#sf21veu

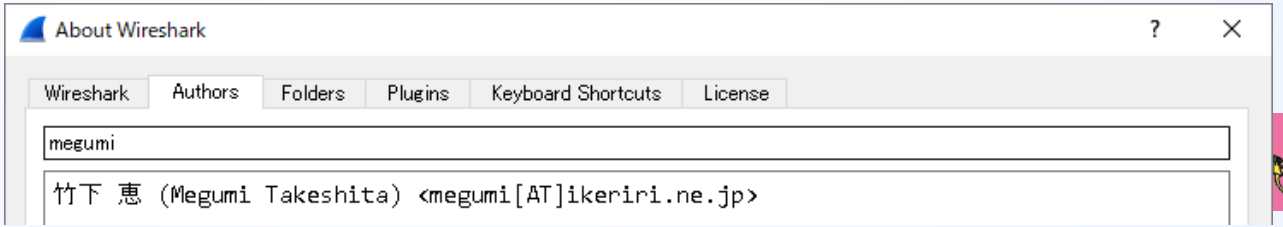
Dissecting WiFi6 using WIreshark

Megumi Takeshita
Ikeriri network service

Megumi Takeshita, packet otaku

- Founder, ikeriri network service co., ltd
- Reseller of CACE technologies in 2008
- Worked SE/IS at BayNetwork, Nortel
- Wrote 10+ books about Wireshark
- Instruct Wireshark to JSDF and other company
- Reseller of packet capture / wireless tools
- One of contributors of Wireshark
  Translate Wireshark into Japanese

#sf21veu



18 Dissecting WiFi6 using WIreshark

#sf21veu

It's time to capture WiFi6 and dissect IEEE802.11ax using Wireshark!! new method to capture traffic and filter, profile and so on. Wireless protocol

evolves year by year, now new HE (High-Efficiency) ages comes to us, the instructor will show you IEEE802.11ax protocols and the difference with

former Wi-Fi, And she will demonstrate the way to capture WiFi6 with new software/hardware. The session will also include a Wi-Fi6 specified profile

including display filter/ filter button, coloring rule and so on

Wi-Fi specification of IEEE802.11
Wi-Fi alliance named as Wi-Fi X

#sf21veu

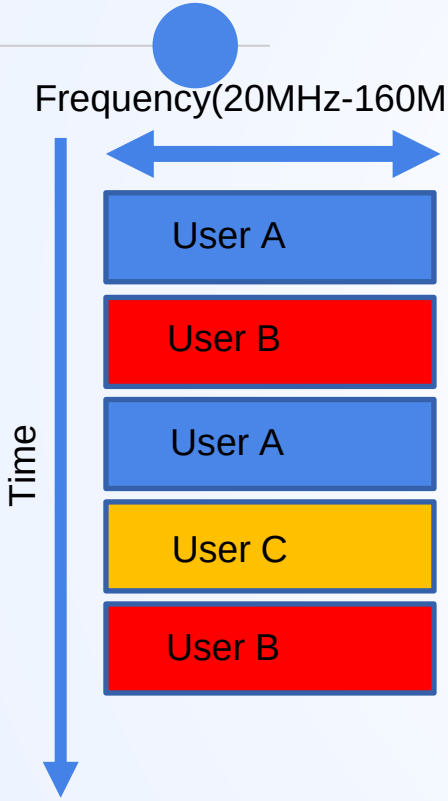
- WiFi4 IEEE802.11n 2.4GHz/5GHz ～1.2Gbps/64QAM
- WiFi5 IEEE802.11ac works only 5GHz ～3.5Gbps/256QAM
- WiFi6 IEEE802.11ax 2.4GHz/5GHz ～9.6Gbps/1024QAM
- WiFi6E IEEE802.11ax and 6GHz ～9.6Gbps/1024QAM
  Unfortunately Japanese Ministry of Internal Affairs and Communications may not allow 6GHz until 2022..
- Wi-Fi7 IEEE802.11be and 2.4/5/6GHz ～46Gbps/4096QAM

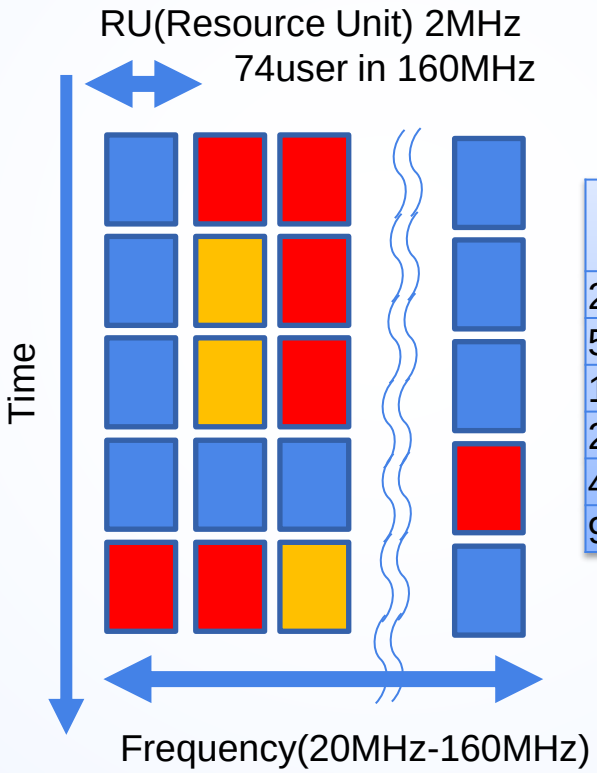
WiFi6 is common specification of wireless standard

Big change of Wi-Fi 6

- Wi-Fi is a kind of repeater of 10BASE2/5 until WiFi5
- All Clients connected with AP never send a packet at a time, clients share a frequency and one uses the channel, the others have to wait for the end of sending. (a.k.a Wired CSMA/CD, Wireless CSMA/CA)
- WiFi6 uses OFDMA as well as OFDM OFDMA (Orthogonal Frequency Division Multiple Access) is used by LTE too.

From OFDM to OFDMA





- OFDMA divide channel by RU to assign users

Resource Unit /Bandwidth	20	30	80	160
26-Tone RU	9	18	37	74
52-Tone RU	4	8	16	32
106-Tone RU	2	4	8	16
242-Tone RU	1	2	4	8
484-Tone RU	N/A	1	2	4
996-Tone RU	N/A	N/A	1	2

- WiFi6 also uses MU-MIMO with multiple antennas/streams

MCS Modulation and Coding Scheme

Wi-Fi physical spec has different sets of Spatial streams,

Modulation type: Way to send bit by 1 wave (signal),

Coding Rate: Percentage of data stream used to transmit data,
Guard interval: time between each frame and bandwidth
MCS determines logical speed of wireless network

- WiFi4 HT High Throughput ~64QAM / 40MHz BW
- Wi-Fi5 VHT Very High Throughput ~256QAM / 160MHz BW
- WiFi6/WiFi6E HE High Efficiency ~1024QAM / 160MHz BW
- Wi-Fi7 EHT Extremely High Throughput ~4096QAM / 320MHz

mscindex.com(MU-OFDMA 802.11ax)

#sf21veu

MCS Index	Spatial Stream	Modulation	Coding	MU-OFDMA (802.11ax)																
				26-tone RU			52-tone RU			106-tone RU			242-tone RU			484-tone RU			996-tone RU		
				0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI
0	1	BPSK	1/2	0.9	0.8	0.8	1.8	1.7	1.5	3.8	3.5	3.2	8.6	8.1	7.3	17.2	16.3	14.6	36	34	30.6
1	1	QPSK	1/2	1.8	1.7	1.5	3.5	3.3	3	7.5	7.1	6.4	17.2	16.3	14.6	34.4	32.5	29.3	72.1	68.1	61.3
2	1	QPSK	3/4	2.6	2.5	2.3	5.3	5	4.5	11.3	10.6	9.6	25.8	24.4	21.9	51.6	48.8	43.9	108.1	102.1	91.9
3	1	16-QAM	1/2	3.5	3.3	3	7.1	6.7	6	15	14.2	12.8	34.4	32.5	29.3	68.8	65	58.5	144.1	136.1	122.5
4	1	16-QAM	3/4	5.3	5	4.5	10.6	10	9	22.5	21.3	19.1	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8
5	1	64-QAM	2/3	7.1	6.7	6	14.1	13.3	12	30	28.3	25.5	68.8	65	58.5	137.6	130	117	288.2	272.2	245
6	1	64-QAM	3/4	7.9	7.5	6.8	15.9	15	13.5	33.8	31.9	28.7	77.4	73.1	65.8	154.9	146.3	131.6	324.3	306.3	275.6
7	1	64-QAM	5/6	8.8	8.3	7.5	17.6	16.7	15	37.5	35.4	31.9	86	81.3	73.1	172.1	162.5	146.3	360.3	340.3	306.3
8	1	256-QAM	3/4	10.6	10	9	21.2	20	18	45	42.5	38.3	103.2	97.5	87.8	206.5	195	175.5	432.4	408.3	367.5
9	1	256-QAM	5/6	11.8	11.1	10	23.5	22.2	20	50	47.2	42.5	114.7	108.3	97.5	229.4	216.7	195	480.4	453.7	408.3
10	1	1024-QAM	3/4	13.2	12.5	11.3	26.5	25	22.5	56.3	53.1	47.8	129	121.9	109.7	258.1	243.8	219.4	540.4	510.4	459.4
11	1	1024-QAM	5/6	14.7	13.9	12.5	29.4	27.8	25	62.5	59	53.1	143.4	135.4	121.9	286.8	270.8	243.8	600.5	567.1	510.4
0	2	BPSK	1/2	1.8	1.7	1.5	3.5	3.3	3	7.5	7.1	6.4	17.2	16.3	14.6	34.4	32.5	29.3	72.1	68.1	61.3
1	2	QPSK	1/2	3.5	3.3	3	7.1	6.7	6	15	14.2	12.8	34.4	32.5	29.3	68.8	65	58.5	144.1	136.1	122.5
2	2	QPSK	3/4	5.3	5	4.5	10.6	10	9	22.5	21.3	19.1	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8
3	2	16-QAM	1/2	7.1	6.7	6	14.1	13.3	12	30	28.3	25.5	68.8	65	58.5	137.6	130	117	288.2	272.2	245
4	2	16-QAM	3/4	10.6	10	9	21.2	20	18	45	42.5	38.3	103.2	97.5	87.8	206.5	195	175.5	432.4	408.3	367.5
5	2	64-QAM	2/3	14.1	13.3	12	28.2	26.7	24	60	56.7	51	137.6	130	117	275.3	260	234	576.5	544.4	490
6	2	64-QAM	3/4	15.9	15	13.5	31.8	30	27	67.5	63.8	57.4	154.9	146.3	131.6	309.7	292.5	263.3	648.5	612.5	551.3
7	2	64-QAM	5/6	17.6	16.7	15	35.3	33.3	30	75	70.8	63.8	172.1	162.5	146.3	344.1	325	292.5	720.6	680.6	612.5
8	2	256-QAM	3/4	21.2	20	18	42.4	40	36	90	85	76.5	206.5	195	175.5	412.9	390	351	864.7	816.7	735
9	2	256-QAM	5/6	23.5	22.2	20	47.1	44.4	40	100	94.4	85	229.4	216.7	195	458.8	433.3	390	960.8	907.4	816.7
10	2	1024-QAM	3/4	26.5	25	22.5	52.9	50	45	112.5	106.3	95.6	258.1	243.8	219.4	516.2	487.5	438.8	1080.9	1020.8	918.8
11	2	1024-QAM	5/6	29.4	27.8	25	58.8	55.6	50	125	118.1	106.3	286.8	270.8	243.8	573.5	541.7	487.5	1201	1134.3	1020.8
0	3	BPSK	1/2	2.6	2.5	2.3	5.3	5	4.5	11.3	10.6	9.6	25.8	24.4	21.9	51.6	48.8	43.9	108.1	102.1	91.9
1	3	QPSK	1/2	5.3	5	4.5	10.6	10	9	22.5	21.3	19.1	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8
2	3	QPSK	3/4	7.9	7.5	6.8	15.9	15	13.5	33.8	31.9	28.7	77.4	73.1	65.8	154.9	146.3	131.6	324.3	306.3	275.6
3	3	16-QAM	1/2	10.6	10	9	21.2	20	18	45	42.5	38.3	103.2	97.5	87.8	206.5	195	175.5	432.4	408.3	367.5
4	3	16-QAM	3/4	15.9	15	13.5	31.8	30	27	67.5	63.8	57.4	154.9	146.3	131.6	309.7	292.5	263.3	648.5	612.5	551.3
5	3	64-QAM	2/3	21.2	20	18	42.4	40	36	90	85	76.5	206.5	195	175.5	412.9	390	351	864.7	816.7	735
6	3	64-QAM	3/4	23.8	22.5	20.3	47.6	45	40.5	101.3	95.6	86.1	232.3	219.4	197.4	464.6	438.8	394.9	972.8	918.8	826.9
7	3	64-QAM	5/6	26.5	25	22.5	52.9	50	45	112.5	106.3	95.6	258.1	243.8	219.4	516.2	487.5	438.8	1080.9	1020.8	918.8
8	3	256-QAM	3/4	31.8	30	27	63.5	60	54	135	127.5	114.8	309.7	292.5	263.3	619.4	585	526.5	1297.1	1225	1102.5
9	3	256-QAM	5/6	35.3	33.3	30	70.6	66.7	60	150	141.7	127.5	344.1	325	292.5	688.2	650	585	1441.2	1361.1	1225
10	3	1024-QAM	3/4	39.7	37.5	33.8	79.4	75	67.5	168.8	159.4	143.4	387.1	365.6	329.1	774.3	731.3	658.1	1621.3	1531.3	1378.1
11	3	1024-QAM	5/6	44.1	41.7	37.5	88.2	83.3	75	187.5	177.1	159.4	430.1	406.3	365.6	860.3	812.5	731.3	1801.5	1701.4	1531.3

Capturing WiFi6 in Windows10

There are many new features such as OFDMA, MU-MIMO, beam forming, higher order of modulation, power consumption, new interval/symbols/FFT(Fast Fourier Transform size), etc.

https://standards.ieee.org/project/802_11ax.html

OK, its time to capture WiFi6, We wants to capture WiFi6 in Windows10 environment, so we choose TamoSoft CommView for Wi-Fi and Intel AX200 M.2 Wireless card.

Note: there are another way to capture WiFi6 such as using extcap interface of Wireshark to connect access point worked as sniffer mode, Linux way, or MacOS way.

ASUS RT-AX89X Wi-Fi 6, 1024QAM MU-MIMO, HE160 and HE80+80

https://deviwiki.com/wiki/ASUS_RT-AX89X

This time we test RT-AC89X and iPad Pro 11(2nd gen), iOS 14.6,

802.11ax Wi-Fi 6 2x2 MIMO

5GHz max PHY 1200Mbps

Bandwidth 80MHz

Max MCS11(HE)

https://support.apple.com/ja-jp/guide/deployment-reference-ios/apd9f0a6151e/web

(Qualcomm Snapdragon X55 5G Modem)

ASUS RT-AX89X
Availability: unreleased

Manuf/OEM/ODM Askey

Country of manuf.: China
Series: AX6000

Type: wireless router

FCC ID: MSQ-RTAX2E00

Power: 19 VDC, 3.42 A
Connector type: barrel

CPU1: Qualcomm IPQ8078 (2.2 GHz, 4 cores)
FLA1: 256 MiB (Macronix MX30UF2G18AC-XKI)
RAM1: 1 GiB (Micron MT41K256M16TW-107 × 2)

Expansion IFs: USB 3.0, SFP+
USB ports: 2
SFP ports: 1
Serial: yes, 4-pin header, J901

WI1 chip1: Qualcomm QCN5054
WI1 chip2: Qualcomm QCN5054
WI1 802dot11 protocols: an+ac+ax
WI1 MIMO config: 8x8:8
WI1 antenna connector: MHF4
WI2 chip1: Qualcomm QCN5024
WI2 802dot11 protocols: bgn+ax
WI2 MIMO config: 4x4:4
WI2 antenna connector: MHF4

ETH chip1: Atheros AR8035-A
ETH chip2: Aquantia AQR109
ETH chip3: Atheros AR8033
Switch: Qualcomm Atheros QCA8337
LAN speed: 1G
LAN ports: 8
WAN speed: 10G
WAN ports: 2

abgn+ac+ax

https://wikidevi.wi-cat.ru/Intel_Wi-Fi_6_AX200_(AX200NGW)

- Windows10 Pro 64bit
- Intel AX200 NGW
- TamoSoft CommView for Wi-Fi

You can capture WiFi6 frames with 160MHz bandwidth, 1024QAM by Intel AX200 NGW and CommView for Wi-Fi

Interface: NGFF
Connector: M.2 Form factor tags: 2230 (Key A/E)
ID: 8086:2723 (1 addl. devices) Windows: PCI¥VEN_8086&DEV_2723
FCC ID: PD9AX200NG, MSQAX200NG, RWO-RZ090301, RWO-RZ090287 IC ID: 1000M-AX200NG, 3568A-AX200NG, 8092D-RZ090301
WI1 chip1: Intel WCSAX200
Probable Linux driver iwlwifi *Full support it is available in 5.5.0-rc kernel* (see also passys)
Windows driver ***Win10*** *(64-bit only)*
Antenna connector: MHF4
abgn+ac+ax, 2x2:2
Flags: Wi-Fi 6, 1024QAM, HE160, VHT160, DFS (slave), Bluetooth 5.0
OUI: 9C:FC:E8 (-, 1 W)

DEMO1 Ping to wired PC (cleartext)

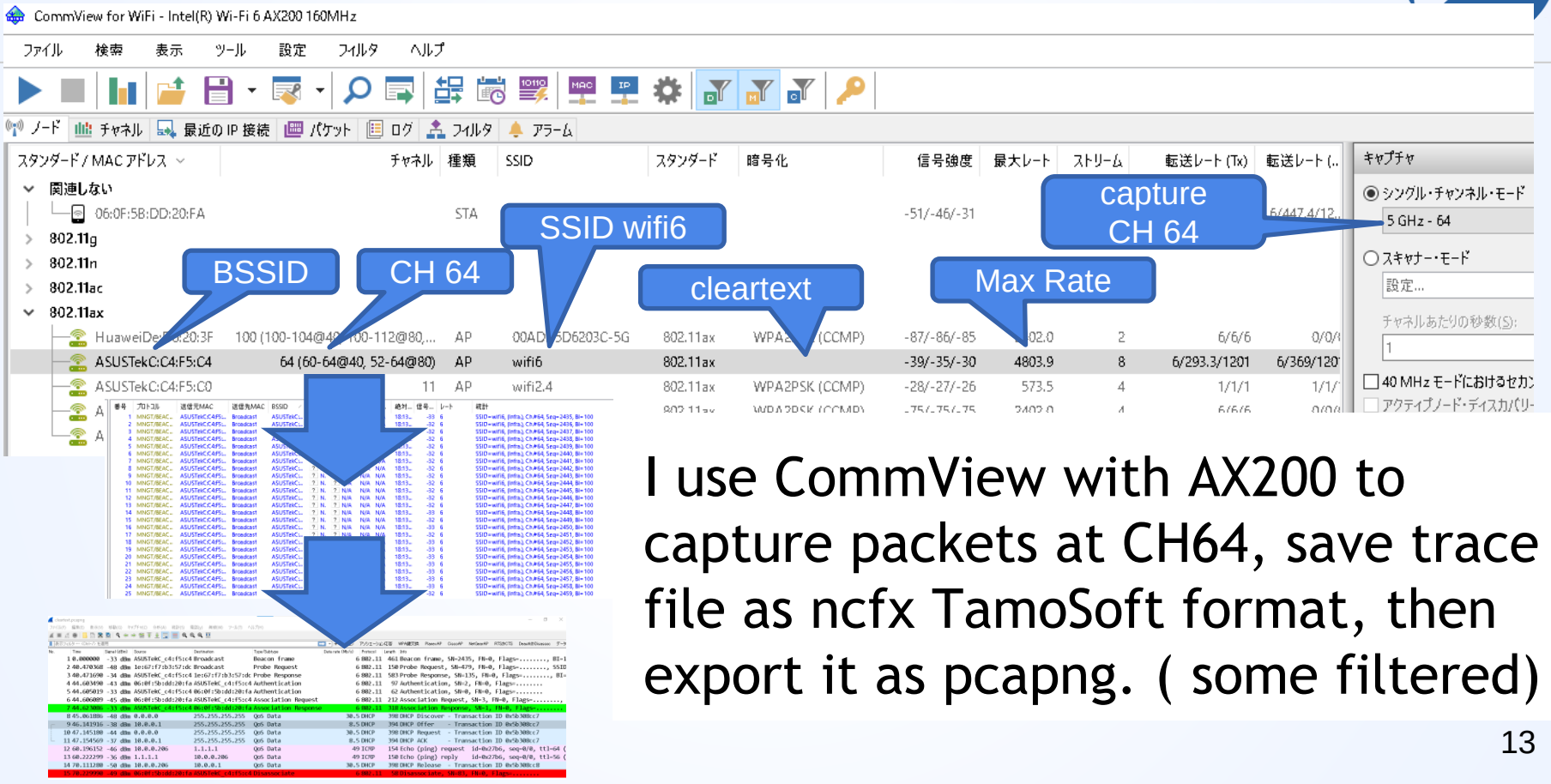
- SSID:wifi6
- Security: cleartext
- BSSID:F02F74C4F5C0
- STA iPad:060F5BDD20FA
- Channel 128MHz

(1)Connect iPad to AP

(2)Ping to a wired PC

(3)Click Forget Network to disconnect AP

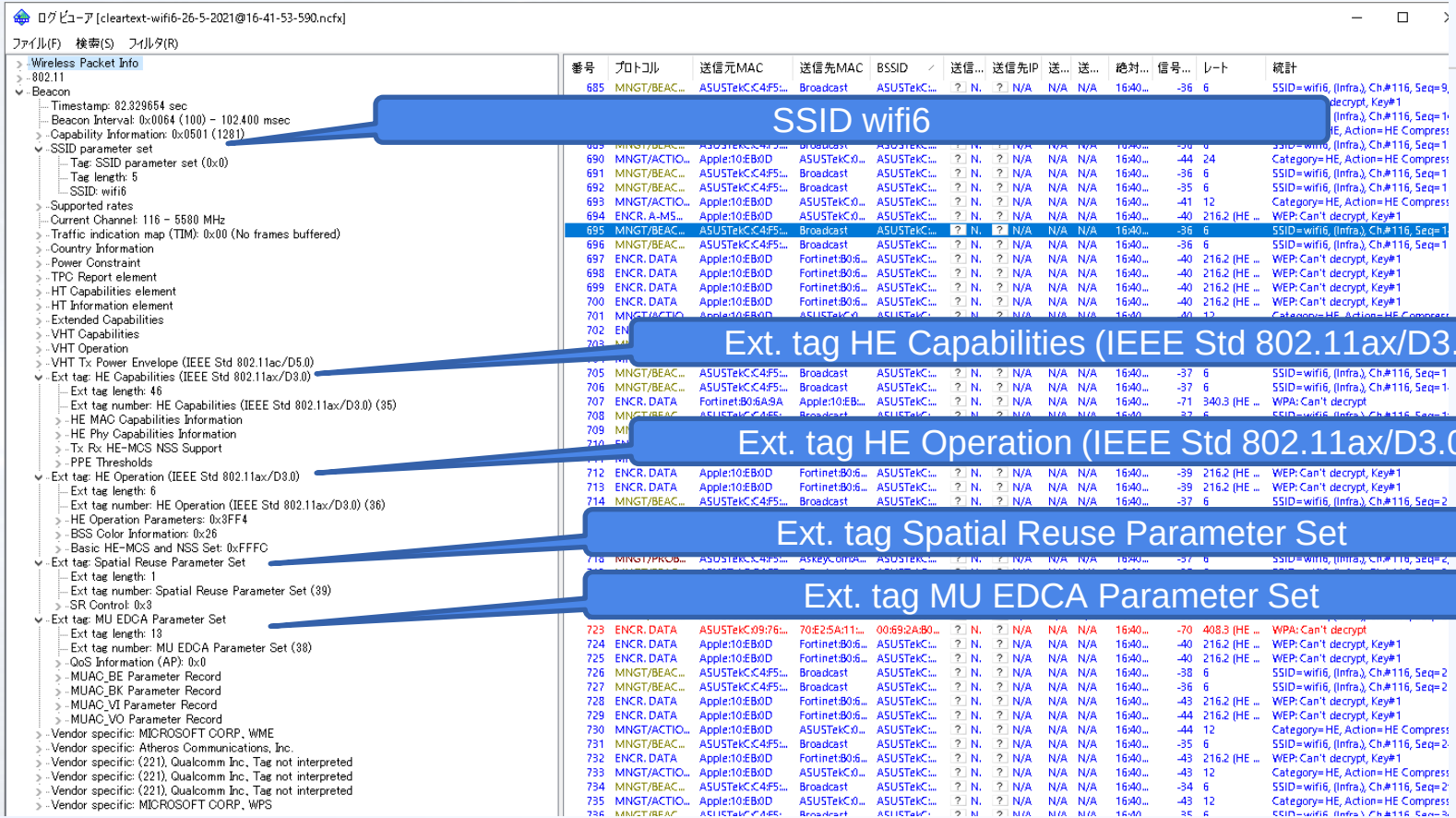
Use CommView to capture packets



I use CommView with AX200 to capture packets at CH64, save trace file as ncfx TamoSoft format, then export it as pcapng. (some filtered)

Original ncfx file:beacon frame from AP

#sf21veu



Sample trace file: cleartext.pcapng

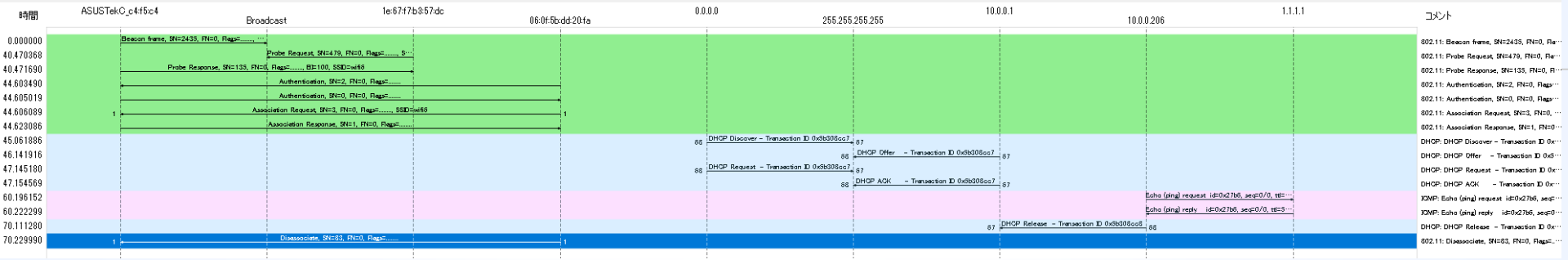
No.	Time	Signal (dBm)	Source	Destination	Type/Subtype	Data rate (Mb/s)	Protocol	Length	Info
1	0.000000	-33 dBm	ASUSTekC_c4:f5:c4	Broadcast	Beacon frame	6	802.11	461	Beacon frame, SN=2435, FN=0, Flags=........, BI=1
2	40.470368	-48 dBm	1e:67:f7:b3:57:dc	Broadcast	Probe Request	6	802.11	150	Probe Request, SN=479, FN=0, Flags=........, SSID
3	40.471690	-34 dBm	ASUSTekC_c4:f5:c4	1e:67:f7:b3:57:dc	Probe Response	6	802.11	583	Probe Response, SN=135, FN=0, Flags=........, BI=
4	44.603490	-43 dBm	06:0f:5b:dd:20:fa	ASUSTekC_c4:f5:c4	Authentication	6	802.11	97	Authentication, SN=2, FN=0, Flags=........
5	44.605019	-33 dBm	ASUSTekC_c4:f5:c4	06:0f:5b:dd:20:fa	Authentication	6	802.11	62	Authentication, SN=0, FN=0, Flags=........
6	44.606089	-45 dBm	06:0f:5b:dd:20:fa	ASUSTekC_c4:f5:c4	Association Request	6	802.11	212	Association Request, SN=3, FN=0, Flags=........,
7	44.623086	-33 dBm	ASUSTekC_c4:f5:c4	06:0f:5b:dd:20:fa	Association Response	6	802.11	318	Association Response, SN=1, FN=0, Flags=........
8	45.061886	-48 dBm	0.0.0.0	255.255.255.255	QoS Data	30.5	DHCP	398	DHCP Discover - Transaction ID 0x5b308cc7
9	46.141916	-38 dBm	10.0.0.1	255.255.255.255	QoS Data	8.5	DHCP	394	DHCP Offer - Transaction ID 0x5b308cc7
10	47.145180	-44 dBm	0.0.0.0	255.255.255.255	QoS Data	30.5	DHCP	398	DHCP Request - Transaction ID 0x5b308cc7
11	47.154569	-37 dBm	10.0.0.1	255.255.255.255	QoS Data	8.5	DHCP	394	DHCP ACK - Transaction ID 0x5b308cc7
12	60.196152	-46 dBm	10.0.0.206	1.1.1.1	QoS Data	49	ICMP	154	Echo (ping) request id=0x27b6, seq=0/0, ttl=64 (
13	60.222299	-36 dBm	1.1.1.1	10.0.0.206	QoS Data	49	ICMP	150	Echo (ping) reply id=0x27b6, seq=0/0, ttl=56 (
14	70.111280	-50 dBm	10.0.0.206	10.0.0.1	QoS Data	30.5	DHCP	398	DHCP Release - Transaction ID 0x5b308cc8
15	70.229990	-49 dBm	06:0f:5b:dd:20:fa	ASUSTekC_c4:f5:c4	Disassociate	6	802.11	58	Disassociate, SN=83, FN=0, Flags=........

cleartext.pcapng is a kind of typical communication between STA(06:0f:5b:dd:20:fa) and AP(ASUSTekC_c4:f5:c4)

Note: iPad pro uses private mac address so Probe Request and Probe Response frame's mac address is not match correctly.

There are tons of fields, so we focus main fields and functions.

Sample trace file: cleartext.pcapng



- #1 STA(iPad Pro) receive ASUS(SSID is wifi6) Beacon
- #2 #3 Probe Request <> Probe Response
- #4 #5 Authentication (Open System)
- #6 #7 Association Request <> Association Response
- #8-#14 Plaintext Data such as DHCP, ICMP
- #15 Disassociate from STA

#1 Beacon from AP

#sf21veu

```
> Frame 1: 461 bytes on wire (3688 bits), 461 bytes captured (3688 bits) on interface unknown, id 0
> Radiotap Header v0, Length 32
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (393 bytes)
    > Tag: SSID parameter set: wifi
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 64
    > Tag: Traffic Indication Map (TIM): DTIM 1 of 1 bitmap
    > Tag: Country Information: Country Code JP, Environment Any
    > Tag: Power Constraint: 3
    > Tag: TPC Report Transmit Power: 20, Link Margin: 0
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: HT Information (802.11n D1.10)
    > Tag: Extended Capabilities (10 octe
    > Tag: VHT Capabilities
    > Tag: VHT Operation
    > Tag: VHT Tx Power Envelope
    > Ext Tag: HE Capabilities (IEEE Std 802.11ax
    > Ext Tag: HE Operation (IEEE Std 802.11ax/D3.0)
    > Ext Tag: Spatial Reuse Parameter Set
    > Ext Tag: MU EDCA Parameter Set
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Para
    > Tag: Vendor Specific: Atheros Communications, Inc.:
    > Tag: Vendor Specific: Qualcomm Inc.
    > Tag: Vendor Specific: Qualcomm Inc.
    > Tag: Vendor Specific: Qualcomm Inc.
    > Tag: Vendor Specific: Microsoft Corp.: WPS
```

SSID wifi6

Ext. tag HE Capabilities (IEEE Std 802.11ax/D3.0)

Ext. tag HE Operation (IEEE Std 802.11ax/D3.0)

Ext. tag Spatial Reuse Parameter Set)

Ext. tag MU EDCA Parameter Set

HE Capabilities show ax specification of AP

#sf21veu

```
Ext Tag: HE Capabilities (IEEE Std 802.11ax/D3.0)
    Tag Number: Element ID Extension (255)
    Ext Tag length: 46
    Ext Tag Number: HE Capabilities (IEEE Std 802.11ax/D3.0) (35)
  > HE MAC Capabilities Information: 0x00401a08010d
  v HE Phy Capabilities Information
    > .... ...0 = Reserved: 0x0
    > 0000 010. = Channel Width Set: 0x02
    > Bits 8 to 23: 0x0c60
    > Bits 24 to 39: 0x7d88
    > Bits 40 to 55: 0x83c7
    > Bits 56 to 71: 0x019c
    > Bits 72 to 87: 0x0008
  v Supported HE-MCS and NSS Set
    v Rx and Tx MCS Maps <= 80 MHz
      v Rx HE-MCS Map <= 80 MHz: 0xaaaa
          .... .... .... ..10 = Max HE-MCS for 1 SS: Support for HE-MCS 0-11 (0x2)
          .... .... .... 10.. = Max HE-MCS for 2 SS: Support for HE-MCS 0-11 (0x2)
          .... .... ..10 .... = Max HE-MCS for 3 SS: Support for HE-MCS 0-11 (0x2)
          .... .... 10.. .... = Max HE-MCS for 4 SS: Support for HE-MCS 0-11 (0x2)
          .... ..10 .... .... = Max HE-MCS for 5 SS: Support for HE-MCS 0-11 (0x2)
          .... 10.. .... .... = Max HE-MCS for 6 SS: Support for HE-MCS 0-11 (0x2)
          ..10 .... .... .... = Max HE-MCS for 7 SS: Support for HE-MCS 0-11 (0x2)
          10.. .... .... .... = Max HE-MCS for 8 SS: Support for HE-MCS 0-11 (0x2)
      v Tx HE-MCS Map <= 80 MHz: 0xaaaa
          .... .... .... ..10 = Max HE-MCS for 1 SS: Support for HE-MCS 0-11 (0x2)
          .... .... .... 10.. = Max HE-MCS for 2 SS: Support for HE-MCS 0-11 (0x2)
          .... .... ..10 .... = Max HE-MCS for 3 SS: Support for HE-MCS 0-11 (0x2)
          .... .... 10.. .... = Max HE-MCS for 4 SS: Support for HE-MCS 0-11 (0x2)
          .... ..10 .... .... = Max HE-MCS for 5 SS: Support for HE-MCS 0-11 (0x2)
          .... 10.. .... .... = Max HE-MCS for 6 SS: Support for HE-MCS 0-11 (0x2)
          ..10 .... .... .... = Max HE-MCS for 7 SS: Support for HE-MCS 0-11 (0x2)
          10.. .... .... .... = Max HE-MCS for 8 SS: Support for HE-MCS 0-11 (0x2)
  v PPE Thresholds
      .... .111 = NSS: 7
      111 1... = RU Index Bitmask: 0xf
    v NSS 0
      > RU allocation: 242
      > RU allocation: 484
      > RU allocation: 996
      > RU allocation: 2x996
```

HE Capabilities are parts of IEEE802.11 Wireless Management header of Beason frame, and they include AP's specification of IEEE802.11ax, there are a lot of fields, for example, supported HE-MCS and NSS Set with RX/TX MCS number with Spatial Streams and RU allocation.

#2 Probe Request from STA

#sf21veu

```
> Frame 2: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on i
> Radiotap Header v0, Length 32
> 802.11 radio information
> IEEE 802.11 Probe Request, Flags: ........
v IEEE 802.11 Wireless Management
  v Tagged parameters (94 bytes)
    > Tag: SSID parameter set: Wildcard SSID
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: Extended Capabilities (8 octets)
    > Tag: VHT Capabilities
    v Ext Tag: HE Capabilities (IEEE Std 802.11ax/D3.0)
        Tag Number: Element ID Extension (255)
        Ext Tag length: 27
        Ext Tag Number: HE Capabilities (IEEE Std 802.11ax/D3.0)
      > HE MAC Capabilities Information: 0x800000080801
      v HE Phy Capabilities Information
        > .... ...0 = Reserved: 0x0
        > 0100 010. = Channel Width Set: 0x22
        > Bits 8 to 23: 0x0230
        > Bits 24 to 39: 0x1d00
        > Bits 40 to 55: 0x9f00
        > Bits 56 to 71: 0x0008
        > Bits 72 to 87: 0x000c
      v Supported HE-MCS and NSS Set
        v Rx and Tx MCS Maps <= 80 MHz
          > Rx HE-MCS Map <= 80 MHz: 0xfffa
          > Tx HE-MCS Map <= 80 MHz: 0xfffa
      > PPE Thresholds
```

Wildcard SSID (for the first time from STA)

Ext. tag HE Capabilities (IEEE Std 802.11ax/D3.0)

HE MAC Capabilities

HE PHY Capabilities

Supported HE-MCS and NSS Set

PPE Thresholds

STA sends ax specification of AP


```
Ext Tag: HE Capabilities (IEEE Std 802.11ax/D3.0)
  Tag Number: Element ID Extension (255)
  Ext Tag length: 27
  Ext Tag Number: HE Capabilities (IEEE Std 802.11ax/D3.0) (35)
> HE MAC Capabilities Information: 0x800000080801
v HE Phy Capabilities Information
  > .... ...0 = Reserved: 0x0
  > 0100 010. = Channel Width Set: 0x22
  > Bits 8 to 23: 0x0230
  > Bits 24 to 39: 0x1d00
  > Bits 40 to 55: 0x9f00
  > Bits 56 to 71: 0x0008
  > Bits 72 to 87: 0x000c
v Supported HE-MCS and NSS Set
  v Rx and Tx MCS Maps <= 80 MHz
    v Rx HE-MCS Map <= 80 MHz: 0xfffa
        .... .... .... ..10 = Max HE-MCS for 1 SS: Support for HE-MCS 0-11 (0x2)
        .... .... .... 10.. = Max HE-MCS for 2 SS: Support for HE-MCS 0-11 (0x2)
        .... .... ..11 .... = Max HE-MCS for 3 SS: Not supported for HE PPDUs (0x3)
        .... .... 11.. .... = Max HE-MCS for 4 SS: Not supported for HE PPDUs (0x3)
        .... ..11 .... .... = Max HE-MCS for 5 SS: Not supported for HE PPDUs (0x3)
        .... 11.. .... .... = Max HE-MCS for 6 SS: Not supported for HE PPDUs (0x3)
        ..11 .... .... .... = Max HE-MCS for 7 SS: Not supported for HE PPDUs (0x3)
        11.. .... .... .... = Max HE-MCS for 8 SS: Not supported for HE PPDUs (0x3)
    > Tx HE-MCS Map <= 80 MHz: 0xfffa
v PPE Thresholds
    .... .001 = NSS: 1
    .011 1... = RU Index Bitmask: 0x7
  v NSS 0
    > RU allocation: 242
    > RU allocation: 484
    > RU allocation: 996
  > NSS 1
```

STA sends IEEE802.11ax specification in Probe Request frame. There are a lot of fields,

For example, STA sends supported MCS, bandwidth, RU allocation in HE-MCS and NSS Set and PPE Thresholds fields.

#3 Probe Response from AP

#sf21veu

```
> Frame 3: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on i
> Radiotap Header v0, Length 32
> 802.11 radio information
> IEEE 802.11 Probe Response, Flags: ........
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (515 bytes)
    > Tag: SSID parameter set: wifi6
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 64
    > Tag: Country Information: Country Code JP, Environment Any
    > Tag: Power Constraint: 3
    > Tag: TPC Report Transmit Power: 20, Link Margin: 0
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: HT Information (802.11n D1.10)
    > Tag: Extended Capabilities (10 octets)
    > Tag: VHT Capabilities
    > Tag: VHT Operation
    > Tag: VHT Tx Power Envelope
    > Ext Tag: HE Capabilities (IEEE Std 802.11ax/D3.0)
    > Ext Tag: HE Operation (IEEE Std 802.11ax/D3.0)
    > Ext Tag: Spatial Reuse Parameter Set
    > Ext Tag: MU EDCA Parameter Set
    > Tag: Vendor Specific: Microsoft Corp.: [illegible]
    > Tag: Vendor Specific: Atheros Communications, Inc.: [illegible]
    > Tag: Vendor Specific: Qualcomm Inc.
    > Tag: Vendor Specific: Microsoft Corp.: WPS
    > Tag: Vendor Specific: Qualcomm Inc.
    > Tag: Vendor Specific: Qualcomm Inc.
```

SSID: wifi6

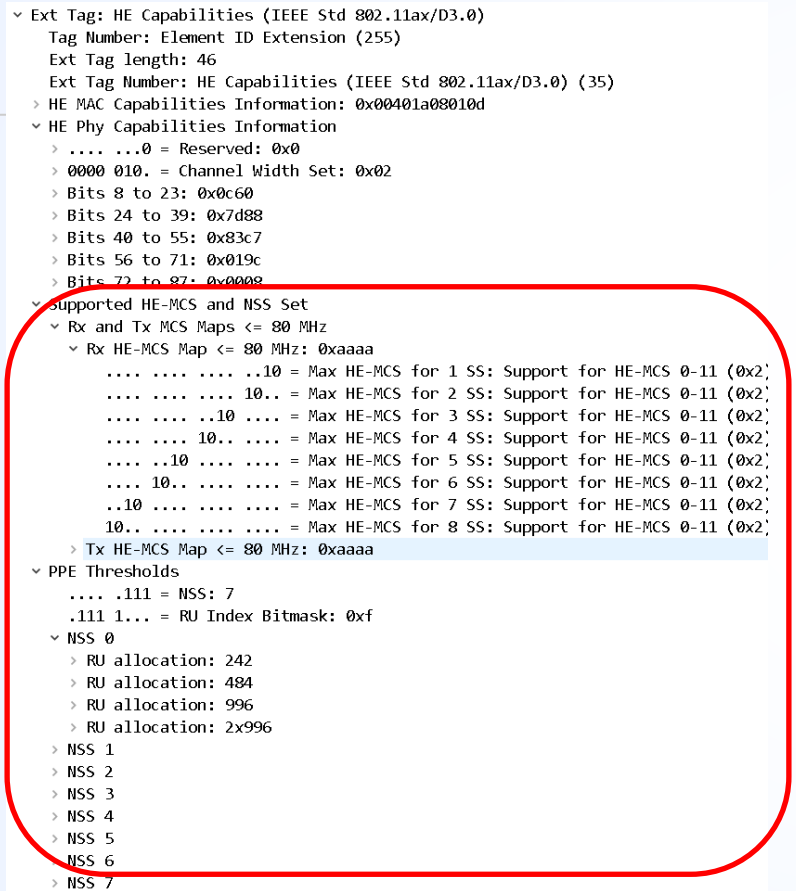
Ext. tag HE Capabilities (IEEE Std 802.11ax/D3.0)

Ext. tag HE Operation (IEEE Std 802.11ax/D3.0)

Ext. tag Spatial Reuse Parameter Set

Ext Tag: MU EDCA Parameter Set

AP sends IEEE802.11ax specification



#sf21veu

HE Capabilities are parts of IEEE802.11 Wireless Management header of Probe Response frame, and they include AP's .11ax setting to STA. There are a lot of fields, for example, supported HE-MCS and NSS Set with RX/TX MCS number with Spatial Streams and RU allocation.

#4 #5 Authentication (Open System)

```
> Frame 4: 97 bytes on wire (776 bits), 97 bytes
> Radiotap Header v0, Length 32
> 802.11 radio information
> IEEE 802.11 Authentication, Flags: ........
v IEEE 802.11 Wireless Management
  v Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0001
      Status code: Successful (0x0000)
  v Tagged parameters (35 bytes)
    > Tag: Extended Capabilities (8 octets)
    > Tag: Vendor Specific: Apple, Inc.
    > Tag: Vendor Specific: Broadcom
```

```
> Frame 5: 62 bytes on wire (496 bits), 62 bytes
> Radiotap Header v0, Length 32
> 802.11 radio information
> IEEE 802.11 Authentication, Flags: ........
v IEEE 802.11 Wireless Management
  v Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0002
      tus code: Successful (0x0000)
```

Authentication Algorithm: Open System

Status code: Successful

Tag: Extend Capabilities

Tag: Vendor Specific: Apple and Broadcom

Authentication process of 11ax is the same as other legacy Wi-Fi, just check SSID name using Open System algorithm

#6 Association Request from STA

#sf21veu

```
> Frame 6: 212 bytes on wire (1696 bits), 212 bytes captured (1696 bits) on inter
> Radiotap Header v0, Length 32
> 802.11 radio information
> IEEE 802.11 Association Request, Flags: ........
v IEEE 802.11 Wireless Management
  > Fixed parameters (4 bytes)
  v Tagged parameters (152 bytes)
    > Tag: SSID parameter set: wifi6
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: Power Capability Min: -7, Max: 20
    > Tag: Supported Channels
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: Extended Capabilities (8 octets)
    > Tag: VHT Capabilities
    v Ext Tag: HE Capabilities (IEEE Std 802.11ax/D3.0)
        Tag Number: Element ID Extension (255)
        Ext Tag length: 27
        Ext Tag Number: HE Capabilities (IEEE Std 802.11ax/D
      > HE MAC Capabilities Information: 0x800000080801
      > HE Phy Capabilities Information
      > Supported HE-MCS and NSS Set
      > PPE Thresholds
    > Tag: Vendor Specific: Apple, Inc.
    > Tag: Vendor Specific: Epigram, Inc.
    > Tag: Vendor Specific: Broadcom
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information Element
```

SSID: wifi6

Ext. tag HE Capabilities (IEEE Std 802.11ax/D3.0)

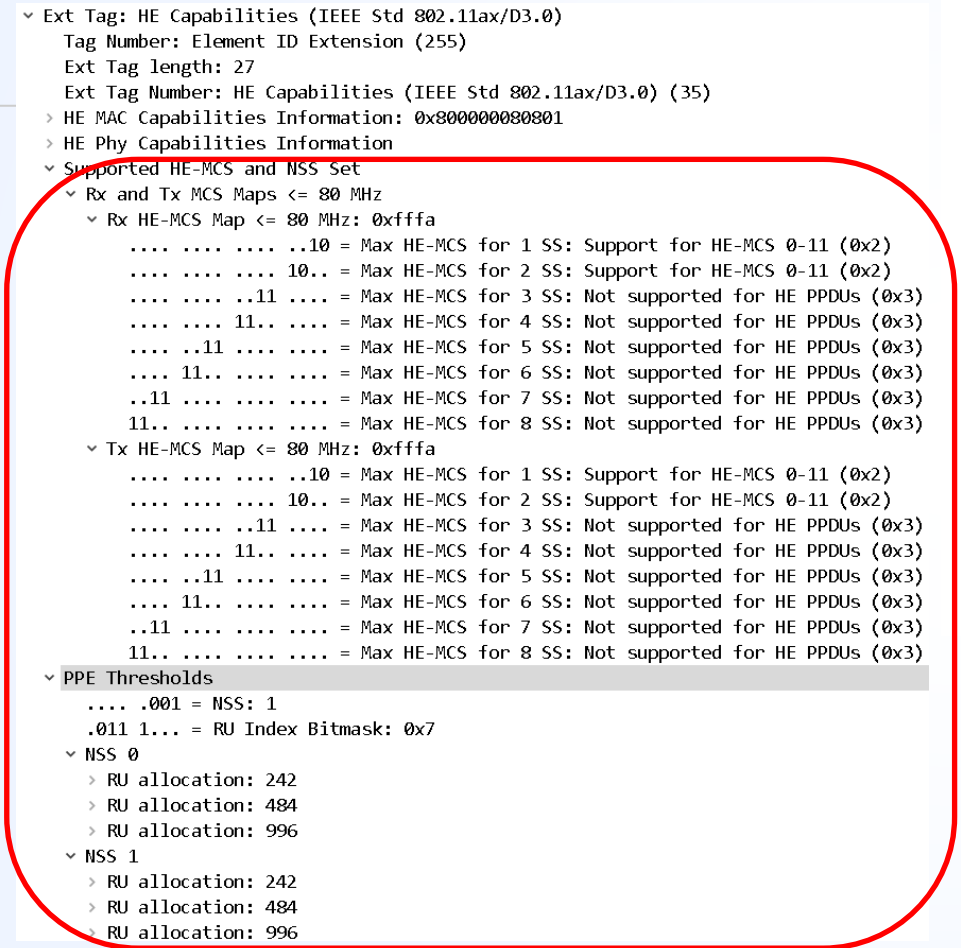
HE MAC Capabilities Information

HE PHY Capabilities Information

Supported HE-MCS and NSS Set

PPE Thresholds

STA sends actual connection settings



```
Ext Tag: HE Capabilities (IEEE Std 802.11ax/D3.0)
    Tag Number: Element ID Extension (255)
    Ext Tag length: 27
    Ext Tag Number: HE Capabilities (IEEE Std 802.11ax/D3.0) (35)
  > HE MAC Capabilities Information: 0x800000080801
  > HE Phy Capabilities Information
  v Supported HE-MCS and NSS Set
    v Rx and Tx MCS Maps <= 80 MHz
      v Rx HE-MCS Map <= 80 MHz: 0xfffa
          .... .... .... ..10 = Max HE-MCS for 1 SS: Support for HE-MCS 0-11 (0x2)
          .... .... .... 10.. = Max HE-MCS for 2 SS: Support for HE-MCS 0-11 (0x2)
          .... .... ..11 .... = Max HE-MCS for 3 SS: Not supported for HE PPDUs (0x3)
          .... .... 11.. .... = Max HE-MCS for 4 SS: Not supported for HE PPDUs (0x3)
          .... ..11 .... .... = Max HE-MCS for 5 SS: Not supported for HE PPDUs (0x3)
          .... 11.. .... .... = Max HE-MCS for 6 SS: Not supported for HE PPDUs (0x3)
          ..11 .... .... .... = Max HE-MCS for 7 SS: Not supported for HE PPDUs (0x3)
          11.. .... .... .... = Max HE-MCS for 8 SS: Not supported for HE PPDUs (0x3)
      v Tx HE-MCS Map <= 80 MHz: 0xfffa
          .... .... .... ..10 = Max HE-MCS for 1 SS: Support for HE-MCS 0-11 (0x2)
          .... .... .... 10.. = Max HE-MCS for 2 SS: Support for HE-MCS 0-11 (0x2)
          .... .... ..11 .... = Max HE-MCS for 3 SS: Not supported for HE PPDUs (0x3)
          .... .... 11.. .... = Max HE-MCS for 4 SS: Not supported for HE PPDUs (0x3)
          .... ..11 .... .... = Max HE-MCS for 5 SS: Not supported for HE PPDUs (0x3)
          .... 11.. .... .... = Max HE-MCS for 6 SS: Not supported for HE PPDUs (0x3)
          ..11 .... .... .... = Max HE-MCS for 7 SS: Not supported for HE PPDUs (0x3)
          11.. .... .... .... = Max HE-MCS for 8 SS: Not supported for HE PPDUs (0x3)
  v PPE Thresholds
      .... .001 = NSS: 1
      .011 1... = RU Index Bitmask: 0x7
    v NSS 0
      > RU allocation: 242
      > RU allocation: 484
      > RU allocation: 996
    v NSS 1
      > RU allocation: 242
      > RU allocation: 484
      > RU allocation: 996
```

STA sends actual connection settings to AP.

- Bandwidth <=80MHz
- MCS 0-11
- Spatial Streams 1-2
- RU 242,484,996

There are other many setting information in HE MAC Capabilities and HE PHY Capabilities, Supported Channels, SSID and so on.

3.2μs Guard Interval Supported

```
HE Phy Capabilities Information
  .... ...0 = Reserved: 0x0
  0100 010. = Channel Width Set: 0x22
     .... ..0. = 40MHz in 2.4GHz band: Not supported
     .... .1.. = 40 & 80MHz in the 5GHz band: Supported
     .... 0... = 160MHz in the 5GHz band: Not supported
     ...0 .... = 160/80+80MHz in the 5GHz band: Not supported
     ..0. .... = 242 tone RUs in the 2.4GHz band: Not supported
     .1.. .... = 242 tone RUs in the 5GHz band: Supported
     0... .... = Reserved: 0x0
  Bits 8 to 23: 0x0230
     .... .... .... 0000 = Punctured Preamble RX: 0x0
     .... .... ...1 .... = Device Class: Class B Device (0x1)
     .... .... ..1. .... = LDPC Coding In Payload: Supported
     .... .... .0.. .... = HE SU PPDU With 1x HE-LTF and 0.8us GI: Not supported
     .... ...0 0... .... = Midamble Rx Max NSTS: 1 Space-Time Stream (0x0)
     .... ..1. .... .... = NDP With 4x HE-LTF and 3.2us GI: Supported
     .... .0.. .... .... = STBC Tx <= 80 MHz: Not supported
     .... 0... .... .... = STBC Rx <= 80 MHz: Not supported
     ...0 .... .... .... = Doppler Tx: Not supported
     ..0. .... .... .... = Doppler Rx: Not supported
     .0.. .... .... .... = Full Bandwidth UL MU-MIMO: Not supported
```

(802.11ax)

MCS Index	Spatial Stream	Modulation	Coding	242-tone RU			484-tone RU			996-tone RU		
				0.8μs GI	1.6μs GI	3.2μs GI	0.8μs GI	1.6μs GI	3.2μs GI	0.8μs GI	1.6μs GI	3.2μs GI
0	1	BPSK	1/2	8.6	8.1	7.3	17.2	16.3	14.6	36	34	30.6
1	1	QPSK	1/2	17.2	16.3	14.6	34.4	32.5	29.3	72.1	68.1	61.3
2	1	QPSK	3/4	25.8	24.4	21.9	51.6	48.8	43.9	108.1	102.1	91.9
3	1	16-QAM	1/2	34.4	32.5	29.3	68.8	65	58.5	144.1	136.1	122.5
4	1	16-QAM	3/4	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8
5	1	64-QAM	2/3	68.8	65	58.5	137.6	130	117	288.2	272.2	245
6	1	64-QAM	3/4	77.4	73.1	65.8	154.9	146.3	131.6	324.3	306.3	275.6
7	1	64-QAM	5/6	86	81.3	73.1	172.1	162.5	146.3	360.3	340.3	306.3
8	1	256-QAM	3/4	103.2	97.5	87.8	206.5	195	175.5	432.4	408.3	367.5
9	1	256-QAM	5/6	114.7	108.3	97.5	229.4	216.7	195	480.4	453.7	408.3
10	1	1024-QAM	3/4	129	121.9	109.7	258.1	243.8	219.4	540.4	510.4	459.4
11	1	1024-QAM	5/6	143.4	135.4	121.9	286.8	270.8	243.8	600.5	567.1	510.4
0	2	BPSK	1/2	17.2	16.3	14.6	34.4	32.5	29.3	72.1	68.1	61.3
1	2	QPSK	1/2	34.4	32.5	29.3	68.8	65	58.5	144.1	136.1	122.5
2	2	QPSK	3/4	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8
3	2	16-QAM	1/2	68.8	65	58.5	137.6	130	117	288.2	272.2	245
4	2	16-QAM	3/4	103.2	97.5	87.8	206.5	195	175.5	432.4	408.3	367.5
5	2	64-QAM	2/3	137.6	130	117	275.3	260	234	576.5	544.4	490
6	2	64-QAM	3/4	154.9	146.3	131.6	309.7	292.5	263.3	648.5	612.5	551.3
7	2	64-QAM	5/6	172.1	162.5	146.3	344.1	325	292.5	720.6	680.6	612.5
8	2	256-QAM	3/4	206.5	195	175.5	412.9	390	351	864.7	816.7	735
9	2	256-QAM	5/6	229.4	216.7	195	458.8	433.3	390	960.8	907.4	816.7
10	2	1024-QAM	3/4	258.1	243.8	219.4	516.2	487.5	438.8	1080.9	1020.8	918.8
11	2	1024-QAM	5/6	286.8	270.8	243.8	573.5	541.7	487.5	1201	1134.3	1020.8

STA support 1.6μs/3.2μs Guard Interval, so logical rate is determined by MCS index from 7.3Mbps to1134.3Mbps (if STA uses Wi-Fi6 mode)

#8 Association Response from AP

```
IEEE 802.11 Association Response, Flags: ........
  Type/Subtype: Association Response (0x0001)
> Frame Control Field: 0x1000
  .000 0000 0011 1100 = Duration: 60 microseconds
  Receiver address: 06:0f:5b:dd:20:fa (06:0f:5b:dd:20:fa)
  Destination address: 06:0f:5b:dd:20:fa (06:0f:5b:dd:20:fa)
  Transmitter address: ASUSTekC_c4:f5:c4 (f0:2f:74:c4:f5:c4)
  Source address: ASUSTekC_c4:f5:c4 (f0:2f:74:c4:f5:c4)
  BSS Id: ASUSTekC_c4:f5:c4 (f0:2f:74:c4:f5:c4)
  .... .... .... 0000 = Fragment number: 0
  0000 0000 0001 .... = Sequence number: 1
IEEE 802.11 Wireless Management
  Fixed parameters (6 bytes)
    Capabilities Information: 0x0501
    Status code: Successful (0x0000)
    ..00 0000 0000 0001 = Association ID: 0x0001
  Tagged parameters (256 bytes)
    Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    Tag: HT Capabilities (802.11n D1.10)
    Tag: HT Information (802.11n D1.10)
    Tag: Extended Capabilities (10 octets)
    Tag: VHT Capabilities
    Tag: VHT Operation
    Ext Tag: HE Capabilities (IEEE Std 802.11ax/D3.0)
    Ext Tag: HE Operation (IEEE Std 802.11ax/D3.0)
    Ext Tag: Spatial Reuse Parameter Set
    Ext Tag: MU EDCA Parameter Set
    Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    Tag: Vendor Specific: Qualcomm Inc.
    Tag: Vendor Specific: Qualcomm Inc.
    Tag: Vendor Specific: Microsoft Corp.: WPS
```

```
================================================================================
OP Mode          : AP
SSID             : wifi6
BSSID            : F0:2F:74:C4:F5:C4
MAC address      : F0:2F:74:C4:F5:C4
Phy Mode         : 11a/n/ac/ax
Bit Rate         : 4.8039 Gb/s
Channel          : 64

Stations List
--------------------------------------------------------------------------------
idx               MAC                PhyMode          RSSI TX_RATE RX_RATE
Main              06:0F:5B:DD:20:FA 11AXA_HE80        -32    720M    286M
```

Status Code Successful

Association ID: 0x00001

Ext. tag HE Capabilities (IEEE Std 802.11ax/D3.0)

Ext. tag HE Operation (IEEE Std 802.11ax/D3.0)

Ext. tag Spatial Reuse Parameter Set

Ext Tag: MU EDCA Parameter Set

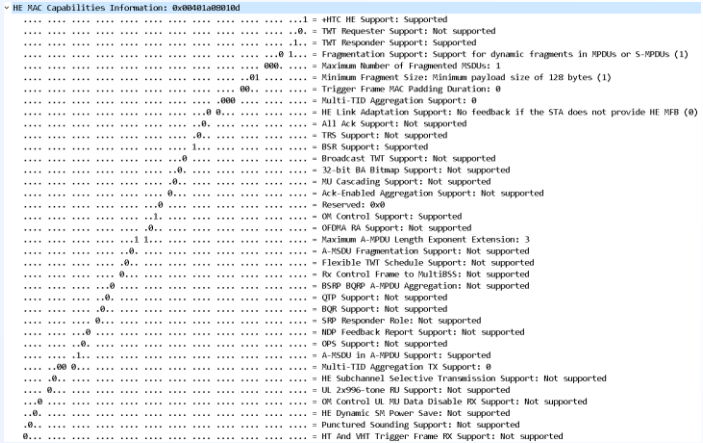
AP linked up layer2 connection to STA

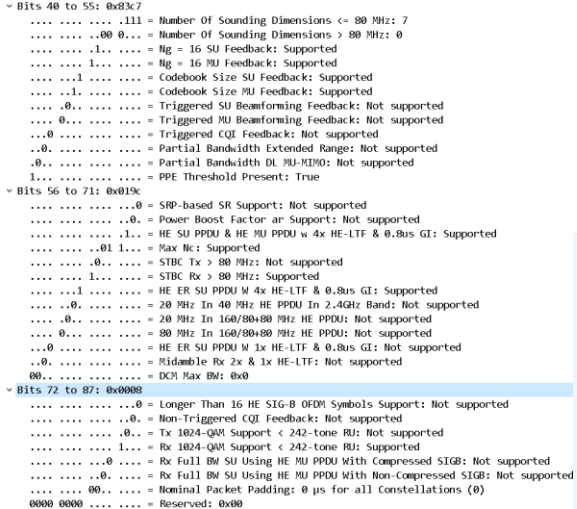
```
================================================================================
OP Mode          : AP
SSID             : wifi6
BSSID            : F0:2F:74:C4:F5:C4
MAC address      : F0:2F:74:C4:F5:C4
Phy Mode         : 11a/n/ac/ax
Bit Rate         : 4.8039 Gb/s
Channel          : 64

Stations List
--------------------------------------------------------------------------------
idx              MAC                PhyMode          RSSI TX_RATE RX_RATE
Main             06:0F:5B:DD:20:FA 11AXA_HE80        -32     720M     286M
```

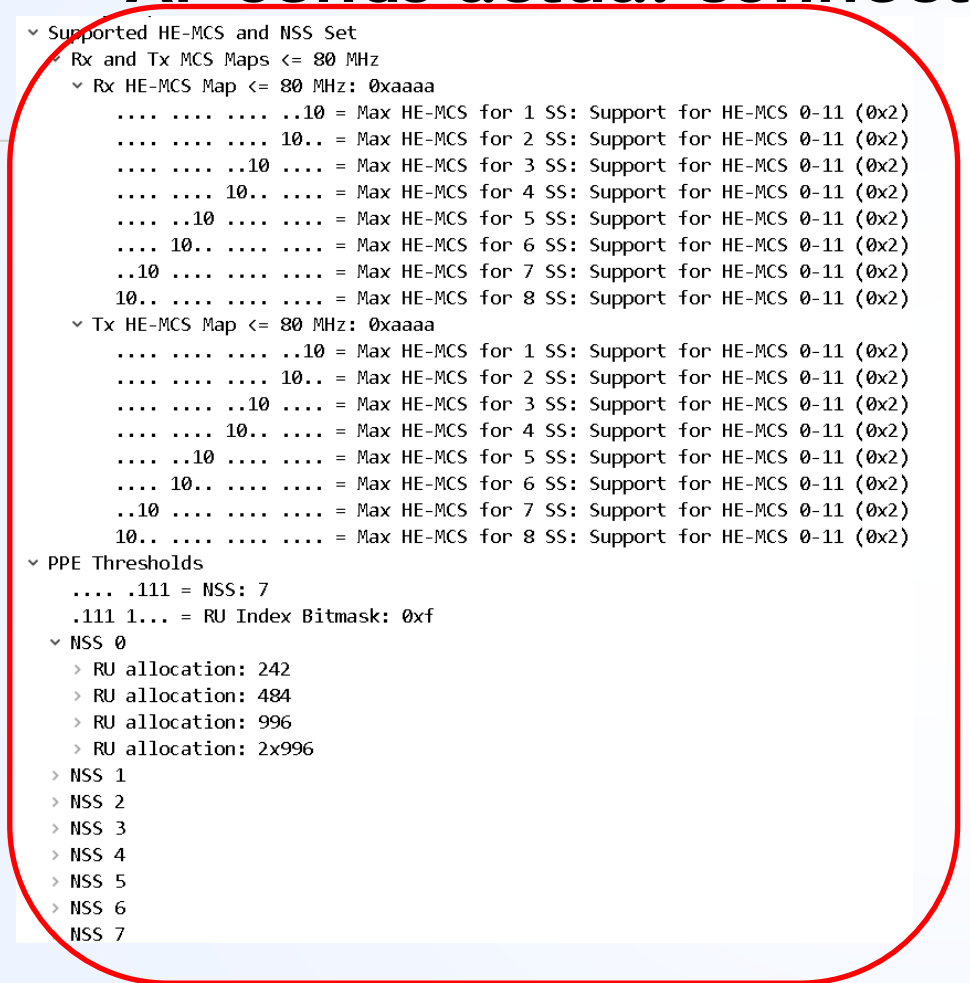
Association Response means AP determined setting configuration, confirmed connection from STA, and linked up and start actual data communication with STA.

AP also logged association (HE Bandwidth 80MHz TX Max 720Mbps RX Max 286Mbps)





AP sends actual connection settings

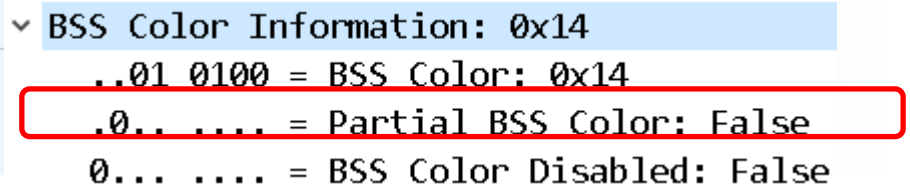


AP sends actual connection settings to STA.

- Bandwidth <=80MHz
- MCS 0-11
- Spatial Streams 1-2
- RU 242,484,996,2x996

There are other many setting information in HE MAC Capabilities and HE PHY Capabilities, Supported Channels, SSID and so on.

new function: BSS coloring, modified CSMA/CA



There are many other wireless access point in todays Wi-Fi, you may see tons of SSID if you are in downtown. WiFi6 uses BSS(Basic Service Set) Coloring, a group of AP and STAs connected with AP set “Color” to identify communication.

In Carrier Sense process, AP/STAs wait for a while (timer + random), then send frames when they receive frames in the same color over RSSI signal threshold.

AP changes Carrier Sense threshold dynamically if the color is not same.

It means “Oh, other system use the same Wi-Fi Channel, but not me, so I loose interferer threshold”

BSS Coloring utilize RF band more efficiently and get better performance (especially in outdoor, downtown and other congestion wireless network)

new function: Triger frame for TWT

```
HE MAC Capabilities Information: 0x00401a08010d
.... ..0. = TWT Requester Support: Not supported
.... .1.. = TWT Responder Support: Supported
.... .... = Trigger Frame MAC Padding Duration: 0
```

```
Ext Tag: HE Operation (IEEE Std 802.11ax/D3.0)
  Tag Number: Element ID Extension (255)
  Ext Tag length: 6
  Ext Tag Number: HE Operation (IEEE Std 802.11ax/D3.0) (36)
  HE Operation Parameters: 0x003ff4
    .... .... .... .... .... .100 = Default PE Duration: 4
    .... .... .... .... .... 0... = TWT Required: Not required
```

```
HE Phy Capabilities Information
Bits 40 to 55: 0x83c7
  .... .... .... .111 = Number Of Sounding Dimensions <= 80 MHz: 7
  .... .... ..00 0... = Number Of Sounding Dimensions > 80 MHz: 0
  .... .... .1.. .... = Ng = 16 SU Feedback: Supported
  .... .... 1... .... = Ng = 16 MU Feedback: Supported
  .... ...1 .... .... = Codebook Size SU Feedback: Supported
  .... ..1. .... .... = Codebook Size MU Feedback: Supported
  .... .0.. .... .... = Triggered SU Beamforming Feedback: Not supported
  .... 0... .... .... = Triggered MU Beamforming Feedback: Not supported
  ...0 .... .... .... = Triggered CQI Feedback: Not supported
```

In legacy Wi-Fi we have to use power management flag to sleep or wake up all STAs in BSS

```
Flags: 0x00
  .... ..00 = DS status: Not leaving DS
  .... .0.. = More Fragments: This is th
  .... 0... = Retry: Frame is not being
  ...0 .... = PWR MGT: STA will stay up
```

TWT (Target Wake Time) is the new Wi-Fi6 mechanism that set individual sleep time between AP and STAs

STA set individual wake time in association. AP sends trigger packet to wake up the STA and STA sends back if needed.

WiFi6 also use CSI(Channel State Information) from chipset for beamforming.

TWT (Target Wake Time) is the best solution for IoT devices

AP specification

```
HE Phy Capabilities Information
  .... ...0 = Reserved: 0x0
  0100 010. = Channel Width Set: 0x22
     .... ..0. = 40MHz in 2.4GHz band: Not supported
     .... .1.. = 40 & 80MHz in the 5GHz band: Supported
     .... 0... = 160MHz in the 5GHz band: Not supported
     ...0 .... = 160/80+80MHz in the 5GHz band: Not supported
     ..0. .... = 242 tone RUs in the 2.4GHz band: Not supported
     .1.. .... = 242 tone RUs in the 5GHz band: Supported
     0... .... = Reserved: 0x0
  Bits 8 to 23: 0x0230
     .... .... .... 0000 = Punctured Preamble RX: 0x0
     .... .... ...1 .... = Device Class: Class B Device (0x1)
     .... .... ..1. .... = LDPC Coding In Payload: Supported
     .... .... .0.. .... = HE SU PPDU With 1x HE-LTF and 0.8us GI: Not supported
     .... ...0 0... .... = Midamble Rx Max NSTS: 1 Space-Time Stream (0x0)
     .... ..1. .... .... = NDP With 4x HE-LTF and 3.2us GI: Supported
     .... .0.. .... .... = STBC Tx <= 80 MHz: Not supported
     .... 0... .... .... = STBC Rx <= 80 MHz: Not supported
     ...0 .... .... .... = Doppler Tx: Not supported
     ..0. .... .... .... = Doppler Rx: Not supported
     .0.. .... .... .... = Full Bandwidth UL MU-MIMO: Not supported
```

```
Supported HE-MCS and NSS Set
  Rx and Tx MCS Maps <= 80 MHz
    Rx HE-MCS Map <= 80 MHz: 0xaaaa
       .... .... .... ..10 = Max HE-MCS for 1 SS: Support for HE-MCS 0-11 (0x2)
       .... .... .... 10.. = Max HE-MCS for 2 SS: Support for HE-MCS 0-11 (0x2)
       .... .... ..10 .... = Max HE-MCS for 3 SS: Support for HE-MCS 0-11 (0x2)
       .... .... 10.. .... = Max HE-MCS for 4 SS: Support for HE-MCS 0-11 (0x2)
       .... ..10 .... .... = Max HE-MCS for 5 SS: Support for HE-MCS 0-11 (0x2)
       .... 10.. .... .... = Max HE-MCS for 6 SS: Support for HE-MCS 0-11 (0x2)
       ..10 .... .... .... = Max HE-MCS for 7 SS: Support for HE-MCS 0-11 (0x2)
       10.. .... .... .... = Max HE-MCS for 8 SS: Support for HE-MCS 0-11 (0x2)
    Tx HE-MCS Map <= 80 MHz: 0xaaaa
       .... .... .... ..10 = Max HE-MCS for 1 SS: Support for HE-MCS 0-11 (0x2)
       .... .... .... 10.. = Max HE-MCS for 2 SS: Support for HE-MCS 0-11 (0x2)
       .... .... ..10 .... = Max HE-MCS for 3 SS: Support for HE-MCS 0-11 (0x2)
       .... .... 10.. .... = Max HE-MCS for 4 SS: Support for HE-MCS 0-11 (0x2)
       .... ..10 .... .... = Max HE-MCS for 5 SS: Support for HE-MCS 0-11 (0x2)
       .... 10.. .... .... = Max HE-MCS for 6 SS: Support for HE-MCS 0-11 (0x2)
       ..10 .... .... .... = Max HE-MCS for 7 SS: Support for HE-MCS 0-11 (0x2)
       10.. .... .... .... = Max HE-MCS for 8 SS: Support for HE-MCS 0-11 (0x2)
PPE Thresholds
     .... .111 = NSS: 7
     .111 1... = RU Index Bitmask: 0xf
  NSS 0
    RU allocation: 242
    RU allocation: 484
    RU allocation: 996
    RU allocation: 2x996
```

AP support 0.8μs/1.6μs Guard Interval, 8 Spatial Streams, HE MCS 0-11 and RU tone 242,484,996.

#8-#14 Plaintext Data such as DHCP, ICMP

#sf21veu

```
> Frame 8: 398 bytes on wire (3184 bits), 398 bytes captured (3184 bits) o
> Radiotap Header v0, Length 32
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: o......T
    Type/Subtype: QoS Data (0x0028)
  v Frame Control Field: 0x8881
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
    v Flags: 0x81
        .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 Fr
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        1... .... = +HTC/Order flag: Strictly ordered
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: ASUSTekC_c4:f5:c4 (f0:2f:74:c4:f5:c4)
    Transmitter address: 06:0f:5b:dd:20:fa (06:0f:5b:dd:20:fa)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: 06:0f:5b:dd:20:fa (06:0f:5b:dd:20:fa)
    BSS Id: ASUSTekC_c4:f5:c4 (f0:2f:74:c4:f5:c4)
    STA address: 06:0f:5b:dd:20:fa (06:0f:5b:dd:20:fa)
    .... .... .... 0000 = Fragment number: 0
    0000 0000 0001 .... = Sequence number: 1
  > Qos Control: 0x2116
  v HT Control (+HTC): 0x0000b20f
      .... .... .... .... .... .... .... ...1 = VHT: True
      .... .... .... .... .... .... .... ..1. = HE: True
    v Aggregate Control: 0x2c83
        Control ID: 3: Buffer status rep
      v Buffer Status Report: 0x000002c8
          .... .... .... .... .... .... .... 1000 =                 : 0x8
          .... .... .... .... .... .... .... ..00 = Delta
          .... .... .... .... .... .... 11.. .... = ACI High: 0
          .... .... .... .... .... ..10 .... .... = Scaling Factor: 0
          .... .... .... ..00 0000 00.. .... .... = Queue Size High: 0x00
          .... ..00 0000 00.. .... .... .... .... = Queue Size All: 0x00
> Logical-Link Control
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
```

Frame type_subtype: Data Subtype 8

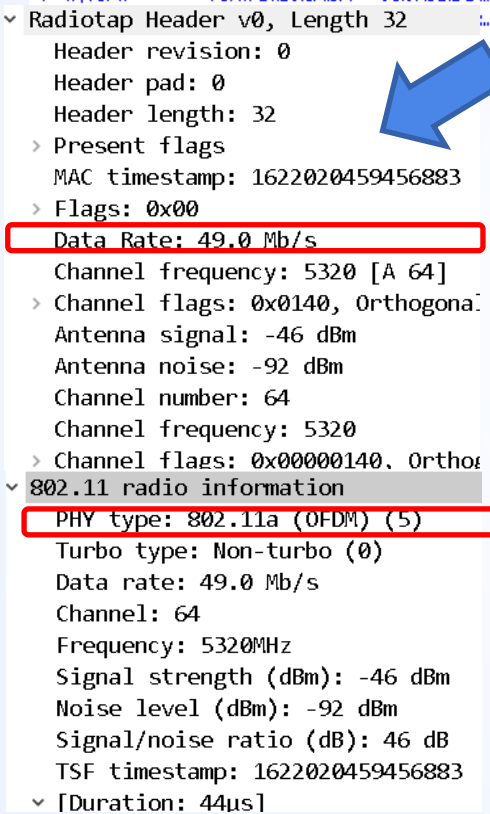
Data frames uses common IEEE802.11 mac frame format including HT Control information the the same IEEE802.11, Data frames have HT Control header that have HE (IEEE802.11ax) flag is True

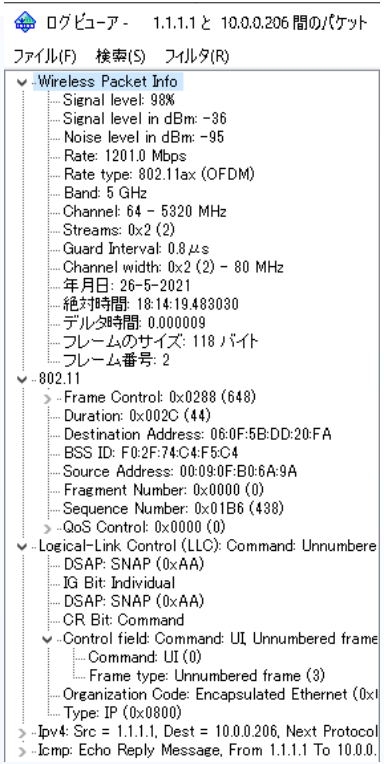
HT Control (+HTC) header

HE: True (IEEE802.11ax)

Aggregate Control Header

Unfortunately some Radiotap Header and RF information do not export correctly (for now)





CommView does not export all fields in pcapng correctly, PHY Type, MCS, number of Spatial Streams, Channel bandwidth and some fields are omitted, PHY type, Data rate fields are not dissected correctly (for now) and Richard-san (Richard Sharpe) and Guy-san (Guy Harris) work for Wireshark-side

#15 Disassociate from STA

#sf21veu

```
> Frame 15: 58 bytes on wire (464 bits), 58 bytes captured (464
> Radiotap Header v0, Length 32
> 802.11 radio information
v IEEE 802.11 Disassociate, Flags: ........
    Type/Subtype: Disassociate (0x000a)
  > Frame Control Field: 0xa000
    .000 0000 0011 1100 = Duration: 60 microseconds
    Receiver address: ASUSTekC_c4:f5:c4 (f0:2f:74:c4:f5:c4)
    Destination address: ASUSTekC_c4:f5:c4 (f0:2f:74:c4:f5:c4)
    Transmitter address: 06:0f:5b:dd:20:fa (06:0f:5b:dd:20:fa)
    Source address: 06:0f:5b:dd:20:fa (06:0f:5b:dd:20:fa)
    BSS Id: ASUSTekC_c4:f5:c4 (f0:2f:74:c4:f5:c4)
    .... .... .... 0000 = Fragment number: 0
    0000 0101 0011 .... = Sequence number: 83
v IEEE 802.11 Wireless Management
  v Fixed parameters (2 bytes)
      Reason code: Disassociated because sending STA is leaving
```

Type/Subtype: Disassociate

From STA address

Disassociate from STA

Last frame is common in Wi-Fi, STA says goodbye to AP using disassociate frame. And AP delete association and authentication state and disconnect datalink. Done.

Appendix Ping/iperf3 to wired PC with WPA2

ASUSTekC:C4:F5:C4	116 (116-120@40, 116-128@80)	AP	wifi6	802.11ax	WPA2PSK (CCMP)	-34/-33/-33	4803.9	8

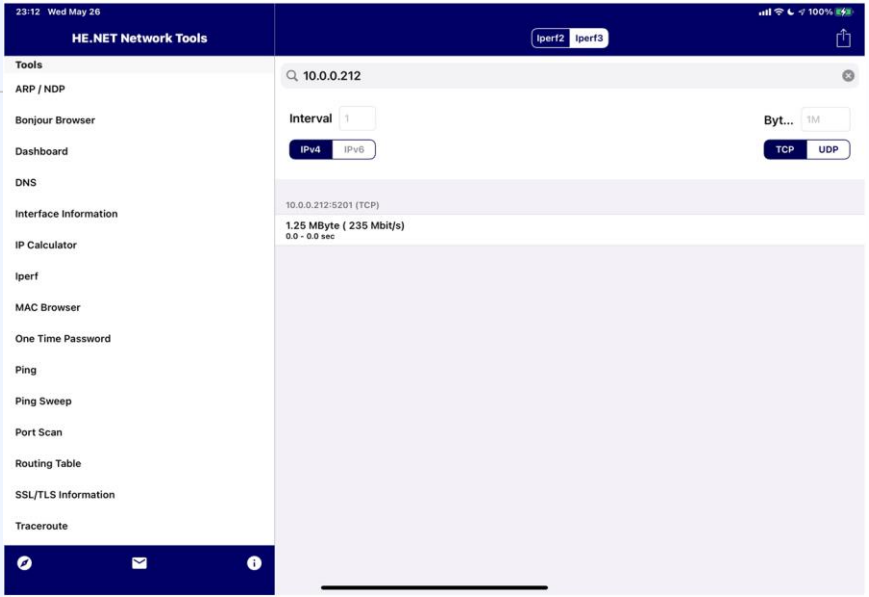
- SSID:wifi6
- Passphrase: Wireshark
- BSSID:F02F74C4F5C0
- STA iPad:060F5BDD20FA
- Channel 128MHz

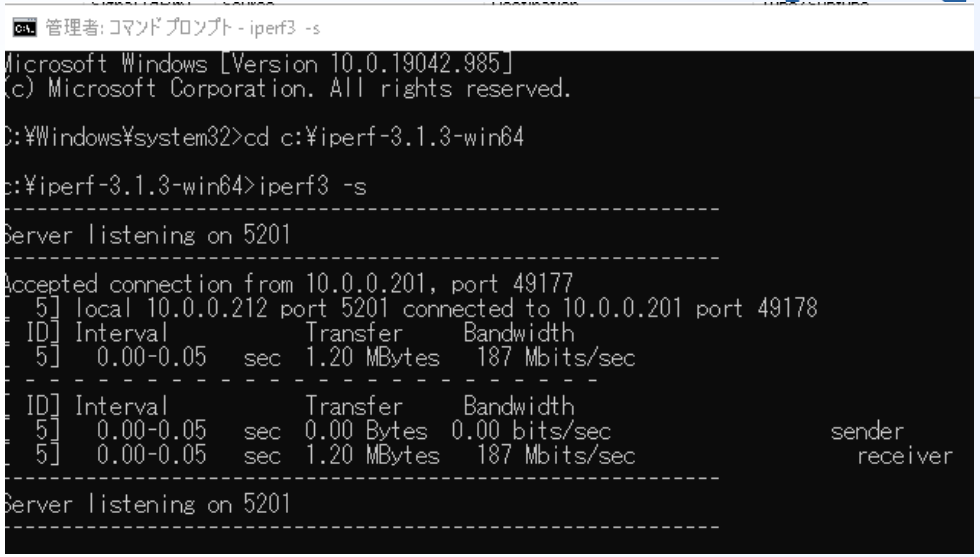
(1)Connect iPad to AP

(2)Ping to a wired PC

(3)Use iperf3 to measure throughput

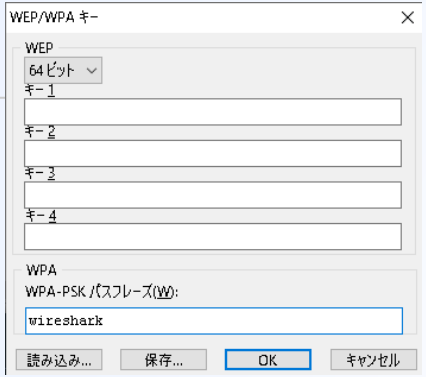
Appendix Ping/iperf3 to wired PC with WPA2

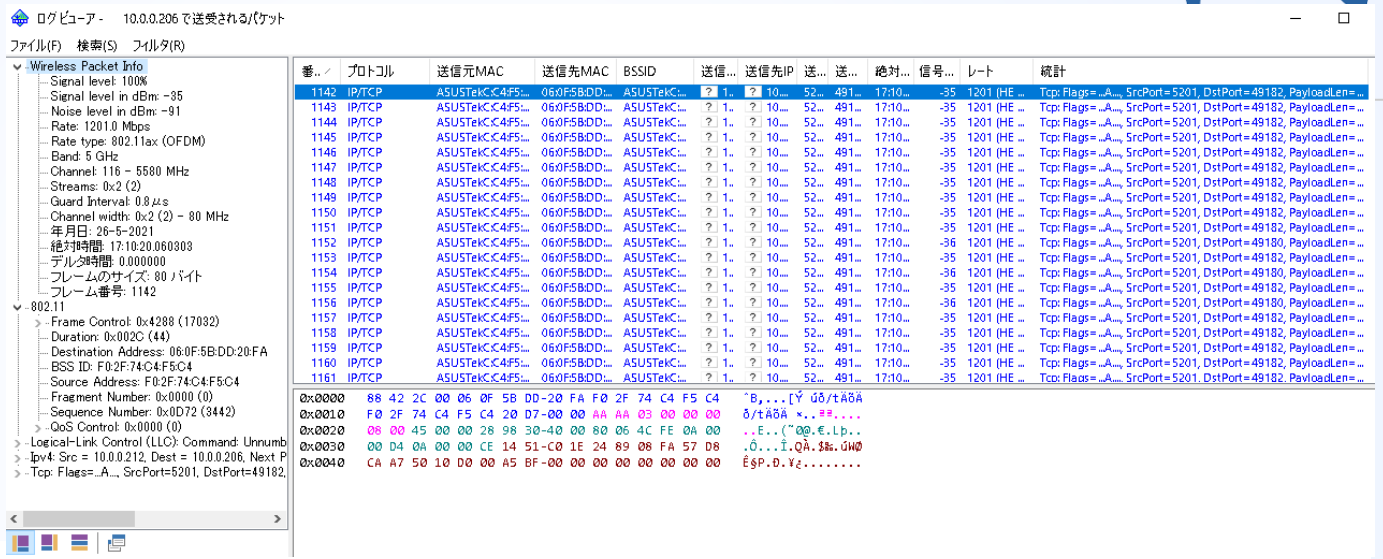




Actual throughput is about 200Mbps

Appendix Ping/iperf3 to wired PC with WPA2





CommView can decrypt WPA2-PSK, so we can see plain iperf frame if we capture complete 4 set of EAPOL handshake and enter WPA-PSK passphrase in WEP/WPA key settings.

Export pcapng file is plain text IEEE802.11 trace file.

Its just an entrance of dissecting WiFi6!!

We dissected a simpleWiFi6 connection setup process,

You may find there are tons of header and field we omitted this time, WiFi6 added many tag, fields, header in IEEE802.11 frame.

And we use WPA2/WPA3 encryption, and there are controllers in enterprise network.

So it is just an entrance of dissecting Wi-Fi6,

We may get better tools for capturing and Wireshark dissector also improve within a few years.

USE WIRESHARK

#sf21veu

Thank you for watching !!

Please complete the SharkFest Europe app-based survey

Supplemental file

http://www.ikeriri.ne.jp/sharkfest

ikeriri network service

http://www.ikeriri.ne.jp