UNRAVELING THE EVOLUTION OF WI-FI: A JOURNEY FROM 1 TO 7

Christopher Hansen, Ph.D.

Covariant Corporation

November 7, 2023

OUTLINE

- What is Wi-Fi?
- Wi-Fi History
  - IEEE 802.11 and the Wi-Fi Alliance
  - Key enabling technologies
- Wi-Fi Present (IEEE 802.11be / Wi-Fi 7)

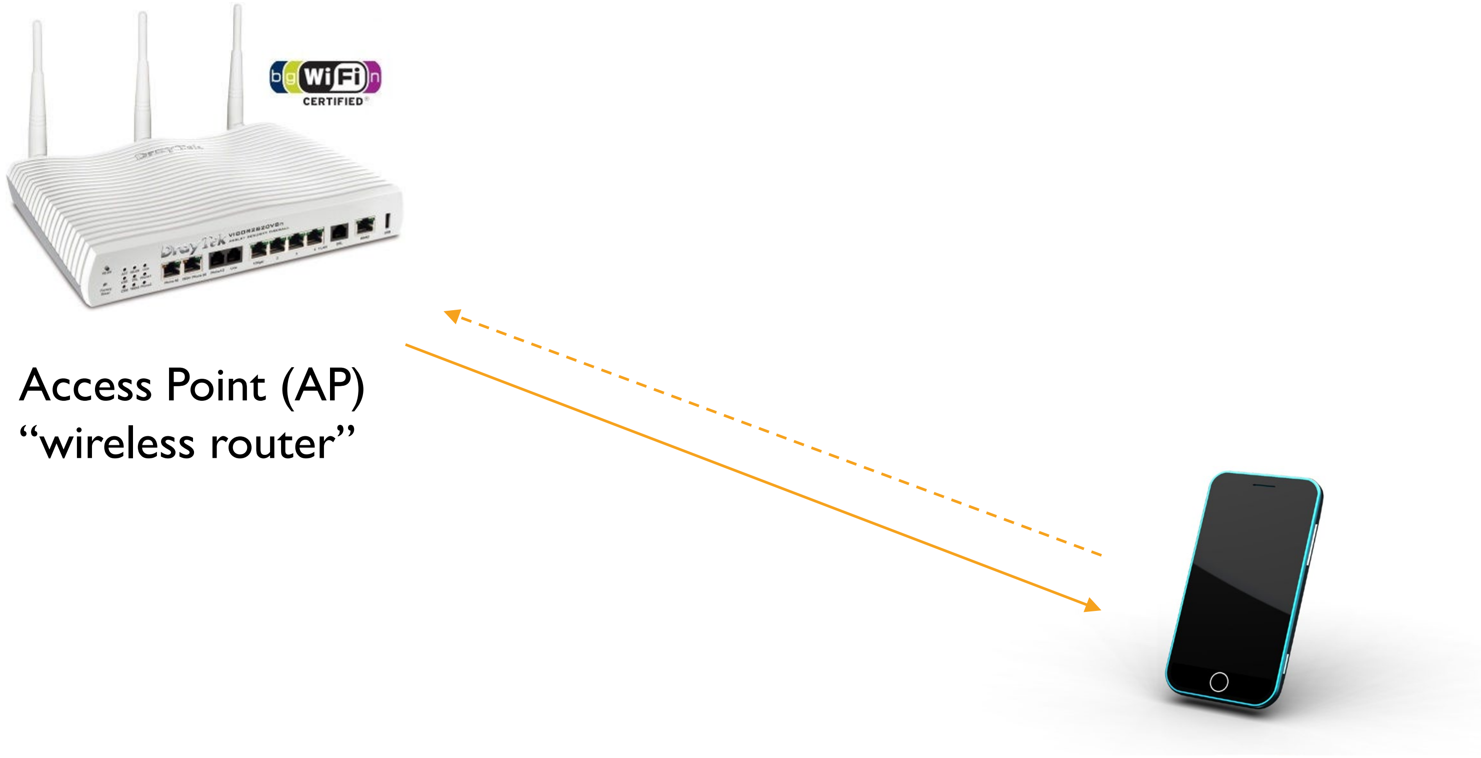
WHAT IS WI-FI?

- Free internet access?

  or

- ‘Wireless Ethernet’ based on IEEE Standards?

WHAT IS WI-FI?



Access Point (AP)
"wireless router"

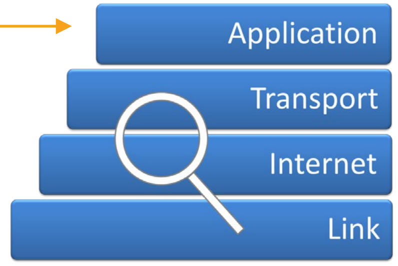
Station (STA)
"client"

- Wi-Fi is a ***brand name*** for devices that have passed a certification test from the Wi-Fi Alliance
- Wi-Fi devices implement the IEEE (Institute of Electrical and Electronics Engineers) 802.11 protocol
  - the letters "a/b/g/n/ac/ax/be" are amendments
- Wi-Fi devices transmit and receive IP (internet protocol) packets and control traffic using radio

WHAT IS WI-FI?

Web browser or App

Data with "IP Address" or URL



Protocol stack running on computer or phone processor

Data with "MAC Address"

Wi-Fi Driver

- Encrypt / De-crypt
- Connection management
- Buffering

coax

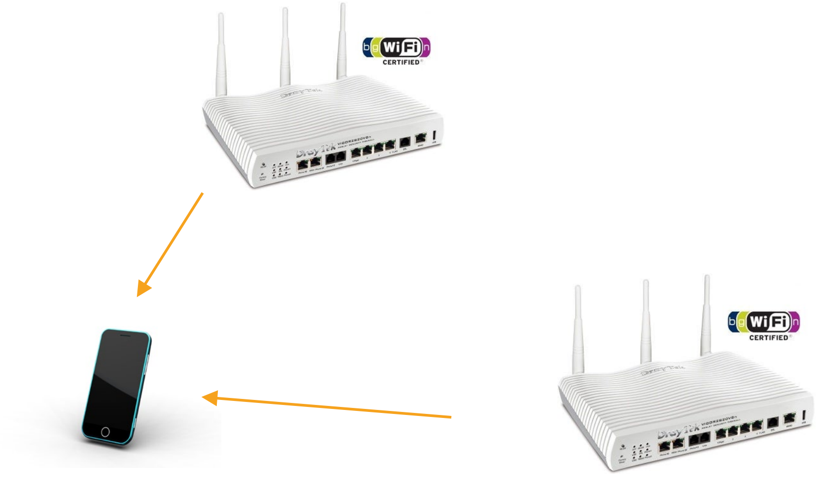
Radio waves to AP and onward to the internet

Wi-Fi Chipset

Wi-Fi
MAC – Media Access Control (who transmits?)
PHY – Physical Layer (bytes to radio and back)

DIFFERENCES BETWEEN WI-FI AND CELLULAR (GSM/LTE/5G)

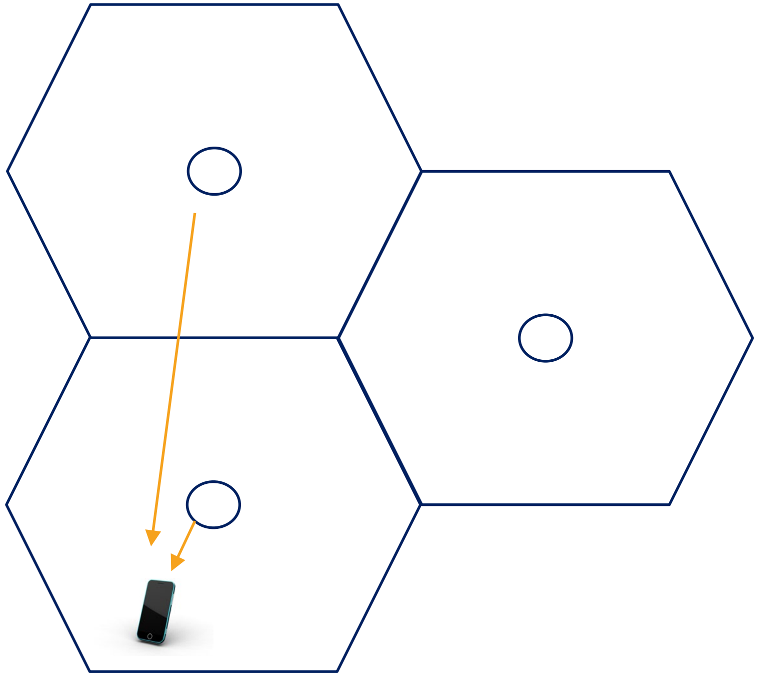
Wi-Fi – Unlicensed Spectrum (2.4 GHz, 5 GHz, 6 GHz)



Uncontrolled interference that is mitigated by protocol design

- Networks will naturally share the radio medium

Cellular – Licensed Spectrum (UHF, microwave bands)



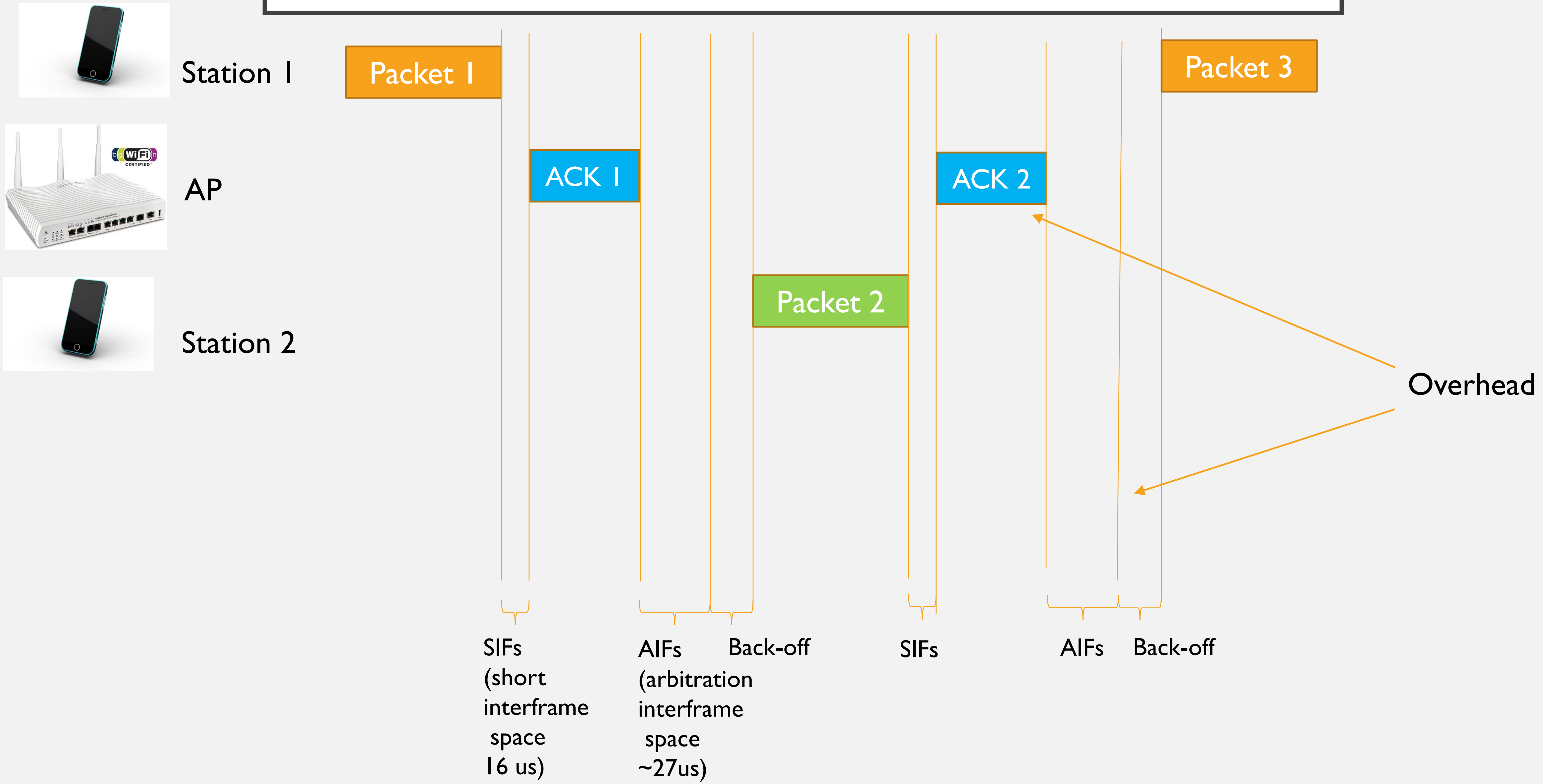
Controlled interference by operator and system design

‘WIRELESS ETHERNET’

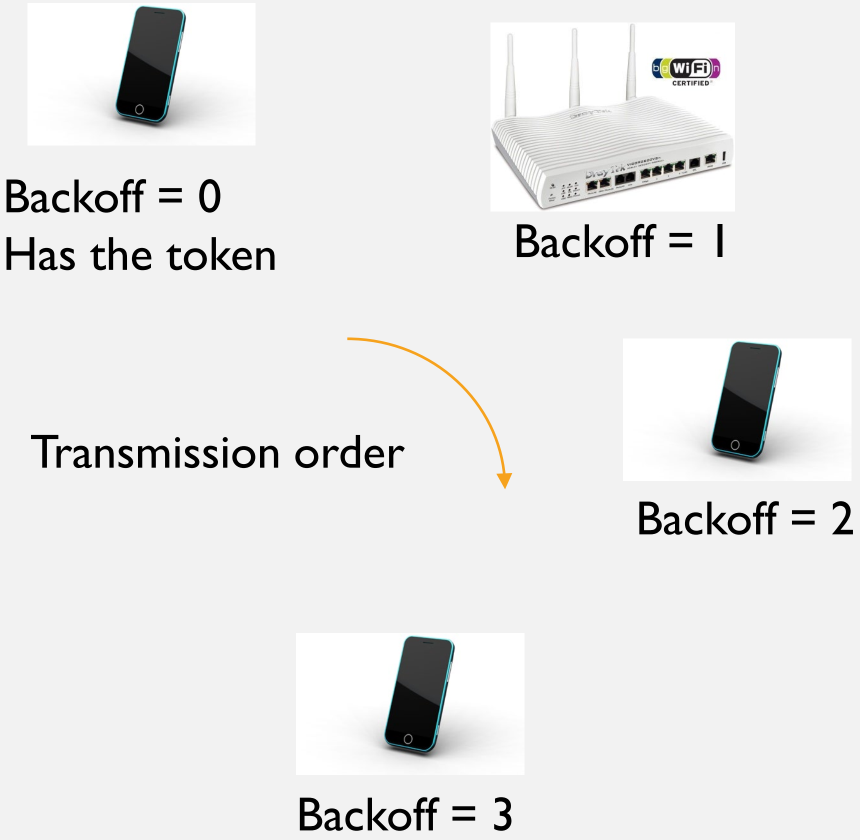
- Wi-Fi is ‘wireless ethernet’
  - Media Access Control (MAC) / Physical layer (PHY) for carrying packets over unlicensed radio bands
  - Time division duplexed (i.e. one station transmits at a time) - CSMA/CA (Carrier sense multiple access with collision avoidance)
    - Stations each select a random backoff time to wait before transmission
    - Count down when channel is clear
    - Packets are acknowledged by the receiver (ACK)

- No collision detection
- Stations do not receive while transmitting
- Unacknowledged packets are assumed to be lost and are re-transmitted

CHANNEL ACCESS

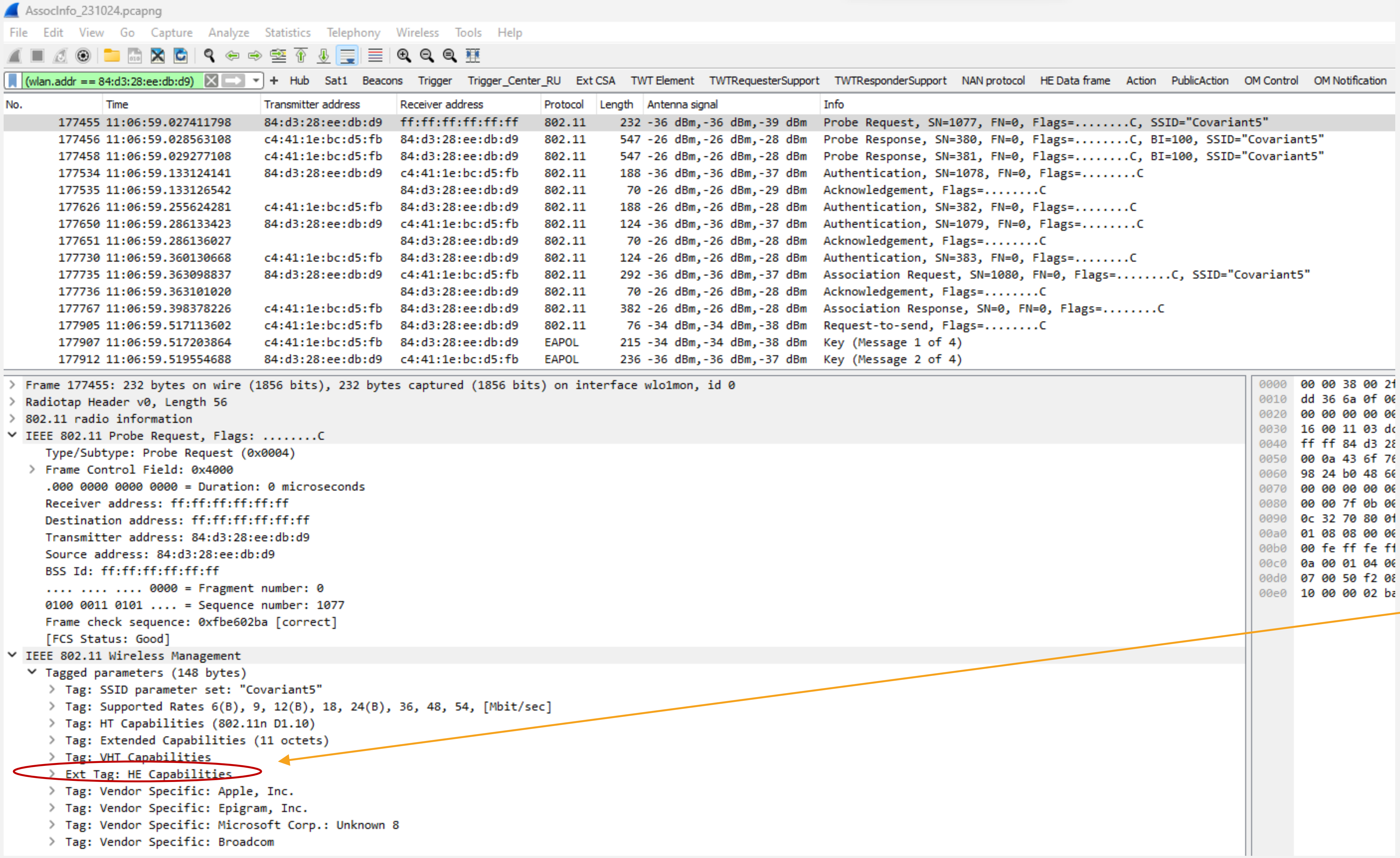


CSMA/CA IS AN IMPLICIT TOKEN BUS



- Backoff time selected corresponds to the position in line to transmit
- After transmitting, a device must select a new backoff time and wait until that time has expired before transmitting again
- Bertsekas and Gallagher, *Data Networks, 2nd* ed. p.333

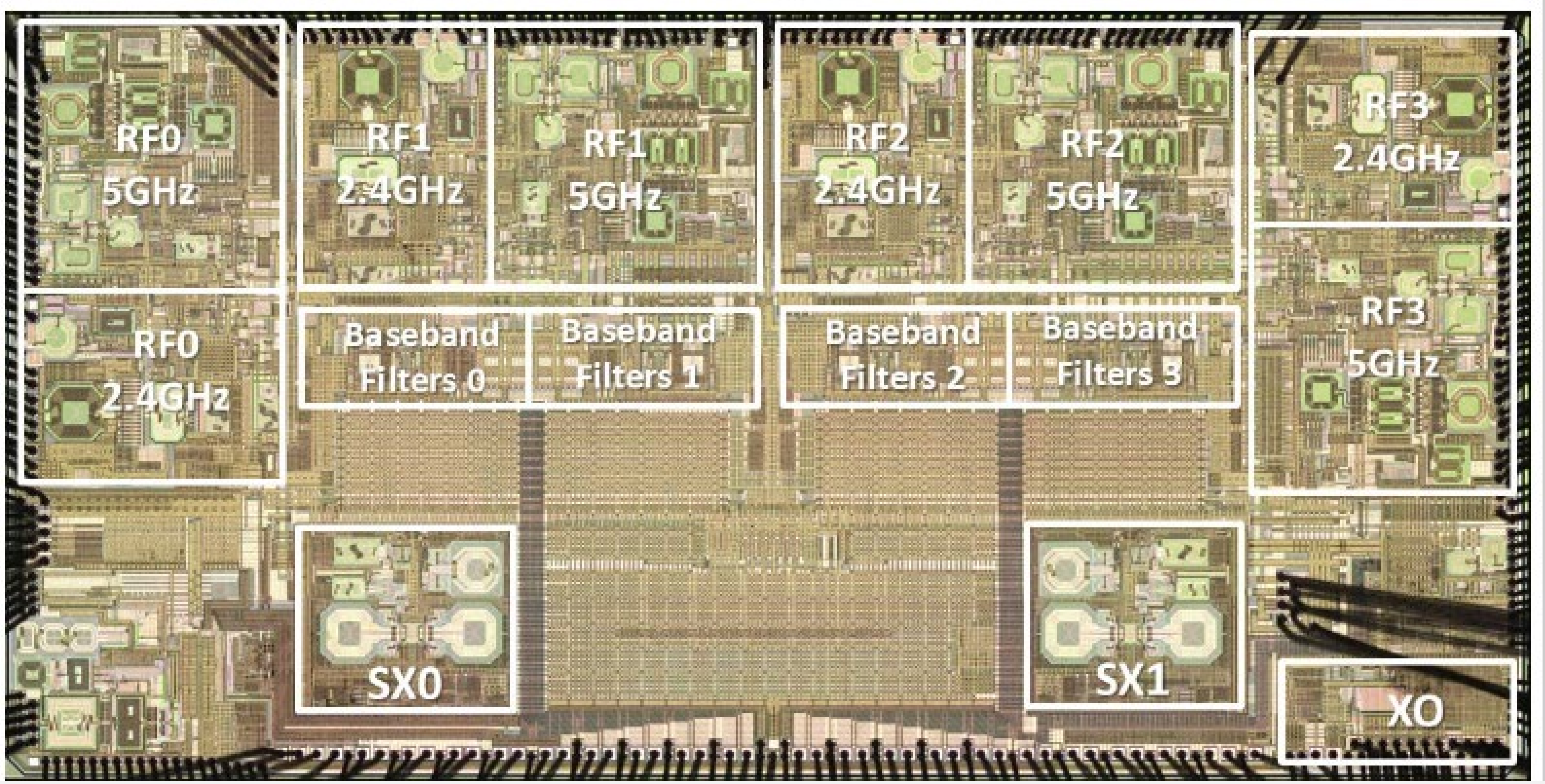
PACKETS OVER THE AIR



Wireshark (free tool) shows iPhone 15 connecting to Covariant office AP

Wi-Fi 6

SINGLE CHIP / PACKAGE



- Example Mediatek 4x4 802.11ax chip from ISSCC 2020 "A 4×4 Dual-Band Dual-Concurrent WiFi 802.11ax Transceiver with Integrated LNA, PA and T/R Switch Achieving +20dBm 1024-QAM MCS11 Pout and -43dB EVM Floor in 55nm"
- Analog front end for an AP (paired with digital chip for modulation / demodulation and MAC functions)

From IEEE ISSCC 2020 p.180

WI-FI PAST

- Example Pre-802.11 Wireless Networking
- Very Close to "Wi-Fi 0"
- 1990 NCR Wavelan – 915MHz / 2.4 GHz bands, 2 Mbps, CSMA/CA

WI-FI PAST

- What enabled Wi-Fi?
  - FCC opened the ISM (Industrial/Scientific/Medical) radio bands for unlicensed data communication using spread spectrum in 1985. (Later added U-NII bands and allowed OFDM in ISM bands.)
  - Desktop computing era of the 1980s and 1990s transitioned to "laptops" in the late 1990s and early 2000s. Apple and IBM both promoted 802.11 in laptops.
  - Moore's Law – scaling of semiconductor transistor sizes to allow lower power / higher performance digital and RF transistors
  - The Internet

WHAT MAKES WI-FI INEXPENSIVE?

- ***Unlicensed spectrum***, ***open standards*** and ***short range*** reduces costs compared to cellular
  - One (2.4 GHz) or two (5 GHz) frequency bands instead of multiple bands
  - Cheap radios (sophisticated design, inexpensive to manufacture - low power, relatively low adjacent channel rejection)
  - Infrastructure costs subsidized – company, university, coffee shop, homeowner

Transmit power

Received Signal power

$$S = \frac{P_t G_t G_r \lambda^2}{(4\pi R)^2}$$

Range

Friis Equation

WI-FI NAMING

- We used to say 802.11b/g/n…..
- Wi-Fi Alliance created Wi-Fi 6 for 802.11ax
  - Then 802.11ac became Wi-Fi 5
  - 802.11n became Wi-Fi 4
- Earlier numbers (1-3) are by "retroactive inference" according to Wikipedia
- IEEE 802.11 standards generally contain many features
  - Wi-Fi alliance and market forces determine which features are employed

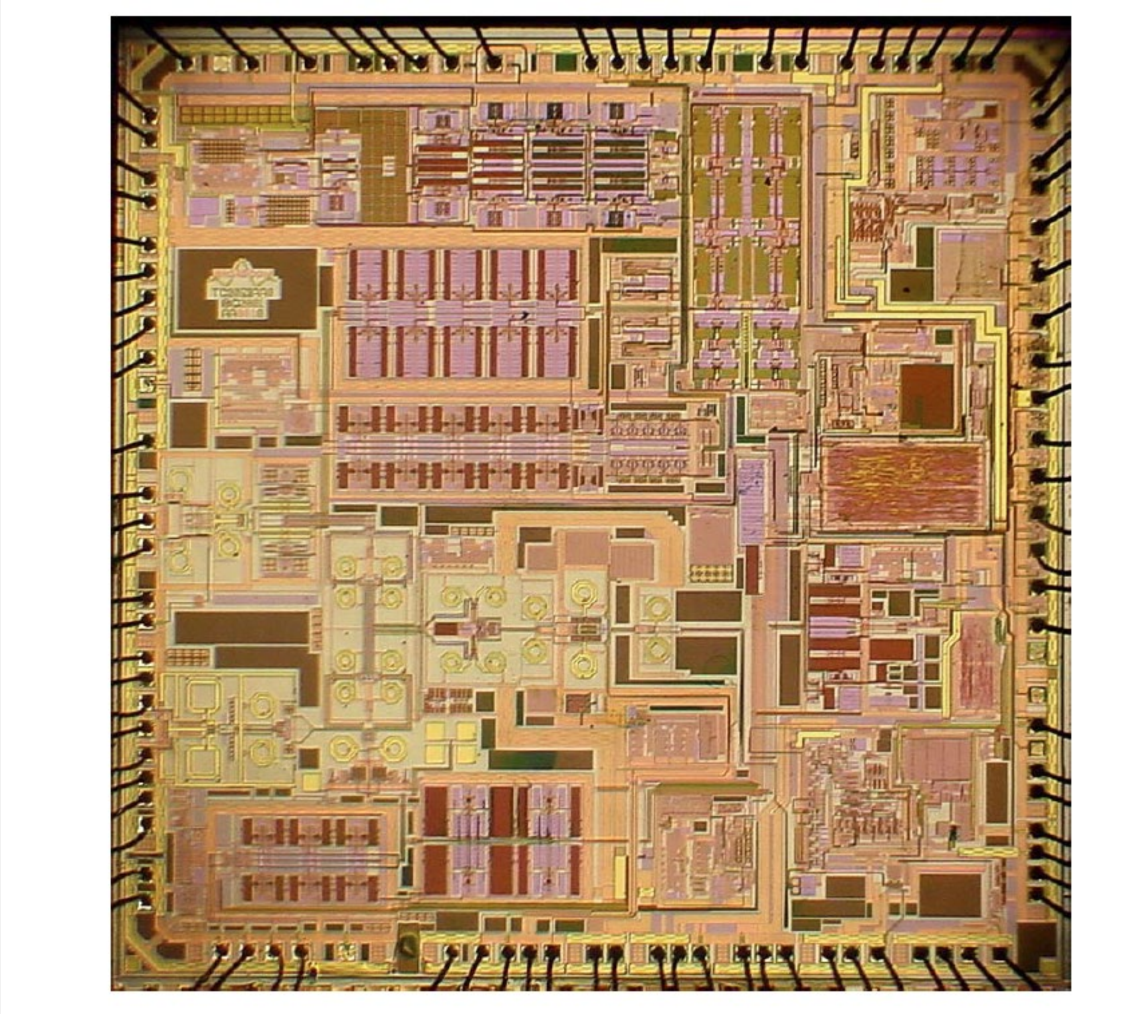
WI-FI 1

- Wireless LAN pioneers got together to form IEEE 802.11 committee in 1990

- Wireless Ethernet Compatibility Alliance (WECA) formed in August 1999 to certify interoperability of 802.11b.

  - 3COM
  - Aironet
  - Lucent Technologies
  - Intersil
  - Nokia
  - Symbol Technologies

SINGLE CHIP CMOS RADIO



2.4 GHz RF TX/RX
Bluetooth mod/demod on chip
Baseband analog interface for 802.11b

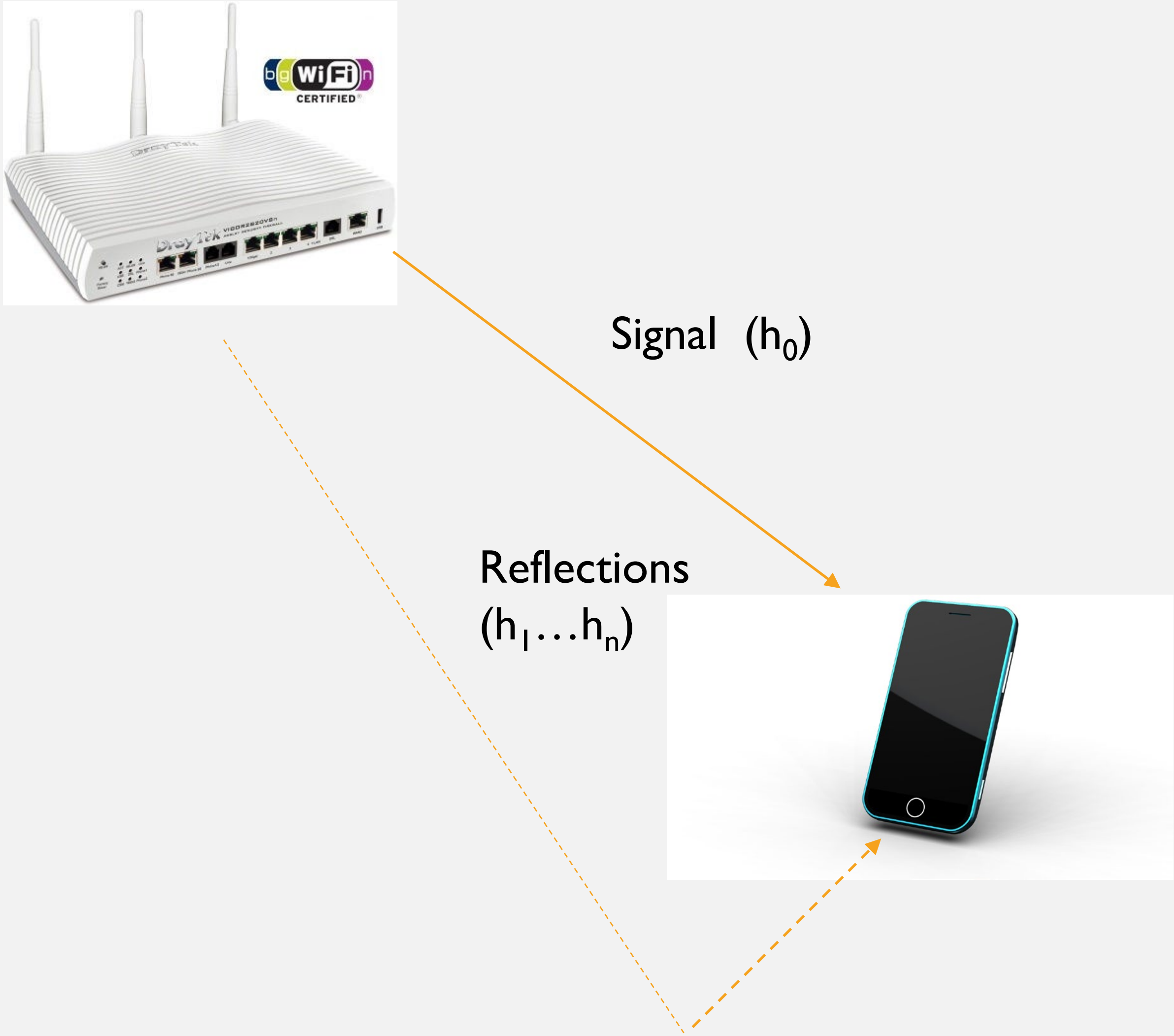
Radios in CMOS mean radios can be integrated with other networking pieces, reducing cost.

IEEE ISSCC 2003, H. Darabi, et al, "A Dual Mode 802.11b/Bluetooth Radio in 0.35um CMOS"

WI-FI DEVELOPMENT

- Technology improves incrementally
  - 802.11a (Wi-Fi 2) / 802.11g (Wi-Fi 3) brought spectral efficiency via OFDM (Orthogonal Frequency Division Multiplexing)
  - 802.11i Makes Wi-Fi data packets secure
  - 802.11n (Wi-Fi 4) brings MIMO (Multiple Input / Multiple Output) and MAC layer aggregation
  - 802.11ac (Wi-Fi 5) brings wider bandwidth, beamforming, and downlink MU-MIMO (multi-user MIMO)
  - 802.11ax (Wi-Fi 6) brings OFDMA (Multiple Access using sets of OFDM subcarriers), Trigger frames, improvements to overlapping cells (BSS)

MITIGATING CHANNEL IMPAIRMENTS



- Multipath channel has nulls in the spectrum
- $t_1 - t_0 = 10$ ns
- null every 100 MHz

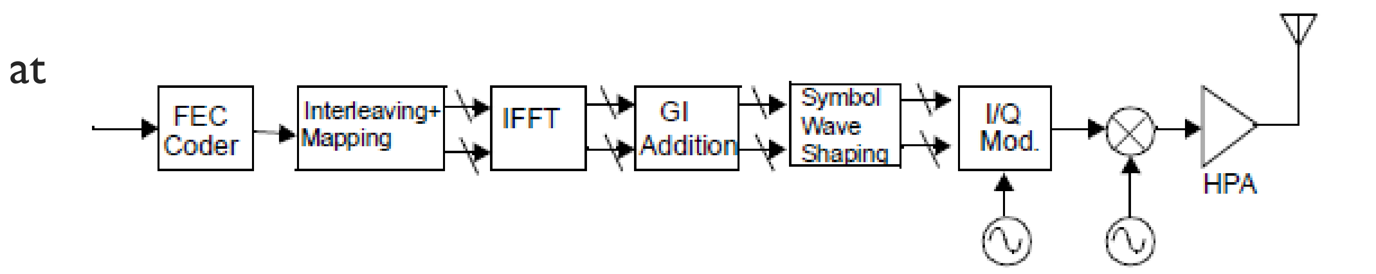
$$h(t) = \sum_{k=0}^{n} h_k \delta(t - t_k)$$

$$H(f) = \sum_{k=0}^{n} h_k e^{j2\pi f t_k}$$

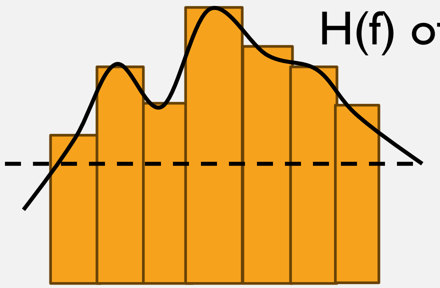
MODERN MODULATION AND CODING

IEEE 802.11-2020 p.2828 Figure 17-12

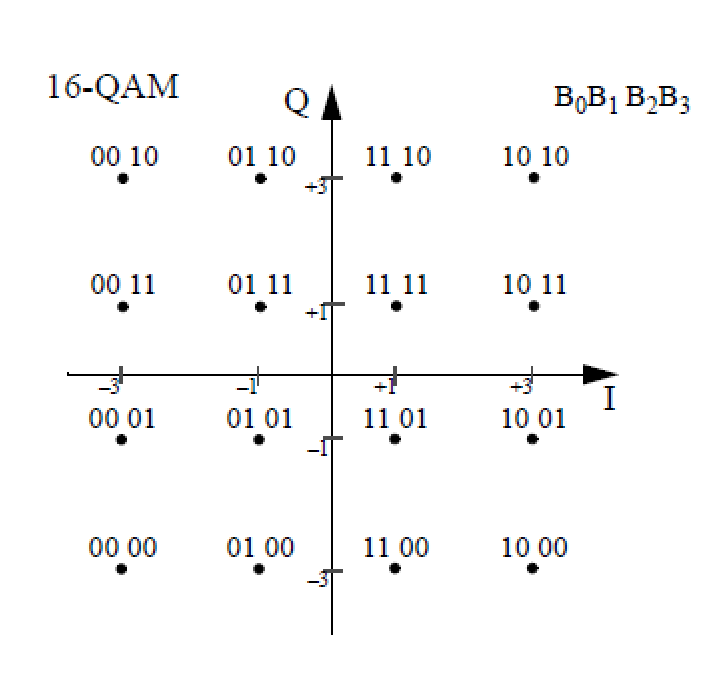
- ***OFDM*** (Orthogonal Frequency Division Multiplexing) – use a discrete Fourier Transform at the transmitter and receiver to generate parallel narrow channels some of which will be "good"



- ***BICM*** (Bit Interleaved Coded Modulation) – use interleaving at the transmitter and receiver to spread encoded data over the narrow channels and rely on channel metrics and a decoder in the receiver to mitigate the "bad channels"



PHY MODULATION AND CODING



802.11-2016 p. 2299

- Signal constellations on each OFDM subcarrier are BPSK or QAM modulated, up to 4096 QAM, depending on the channel SNR
- Gray coding is used – nearest neighbors have Hamming distance of 1
- Example 16 QAM
  - 2 LSBs encode the Q channel (00, 01, 11, 10)
  - 2 MSBs encode the I channel (00, 01, 11, 10)

BIT INTERLEAVED CODED MODULATION

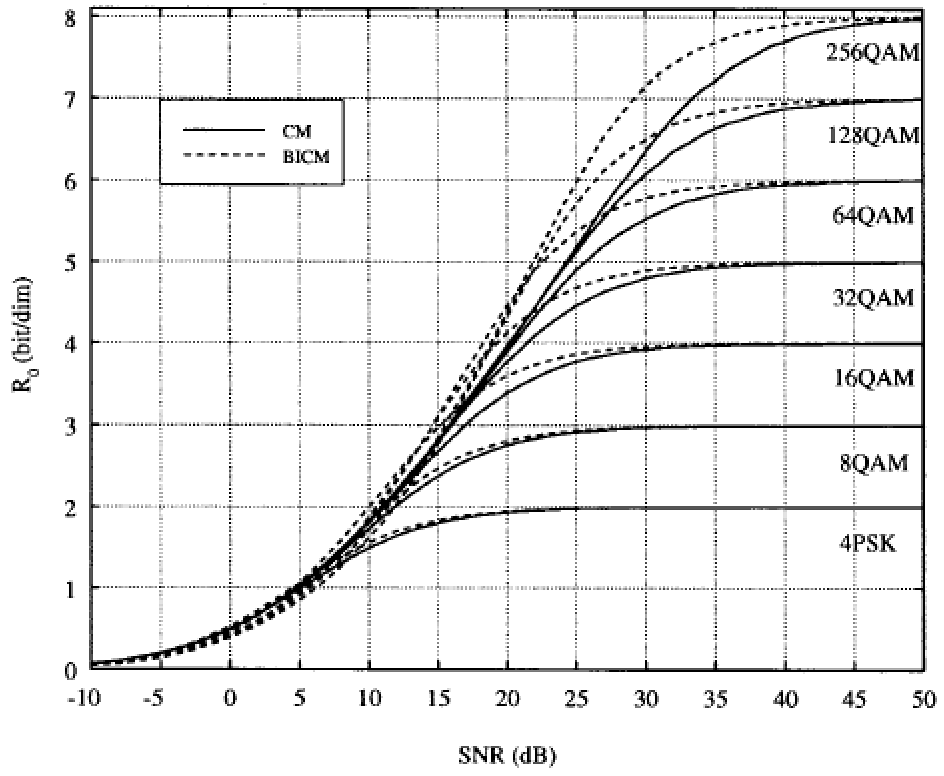


Fig. 7. BICM and CM cutoff rate versus SNR for QAM signal sets with Gray (or quasi-Gray) labeling over Rayleigh fading with coherent detection and perfect CSI.

- From Caire, G., Taricco, G., and Biglieri, E., "Bit-Interleaved Coded Modulation," IEEE Trans. On Information Theory, vol. 44, May 1998.
- See also *Digital Communications, 5th Ed,* Proakis and Salehi section 14.6 and *Foundations of MIMO Communication,* Heath and Lozano, section 1.5.4
- In an AWGN channel, BICM is always inferior to optimized coded modulations (TCM), however in fading channels BICM works better.

CODING

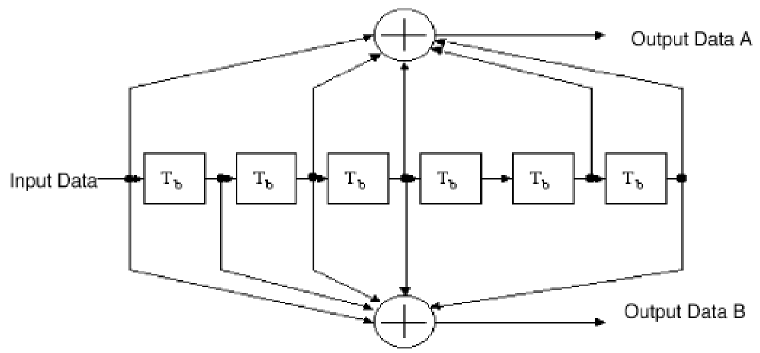


Figure 17-8—Convolutional encoder (k = 7)

Binary Convolutional Code (BCC)
IEEE 802.11-2020 p.2820

- Rate ½ convolutional code with puncturing for other rates
- 12 LDPC code matrices with same encoding structure
- Under most conditions the LDPC code will allow operation at lower signal levels allowing higher data rates or longer range

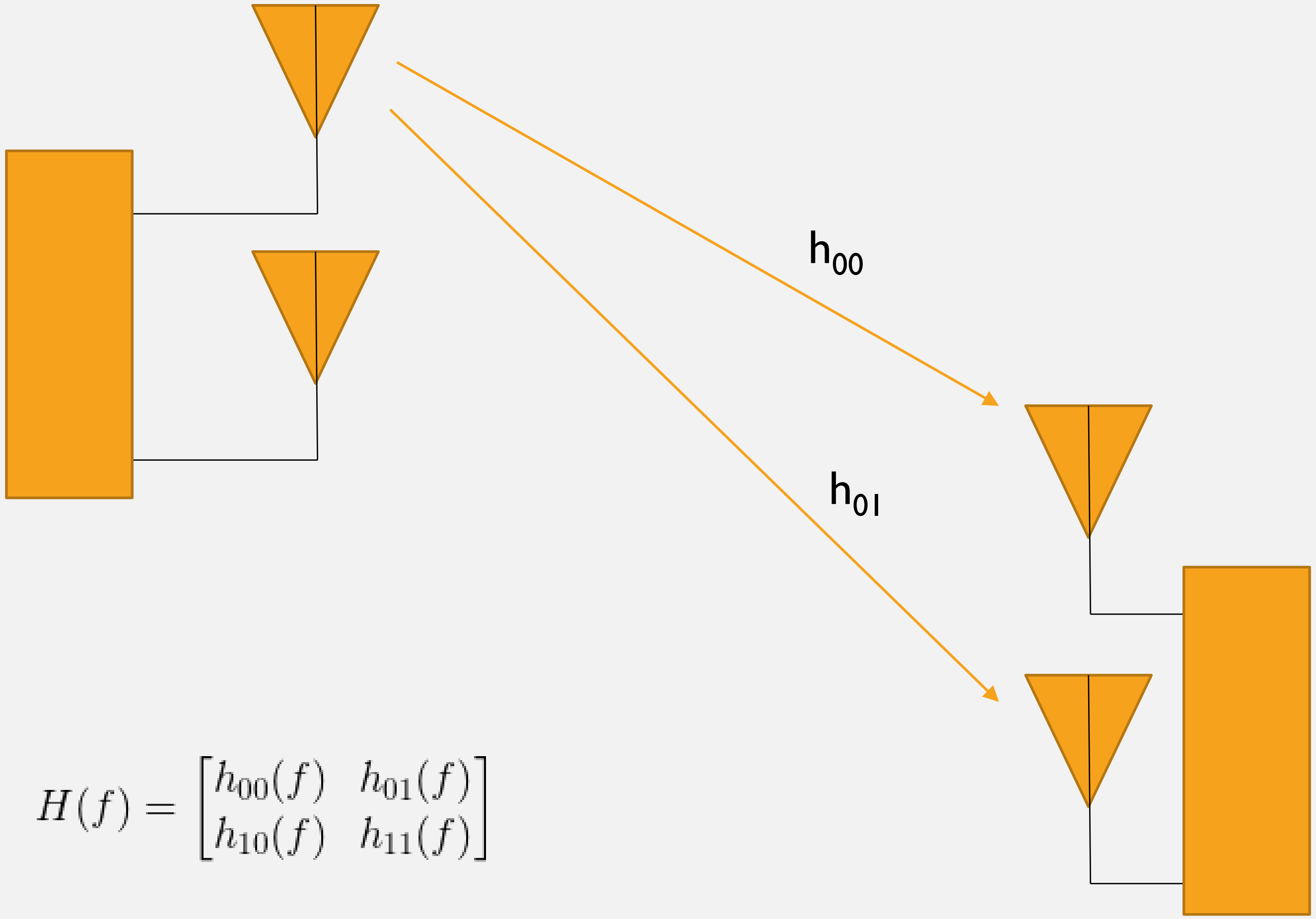
Table F-3—Matrix prototypes for codeword block length *n* = 1944 bits, subblock size is *Z* = 81 bits

(a) Coding rate R = 1/2.

57	-	-	-	50	-	11	-	50	-	79	-	1	0	-	-	-	-	-	-	-	-	-	-
3	-	28	-	0	-	-	-	55	7	-	-	-	0	0	-	-	-	-	-	-	-	-	-
30	-	-	-	24	37	-	-	56	14	-	-	-	-	0	0	-	-	-	-	-	-	-	-
62	53	-	-	53	-	-	3	35	-	-	-	-	-	-	0	0	-	-	-	-	-	-	-
40	-	-	20	66	-	-	22	28	-	-	-	-	-	-	-	0	0	-	-	-	-	-	-
0	-	-	-	8	-	42	-	50	-	-	8	-	-	-	-	-	0	0	-	-	-	-	-
69	79	79	-	-	-	56	-	52	-	-	-	0	-	-	-	-	-	0	0	-	-	-	-
65	-	-	-	38	57	-	-	72	-	27	-	-	-	-	-	-	-	-	0	0	-	-	-
64	-	-	-	14	52	-	-	30	-	-	32	-	-	-	-	-	-	-	-	0	0	-	-
-	45	-	70	0	-	-	-	77	9	-	-	-	-	-	-	-	-	-	-	-	0	0	-
2	56	-	57	35	-	-	-	-	-	12	-	-	-	-	-	-	-	-	-	-	-	0	0
24	-	61	-	60	-	-	27	51	-	-	16	1	-	-	-	-	-	-	-	-	-	-	0

Low Density Parity Check Matrix (1 of 12)
IEEE 802.11-2020 p.4132

MULTIPLE INPUT MULTIPLE OUTPUT (MIMO)



$$H(f) = \begin{bmatrix} h_{00}(f) & h_{01}(f) \\ h_{10}(f) & h_{11}(f) \end{bmatrix}$$

- Wi-Fi added MIMO capabilities in 802.11n (Wi-Fi 4) and expanded them in 802.11ac (Wi-Fi 5)
- Employ multiple antennas and signal processing to generate distinct signal paths
- Processing can be applied at both the transmitter (beamforming) and at the receiver

EXPLOITING MULTIPATH BENEFITS

$$H = \sum_{k=1}^{N} H_k$$

$$max\ rank(H) \leq N$$

- Each path corresponds with a rank 1 channel matrix H_k
- Reflections from walls, floors, and objects in the neighborhood create new paths
  - Spatial multiplexing
- For MIMO to work, it is necessary to have both extra antennas *and* reflections from the radio environment
- In practice, cell phones can usually only support 2 Wi-Fi antennas. Notebook PCs can support 3 or 4.

BACKWARDS COMPATIBLE

From IEEE 802.11ax-2021 p.510

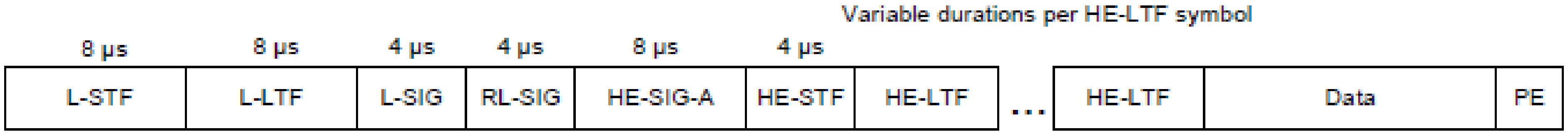


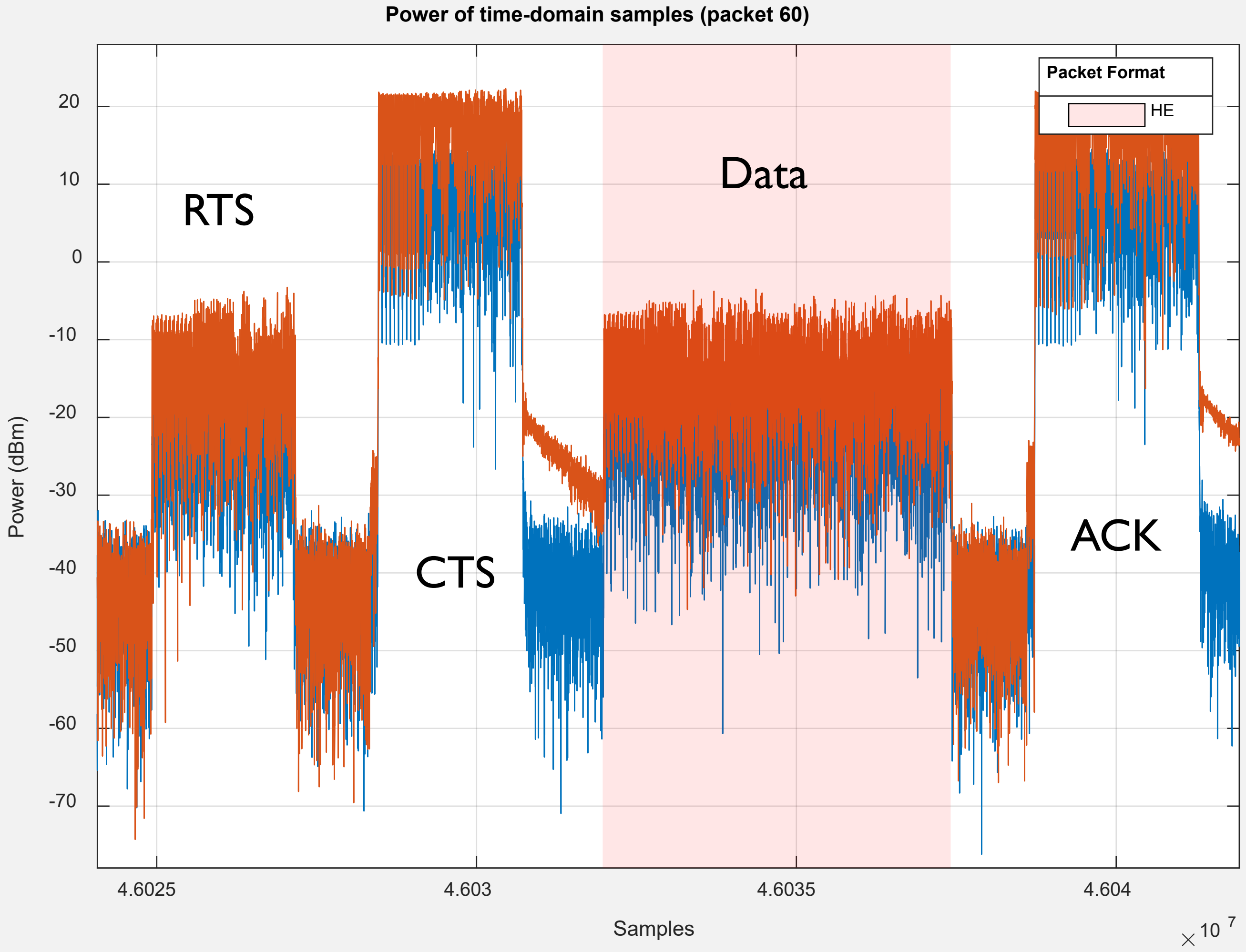
Figure 27-8—HE SU PPDU format

Legacy header for backward compatibility

Receiver training information

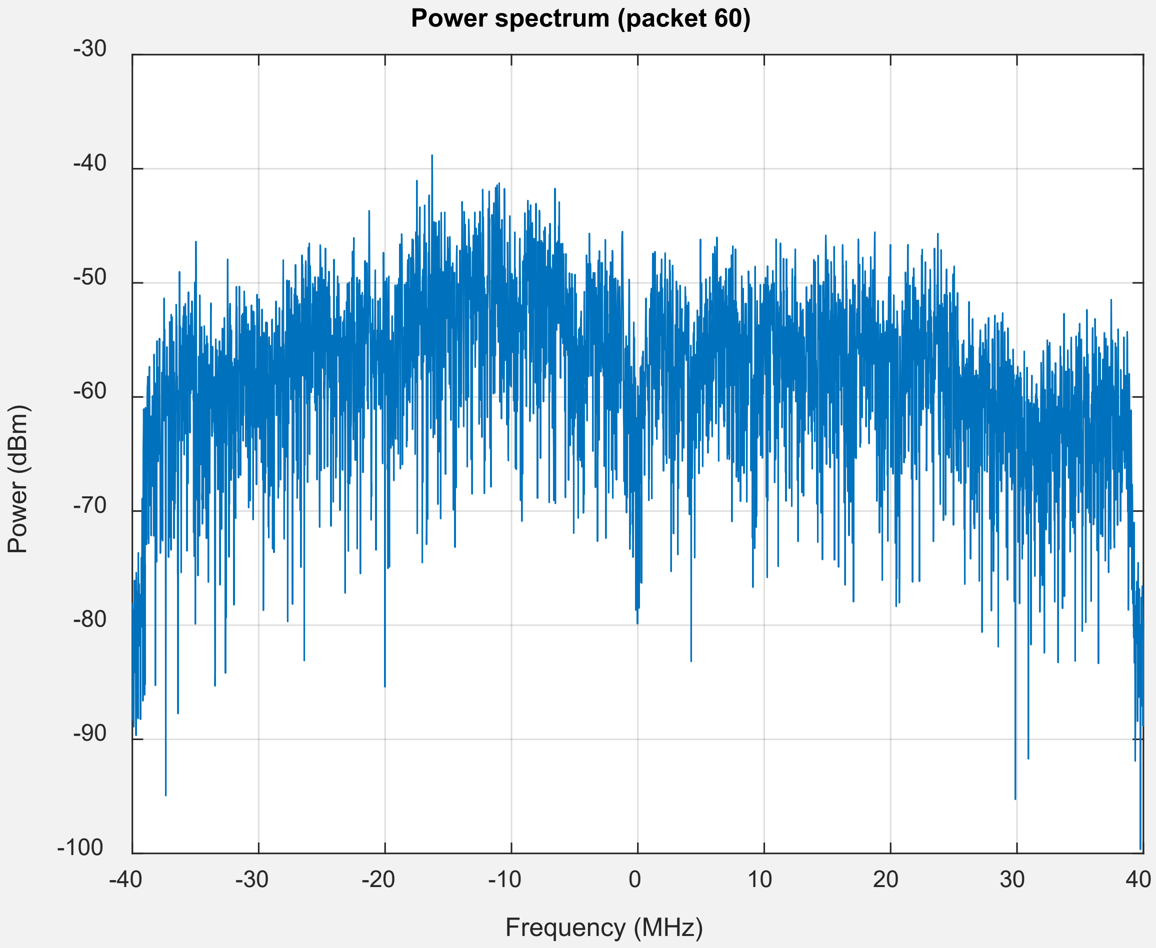
(Overhead)

WI-FI 6 PACKET



- iPhone transmitting data to AP
- Laboratory capture (Aaronia Spectran V6 processed with Matlab WLAN Toolbox)
- Data uses 802.11ax 2x2 MIMO

WI-FI 6 PACKET



- Frequency domain view of the data packet (HE-SU format)

WI-FI 6 PACKET

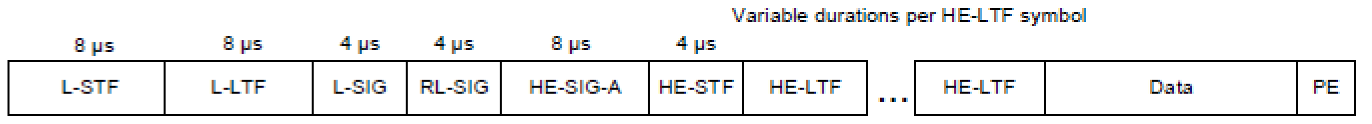
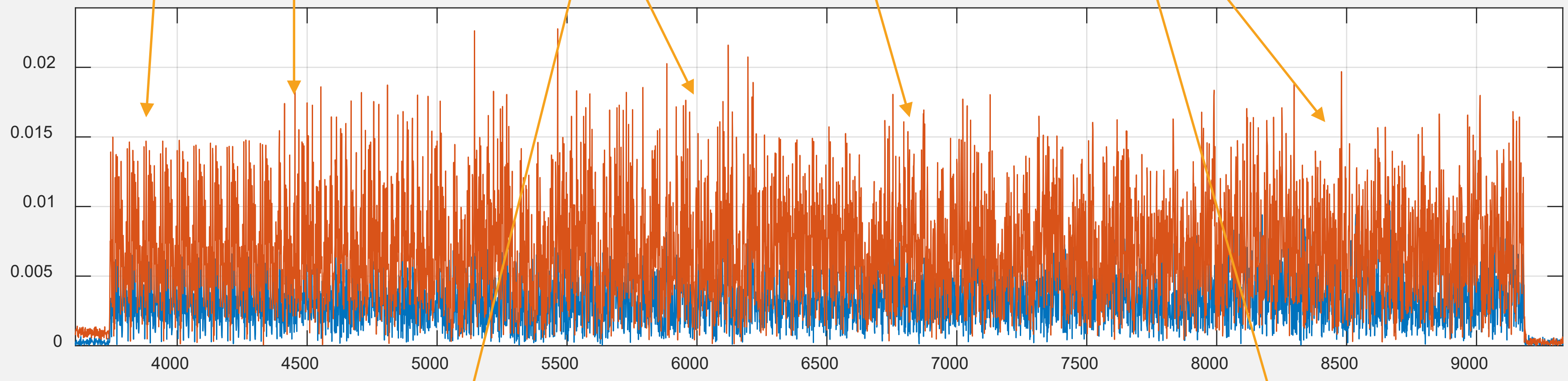
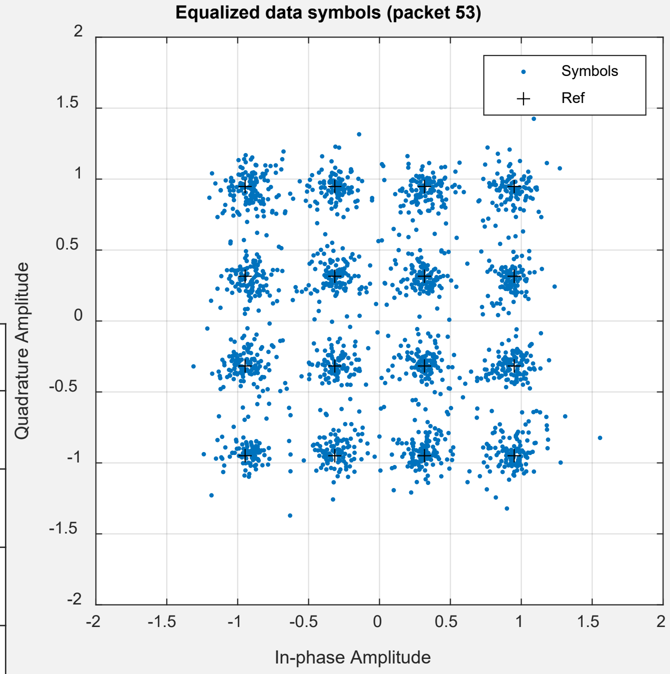


Figure 27-8—HE SU PPDU format





Signaling Field Summary of Packet 53 (HE-SU)

Property	Value	Property	Value	Property	Value
L-SIG Length	31	Spatial Reuse	0	LDPC Extra Symbol	False
L-SIG Rate	0xB	Bandwidth	CBW80	STBC	False
Format	HE-SU	Guard Interval	0.8	Beamformed	False
Beam Change	True	HE-LTF Type	2	Pre-FEC Padding Factor	1
UL/DL Indication	UL	Num Space-Time Streams	2	PE Disambiguity	False
MCS	4	Num HE-LTF Symbols	2	Doppler	False
DCM	False	TXOP	127		
BSS Color	44	Channel Coding	LDPC		

AMPDU/MPDU Number	Address1	Address2	AMPDU/MPDU Decode Status	MAC Frame Type
"AMPDU1_MPDU1"	"C4411EBCD5FB"	"6E34B0D65151"	"Success"	"QoS Data"

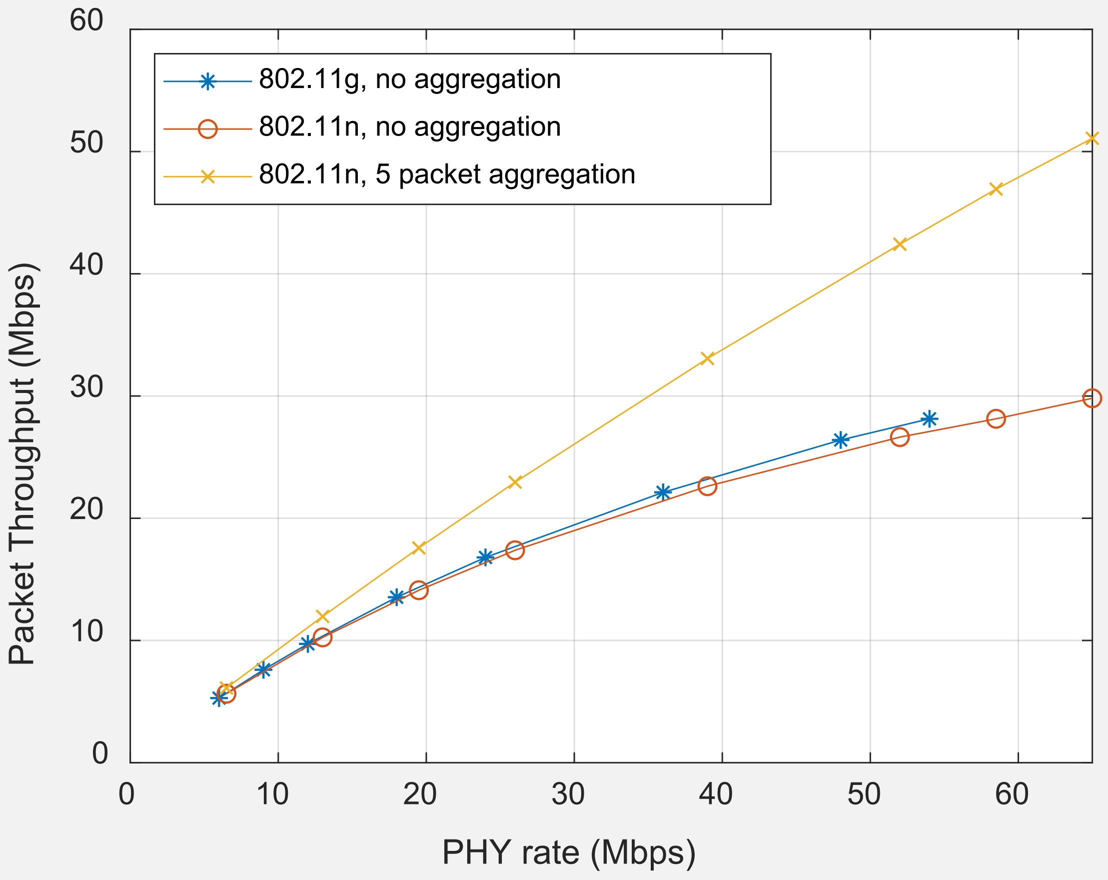
IMPROVING THROUGHPUT

- Throughput is the measure of how quickly useful data is carried from source to destination

$$Throughput = \frac{T_{data}}{T_{data} + T_{overhead}} R_{PHY}$$

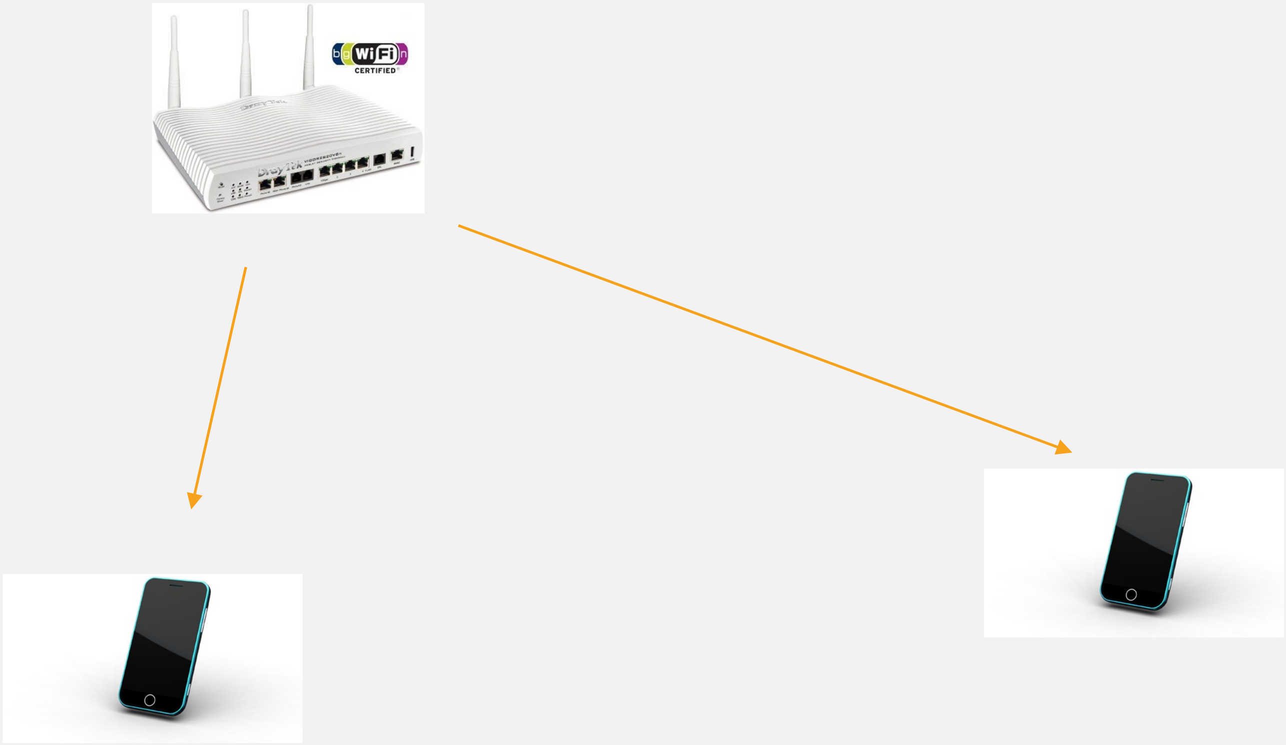
- Limited by the maximum PHY rate and by the overhead time
- Minimum average $T_{overhead}$ = 194.5 microseconds
- ***Efficient transmission requires packets longer than 1 millisecond***

IMPROVING THROUGHPUT



- 802.11n introduced aggregation to put packets together before transmission
- Aggregation increases latency – the time to get data from transmitter to receiver

MULTIUSER MIMO – WI-FI 5



802.11n introduced single user MIMO

- 2 – 4 times PHY data rate

802.11ac introduced MU-MIMO

- AP simultaneously transmit to more than one STA

OFDMA (MULTIPLE ACCESS) – WI-FI 6

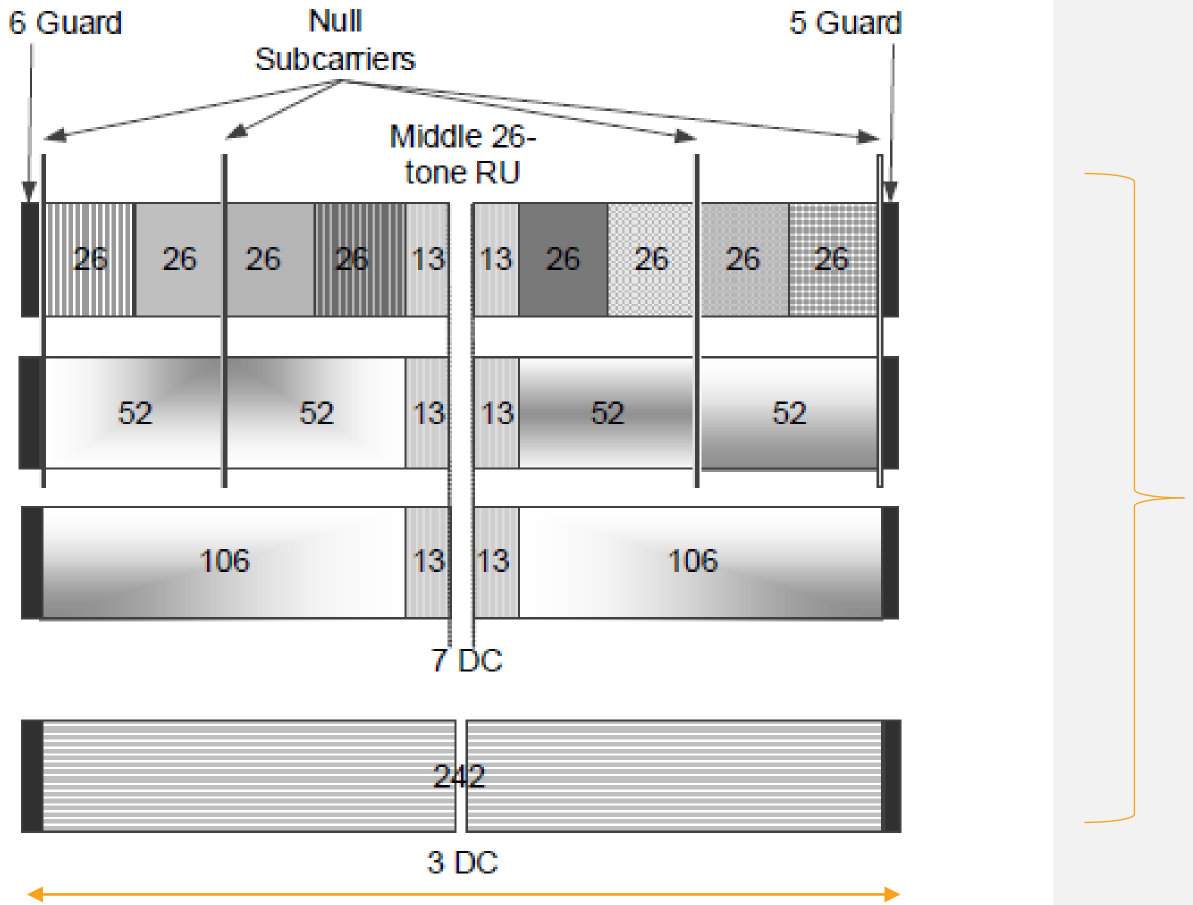


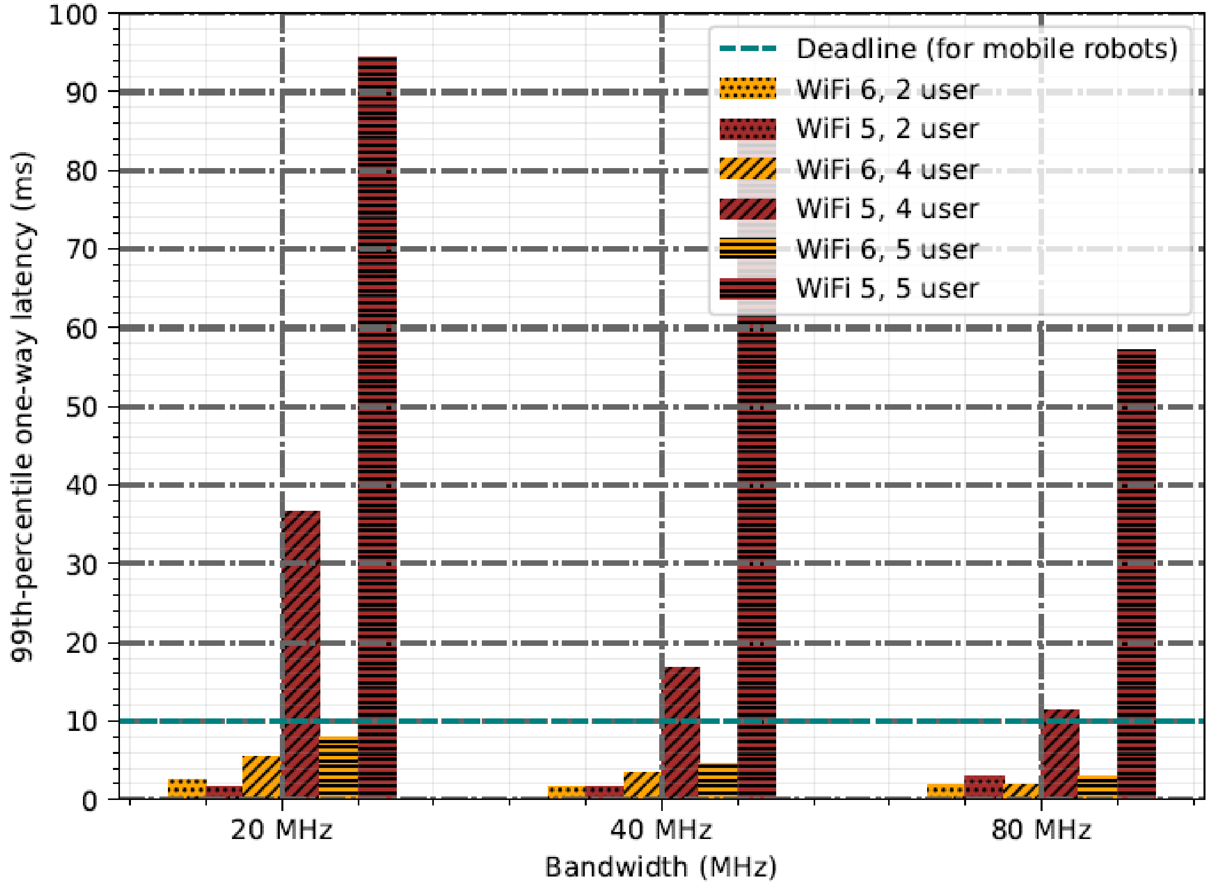
Figure 27-5—RU locations in a 20 MHz HE PPDU(#20870)

Different signaling configuration

20 MHz Channel Bandwidth

From IEEE 802.11ax Draft 4.3 p.503

MOTIVATION FOR OFDMA/MU-MIMO



(b) UL

- Improvements in PHY rate do not improve the network access delay in dense networks that reach saturation
- Wi-Fi 6 reduces access delay by allowing multiple transmissions at the same time and by limiting the number of stations contending at any time
- Experimental results show the benefit is seen more on the uplink than on the downlink

M. Suer, et al, "Experimental evaluation of IEEE 802.11ax – low latency and high reliability with Wi-Fi 6?", 2022 Globecom

SECURITY

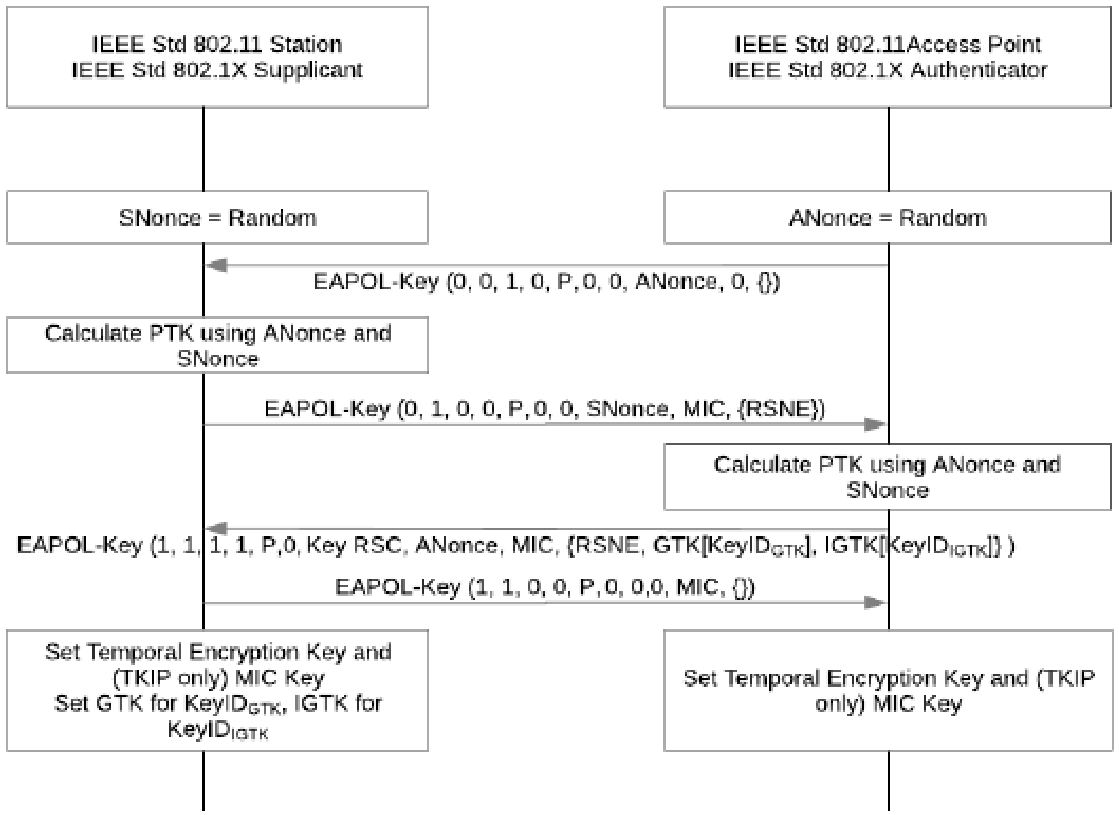


Figure 12-48—Sample 4-way handshake

IEEE 802.11-2020 p.2565

- Original Wi-Fi used WEP (Wired Equivalent Privacy) that was easy to break
- 802.11i made Wi-Fi more secure
- Wi-Fi devices use encryption for the data portion of MAC frames
  - Header (i.e. MAC address is not encrypted)
- Different encryption keys are used for each client device
- Key derivation process from the PMK (pairwise master key) is the 4 way handshake
- Wi-Fi WPA2 PMK was a hash of the password and SSID
- WPA3 uses SAE (Simultaneous Authentication of Equals) which is more secure

WI-FI PRESENT

- 802.11be Extremely High Throughput / Wi-Fi 7
  - Wi-Fi 1 – 5 Faster and Faster
  - Wi-Fi 6 High Efficiency
  - Faster is back – 802.11be standard is still in draft form but products are already on the market (i.e. Google Pixel 8)

WI-FI 6 / WI-FI 7

Table 27-103—HE-MCSs for 2×996-tone RU, N_{SS} = 1

HE-MCS Index	DCM	Modulation	R	N_{BPSCS}	N_{SD}	N_{CBPS}	N_{DBPS}	Data rate (Mb/s) 0.8 µs GI	1.6 µs GI	3.2 µs GI
0	1	BPSK	1/2	1	980	980	490	36.0	34.0	30.6
	0		1/2		1 960	1 960	980	72.1	68.1	61.3
1	1	QPSK	1/2	2	980	1 960	980	72.1	68.1	61.3
	0		1/2		1 960	3 920	1 960	144.1	136.1	122.5
2	N/A		3/4		1 960	3 920	2 940	216.2	204.2	183.8
3	1	16-QAM	1/2	4	980	3 920	1 960	144.1	136.1	122.5
	0		1/2		1 960	7 840	3 920	288.2	272.2	245.0
4	1		3/4		980	3 920	2 940	216.2	204.2	183.8
	0		3/4		1 960	7 840	5 880	432.4	408.3	367.5
5	N/A	64-QAM	2/3	6	1 960	11 760	7 840	576.5	544.4	490.0
6			3/4				8 820	648.5	612.5	551.3
7			5/6				9 800	720.6	680.6	612.5
8		256-QAM	3/4	8		15 680	11 760	864.7	816.7	735.0
9			5/6				13 066	960.7	907.4	816.6
10		1024-QAM	3/4	10		19 600	14 700	1 080.9	1 020.8	918.8
11			5/6				16 333	1 201.0	1 134.2	1 020.8

Twice the bandwidth and 2 more bits/symbol

Table 36-86—EHT-MCSs for 4×996-tone RU, $N_{SS,u}$ = 1

EHT-MCS index	Modulation	R_u	$N_{BPSCS,u}$	$N_{SD,u}$	$N_{CBPS,u}$	$N_{DBPS,u}$	Data rate (Mb/s) 0.8 µs GI	1.6 µs GI	3.2 µs GI
0	BPSK	1/2	1	3 920	3 920	1 960	144.1	136.1	122.5
1	QPSK	1/2	2		7 840	3 920	288.2	272.2	245.0
2		3/4				5 880	432.4	408.3	367.5
3	16-QAM	1/2	4		15 680	7 840	576.5	544.4	490.0
4		3/4				11 760	864.7	816.7	735.0
5	64-QAM	2/3	6		23 520	15 680	1 152.9	1 088.9	980.0
6		3/4				17 640	1 297.1	1 225.0	1 102.5
7		5/6				19 600	1 441.2	1 361.1	1 225.0
8	256-QAM	3/4	8		31 360	23 520	1 729.4	1 633.3	1 470.0
9		5/6				26 133	1 921.5	1 814.8	1 633.3
10	1024-QAM	3/4	10		39 200	29 400	2 161.8	2 041.7	1 837.5
11		5/6				32 666	2 401.9	2 268.5	2 041.6
12	4096-QAM	3/4	12		47 040	35 280	2 594.1	2 450.0	2 205.0
13		5/6				39 200	2 882.4	2 722.2	2 450.0
15	BPSK-DCM	1/2	1	1 960	1 960	980	72.1	68.1	61.3

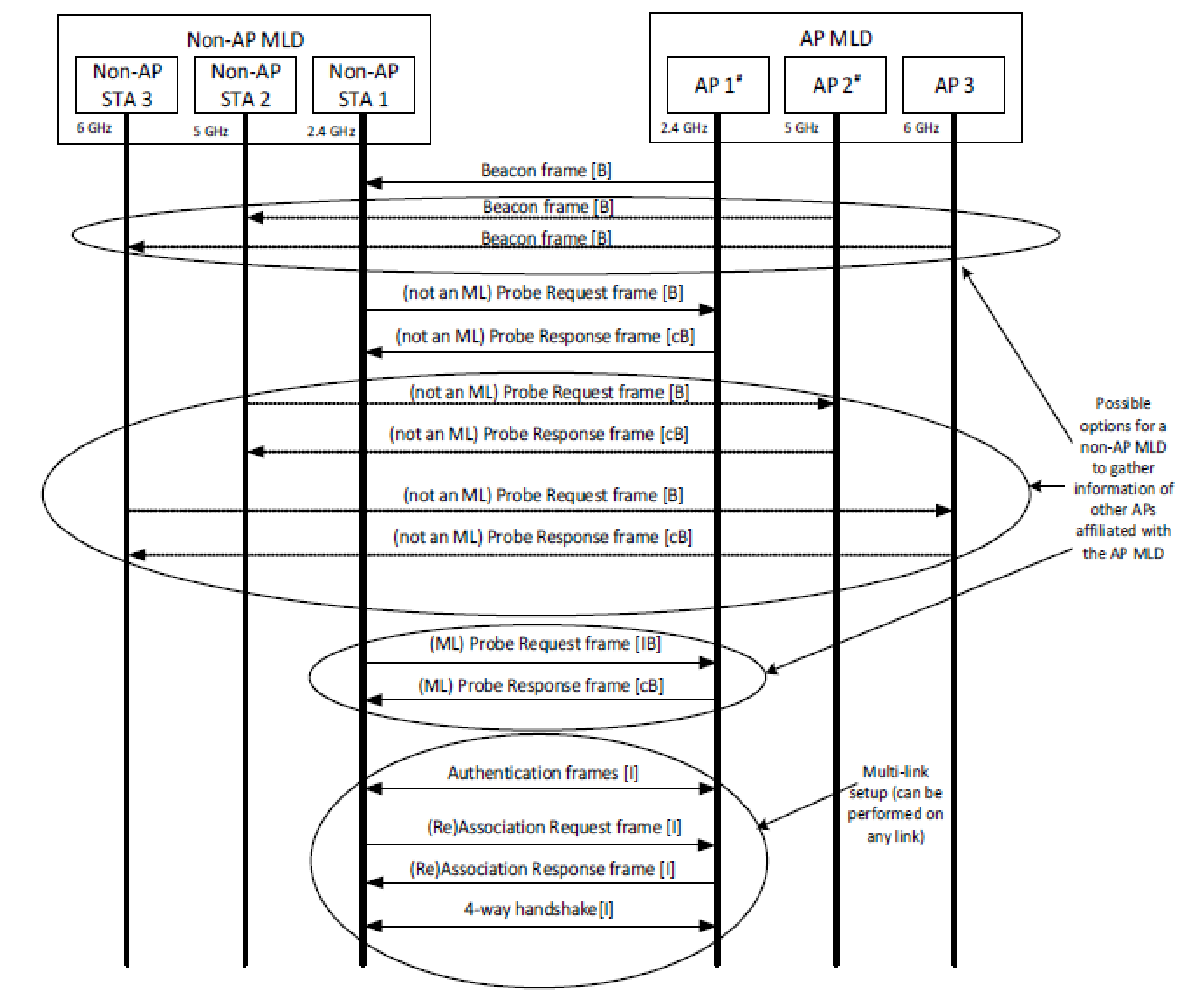
1201 Mbps * (1.2) * 2 = 2882.4 Mbps with 1 antenna

WI-FI 7

- 4096 QAM
- 320 MHz channels, but only in new 6 GHz band
- Multiple Links
- Enhancements to Target Wake Time (TWT) make the Restricted TWT (R-TWT)
  - AP can organize client STAs into sub-groups
  - Limits contention for the medium, allows for efficient access

WI-FI 7 – MULTIPLE LINK OPERATION

Client side



Router side

- Multiple link operation allows simulatenous MAC/PHY connections between a client and an AP
- One association and one security key for multiple connections in lieu of hand offs
- Enhance reliability and reduction of management traffic

802.11be Draft 4.1 Figure 35-5 p.513

WI-FI 7 RESTRICTED TWT

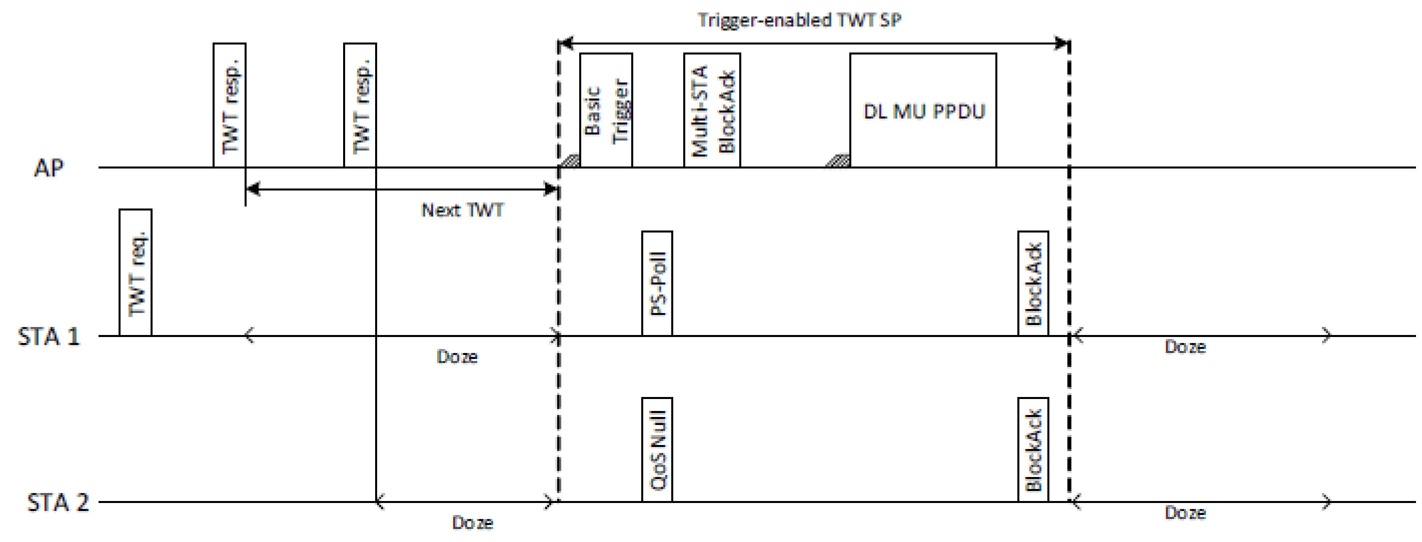
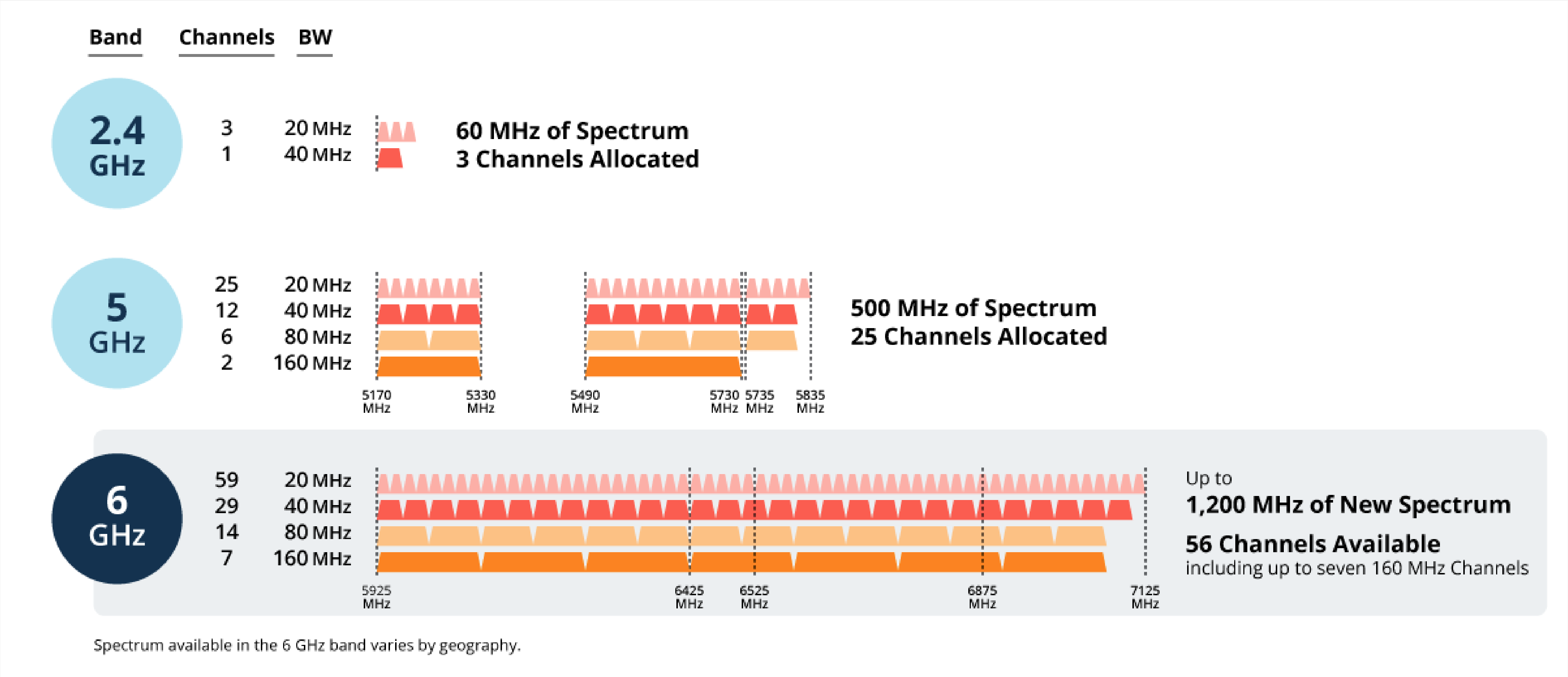


Figure 26-9—Example of individual TWT operation

IEEE 802.11ax-2021 p.387

- Target Wake Time (TWT) allows the AP to organize time periods for communication with groups of client devices
- Outside of that time period, devices can sleep and save power
- Wi-Fi 7 enhances the TWT to simplify setup and reduce possibility of interference

6 GHZ SPECTRUM



- From https://www.arubanetworks.com/faq/what-is-wi-fi-6e/

OTHER 802.11 TECHNOLOGY

- 802.11ah – Wi-Fi HaLow
  - 900 MHz band low rate, longer range wireless networking
- 802.11ad / 802.11ay / WiGig
  - 60 GHz mmWave – low cost alternative to fiber

WI-FI FUTURE

- Next Generation V2X – 802.11bd
- Wireless LAN Sensing – 802.11bf
- Randomized and Changing MAC Addresses – 802.11bh
- Enhanced Data Privacy – 802.11bi
- Ultra-High Reliability – 802.11bn (will be Wi-Fi 8)

LEARN MORE

- https://www.ieee802.org/11/
- www.wi-fi.org
- www.wireshark.org
- Contact me on LinkedIn
  - linkedin.com/in/christopher-hansen-52254