



#sf21veu

# Dissecting WiFi6 using Wireshark



**Megumi Takeshita**  
Ikeriri network service

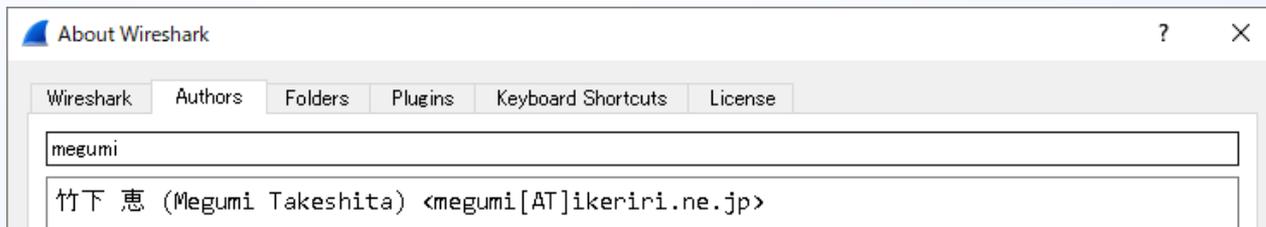
# Megumi Takeshita, packet otaku



#sf21veu



- 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



# 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<sup>3</sup>

# 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

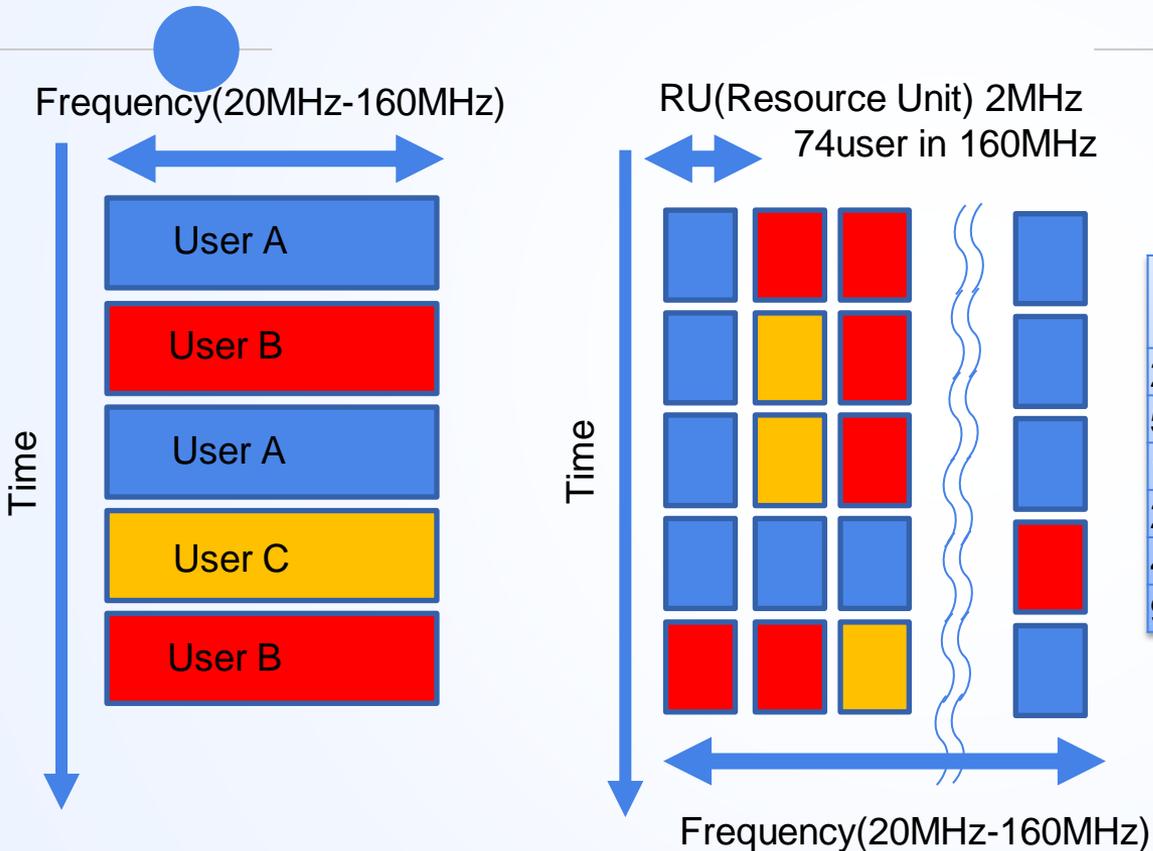


#sf21veu

- 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 #sf21veu

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 <sub>6</sub>

# MCS Modulation and Coding Scheme



#sf21veu

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  $\sim 64\text{QAM}$  / 40MHz BW
- Wi-Fi5 VHT Very High Throughput  $\sim 256\text{QAM}$  / 160MHz BW
- **WiFi6/WiFi6E HE High Efficiency  $\sim 1024\text{QAM}$  / 160MHz BW**
- Wi-Fi7 EHT Extremely High Throughput  $\sim 4096\text{QAM}$  / 320MHz

# mcsindex.com(MU-OFDMA 802.11ax)



#sf21veu

				MU-OFDMA (802.11ax)																	
MCS Index	Spatial Stream	Modulation	Coding	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	58.3	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	288.8	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	288.8	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	618.4	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



#sf21veu

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.

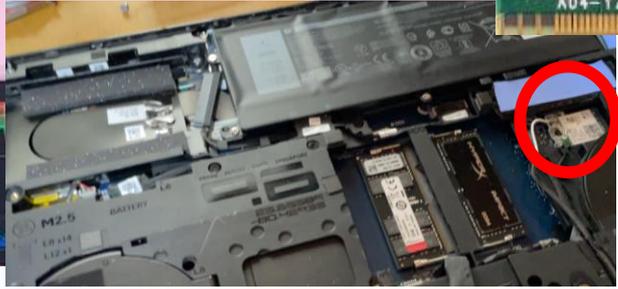
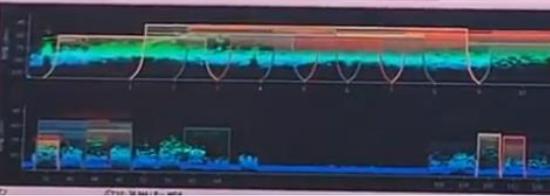
[https://standards.ieee.org/project/802\\_11ax.html](https://standards.ieee.org/project/802_11ax.html)

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.



SSID	セキュリティ	チャンネル	強度	接続済み	接続タイプ	接続モード	接続日時	接続速度	接続状態
SSID1	なし	1	100%	なし	なし	なし	なし	なし	なし
SSID2	なし	6	100%	なし	なし	なし	なし	なし	なし
SSID3	なし	11	100%	なし	なし	なし	なし	なし	なし
SSID4	なし	13	100%	なし	なし	なし	なし	なし	なし
SSID5	なし	14	100%	なし	なし	なし	なし	なし	なし
SSID6	なし	16	100%	なし	なし	なし	なし	なし	なし
SSID7	なし	36	100%	なし	なし	なし	なし	なし	なし
SSID8	なし	40	100%	なし	なし	なし	なし	なし	なし
SSID9	なし	44	100%	なし	なし	なし	なし	なし	なし
SSID10	なし	48	100%	なし	なし	なし	なし	なし	なし
SSID11	なし	52	100%	なし	なし	なし	なし	なし	なし
SSID12	なし	56	100%	なし	なし	なし	なし	なし	なし
SSID13	なし	60	100%	なし	なし	なし	なし	なし	なし
SSID14	なし	64	100%	なし	なし	なし	なし	なし	なし
SSID15	なし	68	100%	なし	なし	なし	なし	なし	なし
SSID16	なし	72	100%	なし	なし	なし	なし	なし	なし
SSID17	なし	76	100%	なし	なし	なし	なし	なし	なし
SSID18	なし	80	100%	なし	なし	なし	なし	なし	なし
SSID19	なし	84	100%	なし	なし	なし	なし	なし	なし
SSID20	なし	88	100%	なし	なし	なし	なし	なし	なし
SSID21	なし	92	100%	なし	なし	なし	なし	なし	なし
SSID22	なし	96	100%	なし	なし	なし	なし	なし	なし
SSID23	なし	100	100%	なし	なし	なし	なし	なし	なし
SSID24	なし	104	100%	なし	なし	なし	なし	なし	なし
SSID25	なし	108	100%	なし	なし	なし	なし	なし	なし
SSID26	なし	112	100%	なし	なし	なし	なし	なし	なし
SSID27	なし	116	100%	なし	なし	なし	なし	なし	なし
SSID28	なし	120	100%	なし	なし	なし	なし	なし	なし
SSID29	なし	124	100%	なし	なし	なし	なし	なし	なし
SSID30	なし	128	100%	なし	なし	なし	なし	なし	なし
SSID31	なし	132	100%	なし	なし	なし	なし	なし	なし
SSID32	なし	136	100%	なし	なし	なし	なし	なし	なし
SSID33	なし	140	100%	なし	なし	なし	なし	なし	なし
SSID34	なし	144	100%	なし	なし	なし	なし	なし	なし
SSID35	なし	148	100%	なし	なし	なし	なし	なし	なし
SSID36	なし	152	100%	なし	なし	なし	なし	なし	なし
SSID37	なし	156	100%	なし	なし	なし	なし	なし	なし
SSID38	なし	160	100%	なし	なし	なし	なし	なし	なし
SSID39	なし	164	100%	なし	なし	なし	なし	なし	なし
SSID40	なし	168	100%	なし	なし	なし	なし	なし	なし
SSID41	なし	172	100%	なし	なし	なし	なし	なし	なし
SSID42	なし	176	100%	なし	なし	なし	なし	なし	なし
SSID43	なし	180	100%	なし	なし	なし	なし	なし	なし
SSID44	なし	184	100%	なし	なし	なし	なし	なし	なし
SSID45	なし	188	100%	なし	なし	なし	なし	なし	なし
SSID46	なし	192	100%	なし	なし	なし	なし	なし	なし
SSID47	なし	196	100%	なし	なし	なし	なし	なし	なし
SSID48	なし	200	100%	なし	なし	なし	なし	なし	なし
SSID49	なし	204	100%	なし	なし	なし	なし	なし	なし
SSID50	なし	208	100%	なし	なし	なし	なし	なし	なし
SSID51	なし	212	100%	なし	なし	なし	なし	なし	なし
SSID52	なし	216	100%	なし	なし	なし	なし	なし	なし
SSID53	なし	220	100%	なし	なし	なし	なし	なし	なし
SSID54	なし	224	100%	なし	なし	なし	なし	なし	なし
SSID55	なし	228	100%	なし	なし	なし	なし	なし	なし
SSID56	なし	232	100%	なし	なし	なし	なし	なし	なし
SSID57	なし	236	100%	なし	なし	なし	なし	なし	なし
SSID58	なし	240	100%	なし	なし	なし	なし	なし	なし
SSID59	なし	244	100%	なし	なし	なし	なし	なし	なし
SSID60	なし	248	100%	なし	なし	なし	なし	なし	なし
SSID61	なし	252	100%	なし	なし	なし	なし	なし	なし
SSID62	なし	256	100%	なし	なし	なし	なし	なし	なし
SSID63	なし	260	100%	なし	なし	なし	なし	なし	なし
SSID64	なし	264	100%	なし	なし	なし	なし	なし	なし
SSID65	なし	268	100%	なし	なし	なし	なし	なし	なし
SSID66	なし	272	100%	なし	なし	なし	なし	なし	なし
SSID67	なし	276	100%	なし	なし	なし	なし	なし	なし
SSID68	なし	280	100%	なし	なし	なし	なし	なし	なし
SSID69	なし	284	100%	なし	なし	なし	なし	なし	なし
SSID70	なし	288	100%	なし	なし	なし	なし	なし	なし
SSID71	なし	292	100%	なし	なし	なし	なし	なし	なし
SSID72	なし	296	100%	なし	なし	なし	なし	なし	なし
SSID73	なし	300	100%	なし	なし	なし	なし	なし	なし
SSID74	なし	304	100%	なし	なし	なし	なし	なし	なし
SSID75	なし	308	100%	なし	なし	なし	なし	なし	なし
SSID76	なし	312	100%	なし	なし	なし	なし	なし	なし
SSID77	なし	316	100%	なし	なし	なし	なし	なし	なし
SSID78	なし	320	100%	なし	なし	なし	なし	なし	なし
SSID79	なし	324	100%	なし	なし	なし	なし	なし	なし
SSID80	なし	328	100%	なし	なし	なし	なし	なし	なし
SSID81	なし	332	100%	なし	なし	なし	なし	なし	なし
SSID82	なし	336	100%	なし	なし	なし	なし	なし	なし
SSID83	なし	340	100%	なし	なし	なし	なし	なし	なし
SSID84	なし	344	100%	なし	なし	なし	なし	なし	なし
SSID85	なし	348	100%	なし	なし	なし	なし	なし	なし
SSID86	なし	352	100%	なし	なし	なし	なし	なし	なし
SSID87	なし	356	100%	なし	なし	なし	なし	なし	なし
SSID88	なし	360	100%	なし	なし	なし	なし	なし	なし
SSID89	なし	364	100%	なし	なし	なし	なし	なし	なし
SSID90	なし	368	100%	なし	なし	なし	なし	なし	なし
SSID91	なし	372	100%	なし	なし	なし	なし	なし	なし
SSID92	なし	376	100%	なし	なし	なし	なし	なし	なし
SSID93	なし	380	100%	なし	なし	なし	なし	なし	なし
SSID94	なし	384	100%	なし	なし	なし	なし	なし	なし
SSID95	なし	388	100%	なし	なし	なし	なし	なし	なし
SSID96	なし	392	100%	なし	なし	なし	なし	なし	なし
SSID97	なし	396	100%	なし	なし	なし	なし	なし	なし
SSID98	なし	400	100%	なし	なし	なし	なし	なし	なし
SSID99	なし	404	100%	なし	なし	なし	なし	なし	なし
SSID100	なし	408	100%	なし	なし	なし	なし	なし	なし



[https://wikidevi.wi-cat.ru/Intel\\_Wi-Fi\\_6\\_AX200\\_\(AX200NGW\)](https://wikidevi.wi-cat.ru/Intel_Wi-Fi_6_AX200_(AX200NGW))

- Windows 10 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:** [PDSAX200NG](#), [MSQAX200NG](#), [RWO-RZ090301](#), [RWO-RZ090287](#)

**IC ID:** 1000M-AX200NG, 3568A-AX200NG, 8092D-RZ090301

**Wi1 chip1:** Intel WCSAX200

**Probable Linux driver:** [iwlmwifi](#)

*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 64ch

(1)Connect iPad to AP

(2)Ping to a wired PC

(3)Click Forget Network to disconnect AP

**Wireless - General**

Set up the wireless related information below.

Enable Smart Connect	<input type="checkbox"/> OFF
Band	5GHz ▾
Network Name (SSID)	wifi6
Hide SSID	<input checked="" type="radio"/> Yes <input type="radio"/> No
Wireless Mode	Auto ▾ <input type="checkbox"/> Optimized for Xbox
802.11ax / Wi-Fi 6 mode	Enable ▾ <small>If compatibility issue occurs when enabling 802.11ax / Wi-Fi 6 mode, please check: <a href="#">FAQ</a></small>
Channel bandwidth	20/40/80 MHz ▾
Control Channel	Auto ▾ <small>Current Control Channel: 116</small> <input checked="" type="checkbox"/> Auto select channel including DFS channels
Extension Channel	Auto ▾
Authentication Method	open System ▾

**Apply**

# Use CommView to capture packets



CommView for WiFi - Intel(R) Wi-Fi 6 AX200 160MHz

ファイル 検索 表示 ツール 設定 フィルタ ヘルプ

モード チャンネル 最近の IP 接続 パケット ログ フィルタ アラーム

標準 / MAC アドレス	チャンネル	種類	SSID	標準	暗号化	信号強度	最大レート	ストリーム	転送レート (Tx)	転送レート (L)	キャプチャ
関連しない											
06:0F:5B:DD:20:FA		STA				-51/-46/-31				6/447.4/12...	<input checked="" type="radio"/> シングル・チャンネル・モード 5 GHz - 64
802.11g											
802.11n											
802.11ac											
802.11ax											<input type="radio"/> スキャナー・モード 設定...
HuaweiDe...:20:3F	100 (100-104@40, 100-112@80, ...)	AP	00AD...D6203C-5G	802.11ax	WPA2PSK (CCMP)	-87/-86/-85	802.0	2	6/6/6	0/0/0	チャンネルあたりの秒数(S): 1
ASUSTeK:C4:F5:C4	64 (60-64@40, 52-64@80)	AP	wifi6	802.11ax	cleartext	-39/-35/-30	4803.9	8	6/293.3/1201	6/369/120	<input type="checkbox"/> 40 MHz モードにおけるセカ...
ASUSTeK:C4:F5:C0	11	AP	wifi2.4	802.11ax	WPA2PSK (CCMP)	-28/-27/-26	573.5	4	1/1/1	1/1/1	<input type="checkbox"/> アクティブモード・ディスカバ...

SSID wifi6

capture CH 64

BSSID

CH 64

cleartext

Max Rate

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	Beacon Frame	234	Beacon Frame, To DS=0, From DS=0, Flags=...
2	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	Probe Request	150	Probe Request, To DS=0, From DS=0, Flags=...
3	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	Probe Response	150	Probe Response, To DS=0, From DS=0, Flags=...
4	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	Authentication	150	Authentication, To DS=0, From DS=0, Flags=...
5	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	Association Request	212	Association Request, To DS=0, From DS=0, Flags=...
6	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	Association Response	150	Association Response, To DS=0, From DS=0, Flags=...
7	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	QoS Data	398	QoS Data, Transaction ID=0x388C7
8	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	QoS Data	398	QoS Data, Transaction ID=0x388C7
9	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	QoS Data	398	QoS Data, Transaction ID=0x388C7
10	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	QoS Data	398	QoS Data, Transaction ID=0x388C7
11	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	QoS Data	398	QoS Data, Transaction ID=0x388C7
12	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	QoS Data	398	QoS Data, Transaction ID=0x388C7
13	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	QoS Data	398	QoS Data, Transaction ID=0x388C7
14	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	QoS Data	398	QoS Data, Transaction ID=0x388C7
15	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	QoS Data	398	QoS Data, Transaction ID=0x388C7
16	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	QoS Data	398	QoS Data, Transaction ID=0x388C7
17	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	QoS Data	398	QoS Data, Transaction ID=0x388C7
18	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	QoS Data	398	QoS Data, Transaction ID=0x388C7
19	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	QoS Data	398	QoS Data, Transaction ID=0x388C7
20	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	QoS Data	398	QoS Data, Transaction ID=0x388C7
21	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	QoS Data	398	QoS Data, Transaction ID=0x388C7
22	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	QoS Data	398	QoS Data, Transaction ID=0x388C7
23	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	QoS Data	398	QoS Data, Transaction ID=0x388C7
24	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	QoS Data	398	QoS Data, Transaction ID=0x388C7
25	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	QoS Data	398	QoS Data, Transaction ID=0x388C7

# Original ncfx file: beacon frame from AP



#sf21veu

ログビュー [cleartext-wifi6-26-5-2021@16-41-53-590.ncfx]

ファイル(F) 検索(S) フィルタ(R)

> Wireless Packet Info  
> 802.11  
v Beacon

- Timestamp: 82.329664 sec
- Beacon Interval: 0x0064 (100) ~ 102.400 msec
- > Capability Information: 0x0501 (1281)
- v SSID parameter set
  - Current Channel: 116 ~ 5680 MHz
  - Tag: SSID parameter set (0x0)
  - Tag length: 5
  - SSID: wifi6
- > Supported rates
  - Current Channel: 116 ~ 5680 MHz
  - Traffic indication map (TIM): 0x00 (No frames buffered)
  - Country Information
  - Power Constraint
  - TPO Report element
  - HT Capabilities element
  - HT Information element
  - Extended Capabilities
  - VHT Capabilities
  - VHT Operation
  - VHT Tx Power Envelope (IEEE Std 802.11ac/D5.0)
- v Ext tag: HE Capabilities (IEEE Std 802.11ax/D3.0)
  - Ext tag length: 46
  - Ext tag number: HE Capabilities (IEEE Std 802.11ax/D3.0) (35)
  - HE MAC Capabilities Information
  - HE PHY Capabilities Information
  - Tx Rx HE-MCS NSS Support
  - PPE Thresholds
- v Ext tag: HE Operation (IEEE Std 802.11ax/D3.0)
  - Ext tag length: 6
  - Ext tag number: HE Operation (IEEE Std 802.11ax/D3.0) (36)
  - HE Operation Parameters: 0x3FF4
  - BSS Color Information: 0x26
  - Basic HE-MCS and NSS Set: 0xFFFC
- v Ext tag: Spatial Reuse Parameter Set
  - Ext tag length: 1
  - Ext tag number: Spatial Reuse Parameter Set (39)
  - SR Control: 0x3
- v Ext tag: MU EDCA Parameter Set
  - Ext tag length: 13
  - Ext tag number: MU EDCA Parameter Set (38)
  - QoS Information (AP): 0x0
  - MUAC\_BE Parameter Record
  - MUAC\_BK Parameter Record
  - MUAC\_VI Parameter Record
  - MUAC\_VO Parameter Record
  - Vendor specific: MICROSOFT CORP. WME
  - Vendor specific: Atheros Communications, Inc.
  - Vendor specific: (221), Qualcomm Inc. Tag not interpreted
  - Vendor specific: (221), Qualcomm Inc. Tag not interpreted
  - Vendor specific: (221), Qualcomm Inc. Tag not interpreted
  - Vendor specific: MICROSOFT CORP. WPS

番号	プロトコル	送信元MAC	送信先MAC	BSSID	送信...	送信先IP	送...	送...	絶対...	信号...	レート	統計
685	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-36	6	SSID=wifi6, (Infra), Ch#116, Seq=9, WEP: Can't decrypt, Key#1
689	MNGT/ACTIO...	Apple10:EB0D	ASUSTekC:0...	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-44	24	Category=HE, Action=HE Compress...
691	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-36	6	SSID=wifi6, (Infra), Ch#116, Seq=1
692	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-35	6	SSID=wifi6, (Infra), Ch#116, Seq=1
693	MNGT/ACTIO...	Apple10:EB0D	ASUSTekC:0...	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-41	12	Category=HE, Action=HE Compress...
694	ENCR.A-MFS...	Apple10:EB0D	ASUSTekC:0...	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-40	216.2 (HE ...	WEP: Can't decrypt, Key#1
695	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-36	6	SSID=wifi6, (Infra), Ch#116, Seq=1
696	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-36	6	SSID=wifi6, (Infra), Ch#116, Seq=1
697	ENCR.DATA	Apple10:EB0D	Fortinet:80...	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-40	216.2 (HE ...	WEP: Can't decrypt, Key#1
698	ENCR.DATA	Apple10:EB0D	Fortinet:80...	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-40	216.2 (HE ...	WEP: Can't decrypt, Key#1
699	ENCR.DATA	Apple10:EB0D	Fortinet:80...	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-40	216.2 (HE ...	WEP: Can't decrypt, Key#1
700	ENCR.DATA	Apple10:EB0D	Fortinet:80...	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-40	216.2 (HE ...	WEP: Can't decrypt, Key#1
701	MNGT/ACTIO...	Apple10:EB0D	ASUSTekC:0...	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-40	12	Category=HE, Action=HE Compress...
702	ENCR...											
703	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-37	6	SSID=wifi6, (Infra), Ch#116, Seq=1
705	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-37	6	SSID=wifi6, (Infra), Ch#116, Seq=1
706	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-37	6	SSID=wifi6, (Infra), Ch#116, Seq=1
707	ENCR.DATA	Fortinet:80...	Apple10:EB...	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-71	340.3 (HE ...	WPA: Can't decrypt
708	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-37	6	SSID=wifi6, (Infra), Ch#116, Seq=1
709	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-37	6	SSID=wifi6, (Infra), Ch#116, Seq=1
710	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-37	6	SSID=wifi6, (Infra), Ch#116, Seq=1
711	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-37	6	SSID=wifi6, (Infra), Ch#116, Seq=1
712	ENCR.DATA	Apple10:EB0D	Fortinet:80...	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-39	216.2 (HE ...	WEP: Can't decrypt, Key#1
713	ENCR.DATA	Apple10:EB0D	Fortinet:80...	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-39	216.2 (HE ...	WEP: Can't decrypt, Key#1
714	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-37	6	SSID=wifi6, (Infra), Ch#116, Seq=2
716	MNGT/PROB...	ASUSTekC:4F5...	Askey:018A...	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-37	6	SSID=wifi6, (Infra), Ch#116, Seq=2
717	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-37	6	SSID=wifi6, (Infra), Ch#116, Seq=2
723	ENCR.DATA	ASUSTekC:0976...	70:E25A:11...	00:69:2A:80...	? N	? N/A	N/A	N/A	1640...	-70	408.3 (HE ...	WPA: Can't decrypt
724	ENCR.DATA	Apple10:EB0D	Fortinet:80...	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-40	216.2 (HE ...	WEP: Can't decrypt, Key#1
725	ENCR.DATA	Apple10:EB0D	Fortinet:80...	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-40	216.2 (HE ...	WEP: Can't decrypt, Key#1
726	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-38	6	SSID=wifi6, (Infra), Ch#116, Seq=2
727	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-36	6	SSID=wifi6, (Infra), Ch#116, Seq=2
728	ENCR.DATA	Apple10:EB0D	Fortinet:80...	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-45	216.2 (HE ...	WEP: Can't decrypt, Key#1
729	ENCR.DATA	Apple10:EB0D	Fortinet:80...	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-44	216.2 (HE ...	WEP: Can't decrypt, Key#1
730	MNGT/ACTIO...	Apple10:EB0D	ASUSTekC:0...	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-44	12	Category=HE, Action=HE Compress...
731	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-35	6	SSID=wifi6, (Infra), Ch#116, Seq=2
732	ENCR.DATA	Apple10:EB0D	Fortinet:80...	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-45	216.2 (HE ...	WEP: Can't decrypt, Key#1
733	MNGT/ACTIO...	Apple10:EB0D	ASUSTekC:0...	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-45	12	Category=HE, Action=HE Compress...
734	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-34	6	SSID=wifi6, (Infra), Ch#116, Seq=2
735	MNGT/ACTIO...	Apple10:EB0D	ASUSTekC:0...	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-43	12	Category=HE, Action=HE Compress...
736	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N/A	N/A	N/A	1640...	-36	6	SSID=wifi6, (Infra), Ch#116, Seq=2

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

# Sample trace file: cleartext.pcapng



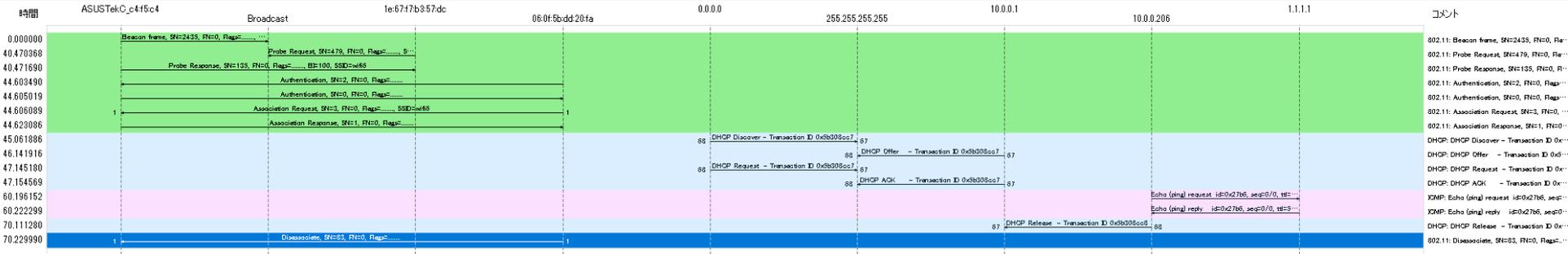
No.	Time	Signal (dBm)	Source	Destination	Type/Subtype	Data rate (Mb/s)	Protocol	Length	Info
1	0.000000	-33 dBm	ASUSTekC_c4:f5:c4	Broadcast	Beacon frame	6 802.11		461	Beacon frame, SN=2435, FN=0, Flags=....., BI=1
2	40.470368	-48 dBm	1e:67:f7:b3:57:dc	Broadcast	Probe Request	6 802.11		150	Probe Request, 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: .....
▼ IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  ▼ Tagged parameters (393 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: 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 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.: WMM/WME: Parameters
    > Tag: Vendor Specific: Atheros Communications, Inc.: WMM
    > 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

```

v 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 Beacon 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 interface
- > Radiotap Header v0, Length 32
- > 802.11 radio information
- > IEEE 802.11 Probe Request, Flags: .....
- ▼ IEEE 802.11 Wireless Management
  - ▼ 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
    - ▼ 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) 1
      - > HE MAC Capabilities Information: 0x8000000080801
      - ▼ 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
    - ▼ Supported HE-MCS and NSS Set
      - ▼ Rx and Tx MCS Maps <= 80 MHz
        - > Rx HE-MCS Map <= 80 MHz: 0xffff
        - > Tx HE-MCS Map <= 80 MHz: 0xffff
      - > 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



#sf21veu

- ▼ 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
    - > .... ..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
  - ▼ Supported HE-MCS and NSS Set
    - ▼ Rx and Tx MCS Maps <= 80 MHz
      - ▼ Rx HE-MCS Map <= 80 MHz: 0xffff
        - .... ..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: 0xffff
    - ▼ PPE Thresholds
      - .... .001 = NSS: 1
      - .011 1... = RU Index Bitmask: 0x7
    - ▼ 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: .....
√ IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  √ 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.: WMM-AC Parameter Set
    > Tag: Vendor Specific: Atheros Communications, Inc.: WMM-AC Parameter Set
    > Tag: Vendor Specific: Qualcomm Inc.: WMM-AC Parameter Set
    > Tag: Vendor Specific: Microsoft Corp.: WPS
    > Tag: Vendor Specific: Qualcomm Inc.: WPS
    > Tag: Vendor Specific: Qualcomm Inc.: 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

# AP sends IEEE802.11ax specification



#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
  - ▼ 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: 0x0000
  - ▼ 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
    - ▼ 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
      - > NSS 1
      - > NSS 2
      - > NSS 3
      - > NSS 4
      - > NSS 5
      - > NSS 6
      - > NSS 7
  - > Ext Tag: HE Operation (IEEE Std 802.11ax/D3.0)
  - > Ext Tag: Spatial Reuse Parameter Set
  - > Ext Tag: MU EDCA Parameter Set

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)



<ul style="list-style-type: none"><li>&gt; Frame 4: 97 bytes on wire (776 bits), 97 bytes</li><li>&gt; Radiotap Header v0, Length 32</li><li>&gt; 802.11 radio information</li><li>&gt; IEEE 802.11 Authentication, Flags: .....</li><li>✓ IEEE 802.11 Wireless Management<ul style="list-style-type: none"><li>✓ Fixed parameters (6 bytes)<ul style="list-style-type: none"><li>Authentication Algorithm: Open System (0)</li><li>Authentication SEQ: 0x0001</li><li>Status code: Successful (0x0000)</li></ul></li><li>✓ Tagged parameters (35 bytes)<ul style="list-style-type: none"><li>&gt; Tag: Extended Capabilities (8 octets)</li><li>&gt; Tag: Vendor Specific: Apple, Inc.</li><li>&gt; Tag: Vendor Specific: Broadcom</li></ul></li></ul></li></ul>	<ul style="list-style-type: none"><li>&gt; Frame 5: 62 bytes on wire (496 bits), 62 bytes</li><li>&gt; Radiotap Header v0, Length 32</li><li>&gt; 802.11 radio information</li><li>&gt; IEEE 802.11 Authentication, Flags: .....</li><li>✓ IEEE 802.11 Wireless Management<ul style="list-style-type: none"><li>✓ Fixed parameters (6 bytes)<ul style="list-style-type: none"><li>Authentication Algorithm: Open System (0)</li><li>Authentication SEQ: 0x0002</li><li>Status code: Successful (0x0000)</li></ul></li></ul></li></ul>
---	---

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 interface
- > Radiotap Header v0, Length 32
- > 802.11 radio information
- > IEEE 802.11 Association Request, Flags: .....
- ✓ IEEE 802.11 Wireless Management
  - > Fixed parameters (4 bytes)
  - ✓ 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
    - ✓ 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) (255)
      - > 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
  < Supported HE-MCS and NSS Set
  < Rx and Tx MCS Maps <= 80 MHz
    < Rx HE-MCS Map <= 80 MHz: 0xffffa
      .... .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)
      .... .111 .... = 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: 0xffffa
      .... .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)
      .... .111 .... = 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)
  < PPE Thresholds
    .... .001 = NSS: 1
    .011 1... = RU Index Bitmask: 0x7
  < NSS 0
    > RU allocation: 242
    > RU allocation: 484
    > RU allocation: 996
  < 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.



# #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-AC 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: 0x0001

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         : FO:2F:74:C4:F5:C4
MAC address   : FO: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)

### HE PHY Capabilities Information: 0x0000000000000000

```
.....1 = HTT HE Support: Supported
.....0 = TWT Requester Support: Not supported
.....1 = TWT Responder Support: Supported
.....0 = Fragmentation Support: Support for dynamic fragments in PPDUs or S-PPDUs (1)
.....000 = Maximum Number of Fragmented MSDUs: 1
.....01 = Minimum Fragment Size: Minimum payload size of 128 bytes (1)
.....00 = Trigger Frame Preamble Duration: 0
.....000 = Multi-TID Aggregation Support: 0
.....0 0... = HE Link Adaptation Support: No feedback if the STA does not provide HE FRB (0)
.....0 = All Ack Support: Not supported
.....0 = TRS Support: Not supported
.....0 = BSR Support: Supported
.....0 = Broadcast TWT Support: Not supported
.....0 = 32-bit BA Bitmap Support: Not supported
.....0 = TWT Cascading Support: Not supported
.....0 = Ack-Enabled Aggregation Support: Not supported
.....0 = Reserved: 0x0
.....1 = QM Control Support: Supported
.....0 = QM Data Rx Support: Not supported
.....1 1... = Maximum A-PPDU Length Exponent Extension: 3
.....0 = A-PPDU Fragmentation Support: Not supported
.....0 = Flexible TWT Schedule Support: Not supported
.....0 = Rx Control Frame to Null/BSR: Not supported
.....0 = BSR RQPP A-PPDU Aggregation: Not supported
.....0 = QTP Support: Not supported
.....0 = BQR Support: Not supported
.....0 = SRP Responder Role: Not supported
.....0 = NDP Feedback Report Support: Not supported
.....0 = OPS Support: Not supported
.....1 = A-MSDU in A-PPDU Support: Supported
.....000 0... = Multi-TID Aggregation TX Support: 0
.....0 = HE Subchannel Selective Transmission Support: Not supported
.....0 = UL 2x96-tone RU Support: Not supported
.....0 = QP Control RU Data Disable Rx Support: Not supported
.....0 = HE Dynamic SR Power Save: Not supported
.....0 = Punctured Sounding Support: Not supported
.....0 = HT And VHT Trigger Frame RX Support: Not supported
```

### HE Phy Capabilities Information

```
.....0 = Reserved: 0x0
.....0000 010 = Channel Width Set: 0x2
.....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
.....0 = 242 tone RUs in the 5GHz band: Not supported
.....0 = Reserved: 0x0
.....0 = Reserved: 0x0x00
.....0000 = Punctured Preamble RX: 0x0
.....0 = Device Class: Class A Device (0x0)
.....1 = LDPC Coding In Payload: Supported
.....1 = HE SU PDU With 1x HE-LTF and 0.8us GI: Supported
.....0 0... = Midamble Rx Max NSTS: 1 Space-Time Stream (0x0)
.....0 = NDP With 4x HE-LTF and 3.2us GI: Not supported
.....1 = STBC Tx <= 80 MHz: Supported
.....0 = STBC Rx <= 80 MHz: Supported
.....0 = Doppler Tx: Not supported
.....0 = Doppler Rx: Not supported
.....0 = Full Bandwidth UL MU-MIMO: Not supported
.....0 = Partial Bandwidth UL MU-MIMO: Not supported
.....0 = Reserved: 0x0
.....0 = Reserved: 0x0
.....00 = DCN Max Constellation Tx: DCN is not supported (0x0)
.....0 = DCN Max NSS Tx: 1 Space-Time Stream (0x0)
.....0 1... = DCN Max Constellation Rx: BPSK (0x1)
.....0 = DCN Max NSS Rx: 1 Space-Time Stream (0x0)
.....0 = Rx HE MU PDU From Non-AP STA: Not supported
.....1 = SU Beamformer: Supported
.....1 = SU Beamformee: Supported
.....0 = MU Beamformer: Not supported
.....0 = Beamformee STS <= 80 MHz: 0x2
.....1 1... = Beamformee STS <= 80 MHz: 0x2
.....011 = Beamformee STS > 80 MHz: 0x3
```

### 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
.....0 = Partial Bandwidth Extended Range: Not supported
.....0 = Partial Bandwidth DL MU-MIMO: Not supported
.....1 = PPE Threshold Present: True
```

### Bits 56 to 71: 0x019c

```
.....0 = SRP-based SR Support: Not supported
.....0 = Power Boost Factor ar Support: Not supported
.....1 = HE SU PDU & HE MU PDU w 4x HE-LTF & 0.8us GI: Supported
.....01 1... = Max IIC: Supported
.....0 = STBC Tx > 80 MHz: Not supported
.....1 = STBC Rx > 80 MHz: Supported
.....1 = HE ER SU PDU w 4x HE-LTF & 0.8us GI: Supported
.....0 = 20 MHz In 40 MHz: HE PDU In 2.4GHz Band: Not supported
.....0 = 20 MHz In 160/80+80 MHz: HE PDU: Not supported
.....0 = 80 MHz In 160/80+80 MHz: HE PDU: Not supported
.....0 = HE ER SU PDU w 1x HE-LTF & 0.8us GI: Not supported
.....0 = Midamble Rx 2x & 1x HE-LTF: Not supported
.....0 = DCN Max IIC: 0x0
```

### Bits 72 to 87: 0x0008

```
.....0 = Longer Than 16 HE SIG-B OFDM Symbols Support: Not supported
.....0 = Non-Triggered CQI Feedback: Not supported
.....0 = Tx 1024-QAM Support < 242-tone RU: Not supported
.....1 = Rx 1024-QAM Support < 242-tone RU: Supported
.....0 = Rx Full BW SU Using HE MU PDU With Compressed SIGB: Not supported
.....0 = Rx Full BW SU Using HE MU PDU With Non-Compressed SIGB: Not supported
.....00 = Nominal Packet Padding: 0 µs for all Constellations (0)
.....0000 0000 = Reserved: 0x00
```

# AP sends actual connection settings



```

v Supported HE-MCS and NSS Set
  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
  > NSS 1
  > NSS 2
  > NSS 3
  > NSS 4
  > NSS 5
  > NSS 6
  > NSS 7

```

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



```
✓ BSS Color Information: 0x14
  ..01 0100 = BSS Color: 0x14
  .0... .... = Partial BSS Color: False
  0... .... = BSS Color Disabled: False
```

There are many other wireless access point in today's 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: Trigger 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
  - .... 0001 = Device Class: Class B Device (0x1)
  - .... 0010 = LDPC Coding To Payload: Supported
  - .... 0011 = HE SU PPDU With 1x HE-LTF and 0.8us GI: Not supported
  - .... 0100 = Midamble Rx Max NSTS: 1 Space-Time Stream (0x0)
  - .... 0101 = NDP With 4x HE-LTF and 3.2us GI: Supported
  - .... 0110 = STBC Tx <= 80 MHz: Not supported
  - .... 0111 = STBC Rx <= 80 MHz: Not supported
  - .... 1000 = Doppler Tx: Not supported
  - .... 1001 = Doppler Rx: Not supported
  - .... 1010 = Full Bandwidth UL MU-MIMO: Not supported
  - .... 1011 = Reserved: Not supported
  - .... 1100 = Reserved: Not supported
  - .... 1101 = Reserved: Not supported
  - .... 1110 = Reserved: Not supported
  - .... 1111 = Reserved: Not supported

## Supported HE-MCS and NSS Set

- ▼ Rx and Tx MCS Maps <= 80 MHz
  - ▼ Rx HE-MCS Map <= 80 MHz: 0xaaaa
    - .... 0000 ..10 = Max HE-MCS for 1 SS: Support for HE-MCS 0-11 (0x2)
    - .... 0001 10.. = Max HE-MCS for 2 SS: Support for HE-MCS 0-11 (0x2)
    - .... 0010 ..10 .... = Max HE-MCS for 3 SS: Support for HE-MCS 0-11 (0x2)
    - .... 0011 10.. .... = Max HE-MCS for 4 SS: Support for HE-MCS 0-11 (0x2)
    - .... 0100 ..10 .... = Max HE-MCS for 5 SS: Support for HE-MCS 0-11 (0x2)
    - .... 0101 10.. .... = Max HE-MCS for 6 SS: Support for HE-MCS 0-11 (0x2)
    - .... 0110 ..10 .... = Max HE-MCS for 7 SS: Support for HE-MCS 0-11 (0x2)
    - .... 0111 10.. .... = Max HE-MCS for 8 SS: Support for HE-MCS 0-11 (0x2)
  - ▼ Tx HE-MCS Map <= 80 MHz: 0xaaaa
    - .... 0000 ..10 = Max HE-MCS for 1 SS: Support for HE-MCS 0-11 (0x2)
    - .... 0001 10.. = Max HE-MCS for 2 SS: Support for HE-MCS 0-11 (0x2)
    - .... 0010 ..10 .... = Max HE-MCS for 3 SS: Support for HE-MCS 0-11 (0x2)
    - .... 0011 10.. .... = Max HE-MCS for 4 SS: Support for HE-MCS 0-11 (0x2)
    - .... 0100 ..10 .... = Max HE-MCS for 5 SS: Support for HE-MCS 0-11 (0x2)
    - .... 0101 10.. .... = Max HE-MCS for 6 SS: Support for HE-MCS 0-11 (0x2)
    - .... 0110 ..10 .... = Max HE-MCS for 7 SS: Support for HE-MCS 0-11 (0x2)
    - .... 0111 10.. .... = Max HE-MCS for 8 SS: Support for HE-MCS 0-11 (0x2)
- ▼ PPE Thresholds
  - .... 0111 = NSS: 7
  - .... 1111 1... = RU Index Bitmask: 0xf
- ▼ NSS 0
  - > RU allocation: 242
  - > RU allocation: 484
  - > RU allocation: 996
  - > RU allocation: 2x996

AP support 0.8 $\mu$ s/1.6 $\mu$ s 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) on  
> Radiotap Header v0, Length 32  
> 802.11 radio information  
v IEEE 802.11 QoS Data, Flags: 0.....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 report  
  v Buffer Status Report: 0x000002c8  
    .... 1000 = ...: 0x8  
    .... 00 .... = Delta  
    .... 11. .... = ACI High: 0x  
    .... .10 .... = Scaling Factor: 0x  
    .... .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 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)



プロトコル	送信元MAC	送信先MAC	BSSID	送信...	送信先IP	送...	送...	絶対...	信号...	レート	統計
1 IP/ICMP	Fortinet:B0:6A:9A	06:0F:5B:DD:...	ASUSTekC:...	1..	? 10...	N/A	N/A	18:14...	-36	1201 (HE MCS 11, 55 2, CW 80)	Icmp: Echo Reply Message, From 1.1.1.1 To 10.0.0.206
▼ Radiotap Header v0, Length 32			ASUSTekC:...	1..	? 10...	N/A	N/A	18:14...	-36	1201 (HE MCS 11, 55 2, CW 80)	Icmp: Echo Reply Message, From 1.1.1.1 To 10.0.0.206

Header revision: 0  
Header pad: 0  
Header length: 32  
> Present flags  
MAC timestamp: 1622020459456883  
> Flags: 0x00  
**Data Rate: 49.0 Mb/s**  
Channel frequency: 5320 [A 64]  
> Channel flags: 0x0140, Orthogona:  
Antenna signal: -46 dBm  
Antenna noise: -92 dBm  
Channel number: 64  
Channel frequency: 5320  
> Channel flags: 0x00000140, Ortho:  
**802.11 radio information**  
**PHY type: 802.11a (OFDM) (5)**  
Turbo type: Non-turbo (0)  
Data rate: 49.0 Mb/s  
Channel: 64  
Frequency: 5320MHz  
Signal strength (dBm): -46 dBm  
Noise level (dBm): -92 dBm  
Signal/noise ratio (dB): 46 dB  
TSF timestamp: 1622020459456883  
▼ [Duration: 44µs]

ログビューア - 1.1.1.1 と 10.0.0.206 間のパケット  
ファイル(F) 検索(S) フィルタ(R)  
▼ Wireless Packet Info  
Signal level: 98K  
Signal level in dBm: -36  
Noise level in dBm: -95  
Rate: 1201.0 Mbps  
Rate type: 802.11ax (OFDM)  
Band: 5 GHz  
Channel: 64 - 5320 MHz  
Streams: 0x2 (2)  
Guard Interval: 0.8µs  
Channel width: 0x2 (2) - 80 MHz  
年月日: 26-5-2021  
絶対時間: 18:14:19.483030  
デルタ時間: 0.000009  
フレームのサイズ: 118 バイト  
フレーム番号: 2  
▼ 802.11  
> Frame Control: 0x0288 (648)  
Duration: 0x002C (44)  
Destination Address: 06:0F:5B:DD:20:FA  
BSS ID: F0:2F:74:C4:F5:C4  
Source Address: 00:09:0F:B0:6A:9A  
Fragment Number: 0x0000 (0)  
Sequence Number: 0x01B6 (438)  
> QoS Control: 0x0000 (0)  
▼ Logical-Link Control (LLC): Command: Unnumbered  
DSAP: SNAP (0xAA)  
IG Bit: Individual  
DSAP: SNAP (0xAA)  
CR Bit: Command  
▼ Control field: Command: UI Unnumbered frame  
... Command: UI (0)  
... Frame type: Unnumbered frame (3)  
Organization Code: Encapsulated Ethernet (0x1)  
Type: IP (0x0800)  
> IPv4: Src = 1.1.1.1, Dest = 10.0.0.206, Next Protocol  
> Icmp: Echo Reply Message, From 1.1.1.1 To 10.0.0.

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
- ▼ 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
- ▼ IEEE 802.11 Wireless Management
  - ▼ 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

**Wireless - General**

Set up the wireless related information below.

Enable Smart Connect	<input type="checkbox"/> OFF
Band	5GHz
Network Name (SSID)	wifi6
Hide SSID	<input type="radio"/> Yes <input type="radio"/> No
Wireless Mode	Auto <input type="checkbox"/> Optimized for Xbox
802.11ax / Wi-Fi 6 mode	Enable <small>If compatibility issue occurs when enabling 802.11ax / Wi-Fi 6 mode, please check: <a href="#">FAQ</a></small>
Channel bandwidth	20/40/80 MHz
Control Channel	Auto <small>Current Control Channel: 116</small> <input checked="" type="checkbox"/> Auto select channel including DFS channels
Extension Channel	Auto
Authentication Method	open System

Apply

# Appendix Ping/iperf3 to wired PC with WPA2

The screenshot shows the HE.NET Network Tools interface. The search bar contains '10.0.0.212'. The 'Interval' is set to 1, and 'Byt...' is set to 1M. The 'IPV4' and 'IPV6' buttons are selected. The 'TCP' and 'UDP' buttons are also visible. The results section shows a test for 10.0.0.212:5201 (TCP) with a throughput of 1.25 MByte (235 Mbit/s) over 0.0 - 0.0 sec.

```
管理者: コマンドプロンプト - iperf3 -s
Microsoft Windows [Version 10.0.19042.985]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd c:\iperf-3.1.3-win64
C:\iperf-3.1.3-win64>iperf3 -s

Server listening on 5201

Accepted connection from 10.0.0.201, port 49177
 5] local 10.0.0.212 port 5201 connected to 10.0.0.201 port 49178
ID] Interval          Transfer      Bandwidth
 5]  0.00-0.05        sec  1.20 MBytes  187 Mbits/sec
-----
ID] Interval          Transfer      Bandwidth
 5]  0.00-0.05        sec  0.00 Bytes  0.00 bits/sec
 5]  0.00-0.05        sec  1.20 MBytes  187 Mbits/sec
-----
Server listening on 5201
```

Actual throughput is about 200Mbps



# Appendix Ping/iperf3 to wired PC with WPA2

WEP/WPA キー

WEP  
64ビット  
キー 1  
キー 2  
キー 3  
キー 4

WPA  
WPA-PSK パスフレーズ(文字):  
wireshark

読み込み... 保存... OK キャンセル

ログビューア 10.0.0.206 で送受されるパケット

ファイル(F) 検索(S) フィルタ(R)

Wireless Packet Info

- Signal level: 100%
- Noise level in dBm: -91
- Rate: 1201.0 Mbps
- Rate type: 802.11ax (OFDM)
- Band: 5 GHz
- Channel: 116 - 5680 MHz
- Streams: 0x2 (2)
- Guard Interval: 0.8 μs
- Channel width: 0x2 (2) - 80 MHz
- 年月日: 26-5-2021
- 絶対時間: 17:10:20.060303
- デルタ時間: 0.000000
- フレームのサイズ: 80 バイト
- フレーム番号: 1142

802.11

- Frame Control: 0x4288 (17092)
- Duration: 0x002C (44)
- Destination Address: 06:0F:5B:DD:20:FA
- BSS ID: F0:2F:74:C4:F5:C4
- Source Address: F0:2F:74:C4:F5:C4
- Fragment Number: 0x0000 (0)
- Sequence Number: 0x0D72 (3442)
- QoS Control: 0x0000 (0)

> Logical-Link Control (LLC): Command: Unnumb  
> -IPv4: Src = 10.0.0.212, Dest = 10.0.0.206, Next p  
> Tcp: Flags=...A..., SrcPort=5201, DstPort=49182,

番./	プロトコル	送信元MAC	送信先MAC	BSSID	送信...	送信先IP	送...	送...	絶対...	信号...	レート	統計
1142	IP/TCP	ASUSTeK.C4:F5:...	06:0F:5B:DD:...	ASUSTeK.C...	? 1.	? 10...	52...	491...	17:10...	-35	1201 (HE)	Tcp: Flags=...A..., SrcPort=5201, DstPort=49182, PayloadLen=...
1143	IP/TCP	ASUSTeK.C4:F5:...	06:0F:5B:DD:...	ASUSTeK.C...	? 1.	? 10...	52...	491...	17:10...	-35	1201 (HE)	Tcp: Flags=...A..., SrcPort=5201, DstPort=49182, PayloadLen=...
1144	IP/TCP	ASUSTeK.C4:F5:...	06:0F:5B:DD:...	ASUSTeK.C...	? 1.	? 10...	52...	491...	17:10...	-35	1201 (HE)	Tcp: Flags=...A..., SrcPort=5201, DstPort=49182, PayloadLen=...
1145	IP/TCP	ASUSTeK.C4:F5:...	06:0F:5B:DD:...	ASUSTeK.C...	? 1.	? 10...	52...	491...	17:10...	-35	1201 (HE)	Tcp: Flags=...A..., SrcPort=5201, DstPort=49182, PayloadLen=...
1146	IP/TCP	ASUSTeK.C4:F5:...	06:0F:5B:DD:...	ASUSTeK.C...	? 1.	? 10...	52...	491...	17:10...	-35	1201 (HE)	Tcp: Flags=...A..., SrcPort=5201, DstPort=49182, PayloadLen=...
1147	IP/TCP	ASUSTeK.C4:F5:...	06:0F:5B:DD:...	ASUSTeK.C...	? 1.	? 10...	52...	491...	17:10...	-35	1201 (HE)	Tcp: Flags=...A..., SrcPort=5201, DstPort=49182, PayloadLen=...
1148	IP/TCP	ASUSTeK.C4:F5:...	06:0F:5B:DD:...	ASUSTeK.C...	? 1.	? 10...	52...	491...	17:10...	-35	1201 (HE)	Tcp: Flags=...A..., SrcPort=5201, DstPort=49182, PayloadLen=...
1149	IP/TCP	ASUSTeK.C4:F5:...	06:0F:5B:DD:...	ASUSTeK.C...	? 1.	? 10...	52...	491...	17:10...	-35	1201 (HE)	Tcp: Flags=...A..., SrcPort=5201, DstPort=49182, PayloadLen=...
1150	IP/TCP	ASUSTeK.C4:F5:...	06:0F:5B:DD:...	ASUSTeK.C...	? 1.	? 10...	52...	491...	17:10...	-35	1201 (HE)	Tcp: Flags=...A..., SrcPort=5201, DstPort=49182, PayloadLen=...
1151	IP/TCP	ASUSTeK.C4:F5:...	06:0F:5B:DD:...	ASUSTeK.C...	? 1.	? 10...	52...	491...	17:10...	-35	1201 (HE)	Tcp: Flags=...A..., SrcPort=5201, DstPort=49182, PayloadLen=...
1152	IP/TCP	ASUSTeK.C4:F5:...	06:0F:5B:DD:...	ASUSTeK.C...	? 1.	? 10...	52...	491...	17:10...	-36	1201 (HE)	Tcp: Flags=...A..., SrcPort=5201, DstPort=49180, PayloadLen=...
1153	IP/TCP	ASUSTeK.C4:F5:...	06:0F:5B:DD:...	ASUSTeK.C...	? 1.	? 10...	52...	491...	17:10...	-35	1201 (HE)	Tcp: Flags=...A..., SrcPort=5201, DstPort=49182, PayloadLen=...
1154	IP/TCP	ASUSTeK.C4:F5:...	06:0F:5B:DD:...	ASUSTeK.C...	? 1.	? 10...	52...	491...	17:10...	-36	1201 (HE)	Tcp: Flags=...A..., SrcPort=5201, DstPort=49180, PayloadLen=...
1155	IP/TCP	ASUSTeK.C4:F5:...	06:0F:5B:DD:...	ASUSTeK.C...	? 1.	? 10...	52...	491...	17:10...	-35	1201 (HE)	Tcp: Flags=...A..., SrcPort=5201, DstPort=49182, PayloadLen=...
1156	IP/TCP	ASUSTeK.C4:F5:...	06:0F:5B:DD:...	ASUSTeK.C...	? 1.	? 10...	52...	491...	17:10...	-36	1201 (HE)	Tcp: Flags=...A..., SrcPort=5201, DstPort=49180, PayloadLen=...
1157	IP/TCP	ASUSTeK.C4:F5:...	06:0F:5B:DD:...	ASUSTeK.C...	? 1.	? 10...	52...	491...	17:10...	-35	1201 (HE)	Tcp: Flags=...A..., SrcPort=5201, DstPort=49182, PayloadLen=...
1158	IP/TCP	ASUSTeK.C4:F5:...	06:0F:5B:DD:...	ASUSTeK.C...	? 1.	? 10...	52...	491...	17:10...	-35	1201 (HE)	Tcp: Flags=...A..., SrcPort=5201, DstPort=49182, PayloadLen=...
1159	IP/TCP	ASUSTeK.C4:F5:...	06:0F:5B:DD:...	ASUSTeK.C...	? 1.	? 10...	52...	491...	17:10...	-35	1201 (HE)	Tcp: Flags=...A..., SrcPort=5201, DstPort=49182, PayloadLen=...
1160	IP/TCP	ASUSTeK.C4:F5:...	06:0F:5B:DD:...	ASUSTeK.C...	? 1.	? 10...	52...	491...	17:10...	-35	1201 (HE)	Tcp: Flags=...A..., SrcPort=5201, DstPort=49182, PayloadLen=...
1161	IP/TCP	ASUSTeK.C4:F5:...	06:0F:5B:DD:...	ASUSTeK.C...	? 1.	? 10...	52...	491...	17:10...	-35	1201 (HE)	Tcp: Flags=...A..., SrcPort=5201, DstPort=49182, PayloadLen=...

0x0000	88 42 2C 00 06 0F 5B DD-20 FA F0 2F 74 C4 F5 C4	*B... [Y ū/tāÅ
0x0010	F0 2F 74 C4 F5 C4 20 D7-00 00 AA AA 03 00 00 00	ō/tāÅA *#.###...
0x0020	08 00 45 00 00 28 98 30-40 00 80 06 4C FE 0A 00	..E... (~0ø€.Lh..
0x0030	00 D4 0A 00 00 CE 14 51-C0 1E 24 89 08 FA 57 08	.Ō...i.Qā.\$\$.GŪ0
0x0040	CA A7 50 10 00 00 A5 BF-00 00 00 00 00 00 00 00	Ĕ\$P..D.Yz.....

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!!



#sf21veu

We dissected a simple Wi-Fi 6 connection setup process, You may think packet dissection is not changed a lot from legacy trace, yes we use the same IEEE802.11 standards, and you may find there are many new headers and fields specified for IEEE802.11ax.

WiFi6/6E is new protocols so capture tools and software is now developing and off course Wireshark dissector will be updated. This is just an entrance of dissecting. **USE WIRESHARK** to troubleshoot and debug Wi-Fi 6!!

# USE WIRESHARK



# Thank you for watching !!

#sf21veu

Please complete the SharkFest Europe app-based survey



Supplemental file

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



ikeriri network service

<http://www.ikeriri.ne.jp>