and max is about 36%

CSMA/CD

- **Carrier Sense Multiple Acces Collision Detect**



- **Used in Ethernet, needs**
  - full duplex trx
  - everyone can hear everyone
  - Inter frame gap to make sure we wait long enough to propagate
  - => impossible in some scenarios for a pair of contending wireless senders to observe a collision event. This happens for instance when the two sending nodes are at opposite extreme of coverage of a wireless access point: Although they share the same medium, one node is hidden from another.

CSMA/CA

- **Carrier Sense Multiple Acces Collision Avoid**
- **Used in WiFi, but**
  - half duplex trx
  - not everyone needs to hear everyone
  - a node is required to sense the activity of the wireless medium before transmitting (listen before talk). I
  - random backoff waiting time is introduced to avoid synchronisation in this decentralised system.
  - carrier sense may fail (due to propagation, mixed PHY, …) → additional mechanisms needed (request-to-send/clear-to-send)

IEEE 802.11 - MAC layer - DFWMAC

- **4 services**
  - **Asynchronous Data Service** (mandatory)
    - exchange of data packets based on “best-effort”
    - support of broadcast and multicast
  - ~~Time-Bounded Service (optional)~~
    - ~~implemented using PCF (Point Coordination Function) – not used~~
  - **QoS** (added later)
  - **TSN** (time-sensitive networking) under construction, brand new
- **Access methods: DFW (Distributed Foundation Wireless MAC)**
  - DFWMAC-DCF CSMA/CA: Distributed Coordination Function (mandatory)
    - collision avoidance via randomized „back-off“ mechanism
    - minimum distance (xIFS) between consecutive packets
    - ACK packet for acknowledgements (not for broadcasts)
  - DFWMAC-DCF w/ RTS/CTS (optional)
    - avoids hidden terminal problem
  - ~~DFWMAC- PCF: Point Coordination Function (optional)~~
    - ~~access point polls terminals according to a list~~

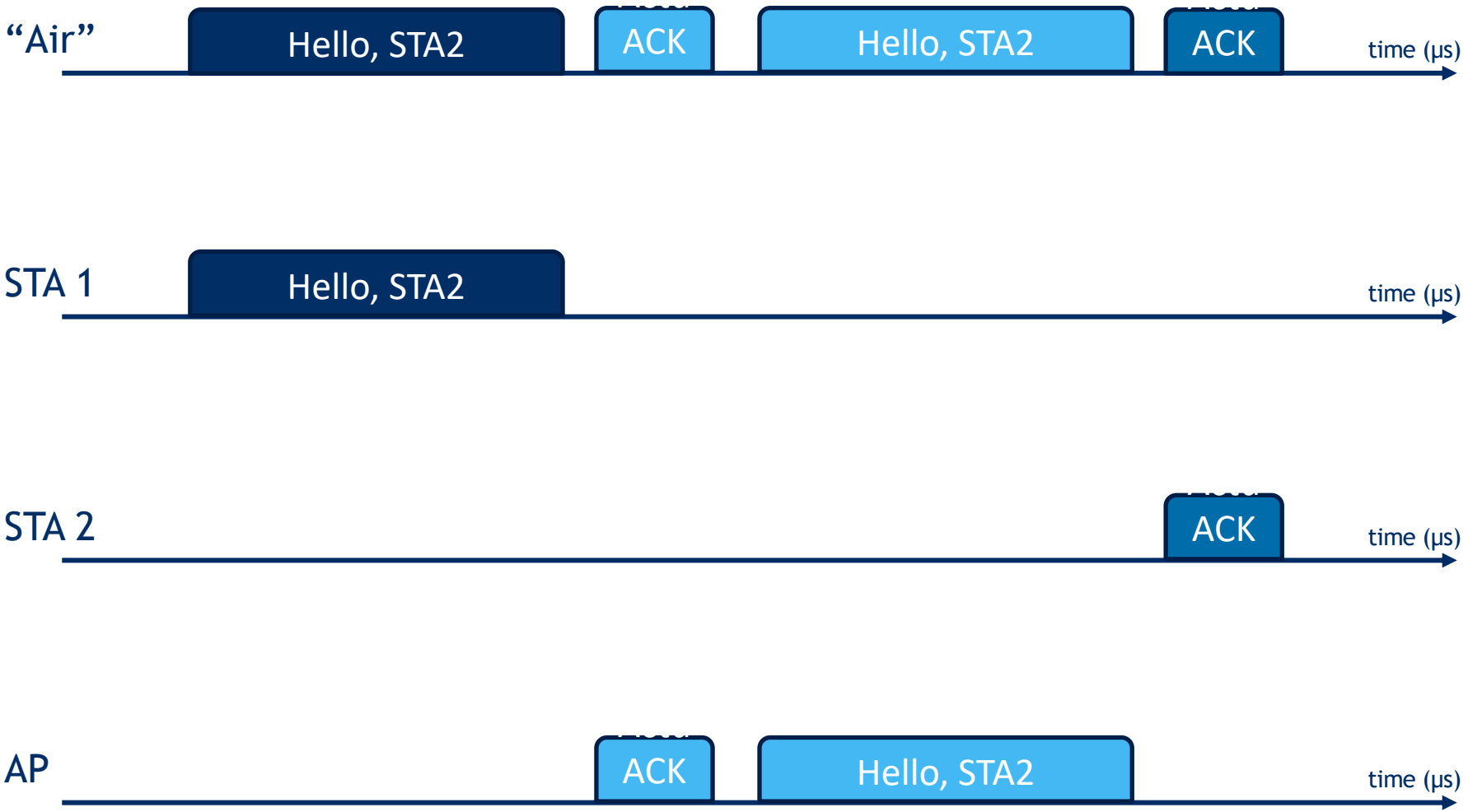
Important timing parameters

- Slots: ~ advantage of slotted ALOHA
- DIFS = DCF Interframe spacing = SIFS + (2×Slot Time)
  - SIFS = Short Interframe spacing = “shortest”
  - DIFS = “standard” wait needed for “normal” frames

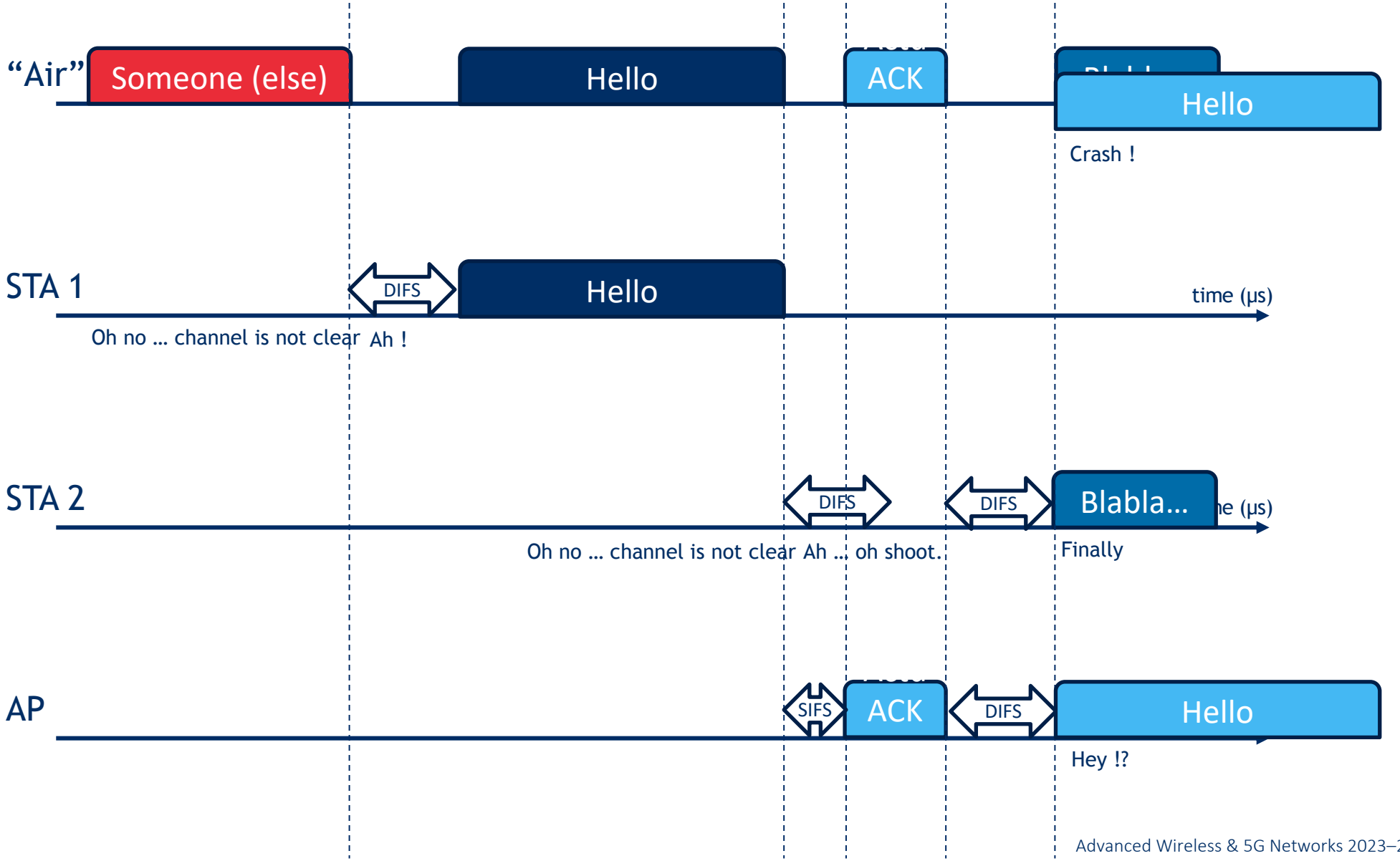
Standard	Slot time (µs)	SIFS (µs)	DIFS (µs)
IEEE 802.11 (DSSS)	20	10	50
IEEE 802.11b	20	10	50
IEEE 802.11a	9	16	34
IEEE 802.11g	9 or 20	10	28 or 50
IEEE 802.11n (2.4 GHz)	9 or 20	10	28 or 50
IEEE 802.11n (5 GHz)	9	16	34
IEEE 802.11ac (5 GHz)	9	16	34
IEEE 802.11ax	9	16	34

This is one potential way to differentiate QoS: use additional xIFS

Timing chart STA1->STA2 (simplified/wrong)

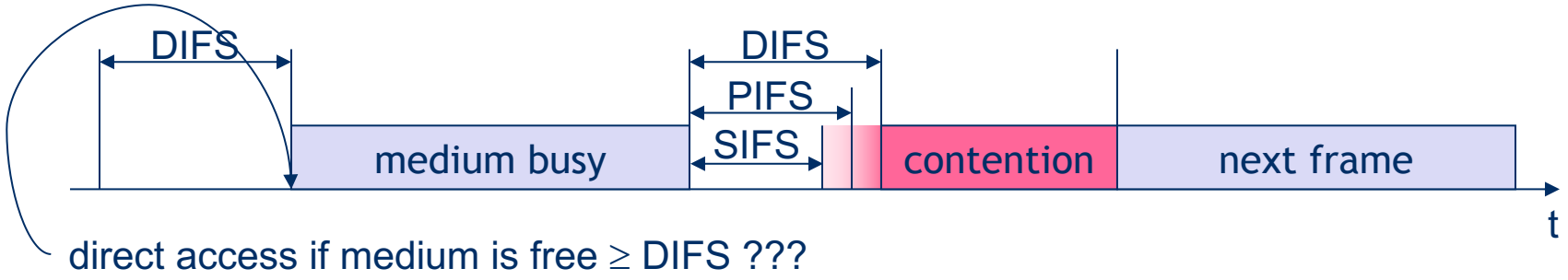


Timing chart STA1->STA2 (better)



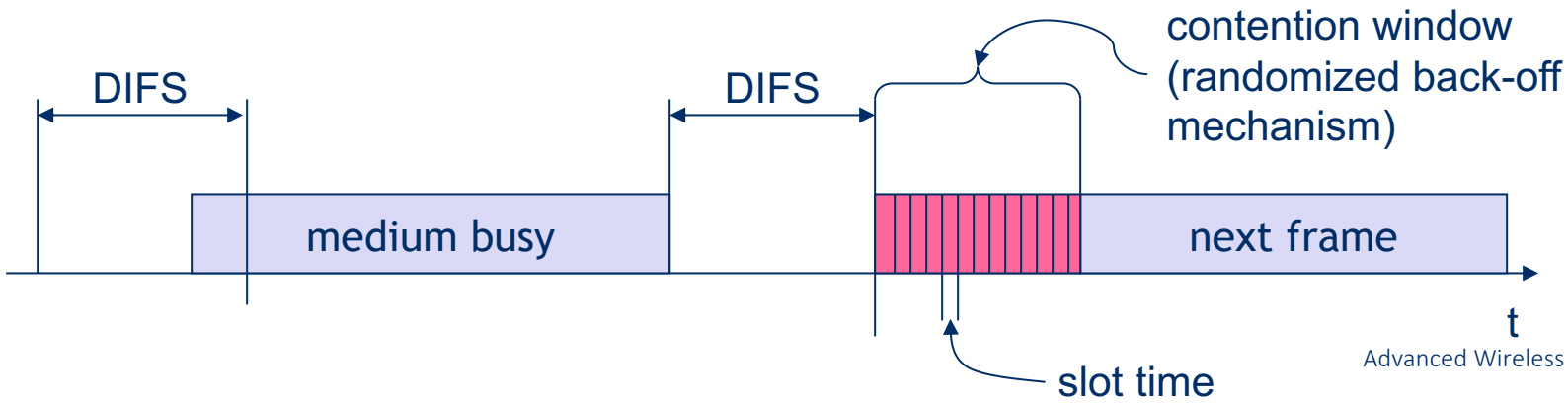
IEEE 802.11 - MAC layer - IFS

- **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

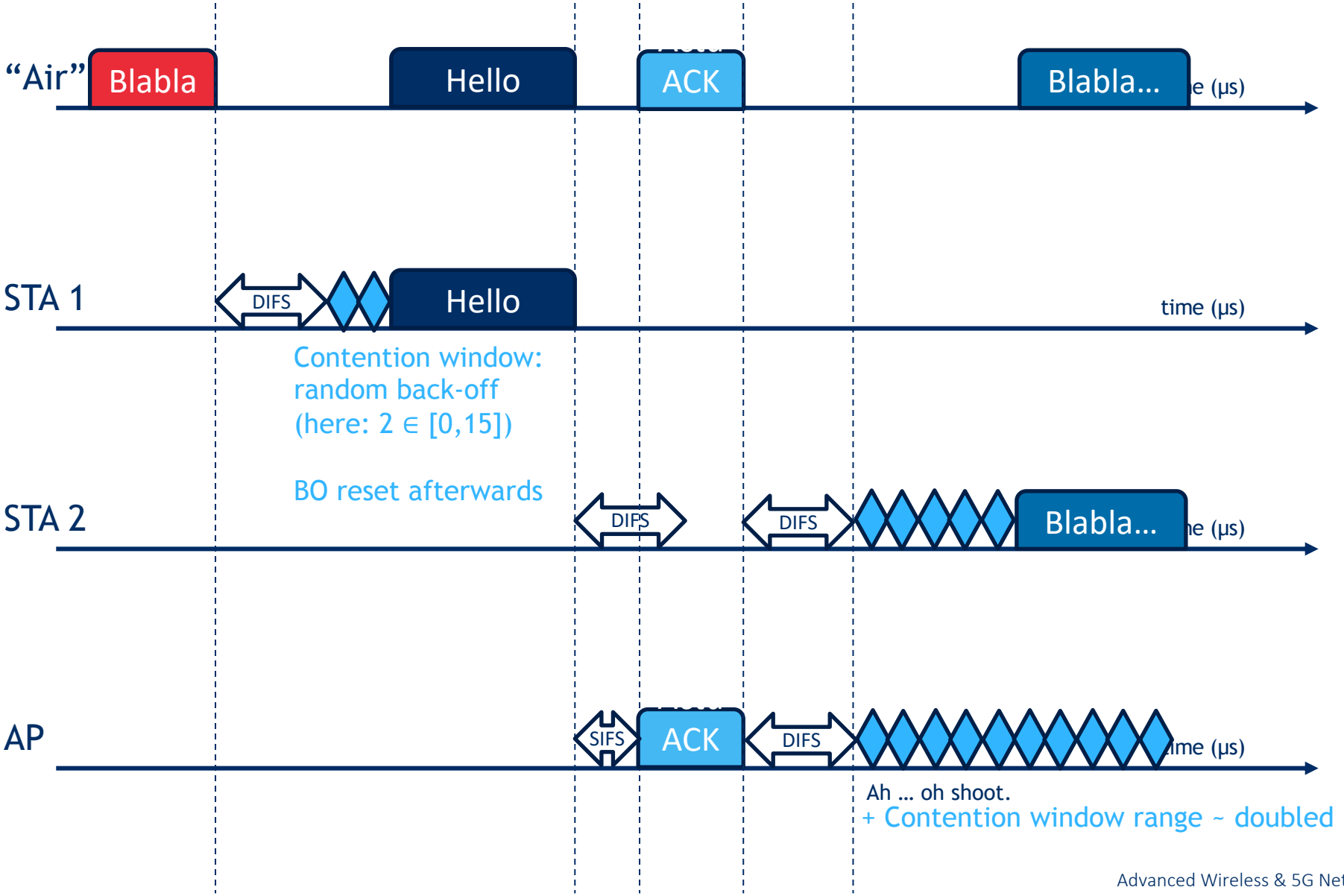


Contention Window CW

- station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment) + Virtual Carrier sense.
- 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)



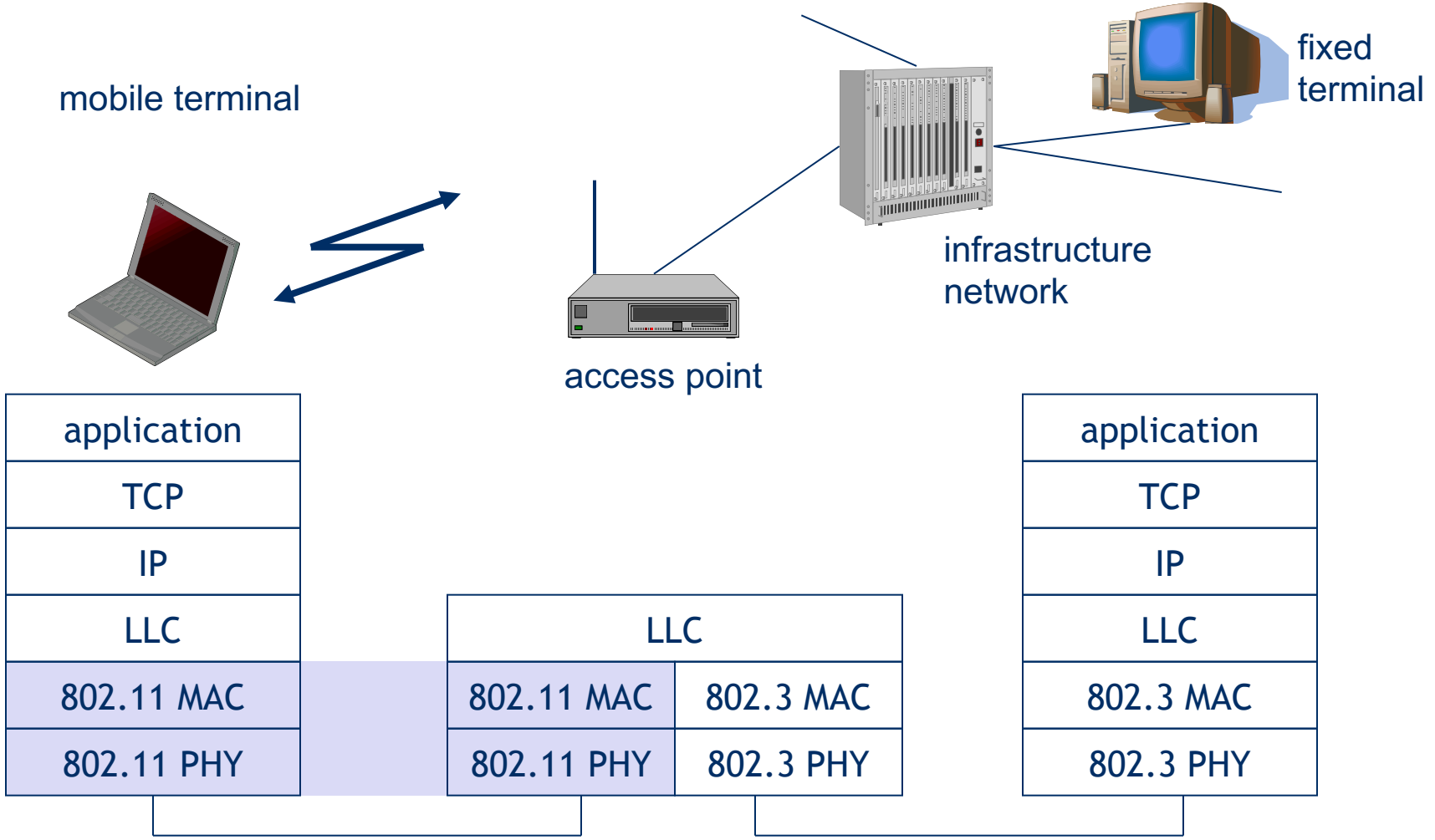
Timing chart STA1->STA2 (almost there…)



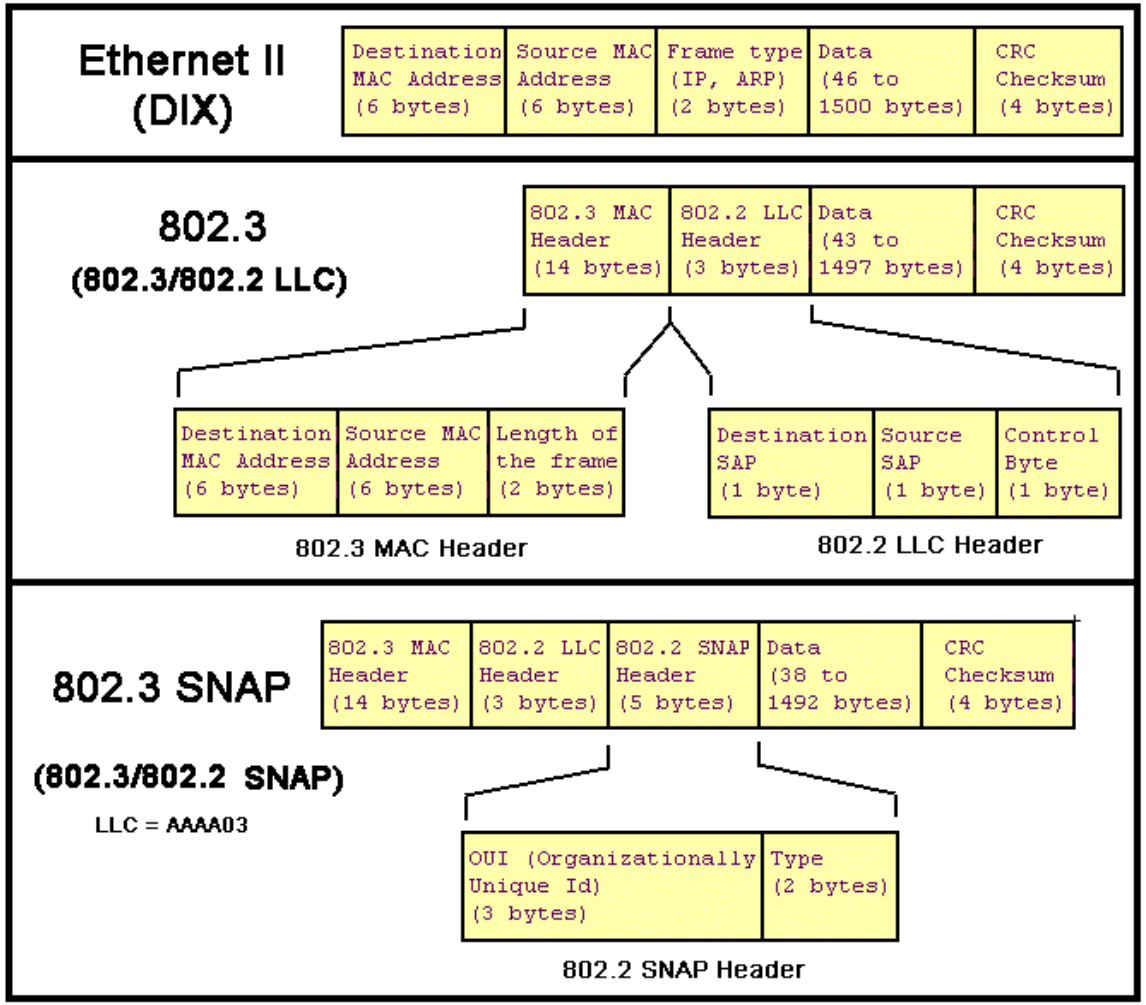
ESS = link layer domain= layer 2

- 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 MAC and PHY Layer

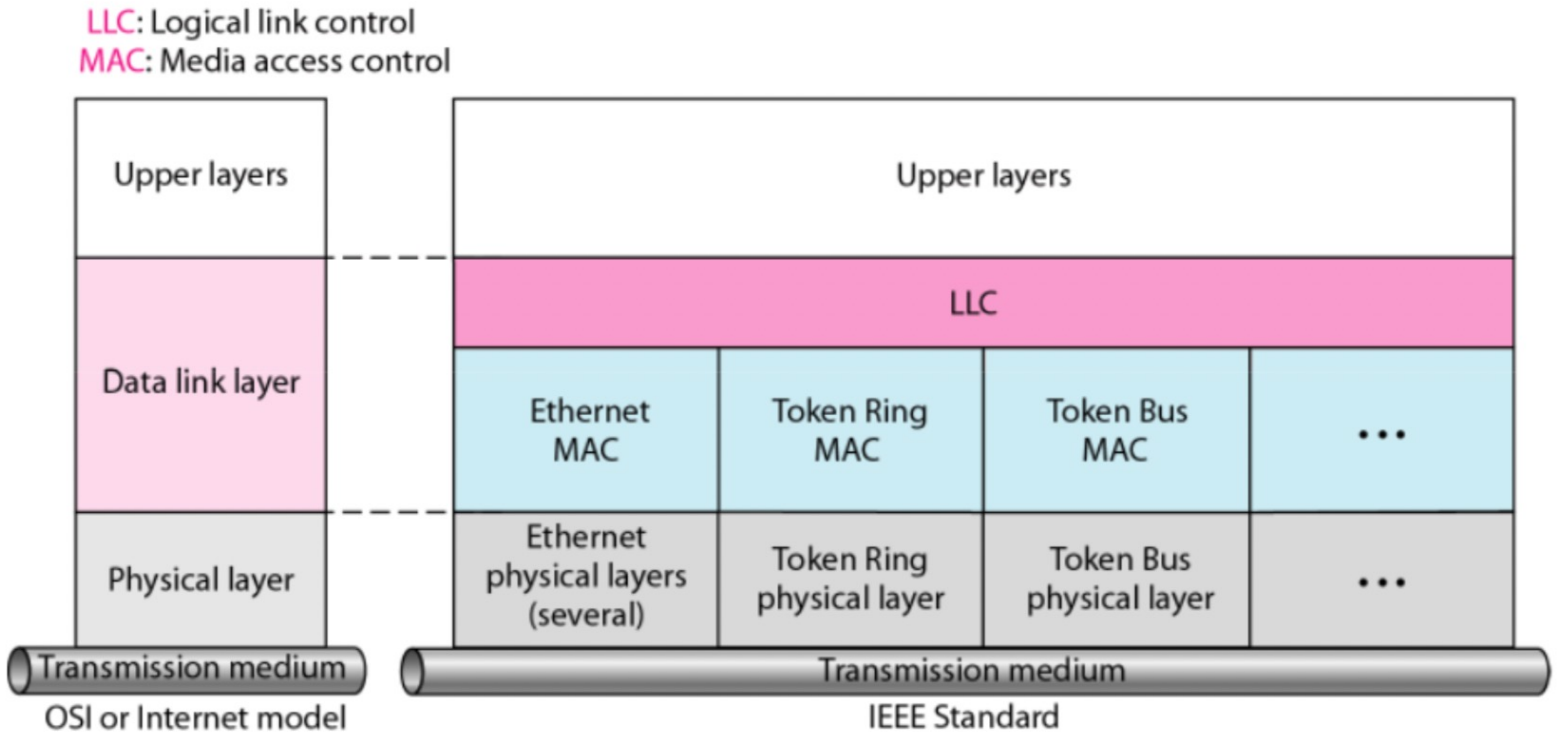


LLC and SNAP



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

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

IEEE 802.11 - Layers and functions

- **PMD Physical Medium Dependent**
  - modulation, coding
  - MAC
- **PHY Management**
  - channel selection, MIB
  - access mechanisms, fragmentation, encryption
- **Station Management**
  - MAC Management
  - coordination of all management functions
  - synchronization, roaming, MIB, power management

- **PLCP P** **e Protocol**
  - clear **rrier sense): accomplished by detecting the** prese **f the carrier**