



#sf21veu

Dissecting WiFi6 using Wireshark



Megumi Takeshita
Ikeriri network service

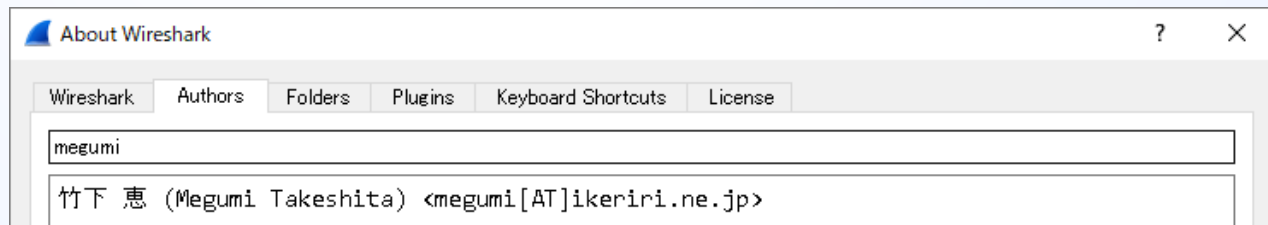
Megumi Takeshita, packet otaku



#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 on³

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

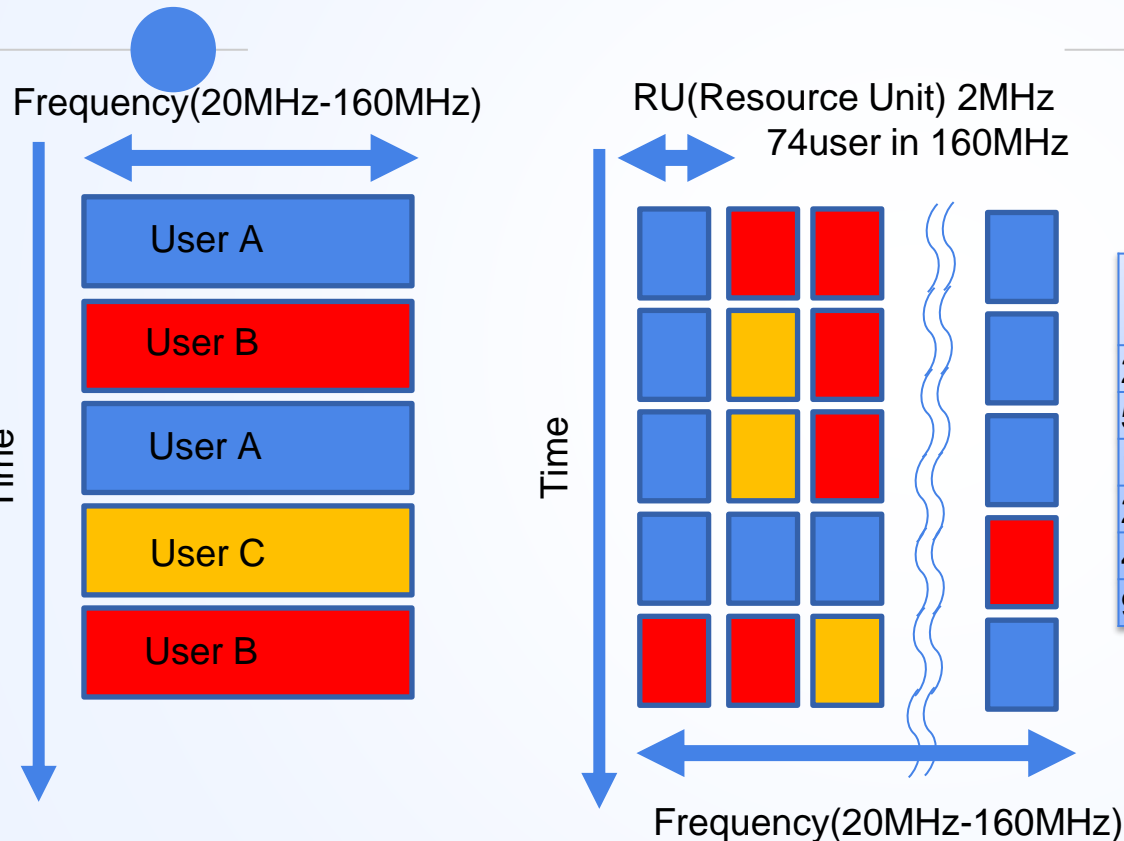


#sf21veu

- 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/streams₆



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

mscindex.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	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



#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

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: N5Q-RT-AX89X
Power: 19 VDC, 3.42 A Connector type: barrel
CPU1: Qualcomm IPQ8078 (2.2 GHz, 4 cores) FLA1: 256 MIB (Macronix MX30UF2G18AC-XX1) RAM1: 1 GiB (Micron MT41K256M16TW-107 x 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_\(AX200NGW\)](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: PD5AAX200NG , MSQAAX200NG , RWO-RZ090301 , RWO-RZ090287 IC ID: 1000M-AX200NG, 3568A-AX200NG, 8092D-RZ090301
Wi1 chip1: Intel WCSAX200
Probable Linux driver iwlwifi <i>Full support it is available in 5.5.0-rc kernel (see also passys)</i>
Windows driver <i>Win10 (64-bit only)</i>
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

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: FAQ</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

ノード 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

スタンダード / MAC アドレス	チャンネル	種類	SSID	スタンダード	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 (Rx)	キャプチャ
▼ 関連しない											◎ シングル・チャンネル・モード 5 GHz - 64
06:0F:5B:DD:20:FA		STA				-51/-46/-31			6/447.4/12...		
> 802.11g											
> 802.11n											
> 802.11ac											
> 802.11ax											
HuaweiDe...:20:3F	100 (100-104@40, 100-112@80, ...)	AP	00AD...D6203C-5G	802.11ax	WPA2... (CCMP)	-87/-86/-85	802.0	2	6/6/6	0/0/0	
ASUSTeK...C4:F5:C4	64 (60-64@40, 52-64@80)	AP	wifi6	802.11ax		-39/-35/-30	4803.9	8	6/293.3/1201	6/369/1201	
ASUSTeK...C4:F5:C0	11	AP	wifi2.4	802.11ax	WPA2PSK (CCMP)	-28/-27/-26	573.5	4	1/1/1	1/1/1	

SSID wifi6

capture CH 64

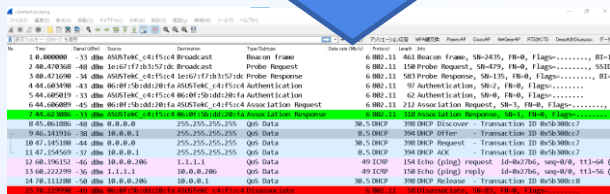
BSSID

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)



Original ncfx file: beacon frame from AP



#sf21veu

ログビューア [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: 82.329654 sec
 Beacon Interval: 0x0064 (100) - 102.400 msec
 Capability Information: 0x0501 (1281)
 v SSID parameter set
 Tag: SSID parameter set (0x0)
 Tag length: 5
 SSID: wifi6
 Supported rates
 Current Channel: 116 - 5580 MHz
 Traffic indication map (TIM): 0x00 (No frames buffered)
 Country Information
 Power Constraint
 TPC Report element
 HT Capabilities element
 HT Information element
 Extended Capabilities
 VHT Capabilities
 VHT Operation
 VHT Tx Power Envelope (IEEE Std 802.11ax/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	N/A	N/A	1640...	-36	6	SSID=wifi6, (Infra), Ch#116, Seq=9, WEP: Can't decrypt, Key#1
689	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N	N/A	N/A	1640...	-36	6	SSID=wifi6, (Infra), Ch#116, Seq=1
690	MNGT/ACTIO...	Apple10:E80D	ASUSTekC:0...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-44	24	Category=HE, Action=HE Compress
691	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N	N/A	N/A	1640...	-36	6	SSID=wifi6, (Infra), Ch#116, Seq=1
692	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N	N/A	N/A	1640...	-35	6	SSID=wifi6, (Infra), Ch#116, Seq=1
693	MNGT/ACTIO...	Apple10:E80D	ASUSTekC:0...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-41	12	Category=HE, Action=HE Compress
694	ENCR. A-M...	Apple10:E80D	ASUSTekC:0...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-40	216.2 (HE ...	WEP: Can't decrypt, Key#1
695	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N	N/A	N/A	1640...	-36	6	SSID=wifi6, (Infra), Ch#116, Seq=1
696	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N	N/A	N/A	1640...	-36	6	SSID=wifi6, (Infra), Ch#116, Seq=1
697	ENCR. DATA	Apple10:E80D	Fortinet80:6...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-40	216.2 (HE ...	WEP: Can't decrypt, Key#1
698	ENCR. DATA	Apple10:E80D	Fortinet80:6...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-40	216.2 (HE ...	WEP: Can't decrypt, Key#1
699	ENCR. DATA	Apple10:E80D	Fortinet80:6...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-40	216.2 (HE ...	WEP: Can't decrypt, Key#1
700	ENCR. DATA	Apple10:E80D	Fortinet80:6...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-40	216.2 (HE ...	WEP: Can't decrypt, Key#1
701	MNGT/ACTIO...	Apple10:E80D	Fortinet80:6...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-40	12	Category=HE, Action=HE Compress
702	ENCR. DATA	Apple10:E80D	Fortinet80:6...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-39	216.2 (HE ...	WEP: Can't decrypt, Key#1
703	ENCR. DATA	Apple10:E80D	Fortinet80:6...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-39	216.2 (HE ...	WEP: Can't decrypt, Key#1
705	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N	N/A	N/A	1640...	-37	6	SSID=wifi6, (Infra), Ch#116, Seq=1
706	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N	N/A	N/A	1640...	-37	6	SSID=wifi6, (Infra), Ch#116, Seq=1
707	ENCR. DATA	Fortinet80:6A9A	Apple10:E80...	Apple10:E80...	? N	? N	N/A	N/A	1640...	-71	340.3 (HE ...	WPA: Can't decrypt
708	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N	N/A	N/A	1640...	-37	6	SSID=wifi6, (Infra), Ch#116, Seq=1
709	ENCR. DATA	Apple10:E80D	Fortinet80:6...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-39	216.2 (HE ...	WEP: Can't decrypt, Key#1
710	ENCR. DATA	Apple10:E80D	Fortinet80:6...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-39	216.2 (HE ...	WEP: Can't decrypt, Key#1
711	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N	N/A	N/A	1640...	-37	6	SSID=wifi6, (Infra), Ch#116, Seq=2
712	ENCR. DATA	Apple10:E80D	Fortinet80:6...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-39	216.2 (HE ...	WEP: Can't decrypt, Key#1
713	ENCR. DATA	Apple10:E80D	Fortinet80:6...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-39	216.2 (HE ...	WEP: Can't decrypt, Key#1
714	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N	N/A	N/A	1640...	-37	6	SSID=wifi6, (Infra), Ch#116, Seq=2
716	MNGT/PROB...	ASUSTekC:4F5...	ASUSTekC:0...	ASUSTekC...	? N	? N	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	N/A	N/A	1640...	-70	408.3 (HE ...	WPA: Can't decrypt
724	ENCR. DATA	Apple10:E80D	Fortinet80:6...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-40	216.2 (HE ...	WEP: Can't decrypt, Key#1
725	ENCR. DATA	Apple10:E80D	Fortinet80:6...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-40	216.2 (HE ...	WEP: Can't decrypt, Key#1
726	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N	N/A	N/A	1640...	-38	6	SSID=wifi6, (Infra), Ch#116, Seq=2
727	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N	N/A	N/A	1640...	-36	6	SSID=wifi6, (Infra), Ch#116, Seq=2
728	ENCR. DATA	Apple10:E80D	Fortinet80:6...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-45	216.2 (HE ...	WEP: Can't decrypt, Key#1
729	ENCR. DATA	Apple10:E80D	Fortinet80:6...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-44	216.2 (HE ...	WEP: Can't decrypt, Key#1
730	MNGT/ACTIO...	Apple10:E80D	ASUSTekC:0...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-44	12	Category=HE, Action=HE Compress
731	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N	N/A	N/A	1640...	-35	6	SSID=wifi6, (Infra), Ch#116, Seq=2
732	ENCR. DATA	Apple10:E80D	Fortinet80:6...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-45	216.2 (HE ...	WEP: Can't decrypt, Key#1
733	MNGT/ACTIO...	Apple10:E80D	ASUSTekC:0...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-45	12	Category=HE, Action=HE Compress
734	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N	N/A	N/A	1640...	-34	6	SSID=wifi6, (Infra), Ch#116, Seq=2
735	MNGT/ACTIO...	Apple10:E80D	ASUSTekC:0...	ASUSTekC...	? N	? N	N/A	N/A	1640...	-43	12	Category=HE, Action=HE Compress
736	MNGT/BEAC...	ASUSTekC:4F5...	Broadcast	ASUSTekC...	? N	? N	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



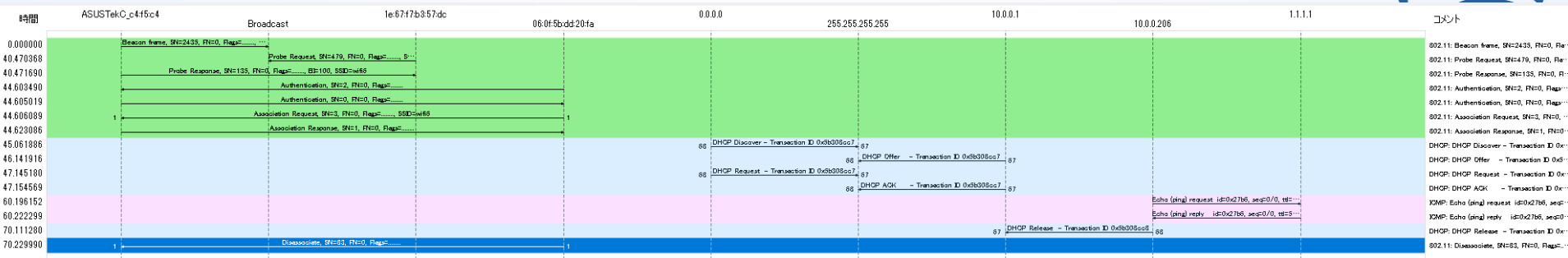
No.	Time	Signal (dBm)	Source	Destination	Type/Subtype	Data rate (Mb/s)	Protocol	Length	Info
1	0.000000	-33 dBm	ASUSTekC_c4:f5:c4	Broadcast	Beacon frame	6 802.11		461	Beacon frame, SN=2435, FN=0, Flags=....., BI=1
2	40.470368	-48 dBm	1e:67:f7:b3:57:dc	Broadcast	Probe Request	6 802.11		150	Probe Request, 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: 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

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.

```
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: 0x0008
  > 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
```


#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)

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: 0xffffa
- Tx HE-MCS Map <= 80 MHz: 0xffffa

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: 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: 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-PM Parameter Set
    > Tag: Vendor Specific: Atheros Communications, Inc.: WMM-PM Parameter Set
    > Tag: Vendor Specific: Qualcomm Inc.: WMM-PM 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: 0x00401a008010d
  > 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: 0xaaaa
    > 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)



> Frame 4: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface0

> Radiotap Header v0, Length 32

> 802.11 radio information

> IEEE 802.11 Authentication, Flags:
IEEE 802.11 Authentication, Seq: 0x0001, Status: Successful (0x0000)

> IEEE 802.11 Wireless Management

> Fixed parameters (6 bytes)

- Authentication Algorithm: Open System (0)
- Authentication SEQ: 0x0001
- Status code: Successful (0x0000)

> 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 captured (496 bits) on interface0

> Radiotap Header v0, Length 32

> 802.11 radio information

> IEEE 802.11 Authentication, Flags:
IEEE 802.11 Authentication, Seq: 0x0002, Status: Successful (0x0000)

> IEEE 802.11 Wireless Management

> Fixed parameters (6 bytes)

- Authentication Algorithm: Open System (0)
- Authentication SEQ: 0x0002
- Status code: Successful (0x0000)

> Tagged parameters (35 bytes)

- > Tag: Extended Capabilities (8 octets)
- > Tag: Vendor Specific: Apple, Inc.
- > Tag: Vendor Specific: Broadcom

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: 0x8000000080801
 - > 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: 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 PPDU (0x3)
        .... ..11.. .... = Max HE-MCS for 4 SS: Not supported for HE PPDU (0x3)
        .... ..11 .... = Max HE-MCS for 5 SS: Not supported for HE PPDU (0x3)
        .... ..11.. .... = Max HE-MCS for 6 SS: Not supported for HE PPDU (0x3)
        .... ..11 .... = Max HE-MCS for 7 SS: Not supported for HE PPDU (0x3)
        .... ..11.. .... = Max HE-MCS for 8 SS: Not supported for HE PPDU (0x3)
      > Tx 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 PPDU (0x3)
        .... ..11.. .... = Max HE-MCS for 4 SS: Not supported for HE PPDU (0x3)
        .... ..11 .... = Max HE-MCS for 5 SS: Not supported for HE PPDU (0x3)
        .... ..11.. .... = Max HE-MCS for 6 SS: Not supported for HE PPDU (0x3)
        .... ..11 .... = Max HE-MCS for 7 SS: Not supported for HE PPDU (0x3)
        .... ..11.. .... = Max HE-MCS for 8 SS: Not supported for HE PPDU (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.

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
  0... .... .... = Reduced Bandwidth UL MU-MIMO: Not supported
  
```

MCS Index	Spatial Stream	Modulation	Coding	(802.11ax)								
				2-tone RU			84-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	288.8	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	288.8	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 to 1134.3Mbps (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.: WPA3-IE 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         : 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)

HE PHY Capabilities Information: 0x00000000

```
.....1 = HE HT Support: Supported
.....0 = TWT Requester Support: Not supported
.....1 = TWT Responder Support: Supported
.....0 1.. = Fragmentation Support: Support for dynamic fragments in PPDU or S-PPDU (1)
.....000... = Maximum Number of Fragmented MSDUs: 1
.....01..... = Minimum Fragment Size: Minimum payload size of 128 bytes (1)
.....000... = Trigger frame PACE Padding Duration: 0
.....000... = Multi-TTD Aggregation Support: 0
.....0 0... = HE Link Adaptation Support: No feedback if the STA does not provide HE RFB (0)
.....0... = A-LLC Support: Not supported
.....0... = TBS Support: Not supported
.....0... = BSM Support: Supported
.....0... = Broadcast TWT Support: Not supported
.....0... = 32-bit BA Bitmap Support: Not supported
.....0... = RU Cascading Support: Not supported
.....0... = Ack-Enabled Aggregation Support: Not supported
.....0... = Reserved: 0x0
.....1 1... = OK Control Support: Supported
.....0... = OFDMA RA Support: Not supported
.....0 1.. = Maximum A-PPDU Length Exponent Extension: 3
.....0... = A-PSDU Fragmentation Support: Not supported
.....0... = Flexible TWT Schedule Support: Not supported
.....0... = Rx Control Frame to Null/BS: Not supported
.....0 0... = BSRP BQPP A-PPDU Aggregation: Not supported
.....0... = QTP Support: Not supported
.....0... = BQR Support: Not supported
.....0... = SRP Responder Role: Not supported
.....0... = BQR Feedback Report Support: Not supported
.....0... = OPS Support: Not supported
.....1.. = A-MSDU in A-PPDU Support: Supported
.....000 0... = Multi-TTD Aggregation TX Support: 0
.....0... = HE Subchannel Selective Transmission Support: Not supported
.....0... = UL 2xPSK-tone RU Support: Not supported
.....0... = OF Control UL 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: 0x02
.....0... = 409Hz in 2.4GHz band: Not supported
.....1.. = 40 & 809Hz in the 5GHz band: Supported
.....0... = 1609Hz in the 5GHz band: Not supported
.....0... = 160/80/409Hz 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
Bits 8 to 23: 0x0c0
.....0000 = Punctured Preamble RX: 0x0
.....0... = Device Class: Class A Device (0x0)
.....1.. = LDPC Coding in Payload: Supported
.....1.. = HE SU PPDU With 1x HE-LTF and 0.8us GI: Supported
.....0 0... = Ridable 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 Rx: Not supported
.....0... = Doppler Rx: Not supported
.....0... = Full Bandwidth UL MU-MIMO: Not supported
.....0... = Partial Bandwidth UL MU-MIMO: Not supported
Bits 24 to 39: 0x0b08
.....0... = 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 PPDU from Non-AP STA: Not supported
.....1.. = SU Beamformer: Supported
.....1.. = SU Beamformee: Supported
.....0... = MU Beamformee: Not supported
.....1 1.. = Beamformer STS <= 80 MHz: 0x7
011..... = Beamformer 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.. = Rg = 16 SU Feedback: Supported
.....1.. = Rg = 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 PPDU & HE MU PPDU w 4x HE-LTF & 0.8us GI: Supported
.....01 1... = Max Rg: Supported
.....0... = STBC Tx > 80 MHz: Not supported
.....1.. = STBC Rx > 80 MHz: Supported
.....1.. = HE ER SU PPDU w 4x HE-LTF & 0.8us GI: Supported
.....0... = 20 MHz In 40 MHz HE PPDU In 2.4GHz Band: Not supported
.....0... = 20 MHz In 160/80/40 MHz HE PPDU: Not supported
.....0... = 80 MHz In 160/80/40 MHz HE PPDU: Not supported
.....0... = HE ER SU PPDU w 1x HE-LTF & 0.8us GI: Not supported
.....0... = Ridable Rx 2x & 1x HE-LTF: Not supported
00..... = DCN Max BW: 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 PPDU With Compressed SIGB: Not supported
.....0... = Rx Full BW SU Using HE MU PPDU 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. Wi-Fi 6 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 In 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

Supported HE-MCS and NSS Set

Rx and Tx MCS Maps <= 80 MHz

Rx HE-MCS Map <= 80 MHz: 0xaaaa

- 0000 = Max HE-MCS for 1 SS: Support for HE-MCS 0-11 (0x2)
- 0001 = Max HE-MCS for 2 SS: Support for HE-MCS 0-11 (0x2)
- 0010 = Max HE-MCS for 3 SS: Support for HE-MCS 0-11 (0x2)
- 0011 = Max HE-MCS for 4 SS: Support for HE-MCS 0-11 (0x2)
- 0100 = Max HE-MCS for 5 SS: Support for HE-MCS 0-11 (0x2)
- 0101 = Max HE-MCS for 6 SS: Support for HE-MCS 0-11 (0x2)
- 0110 = Max HE-MCS for 7 SS: Support for HE-MCS 0-11 (0x2)
- 0111 = Max HE-MCS for 8 SS: Support for HE-MCS 0-11 (0x2)

Tx HE-MCS Map <= 80 MHz: 0xaaaa

- 0000 = Max HE-MCS for 1 SS: Support for HE-MCS 0-11 (0x2)
- 0001 = Max HE-MCS for 2 SS: Support for HE-MCS 0-11 (0x2)
- 0010 = Max HE-MCS for 3 SS: Support for HE-MCS 0-11 (0x2)
- 0011 = Max HE-MCS for 4 SS: Support for HE-MCS 0-11 (0x2)
- 0100 = Max HE-MCS for 5 SS: Support for HE-MCS 0-11 (0x2)
- 0101 = Max HE-MCS for 6 SS: Support for HE-MCS 0-11 (0x2)
- 0110 = Max HE-MCS for 7 SS: Support for HE-MCS 0-11 (0x2)
- 0111 = 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) 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 = Queue Size All: 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)



Protocol / Send MAC / Send MAC / BSSID / Send / Send IP / Send / Send / Absolute / Signal / Rate / Summary

Protocol	Send MAC	Send MAC	BSSID	Send	Send IP	Send	Send	Absolute	Signal	Rate	Summary
1 IP/ICMP	Fortinet.B0:6A:9A	06:0F:5B:DD:20:FA	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, Orthogonal
Antenna signal: -46 dBm
Antenna noise: -92 dBm
Channel number: 64
Channel frequency: 5320
Channel flags: 0x00000140, Orthogonal
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

Log View - 1.1.1.1 to 10.0.0.206 packets
File (F) Search (S) Filter (R)
▼ Wireless Packet Info
Signal level: 98%
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: 0.8 µs
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 10.0.0.206

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

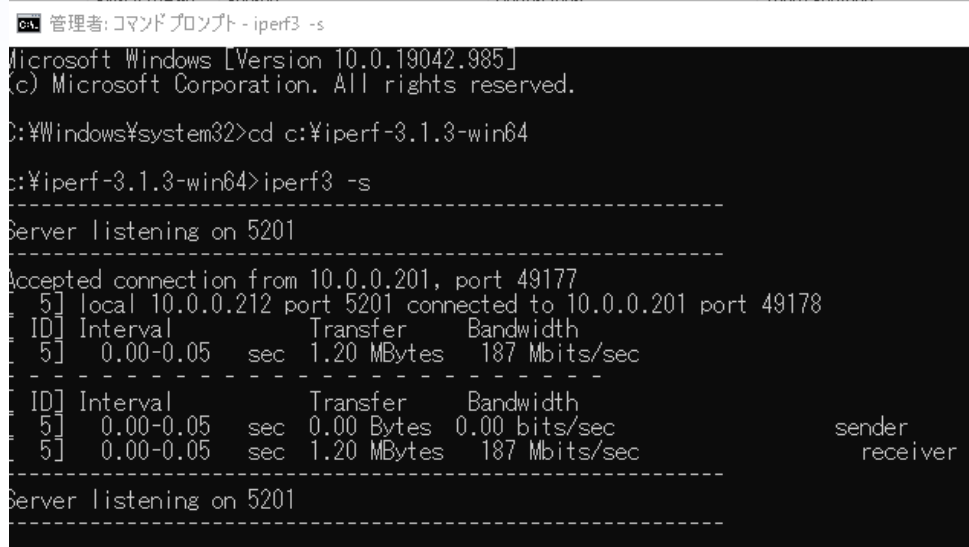
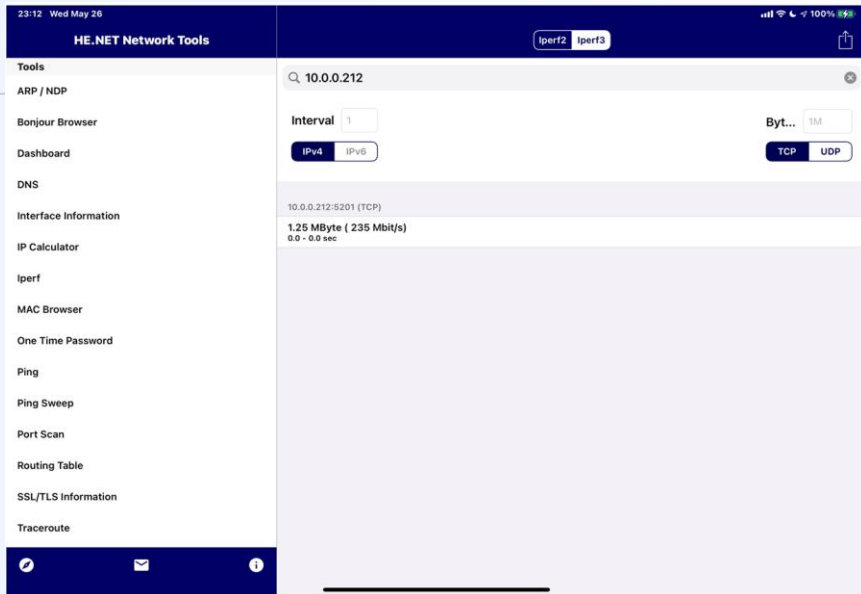
Wireless - General

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: FAQ</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



Actual throughput is about 200Mbps

Appendix Ping/iperf3 to wired PC with WPA2

The screenshot displays the Wireshark interface. On the left, the 'WEP/WPA キー' (WEP/WPA Key) dialog box is open, showing settings for WEP/WPA-PSK. The 'WPA-PSK パスフレーズ(ゆ)' (WPA-PSK Passphrase) field contains 'wireshark'. Below the dialog, there are buttons for '読み込み...' (Load...), '保存...' (Save...), 'OK', and 'キャンセル' (Cancel).

On the right, the 'ログビューア' (Log Viewer) window shows a list of captured packets. The first packet is a 'Wireless Packet Info' (802.11) packet, which is a 'Frame Control' (0x4289 (17092)) packet. The packet details show the following information:

- 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: Unnumbered
- IPv4: Src = 10.0.0.212, Dest = 10.0.0.206, Next P
- Tcp: Flags = A..., SrcPort = 5201, DstPort = 49182

The packet list on the right shows a series of IP/TCP packets (1142-1161) with the following details:

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	ASUSTekC4F5...	060F5BDD...	ASUSTekC...	?	1.	?	10...	52...	491...	1710...	-35 1201 (HE...	Tcp: Flags = A..., SrcPort = 5201, DstPort = 49182, PayloadLen = ...
1143	IP/TCP	ASUSTekC4F5...	060F5BDD...	ASUSTekC...	?	1.	?	10...	52...	491...	1710...	-35 1201 (HE...	Tcp: Flags = A..., SrcPort = 5201, DstPort = 49182, PayloadLen = ...
1144	IP/TCP	ASUSTekC4F5...	060F5BDD...	ASUSTekC...	?	1.	?	10...	52...	491...	1710...	-35 1201 (HE...	Tcp: Flags = A..., SrcPort = 5201, DstPort = 49182, PayloadLen = ...
1145	IP/TCP	ASUSTekC4F5...	060F5BDD...	ASUSTekC...	?	1.	?	10...	52...	491...	1710...	-35 1201 (HE...	Tcp: Flags = A..., SrcPort = 5201, DstPort = 49182, PayloadLen = ...
1146	IP/TCP	ASUSTekC4F5...	060F5BDD...	ASUSTekC...	?	1.	?	10...	52...	491...	1710...	-35 1201 (HE...	Tcp: Flags = A..., SrcPort = 5201, DstPort = 49182, PayloadLen = ...
1147	IP/TCP	ASUSTekC4F5...	060F5BDD...	ASUSTekC...	?	1.	?	10...	52...	491...	1710...	-35 1201 (HE...	Tcp: Flags = A..., SrcPort = 5201, DstPort = 49182, PayloadLen = ...
1148	IP/TCP	ASUSTekC4F5...	060F5BDD...	ASUSTekC...	?	1.	?	10...	52...	491...	1710...	-35 1201 (HE...	Tcp: Flags = A..., SrcPort = 5201, DstPort = 49182, PayloadLen = ...
1149	IP/TCP	ASUSTekC4F5...	060F5BDD...	ASUSTekC...	?	1.	?	10...	52...	491...	1710...	-35 1201 (HE...	Tcp: Flags = A..., SrcPort = 5201, DstPort = 49182, PayloadLen = ...
1150	IP/TCP	ASUSTekC4F5...	060F5BDD...	ASUSTekC...	?	1.	?	10...	52...	491...	1710...	-35 1201 (HE...	Tcp: Flags = A..., SrcPort = 5201, DstPort = 49182, PayloadLen = ...
1151	IP/TCP	ASUSTekC4F5...	060F5BDD...	ASUSTekC...	?	1.	?	10...	52...	491...	1710...	-35 1201 (HE...	Tcp: Flags = A..., SrcPort = 5201, DstPort = 49182, PayloadLen = ...
1152	IP/TCP	ASUSTekC4F5...	060F5BDD...	ASUSTekC...	?	1.	?	10...	52...	491...	1710...	-36 1201 (HE...	Tcp: Flags = A..., SrcPort = 5201, DstPort = 49180, PayloadLen = ...
1153	IP/TCP	ASUSTekC4F5...	060F5BDD...	ASUSTekC...	?	1.	?	10...	52...	491...	1710...	-35 1201 (HE...	Tcp: Flags = A..., SrcPort = 5201, DstPort = 49182, PayloadLen = ...
1154	IP/TCP	ASUSTekC4F5...	060F5BDD...	ASUSTekC...	?	1.	?	10...	52...	491...	1710...	-36 1201 (HE...	Tcp: Flags = A..., SrcPort = 5201, DstPort = 49180, PayloadLen = ...
1155	IP/TCP	ASUSTekC4F5...	060F5BDD...	ASUSTekC...	?	1.	?	10...	52...	491...	1710...	-35 1201 (HE...	Tcp: Flags = A..., SrcPort = 5201, DstPort = 49182, PayloadLen = ...
1156	IP/TCP	ASUSTekC4F5...	060F5BDD...	ASUSTekC...	?	1.	?	10...	52...	491...	1710...	-36 1201 (HE...	Tcp: Flags = A..., SrcPort = 5201, DstPort = 49180, PayloadLen = ...
1157	IP/TCP	ASUSTekC4F5...	060F5BDD...	ASUSTekC...	?	1.	?	10...	52...	491...	1710...	-35 1201 (HE...	Tcp: Flags = A..., SrcPort = 5201, DstPort = 49182, PayloadLen = ...
1158	IP/TCP	ASUSTekC4F5...	060F5BDD...	ASUSTekC...	?	1.	?	10...	52...	491...	1710...	-35 1201 (HE...	Tcp: Flags = A..., SrcPort = 5201, DstPort = 49182, PayloadLen = ...
1159	IP/TCP	ASUSTekC4F5...	060F5BDD...	ASUSTekC...	?	1.	?	10...	52...	491...	1710...	-35 1201 (HE...	Tcp: Flags = A..., SrcPort = 5201, DstPort = 49182, PayloadLen = ...
1160	IP/TCP	ASUSTekC4F5...	060F5BDD...	ASUSTekC...	?	1.	?	10...	52...	491...	1710...	-35 1201 (HE...	Tcp: Flags = A..., SrcPort = 5201, DstPort = 49182, PayloadLen = ...
1161	IP/TCP	ASUSTekC4F5...	060F5BDD...	ASUSTekC...	?	1.	?	10...	52...	491...	1710...	-35 1201 (HE...	Tcp: Flags = A..., SrcPort = 5201, DstPort = 49182, PayloadLen = ...

The packet bytes pane shows the raw data of the selected packet (1142), which is a frame control packet. The data is displayed in hexadecimal and ASCII format.

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 WiFi6 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>