



Capturing WiFi7

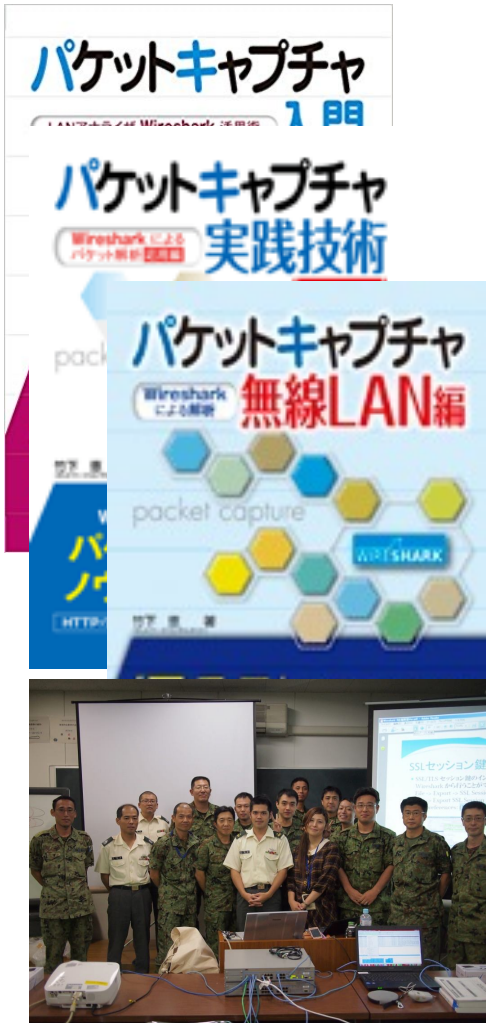
Capturing BE traffic and analyze EHT frame using Wireshark

Megumi Takeshita
Packet Otaku,
ikeriri network service

Sample traces and configurations
https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu.zip



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





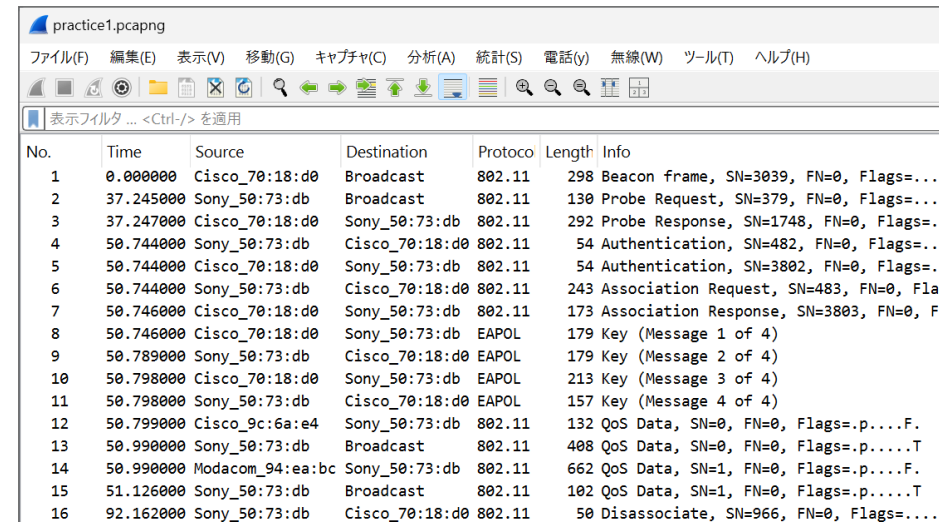
• WiFi has been upgraded in the next phase, and the 7th generation bumped up from 6/6E, enabling over 30Gbps wireless communication using 320MHz, 16 streams, and 4096 QAM modulation. In this session, we try the Intel BE200 adapter to capture the live traffic of WiFi7 and dissect extended tags of IEEE802.11be using Wireshark. We dissect WiFi management, control and data frames and learn mechanisms and standards of IEEE802.11 protocols. It also includes security based on WPA2/WPA3.



- Open practice1.pcapng
it contains a typical WiFi connection example

Customize your Wireshark as a WiFi analyzer

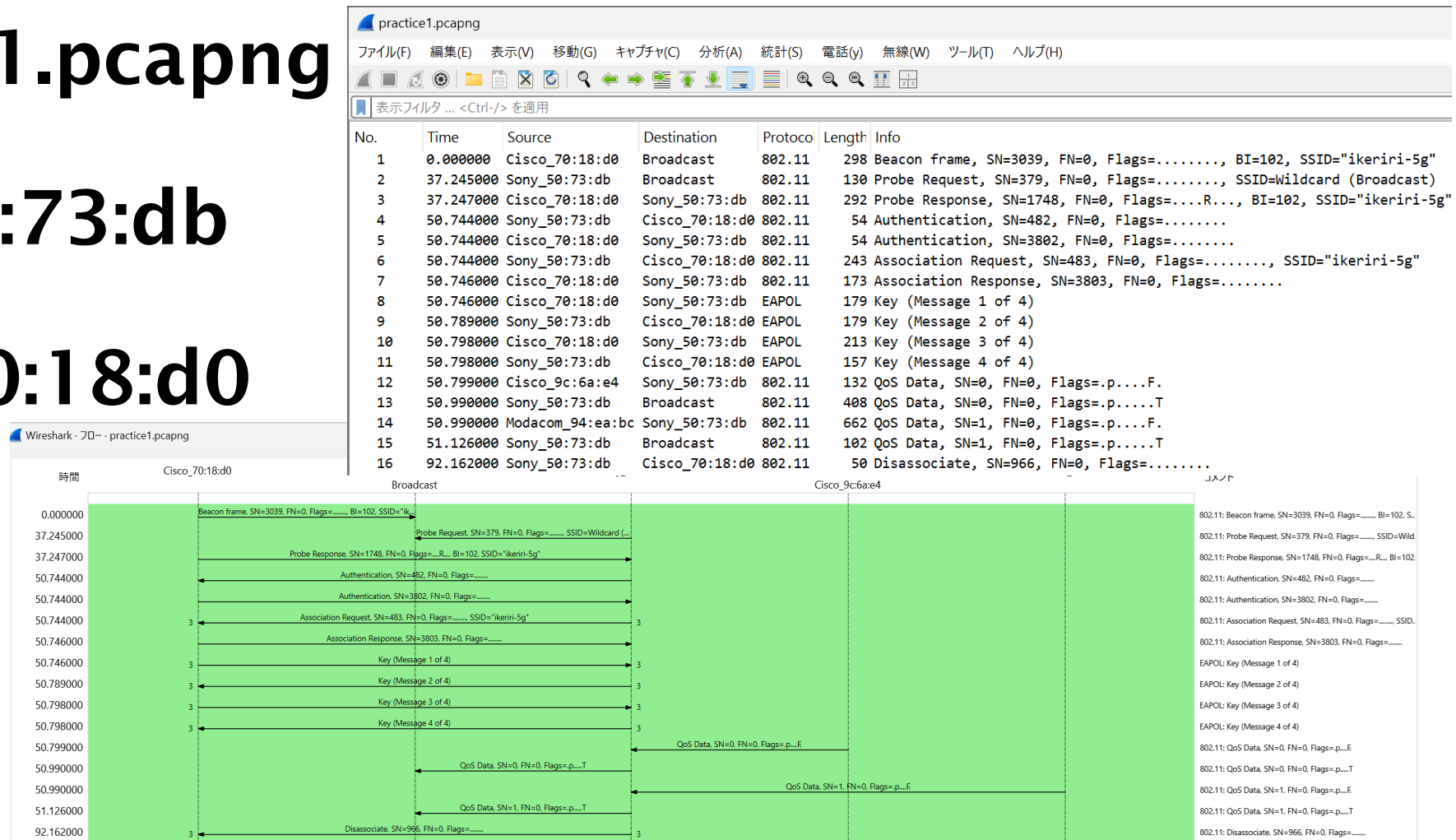
- Filter buttons
- Columns
- Coloring rules
- Statistics>Conversation



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_70:18:d0	Broadcast	802.11	298	Beacon frame, SN=3039, FN=0, Flags=...
2	37.245000	Sony_50:73:db	Broadcast	802.11	130	Probe Request, SN=379, FN=0, Flags=...
3	37.247000	Cisco_70:18:d0	Sony_50:73:db	802.11	292	Probe Response, SN=1748, FN=0, Flags=...
4	50.744000	Sony_50:73:db	Cisco_70:18:d0	802.11	54	Authentication, SN=482, FN=0, Flags=...
5	50.744000	Cisco_70:18:d0	Sony_50:73:db	802.11	54	Authentication, SN=3802, FN=0, Flags=...
6	50.744000	Sony_50:73:db	Cisco_70:18:d0	802.11	243	Association Request, SN=483, FN=0, Fla...
7	50.746000	Cisco_70:18:d0	Sony_50:73:db	802.11	173	Association Response, SN=3803, FN=0, F...
8	50.746000	Cisco_70:18:d0	Sony_50:73:db	EAPOL	179	Key (Message 1 of 4)
9	50.789000	Sony_50:73:db	Cisco_70:18:d0	EAPOL	179	Key (Message 2 of 4)
10	50.798000	Cisco_70:18:d0	Sony_50:73:db	EAPOL	213	Key (Message 3 of 4)
11	50.798000	Sony_50:73:db	Cisco_70:18:d0	EAPOL	157	Key (Message 4 of 4)
12	50.799000	Cisco_9c:6a:e4	Sony_50:73:db	802.11	132	QoS Data, SN=0, FN=0, Flags=p....F.
13	50.990000	Sony_50:73:db	Broadcast	802.11	408	QoS Data, SN=0, FN=0, Flags=p.....T
14	50.990000	Modacom_94:ea:bc	Sony_50:73:db	802.11	662	QoS Data, SN=1, FN=0, Flags=p....F.
15	51.126000	Sony_50:73:db	Broadcast	802.11	102	QoS Data, SN=1, FN=0, Flags=p.....T
16	92.162000	Sony_50:73:db	Cisco_70:18:d0	802.11	50	Disassociate, SN=966, FN=0, Flags=...



practice1.pcapng
STA:
Sony_50:73:db
AP:
Cisco_70:18:d0





- Multiple Probe Requests and Responses
- 2 Authentication (WPA2: Open System) or 4 Authentication (WPA3: SAE (Dragonfly))
- 1 set of Association Request / Response
- EAPOL 4way handshake
- Data / QoS Data
- Tons of Acks / Block Acks and Block Ack Req.
- Deauth/Disassociation sometimes drop...

Sample traces and configurations
https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu.zip

Display Filter Buttons

SharkFest'24 EUROPE



Major WiFi Frame types



Create Display Filter Button

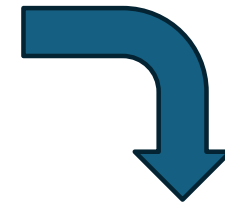
Frame type	Display Filter
Management frame wlan.fc.type==0	Beacon wlan.fc.type_subtype==8
	Probe Request wlan.fc.type_subtype==4
	Probe Response wlan.fc.type_subtype==5
	Authentication wlan.fc.type_subtype==11
	Association Request wlan.fc.type_subtype==0
	Association Response wlan.fc.type_subtype==1
	Disassociation wlan.fc.type_subtype==10
	Deauthentication wlan.fc.type_subtype==12
	Action wlan.fc.type_subtype==13
Control frame wlan.fc.type==1	ACK (ACKnowledge) wlan.fc.type_subtype==29
	RTS (Request To Send) wlan.fc.type_subtype==27
	CTS (Clear To Send) wlan.fc.type_subtype==28
	BAR (Block ACK Request) wlan.fc.type_subtype==24
	BA(Block ACK) wlan.fc.type_subtype==25
Data frame wlan.fc.type==2	Data wlan.fc.type_subtype==2
	Null Data wlan.fc.type_subtype==36
	QoS Data wlan.fc.type_subtype==40



• Wireshark preference>Filter Buttons

Wireshark · Preferences

▼ Appearance	Show in toolbar	Button Label	Filter Expression
Columns	☒	Management//All	wlan.fc.type == 0
Font and Colors	☒	Management//Beacon	wlan.fc.type_subtype == 8
Layout	☒	Management//Probe Request	wlan.fc.type_subtype == 4
Capture	☒	Management//Probe Responses	wlan.fc.type_subtype == 5
Expert	☒	Management//Probe Req and Res	wlan.fc.type_subtype in {4,5}
Filter Buttons	☒	Management//Authentication	wlan.fc.type_subtype == 11
Name Resolution	☒	Management//Association Requests	wlan.fc.type_subtype == 0
> Protocols	☒	Management//Association Responses	wlan.fc.type_subtype == 1
RSA Keys	☒	Management//Association Req and Res	wlan.fc.type_subtype in {0,1}
> Statistics	☒	Management//Disassociation	wlan.fc.type_subtype == 10
Advanced	☒	Management//Deauthentication	wlan.fc.type_subtype == 12
	☒	Management//Disassoc and Deauth	wlan.fc.type_subtype in {10,12}
	☒	Management//Action	wlan.fc.type_subtype == 13
	☒	Control Frames//All	wlan.fc.type == 1
	☒	Control Frames//ACK	wlan.fc.type_subtype == 29
	☒	Control Frames//RTS and CTS	wlan.fc.type_subtype in {27,28}
	☒	Control Frames//BAR and BA	wlan.fc.type_subtype in {24,25}
	☒	Data//All	wlan.fc.type == 2
	☒	Data//Null Data	wlan.fc.type_subtype == 36
	☒	Data//QoS Data	wlan.fc.type_subtype == 40



Management ▼	Control Frames ▼	DATA ▼
All	All	All
Beacon	ACK	Null Data
Probe Request	RTS and CTS	QoS Data
Probe Responses	BAR and BA	
Probe Req and Res		
Authentication		
Association Requests		
Association Responses		
Association Req and Res		
Disassociation		
Deauthentication		
Disassoc and Deauth		

Sample traces and configurations
https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu.zip



Signal strength (dBm)

-100dBm Noise floor	-90dBm Weak Worst MCS	-80dBm bad lower MCS	-70dBm Normal	-65dBm Good Higher MCS	-60dBm Strong Best MCS
--	--	---	--------------------------------	---	---

field	Display filter
radiotap.dbm_antsignal or wlan_radio.signal_dbm	Best Over -60dBm radiotap.dbm_antsignal >=-60
	Better Over -65dBm radiotap.dbm_antsignal >=-65
	Normal Over -70dBm radiotap.dbm_antsignal >=-70
	Worse Over -80dBm radiotap.dbm_antsignal >=-80
	Worst Over -90dBm radiotap.dbm_antsignal >=-90



- Logical Data Rate is shown as `radiotap.datarate` or `wlan_radio.data_rate`

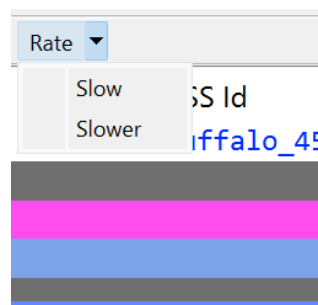
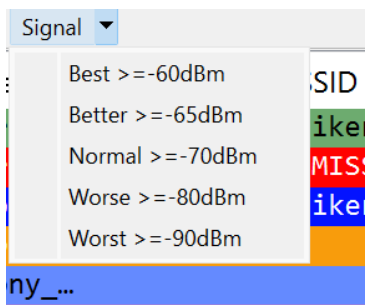
Field	Display filter
<code>radiotap.datarate</code> or <code>wlan_radio.data_rate</code>	Slow under 6.5Mbps
	Slower under 11Mbps

- Sometimes radiotap header has MCS fields `wlan_radio.11n.mcs_index` or `wlan_radio.11ac.mcs` or `radiotap.mcs.index` (depends on environment)
- Generally, under 6.5Mbps uses legacy standards. 11Mbps may remains old standard configurations.
- We can create display filter buttons for these.



• Wireshark preference>Filter Buttons

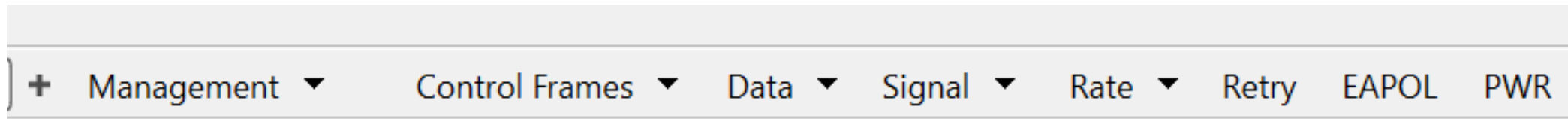
☒	Signal//Best >=-60dBm	radiotap.dbm_antsignal >=-60
☒	Signal//Better >=-65dBm	radiotap.dbm_antsignal >=-65
☒	Signal//Normal >=-70dBm	radiotap.dbm_antsignal >=-70
☒	Signal//Worse >=-80dBm	radiotap.dbm_antsignal >=-80
☒	Signal//Worst >=-90dBm	radiotap.dbm_antsignal >=-90
☒	Rate//Slow	radiotap.datarate<6.5
☒	Rate//Slower	radiotap.datarate<11



Define parents//child style
Display filter buttons to
create hierarchical menus.



- If you filter CSMA/CA retransmission, “wlan.fc.retry==1”
 - If you want to filter the EAPOL 4-way handshake, “eapol”
 - If you filter Power Management, “wlan.fc.pwrmtgt ==1”
- .We customized functional filter buttons for WiFi analysis



Creating other Display Filter Buttons

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



Button Label	Filter Expression		
Management//All	wlan.fc.type == 0	Control Frames//RTS and CTS	wlan.fc.type_subtype in {27,28}
Management//Beacon	wlan.fc.type_subtype == 8	Control Frames//BAR and BA	wlan.fc.type_subtype in {24,25}
Management//Probe Request	wlan.fc.type_subtype == 4	Data//All	wlan.fc.type == 2
Management//Probe Responses	wlan.fc.type_subtype == 5	Data//Null Data	wlan.fc.type_subtype == 36
Management//Probe Req and Res	wlan.fc.type_subtype in {4,5}	Data//QoS Data	wlan.fc.type_subtype == 40
Management//Authentication	wlan.fc.type_subtype == 11	Signal//Best >=-60dBm	radiotap.dbm_antsignal >=-60
Management//Association Requests	wlan.fc.type_subtype == 0	Signal//Better >=-65dBm	radiotap.dbm_antsignal >=-65
Management//Association Responses	wlan.fc.type_subtype == 1	Signal//Normal >=-70dBm	radiotap.dbm_antsignal >=-70
Management//Association Req and Res	wlan.fc.type_subtype in {0,1}	Signal//Worse >=-80dBm	radiotap.dbm_antsignal >=-80
Management//Disassociation	wlan.fc.type_subtype == 10	Signal//Worst >=-90dBm	radiotap.dbm_antsignal >=-90
Management//Deauthentication	wlan.fc.type_subtype == 12	Rate//Slow	radiotap.datarate<6.5
Management//Disassoc and Deauth	wlan.fc.type_subtype in {10,12}	Rate//Slower	radiotap.datarate<11
Management//Action	wlan.fc.type_subtype == 13	Retry	wlan.fc.retry == 1
Control Frames//All	wlan.fc.type == 1	EAPOL	eapol
Control Frames//ACK	wlan.fc.type_subtype == 29	PWR	wlan.fc.pwrmtgt == 1

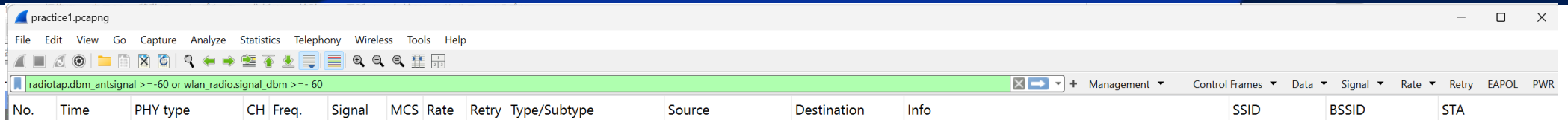
- Create the other Display Filter buttons



	Field	Explanation
MUST	Type/Subtype	To determine the Role of WiFi frame
	Channel	To find the Roaming (ch1 means 2.4GHz and 6GHz)
	Signal	For troubleshooting of RSSI
	Rate	For troubleshooting of data rate
	Retry bit	For calculating retry rate
OPTION	Phy type	To understand WiFi standard
	Frequency	To find the Roaming with Channel
	MCS	For troubleshooting of data rate with MCS
	SSID	Used with Beacon and Probe
	BSSID	To find the Roaming with SSID
	STA	To find Station

Appearance > Columns setting

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



Wireshark · Preferences

Appearance

Columns

Font and Colors

Layout

Capture

Expert

Filter Buttons

Name Resolution

Protocols

RSA Keys

Statistics

Advanced

Displayed	Title	Type	Fields	Field C	Resolved	Width	Alignme
☒	No.	Number				86	Left
☒	Time	Time (format as specified)				86	Default
☒	PHY type	Custom	wlan_radio.phy	0	☒	130	Default
☒	CH	Custom	wlan_radio.channel	0		30	Center
☒	Freq.	Custom	wlan_radio.frequency	0	☒	68	Center
☒	Signal	Custom	radiotap.dbm_antsignal	0	☒	68	Default
☒	MCS	Custom	radiotap.mcs.index	0		42	Default
☒	Rate	Custom	radiotap.datarate	0		50	Default
☒	Type/Subtype	Custom	wlan.fc.type_subtype	0	☒	182	Default
☒	Source	Source address				147	Default
☒	Destination	Destination address				130	Default
☐	Length	Packet length (bytes)				0	Center
☒	Retry	Custom	wlan.fc.retry.expert	0		47	Default
☒	Info	Information				640	Default
☒	SSID	Custom	wlan.ssid	0		112	Default
☒	BSSID	Custom	wlan.bssid	0	☒	130	Default
☒	STA	Custom	wlan.staa	0	☒	121	Default

Create coloring rules



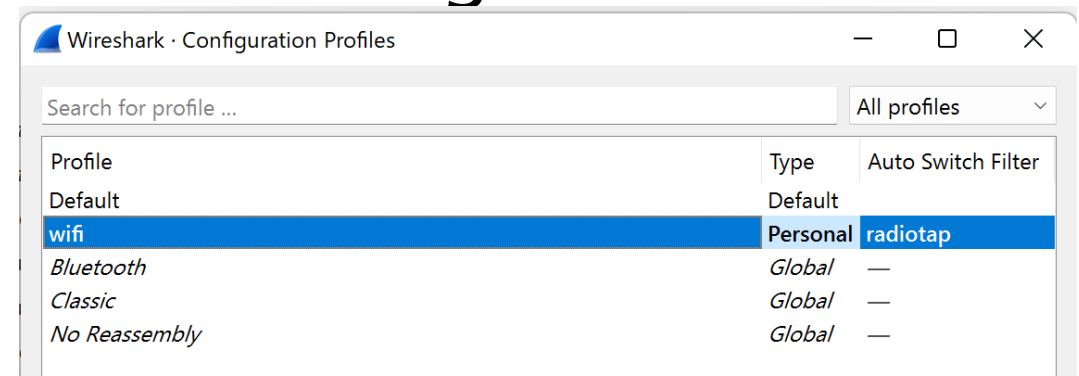
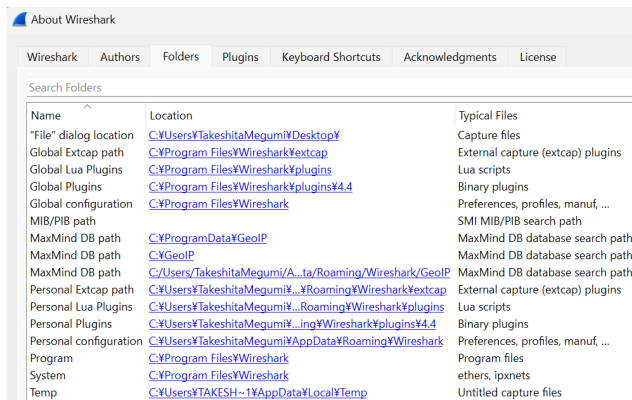
✓ Beacon	wlan.fc.type_subtype == 0x08
✓ Probe Request	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x04)
✓ Probe Response	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x05)
✓ Association Request	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x00)
✓ Association Response	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x01)
✓ Reassociation Request	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x02)
✓ Reassociation Response	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x03)
✓ Disassociate	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x0a)
✓ Authentication	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x0b)
✓ Deauthentication	(wlan.fc.type == 0)&&(wlan.fc.type_subtype == 0x0c)
✓ ACKnowledgement	(wlan.fc.type == 1)&&(wlan.fc.subtype == 13)
✓ RTS - Request To Send	(wlan.fc.type == 1)&&(wlan.fc.type_subtype == 0x1b)
✓ CTS - Clear To Send	(wlan.fc.type == 1)&&(wlan.fc.type_subtype == 0x1c)
✓ BA - Block ACK	(wlan.fc.type == 1)&&(wlan.fc.subtype == 9)
✓ BA_Request	(wlan.fc.type == 1)&&(wlan.fc.subtype == 8)
✓ EAPOL	eapol
✓ Weak signal	radiotap.dbm_antsignal < -90
✓ Slow rate	radiotap.datarate < 6
✓ Retry	wlan.fc.retry == 1

View>Coloring Rules to create

- Set each color by frame type
- Weak signal
- Slow rate
- Retry
- EAPOL



- Create personal configuration with Auto Switch Filter : Recommend to use “radiotap” to filter WiFi
- Copy personal configuration to import/export
C:\Users\username\AppData\Roaming\Wireshark\profiles
- Also recommends to import useful profiles
e.x. Wireshark Profiles Repository (<https://www.cellstream.com/wireshark-profiles-repository/>)
- Use the same profile with the debug team



Sample traces and configurations
https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu.zip



- We usually need to filter traffic between the specified STA and AP(BSSID)
- Set Display filter from Statistics>Conversation is useful. Right click the row and set filter.

Wireshark · Conversations · practice1.pcapng

Conversation Settings

- ☐ Name resolution
- ☐ Absolute start time
- ☒ Limit to display filter

Copy

Follow Stream...

Graph...

Protocol

- ☒ IEEE 802.11

Right click the row you want to filter,
Apply as Filter>Selected> A↔B

Check IEEE 802.11 to show IEEE802.11 tab

Ethernet		IEEE 802.11	
Address A	Address B	Address A	Address B
00:1d:93:94:ea:bc	40:40:a7:50:73:db	40:40:a7:50:73:db	ff:ff:ff:ff:ff:ff
18:80:90:9c:6a:e4	40:40:a7:50:73:db	40:40:a7:50:73:db	ff:ff:ff:ff:ff:ff
40:40:a7:50:73:db	ff:ff:ff:ff:ff:ff	ff:ff:ff:ff:ff:ff	40:40:a7:50:73:db
50:0f:80:70:18:d0	40:40:a7:50:73:db	40:40:a7:50:73:db	ff:ff:ff:ff:ff:ff
50:0f:80:70:18:d0	ff:ff:ff:ff:ff:ff	ff:ff:ff:ff:ff:ff	40:40:a7:50:73:db

Use the customized profile for debugging

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



practice1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_70:18:d0	Broadcast	802.11	298	Beacon frame, SN=3039, FN=0, Fla
2	37.245000	Sony_50:73:db	Broadcast	802.11	130	Probe Request, SN=379, FN=0, Fla
3	37.247000	Cisco_70:18:d0	Sony_50:73:db	802.11	292	Probe Response, SN=1748, FN=0, F
4	50.744000	Sony_50:73:db	Cisco_70:18:d0	802.11	54	Authentication, SN=482, FN=0, F1
5	50.744000	Cisco_70:18:d0	Sony_50:73:db	802.11	54	Authentication, SN=3802, FN=0, F
6	50.744000	Sony_50:73:db	Cisco_70:18:d0	802.11	243	Association Request, SN=483, FN=
7	50.746000	Cisco_70:18:d0	Sony_50:73:db	802.11	173	Association Response, SN=3803, F
8	50.746000	Cisco_70:18:d0	Sony_50:73:db	EAPOL	179	Key (Message 1 of 4)
9	50.789000	Sony_50:73:db	Cisco_70:18:d0	EAPOL	179	Key (Message 2 of 4)

> Frame 1: 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits) on interface unknown, i

> Radiotap Header v0, Length 24

> 802.11 radio information

> IEEE 802.11 Beacon frame, Flags:

> IEEE 802.11 Wireless Management

Wireshark · Configuration Profiles

Search for profile ... All profiles

Profile	Type	Auto Switch Filter
Default	Default	
WiFi	Personal	radiotap
Bluetooth	Global	—
Classic	Global	—
No Reassembly	Global	—

practice1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools

radiotap.dbm_antisignal >=-60 or wlan_radio.signal_dbm >=-60

No.	Time	PHY type	CH	Freq.	Signal	MCS	Rate	Retry	Type/Subtype	Source	Destination	Info	SSID	BSSID	STA
1	0.000000	802.11a (OFDM)	36	5180MHz	-44 dBm	6			Beacon frame	Cisco_70:18:d0	Broadcast	Beacon frame, SN=3039, FN=0, Flags=..... "ikeriri-5g" Cisco_70:18:d0			
2	37.245000	802.11a (OFDM)	36	5180MHz	-50 dBm	6			Probe Request	Sony_50:73:db	Broadcast	Probe Request, SN=379, FN=0, Flags=..... <MISSING> Broadcast			
3	37.247000	802.11a (OFDM)	36	5180MHz	-44 dBm	6	✓		Probe Response	Cisco_70:18:d0	Sony_50:73:db	Probe Response, SN=1748, FN=0, Flags=..... "ikeriri-5g" Cisco_70:18:d0			
5	50.744000	802.11a (OFDM)	36	5180MHz	-44 dBm	6			Authentication	Cisco_70:18:d0	Sony_50:73:db	Authentication, SN=3802, FN=0, Flags=..... Cisco_70:18:d0			
7	50.746000	802.11a (OFDM)	36	5180MHz	-44 dBm	6			Association Response	Cisco_70:18:d0	Sony_50:73:db	Association Response, SN=3803, FN=0, Flag... Cisco_70:18:d0			
8	50.746000	802.11a (OFDM)	36	5180MHz	-44 dBm	6			QoS Data	Cisco_70:18:d0	Sony_50:73:db	Key (Message 1 of 4) Cisco_70:18:d0 Sony_50:73:db			
9	50.789000	802.11a (OFDM)	36	5180MHz	-52 dBm	6			QoS Data	Sony_50:73:db	Cisco_70:18:d0	Key (Message 2 of 4) Cisco_70:18:d0 Sony_50:73:db			
10	50.798000	802.11a (OFDM)	36	5180MHz	-44 dBm	6			QoS Data	Cisco_70:18:d0	Sony_50:73:db	Key (Message 3 of 4) Cisco_70:18:d0 Sony_50:73:db			
11	50.798000	802.11a (OFDM)	36	5180MHz	-52 dBm	6			QoS Data	Sony_50:73:db	Cisco_70:18:d0	Key (Message 4 of 4) Cisco_70:18:d0 Sony_50:73:db			
12	50.799000	802.11ac (VHT)	36	5180MHz	-42 dBm				QoS Data	Cisco_9c:6a:e4	Sony_50:73:db	QoS Data, SN=0, FN=0, Flags=.p....F. Cisco_70:18:d0 Sony_50:73:db			
14	50.990000	802.11ac (VHT)	36	5180MHz	-40 dBm				QoS Data	Modacom_94:ea:bc	Sony_50:73:db	QoS Data, SN=1, FN=0, Flags=.p....F. Cisco_70:18:d0 Sony_50:73:db			
15	51.126000	802.11a (OFDM)	36	5180MHz	-56 dBm			9	QoS Data	Sony_50:73:db	Broadcast	QoS Data, SN=1, FN=0, Flags=.p....T Cisco_70:18:d0 Sony_50:73:db			
16	92.162000	802.11a (OFDM)	36	5180MHz	-50 dBm	6			Disassociate	Sony_50:73:db	Cisco_70:18:d0	Disassociate, SN=966, FN=0, Flags=..... Cisco_70:18:d0			

> Frame 1: 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits) on interface unknown, id 0

> Radiotap Header v0, Length 24

> 802.11 radio information

> IEEE 802.11 Beacon frame, Flags:

> IEEE 802.11 Wireless Management

0010 00 0c 3c 14 40 01 d4 a1 80 00 00 00 ff ff ff ff ..<.@...

0020 ff ff 50 0f 80 70 18 d0 50 0f 80 70 18 d0 f0 bd ..P..p.. P..p...

0030 06 08 d6 09 4b 00 00 00 66 00 11 01 00 0a 69 6bK... f.....ik

0040 65 72 69 72 69 2d 35 67 01 08 8c 92 98 a4 b0 c8 eriri-5g

0050 e0 ec 05 04 00 02 00 00 2d 1a ee 19 1b ff ff 00

0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00



- AP and STA can retry frames if they cannot receive ACK/BA for their data frames
- Capture device cannot request retransmission. Capture rate never reach 100%, drops a lot.
- The capture rate depends on the environment, and radiotap header information also depends on the device and monitor mode driver.
- Linux and macOS support monitor mode, but Windows API is never supported by the spec
→We need commercial products



- Mike-san (Mike Kershaw), famous for creator of Kismet, he says WiFi is haystack.
- We need to deal with the needle in a haystack
- Tons of drops, difficult to find.

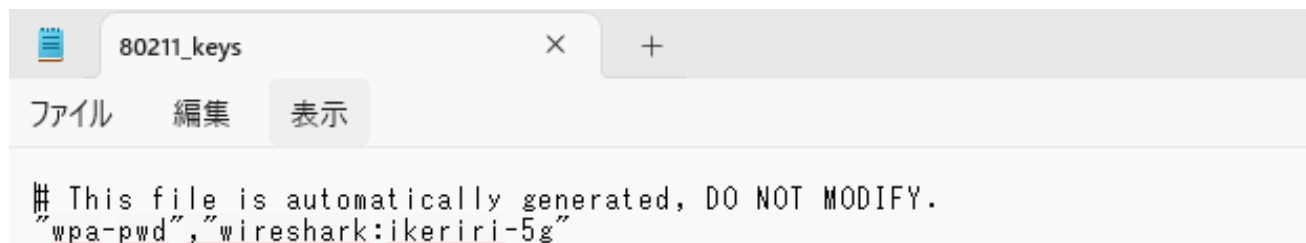




- In practice 1.pcapng, open IEEE802.11 preference, check Enable decryption, click Decryption Keys
- Select Key Type as “wpa-pwd” and set Key as “passphrase:SSID”, “wireshark:ikeriri-5g”

Key Type	Key
wpa-pwd	wireshark:ikeriri-5g

- Wireshark saves Wireless key information into 80211_keys file in your profile



Sample traces and configurations
https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu.zip

Decrypting Practice1.pcapng

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



practice1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter... <Ctrl-/>

No.	Time	PHY type	CH	Freq.	Source	Destination	Signal	MCS	Rate	Retry	Type/Subtype	Info
1	0.000000	802.11a (OFDM)	36	5180MHz	Cisco_70:18:d0	Broadcast	-44 ...	...	6	...	Beacon frame	Beacon frame, SN=3039, FN=0, F
2	37.245000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Broadcast	-50 ...	...	6	...	Probe Request	Probe Request, SN=379, FN=0, F
3	37.247000	802.11a (OFDM)	36	5180MHz	Cisco_70:18:d0	Sony_50:73:db	-44 ...	...	6	✓	Probe Response	Probe Response, SN=1748, FN=0, F
4	50.744000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Cisco_70:18:d0	-64 ...	...	6	...	Authentication	Authentication, SN=482, FN=0, F
5	50.744000	802.11a (OFDM)	36	5180MHz	Cisco_70:18:d0	Sony_50:73:db	-44 ...	...	6	...	Authentication	Authentication, SN=3802, FN=0, F
6	50.744000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Cisco_70:18:d0	-64 ...	...	6	...	Association Request	Association Request, SN=483, F
7	50.746000	802.11a (OFDM)	36	5180MHz	Cisco_70:18:d0	Sony_50:73:db	-44 ...	...	6	...	Association Response	Association Response, SN=3803, F
8	50.746000	802.11a (OFDM)	36	5180MHz	Cisco_70:18:d0	Sony_50:73:db	-44 ...	...	6	...	QoS Data	Key (Message 1 of 4)
9	50.789000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Cisco_70:18:d0	-52 ...	...	6	...	QoS Data	Key (Message 2 of 4)
10	50.798000	802.11a (OFDM)	36	5180MHz	Cisco_70:18:d0	Sony_50:73:db	-44 ...	...	6	...	QoS Data	Key (Message 3 of 4)
11	50.798000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Cisco_70:18:d0	-52 ...	...	6	...	QoS Data	Key (Message 4 of 4)
12	50.799000	802.11ac (VHT)	36	5180MHz	Cisco_9c:6a:e4	Sony_50:73:db	-42 ...	...	...	...	QoS Data	QoS Data, SN=0, FN=0, Flags=.p
13	50.990000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Broadcast	-64 ...	...	9	...	QoS Data	QoS Data, SN=0, FN=0, Flags=.p
14	50.990000	802.11ac (VHT)	36	5180MHz	Modacom_94:ea:bc	Sony_50:73:db	-40 ...	...	...	...	QoS Data	QoS Data, SN=1, FN=0, Flags=.p
15	51.126000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Broadcast	-56 ...	...	9	...	QoS Data	QoS Data, SN=1, FN=0, Flags=.p
16	92.162000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Cisco_70:18:d0	-50 ...	...	6	...	Disassociate	Disassociate, SN=966, FN=0, F



practice1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter... <Ctrl-/>

No.	Time	PHY type	CH	Freq.	Source	Destination	Signal	MCS	Rate	Retry	Type/Subtype	Info
1	0.000000	802.11a (OFDM)	36	5180MHz	Cisco_70:18:d0	Broadcast	-44 ...	...	6	...	Beacon frame	Beacon frame, SN=3039, FN=0, F
2	37.245000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Broadcast	-50 ...	...	6	...	Probe Request	Probe Request, SN=379, FN=0, F
3	37.247000	802.11a (OFDM)	36	5180MHz	Cisco_70:18:d0	Sony_50:73:db	-44 ...	...	6	✓	Probe Response	Probe Response, SN=1748, FN=0, F
4	50.744000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Cisco_70:18:d0	-64 ...	...	6	...	Authentication	Authentication, SN=482, FN=0, F
5	50.744000	802.11a (OFDM)	36	5180MHz	Cisco_70:18:d0	Sony_50:73:db	-44 ...	...	6	...	Authentication	Authentication, SN=3802, FN=0, F
6	50.744000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Cisco_70:18:d0	-64 ...	...	6	...	Association Request	Association Request, SN=483, F
7	50.746000	802.11a (OFDM)	36	5180MHz	Cisco_70:18:d0	Sony_50:73:db	-44 ...	...	6	...	Association Response	Association Response, SN=3803, F
8	50.746000	802.11a (OFDM)	36	5180MHz	Cisco_70:18:d0	Sony_50:73:db	-44 ...	...	6	...	QoS Data	Key (Message 1 of 4)
9	50.789000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Cisco_70:18:d0	-52 ...	...	6	...	QoS Data	Key (Message 2 of 4)
10	50.798000	802.11a (OFDM)	36	5180MHz	Cisco_70:18:d0	Sony_50:73:db	-44 ...	...	6	...	QoS Data	Key (Message 3 of 4)
11	50.798000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Cisco_70:18:d0	-52 ...	...	6	...	QoS Data	Key (Message 4 of 4)
12	50.799000	802.11ac (VHT)	36	5180MHz	192.168.100.3	224.0.0.1	-42 ...	...	...	...	QoS Data	Membership Query, general
13	50.990000	802.11a (OFDM)	36	5180MHz	0.0.0.0	255.255.255.255	-64 ...	...	9	...	QoS Data	DHCP Request - Transaction ID
14	50.990000	802.11ac (VHT)	36	5180MHz	192.168.100.121	192.168.100.121	-40 ...	...	...	...	QoS Data	DHCP ACK - Transaction ID
15	51.126000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Broadcast	-56 ...	...	9	...	QoS Data	ARP Announcement for 192.168.10
16	92.162000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Cisco_70:18:d0	-50 ...	...	6	...	Disassociate	Disassociate, SN=966, FN=0, F

```
> Frame 12: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on in
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .p....F.
> Data (62 bytes)
```

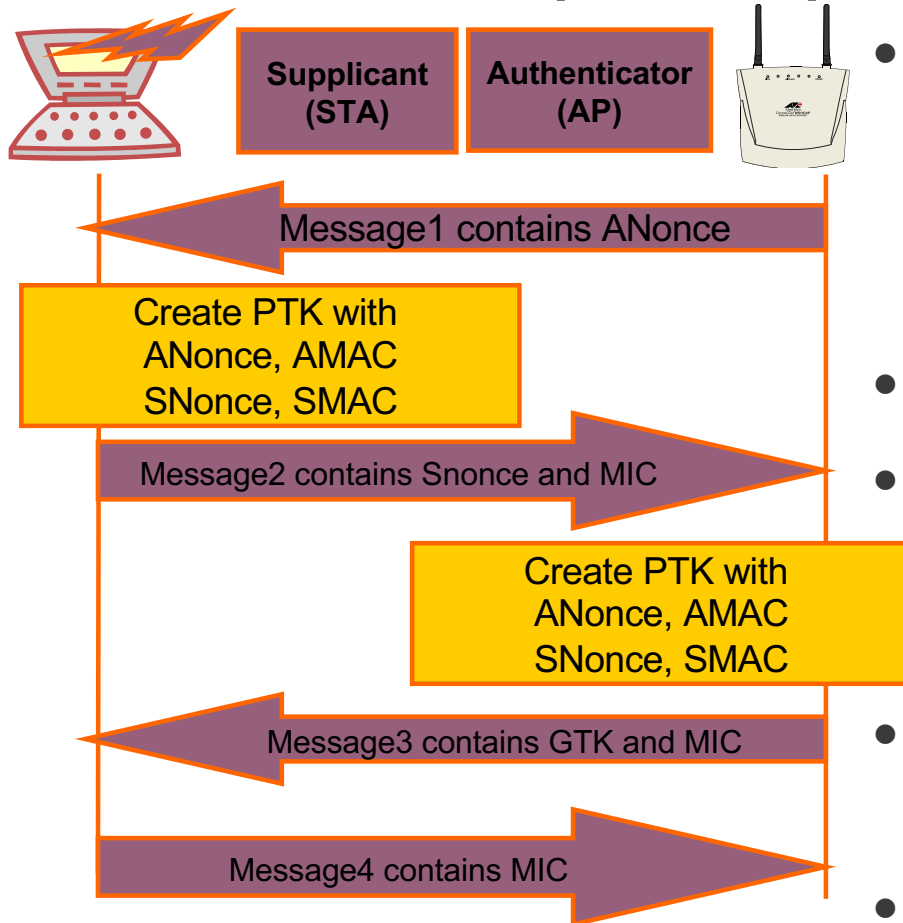
```
> Frame 12: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on in
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .p....F.
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.100.3, Dst: 224.0.0.1
> Internet Group Management Protocol
```

Sample traces and configurations
https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu.zip

Check the 4 way handshake



• Set filter eapol in practice1.pcapng



- We need AP's Nonce, AP's MAC address, STA's Nonce and STA's MAC address to create PTK (Pairwise Transient Key)
- Message1 contains ANonce
- Message2 contains Snonce and MIC (Message Integrity Code), Hash value using PTK
- Message3 contains GTK (Group Transient Key) and MIC
- Message4 contains MIC

Decrypting Practice1.pcapng

- Message1 contains Anonce
- Message2 contains Snonce and MIC (Message Integrity Code), Hash value using PTK

```
▼ 802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: Key (3)
  Length: 117
  Key Descriptor Type: EAPOL RSN Key (2)
  [Message number: 1]
  > Key Information: 0x008a
    Key Length: 16
    Replay Counter: 1
    WPA Key Nonce: 15adf473164f43a34f211ebc34495b588af5b915c0dd4478f5fbc89d2f7e
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Data Length: 22
  > WPA Key Data: dd14000fac04b9c9f71f0c96f62b6c11f545d2dff41b
```

```
▼ 802.1X Authentication
  Version: 802.1X-2001 (1)
  Type: Key (3)
  Length: 117
  Key Descriptor Type: EAPOL RSN Key (2)
  [Message number: 2]
  > Key Information: 0x010a
    Key Length: 0
    Replay Counter: 1
    WPA Key Nonce: 1b9717293f9d9d6979d94b36dbc9d83418bbce09f72edc1eae4fd79821f
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 2f8e7921e572afd75a7c898e625ffb43
    WPA Key Data Length: 22
  > WPA Key Data: 3014010000fac040100000fac040100000fac023c00
```

- Message3 contains GTK (Group Transient Key) and MIC
- Message4 contains MIC

```
▼ 802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: Key (3)
  Length: 151
  Key Descriptor Type: EAPOL RSN Key (2)
  [Message number: 3]
  > Key Information: 0x13ca
    Key Length: 16
    Replay Counter: 2
    WPA Key Nonce: 15adf473164f43a34f211ebc34495b588af5b915c0dd4478f5fbc89d2f7e
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: e481fe9d4a2e0a53dd1119fb36104330
    WPA Key Data Length: 56
  > WPA Key Data: b43c7737faedbf17306b5ea1d5059fd5379d0145fa6ddac1e08d460de93cc
    > Tag: RSN Information
      > Tag: Vendor Specific: Ieee 802.11: RSN GTK
        Tag Number: Vendor Specific (221)
        Tag length: 22
        OUI: 00:0f:ac (Ieee 802.11)
        Vendor Specific OUI Type: 1
        Data Type: GTK KDE (1)
        .... ..01 = Key ID: 0x1
        .... ..0.. = Tx: Temporal key used only for reception
        0000 0... = Reserved: 0x00
        Reserved: 0x00
        GTK: eab4e5b93588db11d1ecfda6eac5606b
    WPA Key Data Padding: dd00
    [CKC: d9eb99b06ea78764cf358998050f017f]
    [KEK: 22fffbcadfbdbd96816884599c16d65dd]
```

```
▼ 802.1X Authentication
  Version: 802.1X-2001 (1)
  Type: Key (3)
  Length: 95
  Key Descriptor Type: EAPOL RSN Key (2)
  [Message number: 4]
  > Key Information: 0x030a
    Key Length: 0
    Replay Counter: 2
    WPA Key Nonce: 00000000000000000000000000000000
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 14ac2c3067058ee2c6fc3f5a7d5a5839
    WPA Key Data Length: 0
```

Sample traces and configurations
https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24-00-2-1-p



- Once, clean up all decryption keys, close Wireshark and try practice2.pcapng
- There are no EAPOL Message 2 and 3 of 4 in a 4way handshake (it means there are no PTK, GTK)
- We cannot decrypt data frames, even if you input the correct wpa-pwd (Passphrase:SSID)
- We need complete sets of 4way handshake if you wants to decrypt by wpa-pwd
- But how about if you know the TK (Temporal Key)? Try with 99775e9a0854ac7899e11147547dd8f7, Wow!! It works because we know the session key.



If you drop to capture the Message 2 and 3 of 4 in 4-way handshake, we cannot decrypt unicast frames as well as broadcast and multicast frames because Wireshark cannot get PTK and GTK (GTK is sent encrypted between the AP and the STA used by its PTK)

No.	Time	PHY type	CH	Freq.	Source	Destination	Signal	MCS	Rate	Retry	Type/Subtype	Info	BSSID	STA
1	0.000000	802.11a (OFDM)	36	5180MHz	Cisco_70:18:d0	Broadcast	-44 dBm			6	Beacon frame	Beacon frame, SN=...	Cisco_70:18:d0	
2	37.245000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Broadcast	-50 dBm			6	Probe Request	Probe Request, SN=...	Broadcast	
3	37.247000	802.11a (OFDM)	36	5180MHz	Cisco_70:18:d0	Sony_50:73:db	-44 dBm			6	Probe Response	Probe Response, SN=17...	Cisco_70:18:d0	
4	50.744000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Cisco_70:18:d0	-64 dBm			6	Authentication	Authentication, SN=482...	Cisco_70:18:d0	
5	50.744000	802.11a (OFDM)	36	5180MHz	Cisco_70:18:d0	Sony_50:73:db	-44 dBm			6	Authentication	Authentication, SN=380...	Cisco_70:18:d0	
6	50.744000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Cisco_70:18:d0	-64 dBm			6	Association Request	Association Request, S...	Cisco_70:18:d0	
7	50.746000	802.11a (OFDM)	36	5180MHz	Cisco_70:18:d0	Sony_50:73:db	-44 dBm			6	Association Response	Association Response, ...	Cisco_70:18:d0	
8	50.746000	802.11a (OFDM)	36	5180MHz	Cisco_70:18:d0	Sony_50:73:db	-44 dBm			6	QoS Data	Key (Message 1 of 4)	Cisco_70:18:d0	Sony_50:73:db
9	50.798000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Cisco_70:18:d0	-52 dBm			6	QoS Data	Key (Message 4 of 4)	Cisco_70:18:d0	Sony_50:73:db
10	50.799000	802.11ac (VHT)	36	5180MHz	Cisco_9c:6a:e4	Sony_50:73:db	-42 dBm				QoS Data	QoS Data, SN=0, FN=0, ...	Cisco_70:18:d0	Sony_50:73:db
11	50.990000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Broadcast	-64 dBm			9	QoS Data	QoS Data, SN=0, FN=0, ...	Cisco_70:18:d0	Sony_50:73:db
12	50.990000	802.11ac (VHT)	36	5180MHz	Modacom_94:ea:...	Sony_50:73:db	-40 dBm				QoS Data	QoS Data, SN=1, FN=0, ...	Cisco_70:18:d0	Sony_50:73:db
13	51.126000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Broadcast	-56 dBm			9	QoS Data	QoS Data, SN=1, FN=0, ...	Cisco_70:18:d0	Sony_50:73:db
14	92.162000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Cisco_70:18:d0	-50 dBm			6	Disassociate	Disassociate, SN=966, ...	Cisco_70:18:d0	

But you can decrypt the datalink,
If you know the TK (Temporal Key), session key,
even if you cannot capture 4-way handshake

Broadcast and Multicast QoS Data frames
cannot be decrypted

6	50.744000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Cisco_70:18:d0	-64 ...			6	Association Request	Association Request, SN=483, FN=0, ...	Cisco_70:18:d0	
7	50.746000	802.11a (OFDM)	36	5180MHz	Cisco_70:18:d0	Sony_50:73:db	-44 ...			6	Association Response	Association Response, SN=3803, FN=0, ...	Cisco_70:18:d0	
8	50.746000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Cisco_70:18:d0	-44 ...			6	QoS Data	Key (Message 1 of 4)	Cisco_70:18:d0	Sony_50:73:db
9	50.789000	802.11a (OFDM)	36	5180MHz	Cisco_70:18:d0	Sony_50:73:db	-52 ...			6	QoS Data	Key (Message 2 of 4)	Cisco_70:18:d0	Sony_50:73:db
10	50.798000	802.11a (OFDM)	36	5180MHz	Cisco_70:18:d0	Sony_50:73:db	-44 ...			6	QoS Data	Key (Message 3 of 4)	Cisco_70:18:d0	Sony_50:73:db
11	50.798000	802.11a (OFDM)	36	5180MHz	Cisco_70:18:d0	Sony_50:73:db	-52 ...			6	QoS Data	Key (Message 4 of 4)	Cisco_70:18:d0	Sony_50:73:db
12	50.799000	802.11ac (VHT)	36	5180MHz	192.168.100.121	224.0.0.1	-42 ...				QoS Data	Membership Query, general	Cisco_70:18:d0	
13	50.990000	802.11a (OFDM)	36	5180MHz	0.0.0.0	255.255.255.255	-64 ...			9	QoS Data	DHCP Request, Transaction ID=...	Cisco_70:18:d0	
14	50.990000	802.11ac (VHT)	36	5180MHz	192.168.100.254	192.168.100.121	-40 ...				QoS Data	DHCP ACK, Transaction ID=...	Cisco_70:18:d0	
15	51.126000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Broadcast	-56 ...				QoS Data	ARP Announcement, eth 192.168.100.121	Cisco_70:18:d0	
16	92.162000	802.11a (OFDM)	36	5180MHz	Sony_50:73:db	Cisco_70:18:d0	-50 ...			6	Disassociate	Disassociate, SN=966, FN=0, ...	Cisco_70:18:d0	

Sample traces and configurations
https://www.ikeriri.com/sharkfest/wifi7_sf24eu.zip



Generation	Name	band	Throughput (Logical)	bandwidth	Maximum Modulation
4 (IEEE802.11n)	HT	2.4/5GHz	1.2Gbps	40MHz	64QAM
5 (IEEE802.11ac)	VHT	5GHz	3.5Gbps	160MHz	256QAM
6 (IEEE802.11ax)	HE	2.4/5GHz	9.6Gbps	160MHz	1024QAM
6E(IEEE802.11ax)	HE	6GHz	9.6Gbps	160MHz	1024QAM
7 (IEEE802.11be)	EHT	2.4/5/6GHz	46Gbps	320MHz	4096QAM

WiFi7 supports
4096QAM
320MHz
46Gbps

- HT High Throughput
- VHT Very High Throughput
- HE High Efficiency
- EHT Extremely High Throughput



- Open plaintext.pcapng and check headers in each frames

No.	Time	PHY type	CH	Freq.	Source	Destination	Signal	MCS	Rate	Retry	Type/Subtype	Info
1	0.000000	802.11b (HR/DSSS)	1	2412MHz	MicroResearc_26...	Broadcast	-32 ...		1		Beacon frame	Beacon frame, SN=734, FN=0, FL...
2	22.356084	802.11b (HR/DSSS)	1	2412MHz	Buffalo_2b:4e:cf	Broadcast	-60 ...		1		Probe Request	Probe Request, SN=1712, FN=0, FL...
3	32.775505	802.11b (HR/DSSS)	1	2412MHz	MicroResearc_26...	Buffalo_2b:4e:cf	-31 ...		1		Probe Response	Probe Response, SN=1212, FN=0, FL...
4	32.776255	802.11b (HR/DSSS)	1	2412MHz	Buffalo_2b:4e:cf	MicroResearc_26...	-60 ...		1		Authentication	Authentication, SN=1716, FN=0, FL...
5	32.777129	802.11b (HR/DSSS)	1	2412MHz	MicroResearc_26...	Buffalo_2b:4e:cf	-32 ...		1		Authentication	Authentication, SN=1213, FN=0, FL...
6	32.781005	802.11b (HR/DSSS)	1	2412MHz	Buffalo_2b:4e:cf	MicroResearc_26...	-60 ...		1		Association Request	Association Request, SN=1717, FN=0, FL...
7	32.782505	802.11b (HR/DSSS)	1	2412MHz	MicroResearc_26...	Buffalo_2b:4e:cf	-38 ...		1		Association Response	Association Response, SN=1214, FN=0, FL...
8	32.886893	802.11b (HR/DSSS)	1	2412MHz	0.0.0.0	255.255.255.255	-60 ...		1		QoS Data	DHCP Discover - Transaction ID 0x00000000
9	98.191343	802.11b (HR/DSSS)	1	2412MHz	192.168.100.24	192.168.100.254	-58 ...		11		QoS Data	Echo (ping) request id=0x0001
10	98.192819	802.11b (HR/DSSS)	1	2412MHz	192.168.100.254	192.168.100.24	-32 ...		11		QoS Data	Echo (ping) reply id=0x0001

> Frame 1: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on

> Radiotap Header v0, Length 20

> 802.11 radio information

> IEEE 802.11 Beacon frame, Flags:C

▼ IEEE 802.11 Wireless Management

> Fixed parameters (12 bytes)

> Tagged parameters (88 bytes)

> Frame 4: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interf

> Radiotap Header v0, Length 20

> 802.11 radio information

> IEEE 802.11 Authentication, Flags:C

▼ IEEE 802.11 Wireless Management

> Fixed parameters (6 bytes)

> Frame 10: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on inte

> Radiotap Header v0, Length 20

> 802.11 radio information

> IEEE 802.11 QoS Data, Flags:F.C

> Logical-Link Control

> Internet Protocol Version 4, Src: 192.168.100.254, Dst: 192.168.100.24

> Internet Control Message Protocol



- Open plaintext.pcapng and check headers

Frame Number	Physical Header	Physical Information	Datalink(MAC) Header	Datalink(LLC) Header	Wireless Management Header
1	Radiotap	802.11 radio information	IEEE802.11 Beacon		802.11 Wireless Management
2	Radiotap	802.11 radio information	IEEE802.11 Probe Request		802.11 Wireless Management
3	Radiotap	802.11 radio information	IEEE802.11 Probe Response		802.11 Wireless Management
4	Radiotap	802.11 radio information	IEEE802.11 Authentication		802.11 Wireless Management
5	Radiotap	802.11 radio information	IEEE802.11 Authentication		802.11 Wireless Management
6	Radiotap	802.11 radio information	IEEE802.11 Association Request		802.11 Wireless Management
7	Radiotap	802.11 radio information	IEEE802.11 Association Response		802.11 Wireless Management
8	Radiotap	802.11 radio information	IEEE802.11 QoS Data	Logical Link Control	
9	Radiotap	802.11 radio information	IEEE802.11 QoS Data	Logical Link Control	
10	Radiotap	802.11 radio information	IEEE802.11 QoS Data	Logical Link Control	

- Data(QoS Data) frames have no 802.11 Management Header
- Data frames have Logical Link Control Header



- Radiotap header contains Physical layer information, it includes fixed fields, such as Data Rate, Channel frequency, Antenna signal and Antenna noise.

```
▼ Radiotap Header v0, Length 20
  Header revision: 0
  Header pad: 0
  Header length: 20
  > Present flags
  > Flags: 0x10
    Data Rate: 1.0 Mb/s
    Channel frequency: 2412 [2.4 GHz 1]
  > Channel flags: 0x00a0, Complementary Code Keying (CCK), 2 GHz spectrum
    Antenna signal: -60 dBm
    Antenna noise: -100 dBm
    Signal Quality: 94
    Antenna: 0
    dB antenna signal: 40 dB
```

- Please refer `phytypes.pcapng` too
- Capture driver creates Radiotap header from IEEE802.16 PLCP, Physical Layer Convergence Procedure, so there are many variations of format, some frame contains MCS, A-MPDU, A-MSDU and HT/VHT/HE/EHT information

Sample traces and configurations:
https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu.zip



- IEEE802.11 radio information header summarize radiotap header information and tells us common style information of WiFi

▼ 802.11 radio information PHY type: 802.11b (HR/DSSS) (4) Short preamble: False Data rate: 1.0 Mb/s Channel: 1 Frequency: 2412MHz Signal strength (dB): 68 dB Signal strength (dBm): -32 dBm Noise level (dBm): -100 dBm Signal/noise ratio (dB): 68 dB > [Duration: 1216µs]	▼ 802.11 radio information PHY type: 802.11a (OFDM) (5) Turbo type: Non-turbo (0) Data rate: 6.0 Mb/s Channel: 40 Frequency: 5200MHz Signal strength (dBm): -43 dBm Noise level (dBm): -94 dBm Signal/noise ratio (dB): 51 dB TSF timestamp: 1633316290347106 > [Duration: 796µs]	▼ 802.11 radio information PHY type: 802.11ac (VHT) (8) Short GI: True Bandwidth: 80 MHz (4) TXOP_PS_NOT_ALLOWED: False > User 0: MCS 9 Data rate: 433.3 Mb/s Channel: 48 Frequency: 5240MHz Signal strength (dBm): -41 dBm Noise level (dBm): -90 dBm Signal/noise ratio (dB): 49 dB TSF timestamp: 1633316333783541 > [Duration: 38µs]
▼ 802.11 radio information PHY type: 802.11g (ERP) (6) Proprietary mode: None (0) Data rate: 6.0 Mb/s Channel: 13 Frequency: 2472MHz Signal strength (dBm): -33 dBm Noise level (dBm): -91 dBm Signal/noise ratio (dB): 58 dB TSF timestamp: 1633316329757266 > [Duration: 56µs]	▼ 802.11 radio information PHY type: 802.11n (HT) (7) MCS index: 15 Bandwidth: 40 MHz (1) Short GI: True Data rate: 300.0 Mb/s Channel: 40 Frequency: 5200MHz Signal strength (dBm): -42 dBm Noise level (dBm): -90 dBm Signal/noise ratio (dB): 48 dB TSF timestamp: 1633316290380650 > [Duration: 44µs]	▼ 802.11 radio information PHY type: 802.11ax (HE) (11) Data rate: 286.8 Mb/s Channel: 36 Frequency: 5180MHz Signal strength (dBm): -47 dBm TSF timestamp: 1490625270 = Last part of an A-MPDU: False = A-MPDU delimiter CRC error: False A-MPDU aggregate ID: 234



- Go back to plaintext.pcapng
- Wireless Management Header contains Wireless Management Information such as SSID and Wireless specifications
- We can identify Wireless standards from Wireless Management
- Note1: Authentication (Open System / SAE) contains Wireless Management header but there are no WiFi spec information.
- Note2: Data frame have no Wireless Management header

```
> Frame 4: 54 bytes on wire (432 bits), 54 bytes
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Authentication, Flags: .....
✓ IEEE 802.11 Wireless Management
  ✓ Fixed parameters (6 bytes)
    Authentication Algorithm: Open System (0)
    Authentication SEQ: 0x0001
    Status code: Successful (0x0000)
```

```
> Frame 12: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .p....F.
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.100.3, Dst: 224.0.0.1
> Internet Group Management Protocol
```

Find WiFi Standards from Beacon



The highest WiFi Standards	Wireless Management Header
IEEE802.11n (WiFi4, HT)	HT Capabilities HT Operations
IEEE802.11ac (WiFi5, VHT)	VHT Capabilities VHT Operations
IEEE802.11ax (WiFi6, HE)	HE Capabilities HE Operations
IEEE802.11be (WiFi7, EHT)	EHT Capabilities EHT Operations

```

> Frame 5: 509 bytes on wire (4072 bits), 509 bytes captured
> 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 (441 bytes)
    > Tag: SSID parameter set: "ikeriri7"
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48,
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    > Tag: Country Information: Country Code JP, Environment
    > Tag: Power Constraint: 0
    > Tag: TPC Report Transmit Power: 22 dBm
    > Tag: Tx Power Envelope
    > Tag: Tx Power Envelope
    > Tag: RM Enabled Capabilities (5 octets)
    > Tag: AP Channel Report: Operating Class 131, Channel Li
    > Tag: RSN Information
    > Tag: QBSS Load Element 802.11e CCA Version
    > Tag: Interworking
    > Tag: Advertisement Protocol
    > Tag: Extended Capabilities (11 octets)
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Paramet
    > Ext Tag: HE Capabilities
    > Ext Tag: HE Operation
    > Ext Tag: Spatial Reuse Parameter Set
    > Ext Tag: MU EDCA Parameter Set
    > Ext Tag: HE 6 GHz Band Capabilities
    > Tag: Vendor Specific: Ralink Technology, Corp.
    > Tag: Vendor Specific: MediaTek Inc.
    > Tag: Vendor Specific: Wi-Fi Alliance: Multi Band Operat
    > Tag: Vendor Specific: MediaTek Inc.
    > Tag: FILS Indication
    > Tag: RSN eXtension (1 octet)
    > Tag: Vendor Specific: MediaTek Inc.
    > Ext Tag: Multi-Link (802.11be D3.0)
    > Ext Tag: EHT Capabilities (802.11be D3.0)
    > Ext Tag: EHT Operation (802.11be D3.0)
    > Tag: Vendor Specific: MediaTek Inc.
  
```

- Open beacons.pcapng, #1 IEEE802.11n, #2 IEEE802.11b, #3 IEEE802.11ax, #4 IEEE802.11ac, #5 IEEE802.11be
- We can identify Wireless standards from Wireless Management

Highest WiFi standards from beacon packets

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



WiFi4(HT)

```
> Frame 1: 365 bytes on wire (2920 bits), 365 bytes captured (2920 bits) on interface0
> Radiotap Header v0, Length 28
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .....C
  > IEEE 802.11 Wireless Management
    > Fixed parameters (12 bytes)
    > Tagged parameters (297 bytes)
      > Tag: SSID parameter set: "apple"
      > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12(B)
      > Tag: DS Parameter set: Current Channel: 7
      > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
      > Tag: ERP Information
      > Tag: RSN Information
      > Tag: Vendor Specific: Microsoft Corp.: WPA Information
      > Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
      > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Set
      > Tag: Vendor Specific: Epigram, Inc.: HT Capabilities (8 octets)
      > Tag: HT Capabilities (802.11n D1.10)
      > Tag: Vendor Specific: Epigram, Inc.: HT Additional Capabilities
      > Tag: HT Information (802.11n D1.10)
      > Tag: Vendor Specific: Atheros Communications, Inc.: Advanced HT Capabilities
      > Tag: Vendor Specific: Atheros Communications, Inc.: Unk
      > Tag: Vendor Specific: Buffalo.Inc
      > Tag: Vendor Specific: Microsoft Corp.: WPS
```

WiFi5(VHT)

```
> Frame 4: 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits) on interface0
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .....
  > IEEE 802.11 Wireless Management
    > Fixed parameters (12 bytes)
    > Tagged parameters (238 bytes)
      > Tag: SSID parameter set: "ikeriri-5g"
      > Tag: Supported Rates 6(B), 9(B), 12(B), 18(B), 24(B), 36(B), 48(B)
      > Tag: Traffic Indication Map (TIM): DTIM 0 of 2 bitmap
      > Tag: HT Capabilities (802.11n D1.10)
      > Tag: RSN Information
      > Tag: HT Information (802.11n D1.10)
      > Tag: Extended Capabilities (8 octets)
      > Tag: Cisco CCX1 CKIP + Device Name
      > Tag: VHT Capabilities
      > Tag: VHT Operation
      > Tag: Tx Power Envelope
      > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Set
      > Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unkn
      > Tag: Vendor Specific: Cisco Systems, Inc.: Aironet CCX
      > Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unkn
      > Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Client
      > Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unkn
```

WiFi6(HE)

```
> Frame 3: 461 bytes on wire (3688 bits), 461 bytes captured (3688 bits) on interface0
> 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(B)
      > Tag: DS Parameter set: Current Channel: 64
      > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
      > Tag: Country Information: Country Code JP, Environment
      > Tag: Power Constraint: 3
      > Tag: TPC Report Transmit Power: 20 dBm
      > 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: Tx Power Envelope
      > Ext Tag: HE Capabilities
      > Ext Tag: HE Operation
      > Ext Tag: Spatial Reuse Parameter Set
      > Ext Tag: MU EDCA Parameter Set
      > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Set
      > Tag: Vendor Specific: Atheros Communications, Inc.: Advanced HT Capabilities
      > Tag: Vendor Specific: Qualcomm Inc.
      > Tag: Vendor Specific: Qualcomm Inc.
      > Tag: Vendor Specific: Qualcomm Inc.
      > Tag: Vendor Specific: Microsoft Corp.: WPS
```

WiFi7(EHT)

```
> Frame 5: 509 bytes on wire (4072 bits), 509 bytes captured (4072 bits) on interface0
> 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 (441 bytes)
      > Tag: SSID parameter set: "ikeriri7"
      > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48(B)
      > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
      > Tag: Country Information: Country Code JP, Environment
      > Tag: Power Constraint: 0
      > Tag: TPC Report Transmit Power: 22 dBm
      > Tag: Tx Power Envelope
      > Tag: Tx Power Envelope
      > Tag: RM Enabled Capabilities (5 octets)
      > Tag: AP Channel Report: Operating Class 131, Channel 131
      > Tag: RSN Information
      > Tag: QSS Load Element 802.11e CCA Version
      > Tag: Interworking
      > Tag: Advertisement Protocol
      > Tag: Extended Capabilities (11 octets)
      > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Set
      > Ext Tag: HE Capabilities
      > Ext Tag: HE Operation
      > Ext Tag: Spatial Reuse Parameter Set
      > Ext Tag: MU EDCA Parameter Set
      > Ext Tag: HE 6 GHz Band Capabilities
      > Tag: Vendor Specific: Ralink Technology, Corp.
      > Tag: Vendor Specific: MediaTek Inc.
      > Tag: Vendor Specific: Wi-Fi Alliance: Multi Band Operation
      > Tag: Vendor Specific: MediaTek Inc.
      > Tag: FILS Indication
      > Tag: RSN eXtension (1 octet)
      > Tag: Vendor Specific: MediaTek Inc.
      > Ext Tag: Multi-Link (802.11be D3.0)
      > Ext Tag: EHT Capabilities (802.11be D3.0)
      > Ext Tag: EHT Operation (802.11be D3.0)
      > Tag: Vendor Specific: Buffalo.Inc
```

#1 IEEE802.11n, #2 IEEE802.11b, #3 IEEE802.11ax, #4 IEEE802.11ac, #5 IEEE802.11be

Sample traces and configurations
https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu.zip



- Andy-san (Andrew Walding, famous for Wireshark Profiles Repository, founder of CELLSTREAM) submits Wireshark Discord,

Standards	Display Filter
Pre-WiFi 4	wlan.fc.type_subtype == 0x0008 and wlan.tag.number == 1 and not ((wlan.tag.number == 61) (wlan.tag.number == 45) (wlan.tag.number == 191) (wlan.ext_tag.number == 192) (wlan.ext_tag.number == 255) (wlan.ext_tag.number == 108))
WiFi4	wlan.fc.type_subtype == 0x0008 and ((wlan.tag.number == 61) (wlan.tag.number == 45)) and not ((wlan.tag.number == 191) (wlan.tag.number == 192) (wlan.ext_tag.number == 255) (wlan.ext_tag.number == 108))
WiFi5	wlan.fc.type_subtype == 0x0008 and ((wlan.tag.number == 191 (wlan.tag.number == 192)) and not ((wlan.ext_tag.number == 255 wlan.ext_tag.number == 108)))
WiFi6	wlan.fc.type_subtype == 0x0008 and wlan.tag.number == 255 and not wlan.ext_tag.number == 108
WiFi7	wlan.fc.type_subtype == 0x0008 and wlan.ext_tag.number == 108

Display filter string to find WiFi standards from Beacons

Data and Authentication frames

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



phytypes.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	PHY type	CH	Freq.	Source	Destination	Signal	MCS	Rate	Retry	Type/Subtype	Info	SSID	BSSID	STA
1	0.000000	802.11n (HT)	40	5200MHz	ASUSTekCOMPU_c4:f5:c5	LiteonTechno_a2:e0:f2	-42 dBm	15	300		QoS Data	QoS Data,...	ASUSTekCOMPU_c4:f5:c5	LiteonTechno_a2:e0:f2	
2	43.402891	802.11ac (VHT)	48	5240MHz	ASUSTekCOMPU_c4:f5:c5	TpLinkTechno_26:76:df	-41 dBm				QoS Data	QoS Data,...	ASUSTekCOMPU_c4:f5:c5	TpLinkTechno_26:76:df	
3	52533672.001950879	802.11ax (HE)	36	5180MHz	4e:a0:3f:b6:04:ff	Broadcast	-46 dBm				QoS Data	QoS Data,...	ASUSTekCOMPU_09:76:64	4e:a0:3f:b6:04:ff	
4	93496226.358398		85	6375MHz	04:23:f4:0d:16:b1	Intel_27:3d:0f	-56 dBm		112.5		QoS Data	QoS Data,...	a4:e8:cb:45:1d:b8	Intel_27:3d:0f	

> Frame 4: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface unknown, id 2

> Radiotap Header v0, Length 32

> 802.11 radio information

- Data rate: 112.5 Mb/s
- Channel: 85
- Frequency: 6375MHz
- Signal strength (dBm): -56 dBm
- Noise level (dBm): -90 dBm
- Signal/noise ratio (dB): 34 dB
- TSF timestamp: 1726812516739048

> IEEE 802.11 QoS Data, Flags: .p....F.

> Data (62 bytes)

```
0000 00 00 20 00 6f 00 04 00 e8 67 a7 de 86 22 06 00 ..o...g..."
0010 40 e1 e7 18 00 00 c8 a6 00 00 00 00 e7 18 55 00 @.....U
0020 88 42 24 00 c8 15 4e 27 3d 0f a4 e8 cb 45 1d b8 B$...N' =...E
0030 04 23 f4 0d 16 b1 70 46 00 00 86 34 00 20 01 00 #...pF...4...
0040 00 02 92 2e ad 10 74 67 96 e8 1b 8f 3b 6c a5 ce ...tg...;l...
0050 64 5b 66 70 28 1e a4 bc e9 39 8c 8e 0a be ea 34 d[fp(...9...4
0060 42 b8 42 45 07 22 fa 81 08 68 f4 8d 65 e2 3c b2 B-BE"...h...e<
0070 6d ca 8e 25 b6 7a e8 b6 e2 0b e2 56 84 b0 b3 d4 m.%z...V...
```

- Open the trace phytypes.pcapng
- #1 is gen4 IEEE802.11n, #2 is gen5 IEEE802.11ac, #3 is gen6 IEEE802.11ax #4 is gen7 IEEE802.11be (but #4 has no PHY type value because the capture driver did not have information, but it is truly EHT IEEE802.11be packet)
- We can find WiFi generation by PHY type (wlan_radio.phy), but It is difficult to find WiFi standards definitely from Data packets because PHY type information is different by capture (monitor) driver

Sample traces and configurations
https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu.zip

Check Rate and MCS, Aggrigation, Frequency

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



#1 is gen4 IEEE802.11n
Bandwidth 40MHz
Data Rate 300Mbps

```
> Frame 1: 114 bytes on wire (912 bits),
▼ Radiotap Header v0, Length 36
  Header revision: 0
  Header pad: 0
  Header length: 36
  > Present flags
  MAC timestamp: 1633316290380650
  > Flags: 0x00
  Channel frequency: 5200 [5 GHz 40]
  > Channel flags: 0x0140, Orthogonal F
  Antenna signal: -42 dBm
  Antenna noise: -90 dBm
  Channel number: 40
  Channel frequency: 5200
  > Channel flags: 0x00000140, Orthogon
  > MCS information
    [Data Rate: 300.0 Mb/s]
▼ 802.11 radio information
  PHY type: 802.11n (HT) (7)
  MCS index: 15
  Bandwidth: 40 MHz (1)
  Short GI: True
  Data rate: 300.0 Mb/s
  Channel: 40
  Frequency: 5200MHz
  Signal strength (dBm): -42 dBm
  Noise level (dBm): -90 dBm
  Signal/noise ratio (dB): 48 dB
  TSF timestamp: 1633316290380650
  > [Duration: 44µs]
> IEEE 802.11 QoS Data, Flags: .p....F.
> Data (44 bytes)
```

#2 is gen5 IEEE802.11ac
MCS index 9
Data Rate 400Mbps

```
> Frame 2: 178 bytes on wire (1424 bits),
▼ Radiotap Header v0, Length 44
  Header revision: 0
  Header pad: 0
  Header length: 44
  > Present flags
  MAC timestamp: 1633316333783541
  > Flags: 0x00
  Channel frequency: 5240 [5 GHz 48]
  > Channel flags: 0x0140, Orthogonal F
  Antenna signal: -41 dBm
  Antenna noise: -90 dBm
  Channel number: 48
  Channel frequency: 5240
  > Channel flags: 0x00000140, Orthogon
  > VHT information
▼ 802.11 radio information
  PHY type: 802.11ac (VHT) (8)
  Short GI: True
  Bandwidth: 80 MHz (4)
  TXOP_PS_NOT_ALLOWED: False
  > User 0: MCS 9
  Data rate: 433.3 Mb/s
  Channel: 48
  Frequency: 5240MHz
  Signal strength (dBm): -41 dBm
  Noise level (dBm): -90 dBm
  Signal/noise ratio (dB): 49 dB
  TSF timestamp: 1633316333783541
  > [Duration: 38µs]
> IEEE 802.11 QoS Data, Flags: .p....F.
> Data (100 bytes)
```

#3 is gen6 IEEE802.11ax
A-MPDU aggregate ID 234
Data Rate 286.8Mbps

```
> Frame 3: 158 bytes on wire (1264 bits),
▼ Radiotap Header v0, Length 76
  Header revision: 0
  Header pad: 0
  Header length: 76
  > Present flags
  MAC timestamp: 1490625270
  > Flags: 0x00
  Channel frequency: 5180 [5 GHz 36]
  > Channel flags: 0x0140, Orthogonal Fre
  Antenna signal: -46 dBm
  > RX flags: 0x0000
  > A-MPDU status
  > timestamp information
  > HE information
  Antenna signal: -50 dBm
  Antenna: 0
  Antenna signal: -47 dBm
  Antenna: 1
▼ 802.11 radio information
  PHY type: 802.11ax (HE) (11)
  Data rate: 286.8 Mb/s
  Channel: 36
  Frequency: 5180MHz
  Signal strength (dBm): -47 dBm
  TSF timestamp: 1490625270
  ....
  ....
  A-MPDU aggregate ID: 234
  > IEEE 802.11 QoS Data, Flags: op.....T
  > Data (44 bytes)
```

#4 is gen6 IEEE802.11be
Frequency 6375MHz
Data Rate 112.5Mbps

Difficult to find PHY type

```
> Frame 4: 128 bytes on wire (1024 bits),
▼ Radiotap Header v0, Length 32
  Header revision: 0
  Header pad: 0
  Header length: 32
  > Present flags
  MAC timestamp: 1726812516739048
  > Flags: 0x40
  Data Rate: 112.5 Mb/s
  Channel frequency: 6375 [6 GHz 85]
  > Channel flags: 0x0000
  Antenna signal: -56 dBm
  Antenna noise: -90 dBm
  Channel number: 85
  Channel frequency: 6375
  > Channel flags: 0x00000000
▼ 802.11 radio information
  Data rate: 112.5 Mb/s
  Channel: 85
  Frequency: 6375MHz
  Signal strength (dBm): -56 dBm
  Noise level (dBm): -90 dBm
  Signal/noise ratio (dB): 34 dB
  TSF timestamp: 1726812516739048
  > IEEE 802.11 QoS Data, Flags: .p....F.
  > Data (62 bvtes)
```

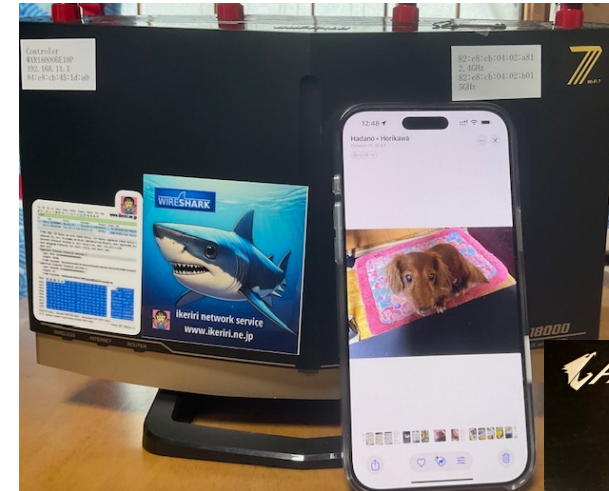
WiFi7 Capture target

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



AP Buffalo WXR1 8000BE1 0P

	CCK、DSSS、OFDM、OFDMA、MIMO、MLO
F R E Q	6GHz : 191~283ch (5955~6415MHz)
	5GHz : W52 36/40/44/48ch (5180~5240MHz)
	W53 52/56/60/64ch (5260~5320MHz)
	W56 100/104/108/112/116/120/124/128/132/136/140/144ch (5500~5720MHz)
	2.4GHz : 1~13ch (2412~2472MHz)
S T A N D A R D S	6GHz : IEEE 802.11be:11529Mbps (320MHz 4x4)
	IEEE 802.11ax:4803Mbps (160MHz 4x4)
	5GHz : IEEE 802.11be:5764Mbps (160MHz 4x4)
	IEEE 802.11ax:4803Mbps (160MHz 4x4)
	IEEE 802.11ac:3466Mbps (160MHz 4x4)
	IEEE 802.11n: 600Mbps (40MHz 4x4)
	IEEE 802.11a: 54Mbps
	2.4GHz : IEEE 802.11be: 688Mbps (40MHz 2x2)
	IEEE 802.11ax: 573Mbps (40MHz 2x2)
	IEEE 802.11n : 300Mbps (40MHz 2x2)
	IEEE 802.11g : 54Mbps
	IEEE 802.11b : 11Mbps



STA iPhone16 Pro Max

STA Windows11 with IntelBE200

STA Windows11 with GC-WIFI7
(Qualcomm QCNM865)

onfigurations
fest/wifi7_sf24eu.zip

Configuration of WXR18000BE10P

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



6 GHz (11be/ax)
☒ 有効

☒ 有効

ikeriri7

WPA3 Personal AES

wireshark

自動

(*):推奨チャンネル

11528Mbps(320MHz)

戻る 設定

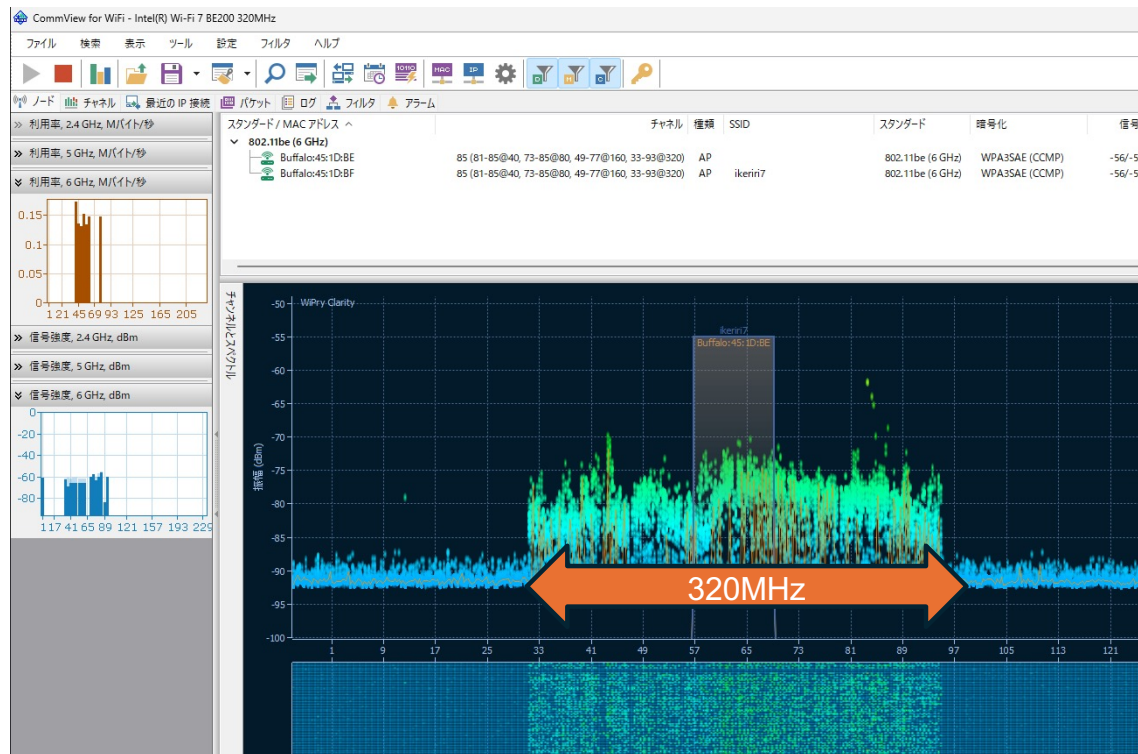
I bring WXR18000BE10P here

- Works only on 6GHz with WiFi6/7
- WPA3 Personal with AES
- SSID ikeriri7
- Passphrase wireshark
- Channel auto
- Bandwidth (max) 320MHz

Sample traces and configurations
https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu.zip



CommView for WiFi with Intel BE200(BE200NGW), WiPry Clarity (Spectrum Analyzer that supports 2.4/5/6GHz) in Windows 11 Pro



We can capture EHT(WiFi7) with 320MHz (Logically) with RF information

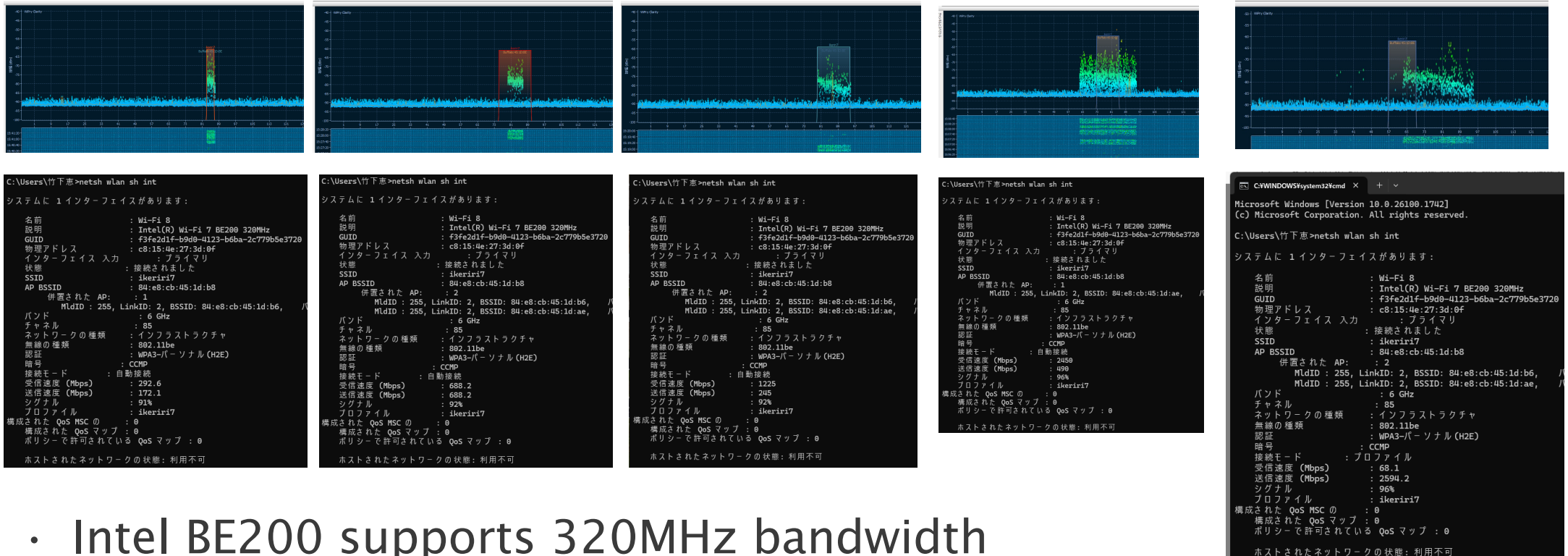
But it is impossible to capture all frames over 10Gbps

WiPry to measure 20/40/80/160/320MHz

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



- 6GHz Spectrum of CommView for WiFi when we test iperf3
- Screenshots of “netsh wlan sh int”



- Intel BE200 supports 320MHz bandwidth

Sample traces and configurations
https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu.zip



- Open the trace file “win11be200-wifi7-320MHz.pcapng”
- Connection between PC with Intel BE200 and WiFi7 AP
85CH 6375MHz SSID ikeriri7 BSSID Buffalo:45:1d:b8
STA: Windows11(Intel:27:3d:0f) AP: Buffalo(Buffer:45:1d:b8)
- Check beacon packet #1 and open 802.11 Wireless Management header > Tagged parameters

win11be200-wifi7-320MHz.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	PHY type	CH	Freq.	Source	Destination	Signal	MCS	Rate	Retry	Type/Subtype	Info	SSID	BSSID	STA
1	0.000000	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:b8	Broadcast	-56 dBm		6		Beacon frame	Beacon frame, SN=176, FN...	"ikeriri7"	Buffalo_45:1d:b8	
2	0.021778	802.11a (OFDM)	85	6375MHz	Intel_27:3d:0f	Broadcast	-62 dBm		6		Probe Request	Probe Request, SN=679, F...		Broadcast	
3	0.022306	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:b8	Broadcast	-56 dBm		6		Probe Response	Probe Response, SN=177, ...	"ikeriri7"	Buffalo_45:1d:b8	
4	0.073011	802.11a (OFDM)	85	6375MHz	Intel_27:3d:0f	Buffalo_45:1d:b8	-75 dBm		6		Authentication	Authentication, SN=10, F...		Buffalo_45:1d:b8	
5	0.074897	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:b8	Intel_27:3d:0f	-56 dBm		6		Authentication	Authentication, SN=3, FN...		Buffalo_45:1d:b8	
6	0.076140	802.11a (OFDM)	85	6375MHz	Intel_27:3d:0f	Buffalo_45:1d:b8	-75 dBm		6		Authentication	Authentication, SN=11, F...		Buffalo_45:1d:b8	
7	0.076701	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:b8	Intel_27:3d:0f	-56 dBm		6		Authentication	Authentication, SN=4, FN...		Buffalo_45:1d:b8	
8	0.078401	802.11a (OFDM)	85	6375MHz	Intel_27:3d:0f	Buffalo_45:1d:b8	-75 dBm		6		Association Request	Association Request, SN=...	"ikeriri7"	Buffalo_45:1d:b8	
9	0.088759	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:b8	Intel_27:3d:0f	-56 dBm		6		Association Response	Association Response, SN...		Buffalo_45:1d:b8	
10	0.116657	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:b8	Intel_27:3d:0f	-56 dBm		6	✓	QoS Data	Key (Message 1 of 4)		Buffalo_45:1d:b8	Intel_27:3d:0f
11	0.124976	802.11a (OFDM)	85	6375MHz	Intel_27:3d:0f	Buffalo_45:1d:b8	-75 dBm		6		QoS Data	Key (Message 2 of 4)		Buffalo_45:1d:b8	Intel_27:3d:0f
12	0.129949	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:b8	Intel_27:3d:0f	-56 dBm		6		QoS Data	Key (Message 3 of 4)		Buffalo_45:1d:b8	Intel_27:3d:0f
13	0.130826	802.11a (OFDM)	85	6375MHz	Intel_27:3d:0f	Buffalo_45:1d:b8	-75 dBm		6		QoS Data	Key (Message 4 of 4)		Buffalo_45:1d:b8	Intel_27:3d:0f
14	0.131610		85	6375MHz	Intel_27:3d:0f	IPv6mcast_ff:05:c9:b0	-67 dBm		30		QoS Data	QoS Data, SN=2, FN=0, FL...		Buffalo_45:1d:b8	Intel_27:3d:0f
15	0.149937	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:a0	Broadcast	-55 dBm		6		Data	Data, SN=2562, FN=0, Fla...		Buffalo_45:1d:b8	Broadcast
16	0.150019	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:a0	Broadcast	-55 dBm		6		Data	Data, SN=2563, FN=0, Fla...		Buffalo_45:1d:b8	Broadcast



- WiFi7's new feature, MLO allows devices to connect multiple bands simultaneously (2.4GHz+5GHz+6GHz), so MLO improves throughput and reduces latency
- For example, Buffalo WXR18000BE10P supports MLO
6GHz(320MHz)11529Mbps
+5GHz(160MHz)5764Mbps
+2.4GHz(40MHz)688Mbps
=17981Mbps(about 18Gbps, Logically)
- Actual throughput is not this value but some test results show us the throughput as 14,423Mbps (14Gbps!!)



MLO test with 2x Buffalo WXR18000BE10P

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



- I tested WiFi7 MLO between two Buffalo WXR18000BE10P by Easy Mesh configuration.



```
C:\Users\竹下恵>iperf3 -c 192.168.11.2
Connecting to host 192.168.11.2, port 5201
[ 4] local 192.168.11.3 port 56811 connected to 192.168.11.2
[ ID] Interval      Transfer    Bandwidth
[ 4] 0.00-1.00 sec  91.5 MBytes 767 Mbits/sec
[ 4] 1.00-2.00 sec  85.0 MBytes 713 Mbits/sec
[ 4] 2.00-3.00 sec  86.2 MBytes 723 Mbits/sec
[ 4] 3.00-4.00 sec  77.1 MBytes 647 Mbits/sec
[ 4] 4.00-5.00 sec  87.9 MBytes 738 Mbits/sec
[ 4] 5.00-6.00 sec  83.8 MBytes 700 Mbits/sec
[ 4] 6.00-7.00 sec  85.8 MBytes 722 Mbits/sec
[ 4] 7.00-8.00 sec  79.8 MBytes 666 Mbits/sec
[ 4] 8.00-9.00 sec  85.8 MBytes 721 Mbits/sec
[ 4] 9.00-10.00 sec 87.4 MBytes 733 Mbits/sec
-----
[ ID] Interval      Transfer    Bandwidth
[ 4] 0.00-10.00 sec 850 MBytes 713 Mbits/sec
[ 4] 0.00-10.00 sec 850 MBytes 713 Mbits/sec
```

Iperf throughput 713Mbps because wired LAN is 1000BASE-TX (between two wired PCs via two wireless WiFi7 AP)
Spectrum Analyzer shows two APs use 2.4,5,6GHz at the same time with 713Mbps throughput

Sample traces and configurations
https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu.zip

Ext Tag:Multi-Link

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



- We can find Ext Tag:Multi-Link, EHT Capabilities and EHT Operation in Wireless Management header
- Open Ext Tag:Multi-Link
- Multi-Link contains MLO (Multi Link Operation) settings
- MLO allows devices to connect multiple bands simultaneously (2.4GHz+5GHz+6GHz)
MLO improves throughput and reduces latency
- It contains MLD (Multi-Link Device) Mac Address for MLO, Link ID for identify each link

- > Ext Tag: Multi-Link (802.11be D3.0)
- > Ext Tag: EHT Capabilities (802.11be D3.0)
- > Ext Tag: EHT Operation (802.11be D3.0)

```
Ext Tag: Multi-Link (802.11be D3.0)
  Ext Tag length: 13 (Tag len: 14)
  Ext Tag Number: Multi-Link (802.11be D3.0) (107)
  Multi-Link Control: 0x0130 Basic
    .... 0000 = Type: Basic (0)
    .... 0... = Reserved: 0x0
    .... 1... = Link ID Info Present: True
    .... 1. .... = BSS Parameters Change Count Present: True
    .... 0... = Medium Synchronization Delay Info Present: False
    .... 0... = EML Capabilities Present: False
    .... 1... = MDL Capabilities Present: True
    .... 0... = AP MLD ID Present: False
    .... 0... = Extended MLD Capabilities and Operations Present: False
    0000 0... = Reserved: 0x00
  Common Info
    Common Info Length: 11
    MLD MAC Address: Buffalo_45:1d:b8 (84:e8:cb:45:1d:b8)
  Link ID subfield: 0x02
    .... 0010 = Link ID: 0x2
    0000 .... = Reserved: 0x0
  BSS Parameters Change Count: 0
  MLD Capabilities: 0x0020
    .... 0000 = Maximum Number of Simultaneous Links: 0
    .... 0... = SRS Support: False
    .... 01. .... = TID-To-Link Mapping Negotiation Support: 1
    .... 0000 0... = Frequency Separation For STR/AP MLD Type Indication: 0
    .... 0... = AAR Support: False
    .... 0... = Link Reconfiguration Operation Support: False
    .... 0... = Aligned TWT Support: False
    .... 0... = Reserved: 0x0
  Basic STA Profile Count: 0
```

Sample traces and
<https://www.ikeriri.ne.jp/sl>

Ext Tag: EHT Capabilities

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



- Open Ext Tag:EHT Capabilities
- It shows the parameters of 11be
- Look for EHT PHY Bits 0-15, EHT PHY Capabilities Information “Support For 320MHz in 6GHz”
- Also check for Supported EHT-MCS and NSS(Number of Spatial Stream) open EHT-MCS Map(BW=320MHz) “Tx Max Nss That Supports EHT-MCS 12-13: 4”

```

  Ext Tag: EHT Capabilities (802.11be D3.0)
    Ext Tag length: 20 (Tag len: 21)
    Ext Tag Number: EHT Capabilities (802.11be D3.0) (108)
    > EHT MAC Capabilities Information: 0x0083, EPCS Priority Access Support, EHT OM Cc
    > EHT PHY Capabilities Information
      > EHT PHY Bits 0-15: 0x6dea
        .... 0 = Reserved: 0x0
        .... 1. = Support For 320 MHz in 6 GHz: Supported
        .... 0.. = Support for 242-tone RU in BW Wider than 20 MHz: Not
        .... 1... = NDP With 4x EHT-LTF And 3.2 us GI: Supported
        .... 0 .... = Partial Bandwidth UL MU-MIMO: Not supported
        .... 1. .... = SU Beamformer: Supported
        .... 1.. .... = SU Beamformee: Supported
        .... 01 1... = Beamformee SS (<= 80 MHz): 0x3
        .... 0 11.. = Beamformee SS (= 160 MHz): 0x3
        .... 011. .... = Beamformee SS (= 320 MHz): 0x3
      > EHT PHY Bits 16-31: 0x1edb
      > EHT PHY Bits 32-39: 0x28
      > EHT PHY Bits 40-63: 0x00f860
      > EHT PHY Bits 64-71: 0x444400
    > Supported EHT-MCS and NSS Set
      > EHT-MCS Map (BW <= 80MHz): 0x444444
      > EHT-MCS Map (BW = 160MHz): 0x444444
      > EHT-MCS Map (BW = 320MHz): 0x444444
        .... 0100 = Rx Max Nss That Supports EHT-MCS 0-9: 4
        .... 0100 .... = Tx Max Nss That Supports EHT-MCS 0-9: 4
        .... 0100 .... = Rx Max Nss That Supports EHT-MCS 10-11: 4
        .... 0100 .... = Tx Max Nss That Supports EHT-MCS 10-11: 4
        .... 0100 .... = Rx Max Nss That Supports EHT-MCS 12-13: 4
        .... 0100 .... = Tx Max Nss That Supports EHT-MCS 12-13: 4
      > Ext Tag: EHT Operation (802.11be D3.0)
      > Tag: Vendor Specific: Buffalo.Inc

```

Sample traces and configurations
https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu.zip

MCS index of WiFi7 (<https://mcsindex.net/>)

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu

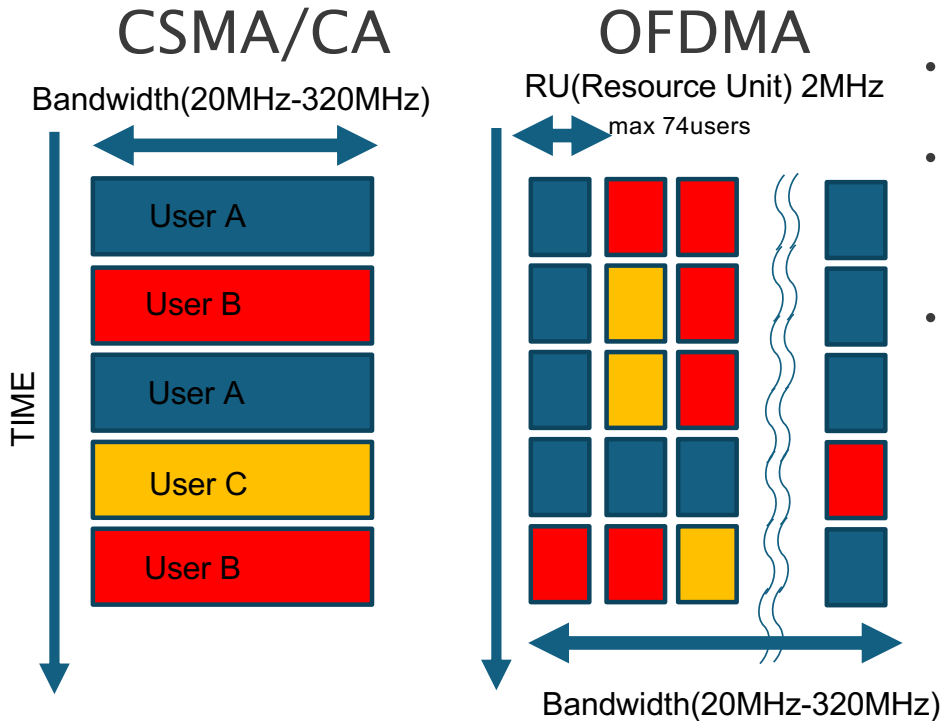


- Check the website <https://mcsindex.net/> to look for IEEE802.11be MCS (Modulation and Coding Scheme)

MCS Table (HT/VHT/HE) - MCS-INDEX													MCS Table HE/EHT													MCS Table sub-1 GHz													The Math behind 8 EHT												
World MCS Index			Full MCS Table (HT/VHT/HE)												MCS Table HE/EHT												Full MCS Table sub-1 GHz												The Math behind 8 EHT												
MCS Index	Modulation	Coding	26-tone RU				52-tone RU				106-tone RU				106-tone RU				106-tone RU				242-tone RU / 2096 Hz				484-tone RU / 4096 Hz				484-tone RU / 4096 Hz																				
			3.2ps CI	1.6ps CI	0.8ps CI	0.4ps CI	3.2ps CI	1.6ps CI	0.8ps CI	0.4ps CI	3.2ps CI	1.6ps CI	0.8ps CI	0.4ps CI	3.2ps CI	1.6ps CI	0.8ps CI	0.4ps CI	3.2ps CI	1.6ps CI	0.8ps CI	0.4ps CI	3.2ps CI	1.6ps CI	0.8ps CI	0.4ps CI	3.2ps CI	1.6ps CI	0.8ps CI	0.4ps CI																					
0	1	BPSK	12	0.4	0.4	0.4	0.8	0.8	0.9	1.1	1.3	1.3	1.6	1.7	1.8	1.9	2.2	2.3	2.6	4.0	4.3	7.3	8.1	8.6	10.8	12.2	12.9	15.1	16.5	17.2	18.5																				
1	1	QPSK	12	1.5	1.7	1.8	3.0	3.3	3.5	4.5	5.0	5.3	6.4	7.1	7.5	7.9	8.8	9.3	14.6	16.3	17.2	29.3	32.5	34.4	43.8	48.8	51.6	61	68	71.4	77.9																				
2	1	QPSK	34	2.3	2.5	2.6	4.5	5.0	5.3	6.8	7.5	7.9	9.6	10.6	11.3	11.8	13.1	13.9	21.9	24.4	25.8	43.9	48.8	51.6	68.8	75.1	77.4	91.9	101	104	114																				
3	1	16-QAM	12	3.0	3.3	3.5	6.0	6.7	7.1	9.0	10.0	10.6	12.8	14.2	15.0	15.8	17.5	18.5	29.3	32.5	34.4	58.8	65.0	68.8	87.8	97.5	103.2	124.5	137.4	143.8	161.3																				
4	1	16-QAM	34	4.5	5.0	5.3	9.0	10.0	10.6	12.8	14.2	15.0	18.0	20.0	21.2	22.5	26.3	27.8	43.9	48.8	51.6	87.8	97.5	103.2	137.4	155.0	160.5	205.3	225.0	230.5	267.8																				
5	1	64-QAM	23	6.0	6.7	7.1	12.0	13.3	14.1	18.0	20.0	21.2	25.0	28.3	30.0	31.5	36.0	37.1	58.5	65.0	68.8	117.0	130.0	137.6	175.5	195.0	205.3	263.3	292.5	307	349																				
6	1	64-QAM	34	6.8	7.5	7.9	13.5	15.0	15.9	20.3	22.5	23.8	31.9	35.4	37.1	38.4	43.8	46.3	71.1	81.3	86.0	146.3	162.5	172.1	219.4	243.8	258.1	329	365.7	377	440																				
7	1	64-QAM	56	7.5	8.3	8.8	15.0	16.7	17.6	22.5	25.0	26.5	31.9	35.4	37.1	38.4	43.8	46.3	71.1	81.3	86.0	146.3	162.5	172.1	219.4	243.8	258.1	329	365.7	377	440																				
8	1	256-QAM	34	9.0	10.0	10.6	18.0	20.0	21.2	27.0	30.0	31.8	38.3	42.5	45.0	47.3	52.5	55.6	87.8	97.5	103.2	175.5	195.0	205.3	263.3	292.5	307	349	370	429	488																				
9	1	256-QAM	56	10.0	11.1	11.8	20.0	22.2	23.5	30.0	33.3	35.3	42.5	46.0	47.3	52.5	55.6	87.8	97.5	103.2	175.5	195.0	205.3	263.3	292.5	307	349	370	429	488	547																				
10	1	1024-QAM	34	11.3	12.5	13.2	22.5	25.0	26.5	33.8	37.5	39.7	47.6	53.1	56.3	59.1	65.6	69.5	107	121	129	194	219.4	243.8	258.1	329	365.7	377	440	500	560																				
11	1	1024-QAM	56	12.5	13.8	14.7	25.0	27.6	29.4	37.5	41.7	44.1	53.1	59.0	62.5	66.6	72.9	77.2	121	135.4	143.4	219.4	243.8	258.1	329	365.7	377	440	500	560	620																				
12	1	4096-QAM	34	13.5	15.0	15.9	27.0	30.0	31.8	40.5	45.0	47.6	57.4	63.8	67.5	70.9	78.8	83.4	131.6	146.3	154.2	243.8	270.6	284.7	354.3	396.7	411.7	499	560	620	680																				
13	1	4096-QAM	56	15.0	16.7	17.6	30.0	33.3	35.3	45.0	50.0	52.9	63.8	70.9	75.0	78.8	87.5	92.6	146.3	162.5	172.1	292.5	325.0	341.1	438.8	487.5	516.2	612	680	740	800																				
14	1	BPSK DCM	12	0.4	0.4	0.4	0.8	0.8	0.9	1.1	1.3	1.3	1.6	1.7	1.8	1.9	2.2	2.3	2.6	4.0	4.3	7.3	8.1	8.6	10.8	12.2	12.9	15.1	16.5	17.2	18.5																				
15	1	BPSK DCM	34	0.8	0.8	0.8	1.6	1.7	1.8	2.3	2.5	2.6	3.2	3.5	3.8	4.1	4.6	4.9	7.9	8.8	9.3	14.6	16.3	17.2	29.3	32.5	34.4	43.8	48.8	51.6	61																				
0	2	BPSK	12	1.5	1.7	1.8	3.0	3.3	3.5	4.5	5.0	5.3	6.4	7.1	7.5	7.9	8.8	9.3	14.6	16.3	17.2	29.3	32.5	34.4	43.8	48.8	51.6	61	68	71.4	77.9																				
1	2	QPSK	12	3.0	3.3	3.5	6.0	6.7	7.1	9.0	10.0	10.6	12.8	14.2	15.0	15.8	17.5	18.5	29.3	32.5	34.4	58.8	65.0	68.8	87.8	97.5	103.2	124.5	137.4	143.8	161.3																				
2	2	QPSK	34	4.5	5.0	5.3	9.0	10.0	10.6	12.8	14.2	15.0	18.0	20.0	21.2	22.5	26.3	27.8	43.9	48.8	51.6	87.8	97.5	103.2	137.4	155.0	160.5	205.3	225.0	230.5	267.8																				
3	2	16-QAM	12	6.0	6.7	7.1	12.0	13.3	14.1	18.0	20.0	21.2	25.0	28.3	30.0	31.5	36.0	37.1	58.5	65.0	68.8	117.0	130.0	137.6	175.5	195.0	205.3	263.3	292.5	307	349																				
4	2	16-QAM	34	9.0	10.0	10.6	18.0	20.0	21.2	27.0	30.0	31.8	38.3	42.5	45.0	47.3	52.5	55.6	87.8	97.5	103.2	175.5	195.0	205.3	263.3	292.5	307	349	370	429	488																				
5	2	64-QAM	23	12.0	13.3	14.1	24.0	26.7	28.2	36.0	40.0	42.4	54.0	60.0	63.5	75.0	80.0	84.7	108.0	120.0	126.0	194.4	216.0	223.2	288.0	324.0	336.0	414.0	460.8	475.2	547.2																				
6	2	64-QAM	34	13.5	15.0	15.9	27.0	30.0	31.8	40.5	45.0	47.6	57.4	63.8	67.5	70.9	78.8	83.4	131.6	146.3	154.2	243.8	270.6	284.7	354.3	396.7	411.7	499	560	620	680																				
7	2	64-QAM	56	15.0	16.7	17.6	30.0	33.3	35.3	45.0	50.0	52.9	63.8	70.9	75.0	78.8	87.5	92.6	146.3	162.5	172.1	292.5	325.0	341.1	438.8	487.5	516.2	612	680	740	800																				
8	2	256-QAM	34	18.0	20.0	21.2	36.0	40.0	42.4	54.0	60.0	63.5	75.0	80.0	84.7	108.0	120.0	126.0	194.4	216.0	223.2	288.0	324.0	336.0	414.0	460.8	475.2	547.2	598.4	612.8	684.8																				
9	2	256-QAM	56	20.0	22.2	23.5	40.0	44.4	47.1	60.0	66.7	70.6	86.0	94.0	100.0	106.7	123.5	130.0	196.7	229.4	240.0	360.0	433.8	458.0	568.0	650.0	682.2	816	896	952	1088																				
10	2	1024-QAM	34	22.5	25.0	26.5	45.0	50.0	52.9	67.5	75.0	79.4	96.0	106.3	112.5	118.1	131.3	139.0	214.4	244.0	258.1	438.8	487.5	516.2	650.0	720.6	737.7	888	976	1032	1184																				
11	2	1024-QAM	56	25.0	27.6	29.4	50.0	55.6	58.8	75.0	83.3	88.2	106.3	116.3	122.5	128.1	141.3	148.8	214.4	244.0	258.1	438.8	487.5	516.2	650.0	720.6	737.7	888	976	1032	1184																				
12	2	4096-QAM	34	27.0	30.0	31.8	54.0	60.0	63.5	81.0	90.0	95.3	114.0	124.5	130.9	136.5	150.0	158.8	263.3	292.5	307	488	556.0	588.0	720.6	806.4	821.7	992	1088	1152	1328																				
13	2	4096-QAM	56	30.0	33.3	35.3	60.0	66.7	70.6	90.0	100.0	105.9	126.0	138.9	145.5	151.1	166.7	175.0	263.3	292.5	307	488	556.0	588.0	720.6	806.4	821.7	992	1088	1152	1328																				
0	3	BPSK	12	2.3	2.5	2.6	4.5	5.0	5.3	6.8	7.5	7.9	9.6	10.6	11.3	11.8	13.1	13.9	24.4	25.8	26.3	43.9	48.8	51.6	68.8	75.1	77.4	91.9	101	104	114																				
1	3	QPSK	12	4.5	5.0	5.3	9.0	10.0	10.6	12.8	14.2	15.0	18.0	20.0	21.2	22.5	26.3	27.8	43.9	48.8	51.6	87.8	97.5	103.2	137.4	155.0	160.5	205.3	225.0	230.5	267.8																				
2	3	QPSK	34	6.8	7.5	7.9	13.5	15.0	15.9	20.3	22.5	23.8	31.9	35.4	37.1	38.4	43.8	46.3	71.1	81.3	86.0	146.3	162.5	172.1	219.4	243.8	258.1	329	365.7	377	440																				
3	3	16-QAM	12	9.0	10.0	10.6	18.0	20.0	21.2	27.0	30.0	31.8	38.3	42.5	45.0	47.3	52.5	55.6	87.8	97.5	103.2	175.5	195.0	205.3	263.3	292.5	307	349	370	429	488																				
4	3	16-QAM	34	13.5	15.0	15.9	27.0	30.0	31.8	40.5	45.0	47.6	57.4	63.8	67.5	70.9	78.8	83.4	131.6	146.3	154.2	243.8	270.6	284.7	354.3	396.7	411.7	499	560	620	680																				
5	3	64-QAM	23	18.0	20.0	21.2	36.0	40.0	42.4	54.0	60.0	63.5	75.0	80.0	84.7	108.0	120.0	126.0	194.4	216.0	223.2	288.0	324.0	336.0	414.0	460.8	475.2	547.2	598.4	612.8	684.8																				
6	3	64-QAM	34	20.3	22.5	23.8	40.5	45.0	47.6	60.0	66.7	70.6	86.0	94.0	100.0	106.7	123.5	130.0	196.7	229.4	240.0	360.0	433.8	458.0	568.0	650.0	682.2	816	896	952	1088																				
7	3	64-QAM	56	22.5	25.0	26.5	45.0	50.0	52.9	67.5	75.0	79.4	96.0	106.3	112.5	118.1	131.3	139.0	214.4	244.0	258.1	438.8	487.5	516.2	650.0	720.6	737.7	888	976	1032	1184																				
8	3	256-QAM	34	27.0	30.0	31.8	54.0	60.0	63.5	81.0	90.0	95.3	114.0	124.5	130.9	136.5	150.0	158.8	263.3	292.5	307	488	556.0	588.0	720.6	806.4	821.7	992	1088	1152	1328																				
9	3	256-QAM	56	30.0	33.3	35.3	60.0	66.7	70.6	90.0	100.0	105.9	126.0	138.9	145.5	151.1	166.7	175.0	263.3	292.5	307	488	556.0	588.0	720.6	806.4	821.7	992	1088	1152	1328																				
10	3	1024-QAM	34	33.8	37.5	39.7	75.0	83.3	88.2	112.5	125.0	132.5	161.3	174.4	180.9	188.2	199.0	208.5	320	366	381	658.1	731.3	743.3	878.7	987.2	1009.9	1184	1312	1376	1568																				
11	3	1024-QAM	56	37.5	41.7</																																														

- Click MCS Table HE/EHT, The table shows the MCS index, Spatial Stream, Modulation, Coding rate, Data Rate divided by Guard Interval and RU (Resource Unit) and bandwidth
- If we use OFDMA, we can divide users by subcarrier, set each user by RUs

Sample traces and configurations
https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu.zip



- The wireless network is Half duplex
- CSMA/CA mechanism sends a user information at a time
- Wi-Fi6/7 supports OFDMA, We can send multiple user's information, divided by RU at a time

Note: all STA should support OFDMA if we get the benefits of OFDMA (and it is difficult)

<https://www.mki.co.jp/knowledge/column131.html>

Sample
<https://www.ike>

No.	Time	C.ID	IP src	IP dst	Protocol	PLCP	RU Size and	MCS	Type/Subtype	Frame direction
166	0.004769	43	192.168.10.65	192.168.10.33	UDP	0x05	106 RU1	256-QAM (5/6)	QoS Data	Received
167	0.004769	28	192.168.10.50	192.168.10.18	UDP	0x05	52 RU3	256-QAM (5/6)	QoS Data	Received
168	0.004769	45	192.168.10.67	192.168.10.117	UDP	0x05	52 RU4	256-QAM (5/6)	QoS Data	Received
169	0.004769	46	192.168.10.68	192.168.10.118	UDP	0x05	52 RU5	256-QAM (5/6)	QoS Data	Received
170	0.004769	31	192.168.10.53	192.168.10.21	UDP	0x05	52 RU6	256-QAM (5/6)	QoS Data	Received
171	0.004769	32	192.168.10.54	192.168.10.22	UDP	0x05	52 RU7	256-QAM (5/6)	QoS Data	Received
172	0.004769	33	192.168.10.55	192.168.10.23	UDP	0x05	52 RU8	256-QAM (5/6)	QoS Data	Received
173	0.004769	34	192.168.10.56	192.168.10.24	UDP	0x05	52 RU9	256-QAM (5/6)	QoS Data	Received
174	0.004769	36	192.168.10.58	192.168.10.26	UDP	0x05	52 RU10	256-QAM (5/6)	QoS Data	Received
175	0.004769	37	192.168.10.59	192.168.10.27	UDP	0x05	52 RU11	256-QAM (5/6)	QoS Data	Received
176	0.004769	22	192.168.10.44	192.168.10.12	UDP	0x05	52 RU12	256-QAM (5/6)	QoS Data	Received
177	0.004769	39	192.168.10.61	192.168.10.29	UDP	0x05	52 RU13	256-QAM (5/6)	QoS Data	Received
178	0.004769	24	192.168.10.46	192.168.10.14	UDP	0x05	52 RU14	256-QAM (5/6)	QoS Data	Received
179	0.004769	25	192.168.10.47	192.168.10.15	UDP	0x05	52 RU15	256-QAM (5/6)	QoS Data	Received
180	0.004769	42	192.168.10.64	192.168.10.32	UDP	0x05	52 RU16	256-QAM (5/6)	QoS Data	Received
181	0.005084	46			802.11	0x06	52 RU5	16-QAM (3/4)	802.11 Block Ack Transmitted	
182	0.005084	45			802.11	0x06	52 RU4	16-QAM (3/4)	802.11 Block Ack Transmitted	
183	0.005084	43			802.11	0x06	106 RU1	16-QAM (3/4)	802.11 Block Ack Transmitted	
184	0.005084	39			802.11	0x06	52 RU13	16-QAM (3/4)	802.11 Block Ack Transmitted	
185	0.005084	36			802.11	0x06	52 RU10	16-QAM (3/4)	802.11 Block Ack Transmitted	
186	0.005084	33			802.11	0x06	52 RU8	16-QAM (3/4)	802.11 Block Ack Transmitted	
187	0.005084	31			802.11	0x06	52 RU6	16-QAM (3/4)	802.11 Block Ack Transmitted	
188	0.005084	25			802.11	0x06	52 RU15	16-QAM (3/4)	802.11 Block Ack Transmitted	

MCS13 in 320MHz



Supported EHT-MCS and NSS Set

> EHT-MCS Map (BW ≤ 80MHz): 0x444444

> EHT-MCS Map (BW = 160MHz): 0x444444

✓ EHT-MCS Map (BW = 320MHz): 0x444444

..... 0100 = Rx Max Nss That Supports EHT-MCS 0-9: 4

..... 0100 = Tx Max Nss That Supports EHT-MCS 0-9: 4

..... 0100 = Rx Max Nss That Supports EHT-MCS 10-11: 4

..... 0100 = Tx Max Nss That Supports EHT-MCS 10-11: 4

..... 0100 = Rx Max Nss That Supports EHT-MCS 12-13: 4

0100 = Tx Max Nss That Supports EHT-MCS 12-13: 4

MCS Index	Spatial Stream	Modulation	Coding
0	1	BPSK	1/2
1	1	QPSK	1/2
2	1	QPSK	3/4
3	1	16-QAM	1/2
4	1	16-QAM	3/4
5	1	64-QAM	2/3
6	1	64-QAM	3/4
7	1	64-QAM	5/6
8	1	256-QAM	3/4
9	1	256-QAM	5/6
10	2	256-QAM	3/4
11	2	256-QAM	5/6
12	4	4096-QAM	3/4
13	4	4096-QAM	5/6

4x996-tone RU / 320 MHz		
3.2μs GI	1.6μs GI	0.8μs GI

1	4	QPSK	1/2
2	4	QPSK	3/4
3	4	16-QAM	1/2
4	4	16-QAM	3/4
5	4	64-QAM	2/3
6	4	64-QAM	3/4
7	4	64-QAM	5/6
8	4	256-QAM	3/4
9	4	256-QAM	5/6
10	4	1024-QAM	3/4
11	4	1024-QAM	5/6
12	4	4096-QAM	3/4
13	4	4096-QAM	5/6

490.0	544.4	576.5
980.0	1088.9	1152.9
1470.0	1633.3	1729.4
1960.0	2177.8	2305.9
2940.0	3266.7	3458.8
3920.0	4355.6	4611.8
4410.0	4900.0	5188.2
4900.0	5444.4	5764.7
5880.0	6533.3	6917.6
6533.3	7259.3	7686.3
7350.0	8166.7	8647.1
8166.7	9074.1	9607.8
8820.0	9800.0	10376.5
9800.0	10888.9	11529.4

Sample traces and configurations
www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu.zip

- Check the rows at MCS13.
- WiFi7 supports 4096-QAM, means 12bit information ($2*2*2*2*2*2*2*2*2*2*2*2$) in one symbol
- Check the rows at MCS13 with 4SS. this AP have four antenna and supports four Spatial Streams
- Check the Columns at 320MHz, 0.8μs GI, the most right side, it says 11529.4Mbps (11.5Gbps) logical PHY performance!!

The Math Behind it (<https://www.mcsindex.net/>)

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



PHY	Modulation		R	N _{SS}	N _{SD}																T _{DFT}	T _{GI}		
	Name	N _{BPSCS}			26-tone	52-tone	52+26-tone	106-tone	106+26-tone	242-tone 20 MHz	484-tone 40 MHz	484+242-tone	996-tone 80 MHz	996+484-tone	996+484+242-tone	2x996-tone 160 MHz	2x996+484-tone	3x996-tone	3x996+484-tone	4x996-tone 320 MHz		Long	Medium	Long
802.11be (EHT)	BPSK	1	1/2	1 to 16	24	48	72	102	126	234	468	702	980	1448	1682	1960	2428	2940	3408	3920	12.8 μs	0.8 μs	1.2 μs	3.2 μs
	QPSK	2	1/2 & 3/4																					
	16-QAM	4	1/2 & 3/4																					
	64-QAM	6	1/2 & 2/3 & 3/4																					
	256-QAM	8	2/3 & 5/6																					
	1024-QAM	10	3/4 & 5/6																					
	4096-QAM	12	3/4 & 5/6																					

The Math Behind it

The new 802.11be standards introduced a few new PHY techniques that will impact data rates:

- New channel widths (320 MHz and MRUs)
- New modulation technique (4K-QAM)
- New set of supported spatial streams (up to 16)
- New transmission techniques (DCM and EHT-DUP)

The following section presents the updated information that is used to calculate 802.11be data rate.

As a reminder, here is the formula used to calculate Wi-Fi data rates with 802.11ax (Wi-Fi 6):

$$\text{Data Rate} = \frac{N_{SD,U} * N_{BPSCS,U} * R * N_{SS}}{T_{DFT} + T_{GI}}$$

Number of Data Subcarriers per Resource Unit (points to $N_{SD,U}$)

Number of Coded Bits per Subcarrier per Stream for the Resource Unit (points to $N_{BPSCS,U}$)

Coding (points to R)

Number of Spatial Streams (points to N_{SS})

OFDM Symbol Duration (points to T_{DFT})

Guard Interval Duration (points to T_{GI})

$$3920 * 12 * 5/6 * 4 / (12.8 + 0.8) = 11529.41176470588$$

Sample traces and configurations
https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu.zip

- Number of subcarriers: 3920
- 1 symbol information: 12bits(4096QAM)
- Coding Rate 3/4 and 5/6
- Number of Spatial Streams 4
- One Symbol time: 12.8μs
- Guard Interval 0.8μs



- Open Ext Tag:EHT Operations
- It shows the modes and methods of IEEE802.11be
- For example, Open the Control, “Channel Width: 320MHz EHT BSS bandwidth”
- There are many spec information in Ext Tag of EHT Capabilities and EHT Operation
Channel bandwidth, Number of Streams
Modulation such as 4096-QAM, Multi-Link Operation
Target Wake Time for low power setting, BSS Coloring
and so on

```
▼ Ext Tag: EHT Operation (802.11be D3.0)
  Ext Tag length: 8 (Tag len: 9)
  Ext Tag Number: EHT Operation (802.11be D3.0) (106)
  ▼ EHT Operation Parameters: 0x01, EHT Operation Information Present
    .... .1 = EHT Operation Information Present: True
    .... ..0. = Disabled Subchannel Bitmap Present: False
    .... .0.. = EHT Default PE Duration: False
    .... 0... = Group Addressed BU Indication Limit: False
    ..00 .... = Group Addressed BU Indication Exponent: 0
    00.. .... = Reserved: 0x0
  Basic EHT-MCS And Nss Set: 0x00000011
  ▼ Control: 0x04, Channel Width: 320 MHz EHT BSS bandwidth
    .... .100 = Channel Width: 320 MHz EHT BSS bandwidth (4)
    0000 0... = Reserved: 0x00
  CCFS0: 0x0000004f
  CCFS1: 0x0000003f
```

#2 Probe Request #3 Probe Response

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



win11be200-wifi7-320MHz.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

Management Control Frames Data Signal Rate Retry EAPOL PWR

No.	Time	PHY type	CH	Freq.	Source	Destination	Signal	MCS	Rate	Retry	Type/Subtype	Info	SSID
1	0.000000	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:b8	Broadcast	-56	...	6	...	Beacon frame	Beacon frame, SN=176,...	"ikeriri7"
2	0.021778	802.11a (OFDM)	85	6375MHz	Intel_27:3d:0f	Broadcast	-62	...	6	...	Probe Request	Probe Request, SN=679,...	80
3	0.022306	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:b8	Broadcast	-56	...	6	...	Probe Response	Probe Response, SN=17,...	"ikeriri7"
4	0.073011	802.11a (OFDM)	85	6375MHz	Intel_27:3d:0f	Buffalo_45:1d:b8	-75	...	6	...	Authentication	Authentication, SN=10,...	
5	0.074897	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:b8	Intel_27:3d:0f	-56	...	6	...	Authentication	Authentication, SN=3,...	
6	0.076140	802.11a (OFDM)	85	6375MHz	Intel_27:3d:0f	Buffalo_45:1d:b8	-75	...	6	...	Authentication	Authentication, SN=11,...	
7	0.076701	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:b8	Intel_27:3d:0f	-56	...	6	...	Authentication	Authentication, SN=4,...	
8	0.078401	802.11a (OFDM)	85	6375MHz	Intel_27:3d:0f	Buffalo_45:1d:b8	-75	...	6	...	Association Re...	Association Request,...	"ikeriri7"
9	0.088759	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:b8	Intel_27:3d:0f	-56	...	6	...	Association Re...	Association Response,...	
10	0.116657	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:b8	Intel_27:3d:0f	-56	...	6	...	QoS Data	Key (Message 1 of 4)	
11	0.124976	802.11a (OFDM)	85	6375MHz	Intel_27:3d:0f	Buffalo_45:1d:b8	-75	...	6	...	QoS Data	Key (Message 2 of 4)	
12	0.129949	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:b8	Intel_27:3d:0f	-56	...	6	...	QoS Data	Key (Message 3 of 4)	
13	0.130826	802.11a (OFDM)	85	6375MHz	Intel_27:3d:0f	Buffalo_45:1d:b8	-75	...	6	...	QoS Data	Key (Message 4 of 4)	
14	0.131610		85	6375MHz	Intel_27:3d:0f	IPv6mcast_ff:05...	-67	...	30	...	QoS Data	QoS Data, SN=2, FN=0,...	
15	0.149937	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:a0	Broadcast	-55	...	6	...	Data	Data, SN=2562, FN=0,...	
16	0.150019	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:a0	Broadcast	-55	...	6	...	Data	Data, SN=2563, FN=0,...	

- Select #2 Probe Request (we use another Probe Request for explanation, sorry)
- Select #3 Probe Response
Buffalo sends IEEE802.11be specification with Ext Tag, EHT Capabilities and EHT Operation

IEEE 802.11 Wireless Management

> Fixed parameters (12 bytes)

> Tagged parameters (385 bytes)

> Tag: SSID parameter set: "ikeriri7"

> Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]

> Tag: RSN Information

> Tag: Extended Capabilities (11 octets)

> Tag: QBSS Load Element 802.11e CCA Version

> Tag: Interworking

> Tag: Advertisement Protocol

> Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

> Tag: RM Enabled Capabilities (5 octets)

> Tag: AP Channel Report: Operating Class 137, Channel List : 31, 63, 95

> Tag: Power Constraint: 0

> Tag: TPC Report Transmit Power: 22 dBm

> Tag: Tx Power Envelope

> Tag: Country Information: Country Code JP, Environment Global operatin

> Ext Tag: HE Capabilities

> Ext Tag: HE Operation

> Ext Tag: Spatial Reuse Parameter Set

> Ext Tag: MU EDCA Parameter Set

> Ext Tag: HE 6 GHz Band Capabilities

> Tag: Vendor Specific: MediaTek Inc.

> Tag: Vendor Specific: Ralink Technology, Corp.

> Tag: Vendor Specific: MediaTek Inc.

> Tag: Vendor Specific: Wi-Fi Alliance: Multi Band Operation - Optimized

> Tag: FILS Indication

> Tag: RSN eXtension (1 octet)

> Tag: Vendor Specific: MediaTek Inc.

> Ext Tag: Multi-Link (802.11be D3.0)

> Ext Tag: EHT Capabilities (802.11be D3.0)

> Ext Tag: EHT Operation (802.11be D3.0)

> Tag: Vendor Specific: Buffalo.Inc

Sample traces and configurations
https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu.zip

#4 #5 #6 #7 Authentication(SAE)

SharkFest'24 EUROPE

Vienna, Austria • #sf24eu



4	0.073011	802.11a (OFDM)	85	6375MHz	Intel_27:3d:0f	Buffalo_45:1d:b8	-75 ...	6	Authentication	Authentication, SN=10...
5	0.074897	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:b8	Intel_27:3d:0f	-56 ...	6	Authentication	Authentication, SN=3,...
6	0.076140	802.11a (OFDM)	85	6375MHz	Intel_27:3d:0f	Buffalo_45:1d:b8	-75 ...	6	Authentication	Authentication, SN=11...
7	0.076701	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:b8	Intel_27:3d:0f	-56 ...	6	Authentication	Authentication, SN=4,...

- The frame #4~#7 are Authentication with SAE (Simultaneous Authentication of Equals), used by WPA3
- In frame #4/#5, STA and AP send Scalar and Finite Field Element values from the point of the Elliptic curve.
- In frame #6/#7, STA and AP send calculated Confirm value
- STA and AP share the value and use it as PMK of 4 way handshake

```

v IEEE 802.11 Wireless Management
  v Fixed parameters (104 bytes)
    Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)
    Authentication SEQ: 0x0001
    Status code: SAE authentication uses direct hashing, instead of looping, to
    SAE Message Type: Commit (1)
    Group Id: 256-bit random ECP group (19)
    Scalar: d5b265595bdc123bb391d4775de30e1514e64656c90554acc32be7443fe8fc62
    Finite Field Element: 042200dfb8bbe161bc0a11d75ebe268cf6eeab0d3629584c812d
  
```

```

v IEEE 802.11 Wireless Management
  v Fixed parameters (40 bytes)
    Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)
    Authentication SEQ: 0x0002
    Status code: Successful (0x0000)
    SAE Message Type: Confirm (2)
    Send-Confirm: 0
    Confirm: a47789bd2da82fc8a0e0ab21412bbc6927463d2bc094df0b333077282686780f
  
```

#8 Association Request from STA (1/4)



- Select #8 Association Request, open EHT Capabilities, open EHT MAC Capabilities Information. There are 16 bits that show the WiFi7 MAC specification
- Windows 11 (Intel BE200) supports EHT OM (Operation Mode) Control that means AP and STA can adjust operation mode dynamically (OM Control is the new feature of WiFi7)
- It means STA can change the channel bandwidth, MCS, number of spatial streams during communication.
- WiFi7 supports OM Control, so it is more difficult to capture

```
▼ IEEE 802.11 Wireless Management
  > Fixed parameters (4 bytes)
  ▼ Tagged parameters (190 bytes)
    > Tag: SSID parameter set: "ikeriri7"
    > Tag: Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
    > Tag: Power Capability Min: 0, Max: 15
    > Tag: RSN Information
    > Tag: Supported Operating Classes
    > Tag: RM Enabled Capabilities (5 octets)
    > Tag: Extended Capabilities (14 octets)
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information Element
    > Tag: Vendor Specific: Intel Wireless Network Group
    > Tag: Vendor Specific: Wi-Fi Alliance: Multi Band Operation - Optimized Connectivity
    > Tag: RSN eXtension (2 octets)
    > Ext Tag: HE Capabilities
    > Ext Tag: HE 6 GHz Band Capabilities
    ▼ Ext Tag: EHT Capabilities (802.11be D3.0)
      Ext Tag length: 20 (Tag len: 21)
      Ext Tag Number: EHT Capabilities (802.11be D3.0) (108)
      ▼ EHT MAC Capabilities Information: 0x0002, EHT OM Control Support, Maximum MPDU Le
        .... 0 = EPCS Priority Access Support: Not supported
        .... 1 = EHT OM Control Support: Supported
        .... 0.. = Triggered TXOP Sharing Mode 1 Support: Not supported
        .... 0... = Triggered TXOP Sharing Mode 2 Support: Not supported
        .... 0.... = Restricted TWT Support: Not supported
        .... 0..... = SCS Traffic Description Support: Not supported
        .... 00... = Maximum MPDU Length: 3 895 (0x0)
        .... 0.... = Maximum A-MPDU Length Exponent Extension: 0
        .... 0..... = EHT TRS Support: Not supported
        .... 0..... = TXOP Return Support In TXOP Sharing Mode 2: Not supported
        .... 0..... = Two BQRs Support: Not supported
        ..00..... = EHT Link Adaptation Support: No feedback (0)
        00..... = Reserved: 0x0
      > EHT PHY Capabilities Information
      > Supported EHT-MCS and NSS Set
```

#8 Association Request from STA (2/4)

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



- Select #8 Association Request, and open EHT Capabilities, open EHT PHY Capabilities Information. There are bits from 0 to 71 that show the WiFi7 specification of STA
- Windows 11 (Intel BE200) supports below, 320MHz in 6GHz
242-tone RU in BW Wider than 20MHz NDP (Null Data Packet) with 4x(Spatial Streams) EHT-LTF (Long Training Field.)
- LTF is used to determine channel BW, number of spatial streams and MCS
- SU(Single User) Beamformee
80/160/320MHz Beamformee SS
Triggered SU Beamforming Feedback
- WiFi7 supports triggered Frame
AP sends the Triggered frame to devices.
And the STA sends feedback about RU, Beamforming(Channel State Information)

```

  Ext Tag: EHT Capabilities (802.11be D3.0)
    Ext Tag length: 20 (Tag len: 21)
    Ext Tag Number: EHT Capabilities (802.11be D3.0) (108)
  > EHT MAC Capabilities Information: 0x0002, EHT OM Control Support, Maximum MPDU Length: 3 895
  > EHT PHY Capabilities Information
    > EHT PHY Bits 0-15: 0xffce
      .... 0 = Reserved: 0x0
      .... 1 = Support For 320 MHz in 6 GHz: Supported
      .... 1.. = Support for 242-tone RU in BW Wider than 20 MHz: Supported
      .... 1... = NDP With 4x EHT-LTF And 3.2 us GI: Supported
      .... 0... = Partial Bandwidth UL MU-MIMO: Not supported
      .... 0. .... = SU Beamformer: Not supported
      .... 1. .... = SU Beamformee: Supported
      .... 11 1... = Beamformee SS (<= 80 MHz): 0x7
      .... 11.. .... = Beamformee SS (= 160 MHz): 0x7
      111. .... .... = Beamformee SS (= 320 MHz): 0x7
    > EHT PHY Bits 16-31: 0x2049
      .... 001 = Number Of Sounding Dimensions (<= 80 MHz): 0x1
      .... 00 1... = Number Of Sounding Dimensions (= 160 MHz): 0x1
      .... 0 01.. .... = Number Of Sounding Dimensions (= 320 MHz): 0x1
      .... 0. .... = Ng = 16 SU Feedback: Not supported
      .... 0.. .... = Ng = 16 MU Feedback: Not supported
      .... 0... .... = Codebook Size = (4,2) SU Feedback: Not supported
      .... 0 .... = Codebook Size = (7,5) MU Feedback: Not supported
      .... 1. .... = Triggered SU Beamforming Feedback: Supported
      .... 0.. .... = Triggered MU Beamforming Partial BW Feedback: Not supported
      0... .... = Triggered CQI Feedback: Not supported

```

#8 Association Request from STA (3/4)

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



- (continues)
EHT MU (Multi-User) PPDU(Physical Protocol Data Unit) with 4x EHT-LTF (4 Spatial Streams EHT-Long Training Frames) and 0.8micro seconds GI
TX/RX 1024-QAM and 4096-QAM less than 242-tone RU
Common Nominal Packet Padding:2
Maximum Number Of Supported EHT-LTFs:
TB(Trigger-Based) sounding Feedback Rate Limit
RX 1024-QAM and 4096-QAM in wider Bandwidth DL(Downlink) OFDMA

```
✓ EHT PHY Bits 32-39: 0x18
.... ..0 = Partial Bandwidth DL MU-MIMO: Not supported
.... ..0. = EHT PSR-Based SR support: Not supported
.... ..0.. = Power Boost Factor Support: Not supported
.... ..1... = EHT MU PPDU With 4x EHT-LTF and 0.8 us GI: Supported
0001 .... = Max Nc: 1
✓ EHT PHY Bits 40-63: 0x800066
.... ..0 = Non-Triggered CQI Feedback: Not supported
.... ..1. = Tx 1024-QAM & 4096-QAM < 242-tone RU Support: Supported
.... ..1.. = Rx 1024-QAM & 4096-QAM < 242-tone-RU Support: Supported
.... ..0... = PPE Thresholds Present: Not Present
.... ..10 .... = Common Nominal Packet Padding: 2
.... ..000 01.. = Maximum Number Of Supported EHT-LTFs: 1
.... ..000 0... = Support Of MCS 15: 0
.... ..0... = Support Of EHT DUP (MCS 14) in 6 GHz: Not supported
.... ..0 .... = Support For 20 MHz Operating STA Receiving NDP With Wid
.... ..0... = Non-OFDMA UL MU-MIMO (BW <= 80 MHz): Not supported
.... ..0.. = Non-OFDMA UL MU-MIMO (BW = 160 MHz): Not supported
.... ..0... = Non-OFDMA UL MU-MIMO (BW = 320 MHz): Not supported
.... ..0... = MU Beamformer (BW <= 80 MHz): Not supported
.... ..0.. = MU Beamformer (BW = 160 MHz): Not supported
.... ..0... = MU Beamformer (BW = 320 MHz): Not supported
1.... .. = TB Sounding Feedback Rate Limit: Supported
✓ EHT PHY Bits 64-71: 0x222203
.... ..1 = Rx 1024-QAM In Wider Bandwidth DL OFDMA Support: Supported
.... ..1. = Rx 4096-QAM In Wider Bandwidth DL OFDMA Support: Supported
0000 00.. = Reserved: 0x00
```

In summary, these bits show
STA's IEEE802.11be MAC
specifications

#8 Association Request from STA (4/4)

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



- Select #8 Association Request, and open EHT Capabilities, open Supported EHT-MCS and NSS Set
- There are bits by bandwidth shows a supported Number of Spatial Streams and MCS number
- Open “EHT-MCS Map (BW=320MHz), STA(Windows 11) supports Receive/Send Max NSS is 2, Supported MCS is 0-13

```
▼ IEEE 802.11 Wireless Management
  ▼ Fixed parameters (4 bytes)
    > Capabilities Information: 0x1130
    Listen Interval: 0x00fa
  ▼ Tagged parameters (190 bytes)
    > Tag: SSID parameter set: "ikeriri7"
    > Tag: Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
    > Tag: Power Capability Min: 0, Max: 15
    > Tag: RSN Information
    > Tag: Supported Operating Classes
    > Tag: RM Enabled Capabilities (5 octets)
    > Tag: Extended Capabilities (14 octets)
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information Element
    > Tag: Vendor Specific: Intel Wireless Network Group
    > Tag: Vendor Specific: Wi-Fi Alliance: Multi Band Operation - Optimized Connectiv:
    > Tag: RSN eXtension (2 octets)
    > Ext Tag: HE Capabilities
    > Ext Tag: HE 6 GHz Band Capabilities
  ▼ Ext Tag: EHT Capabilities (802.11be D3.0)
    Ext Tag length: 20 (Tag len: 21)
    Ext Tag Number: EHT Capabilities (802.11be D3.0) (108)
    > EHT MAC Capabilities Information: 0x0002, EHT OM Control Support, Maximum MPDU
    > EHT PHY Capabilities Information
  ▼ Supported EHT-MCS and NSS Set
    > EHT-MCS Map (BW <= 80MHz): 0x222222
    > EHT-MCS Map (BW = 160MHz): 0x222222
    ▼ EHT-MCS Map (BW = 320MHz): 0x222222
      .... 0010 = Rx Max Nss That Supports EHT-MCS 0-9: 2
      .... 0010 = Tx Max Nss That Supports EHT-MCS 0-9: 2
      .... 0010 = Rx Max Nss That Supports EHT-MCS 10-11: 2
      .... 0010 = Tx Max Nss That Supports EHT-MCS 10-11: 2
      .... 0010 = Rx Max Nss That Supports EHT-MCS 12-13: 2
      0010 = Tx Max Nss That Supports EHT-MCS 12-13: 2
```

#9 Association Response from AP (1/2)

- Select #9 Association Response, and open EHT Capabilities,
- Open EHT MAC Capabilities Information. There are 16 bits that show the WiFi7 MAC specification
- Open EHT PHY Capabilities Information. There are bits from 0 to 72 that show the WiFi7 specification of AP
- STA and AP exchange these information to confirm with each spec of WiFi7

```
Ext Tag: EHT Capabilities (802.11be D3.0)
Ext Tag Length: 20 (Tag Len: 21)
Ext Tag Number: EHT Capabilities (802.11be D3.0) (108)
EHT MAC Capabilities Information: 0x0083, EPCS Priority Access Support, EHT OM Control Support,
.....1 = EPCS Priority Access Support: Supported
.....1 = EHT OM Control Support: Supported
.....0 = Triggered TXOP Sharing Mode 1 Support: Not supported
.....0 = Triggered TXOP Sharing Mode 2 Support: Not supported
.....0 = Restricted TWT Support: Not supported
.....0 = SCS Traffic Description Support: Not supported
.....10 = Maximum MPDU Length: 11 454 (0x2)
.....0 = Maximum A-MPDU Length Exponent Extension: 0
.....0 = EHT TRS Support: Not supported
.....0 = TXOP Return Support In TXOP Sharing Mode 2: Not supported
.....0 = Two BQPs Support: Not supported
.....00 = EHT Link Adaptation Support: No feedback (0)
00.. = Reserved: 0x0
EHT PHY Capabilities Information
EHT PHY Bits 0-15: 0x6dea
.....0 = Reserved: 0x0
.....1 = Support For 320 MHz in 6 GHz: Supported
.....0 = Support for 242-tone RU in BW Wider than 20 MHz: Not supported
.....1 = NDP With 4x EHT-LTF And 3.2 us GI: Supported
.....0 = Partial Bandwidth UL MU-MIMO: Not supported
.....1 = SU Beamformer: Supported
.....1 = SU Beamformee: Supported
.....01 = Beamformee SS (<= 80 MHz): 0x3
.....011 = Beamformee SS (= 160 MHz): 0x3
.....011 = Beamformee SS (= 320 MHz): 0x3
EHT PHY Bits 16-31: 0x1e0b
.....011 = Number Of Sounding Dimensions (<= 80 MHz): 0x3
.....011 = Number Of Sounding Dimensions (= 160 MHz): 0x3
.....011 = Number Of Sounding Dimensions (= 320 MHz): 0x3
.....1 = Ng = 16 SU Feedback: Supported
.....1 = Ng = 16 MU Feedback: Supported
.....1 = Codebook Size = (4,2) SU Feedback: Supported
.....1 = Codebook Size = (7,5) MU Feedback: Supported
.....0 = Triggered SU Beamforming Feedback: Not supported
.....0 = Triggered MU Beamforming Partial BW Feedback: Not supported
.....0 = Triggered CQI Feedback: Not supported
EHT PHY Bits 32-39: 0x28
.....0 = Partial Bandwidth DL MU-MIMO: Not supported
.....0 = EHT PSR-Based SR support: Not supported
.....0 = Power Boost Factor Support: Not supported
.....1 = EHT MU PPDU With 4x EHT-LTF and 0.8 us GI: Supported
0010 = Max Nc: 2
EHT PHY Bits 40-63: 0x00f860
.....0 = Non-Triggered CQI Feedback: Not supported
.....0 = Tx 1024-QAM & 4096-QAM < 242-tone RU Support: Not supported
.....0 = Rx 1024-QAM & 4096-QAM < 242-tone RU Support: Not supported
.....0 = PPE Thresholds Present: Not Present
.....10 = Common Nominal Packet Padding: 2
.....0001 = Maximum Number Of Supported EHT-LTFs: 1
.....111 = Support Of MCS 15: 15
.....1 = Support Of EHT DUP (MCS 14) in 6 GHz: Supported
.....0 = Support For 20 MHz Operating STA Receiving NDP With Wider BW
.....0 = Non-OFDMA UL MU-MIMO (BW <= 80 MHz): Not supported
.....0 = Non-OFDMA UL MU-MIMO (BW = 160 MHz): Not supported
.....0 = Non-OFDMA UL MU-MIMO (BW = 320 MHz): Not supported
.....0 = MU Beamformer (BW <= 80 MHz): Not supported
.....0 = MU Beamformer (BW = 160 MHz): Not supported
.....0 = MU Beamformer (BW = 320 MHz): Not supported
.....0 = TB Sounding Feedback Rate Limit: Not supported
EHT PHY Bits 64-71: 0x444400
.....0 = Rx 1024-QAM In Wider Bandwidth DL OFDMA Support: Not supported
.....0 = Rx 4096-QAM In Wider Bandwidth DL OFDMA Support: Not supported
000000 = Reserved: 0x00
Supported EHT-MCS and NSS Set
> EHT-MCS Map (BW <= 80MHz): 0x444444
> EHT-MCS Map (BW = 160MHz): 0x444444
> EHT-MCS Map (BW = 320MHz): 0x444444
.....0100 = Rx Max Nss That Supports EHT-MCS 0-9: 4
.....0100 = Tx Max Nss That Supports EHT-MCS 0-9: 4
.....0100 = Rx Max Nss That Supports EHT-MCS 10-11: 4
.....0100 = Tx Max Nss That Supports EHT-MCS 10-11: 4
.....0100 = Rx Max Nss That Supports EHT-MCS 12-13: 4
.....0100 = Tx Max Nss That Supports EHT-MCS 12-13: 4
```

#9 Association Response from AP (2/2)

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



- Select #9 Association Response, and open EHT Operations, open header
- There are WiFi7 operational info, such as MCS and Number of SS.
- In usual, we do not have to dig into EHT Capabilities and EHT Operation, just check Fixed parameters, “Status code: Successful”, “Association ID: 0x0001” to determine AP and STA are connected and the datalink is up.

```
Ext Tag: EHT Capabilities (802.11be D3.0)
▼ Ext Tag: EHT Operation (802.11be D3.0)
  Ext Tag length: 8 (Tag len: 9)
  Ext Tag Number: EHT Operation (802.11be D3.0) (106)
  ▼ EHT Operation Parameters: 0x01, EHT Operation Information Present
    .... 1 = EHT Operation Information Present: True
    .... 0 = Disabled Subchannel Bitmap Present: False
    .... 0 = EHT Default PE Duration: False
    .... 0 = Group Addressed BU Indication Limit: False
    ..00 .... = Group Addressed BU Indication Exponent: 0
    00.. .... = Reserved: 0x0
  Basic EHT-MCS And Nss Set: 0x00000011
  ▼ Control: 0x04, Channel Width: 320 MHz EHT BSS bandwidth
    .... 100 = Channel Width: 320 MHz EHT BSS bandwidth (4)
    0000 0... = Reserved: 0x00
  CCFS0: 0x0000004f
  CCFS1: 0x0000003f

> Frame 9: 339 bytes on wire (2712 bits), 339 bytes
> Radiotap Header v0, Length 32
> 802.11 radio information
> IEEE 802.11 Association Response, Flags: .....
▼ IEEE 802.11 Wireless Management
  ▼ Fixed parameters (6 bytes)
    > Capabilities Information: 0x1131
      Status code: Successful (0x0000)
      ..00 0000 0000 0001 = Association ID: 0x0001
```

#10 #11 #12 #13 4 way handshake of EAPOL

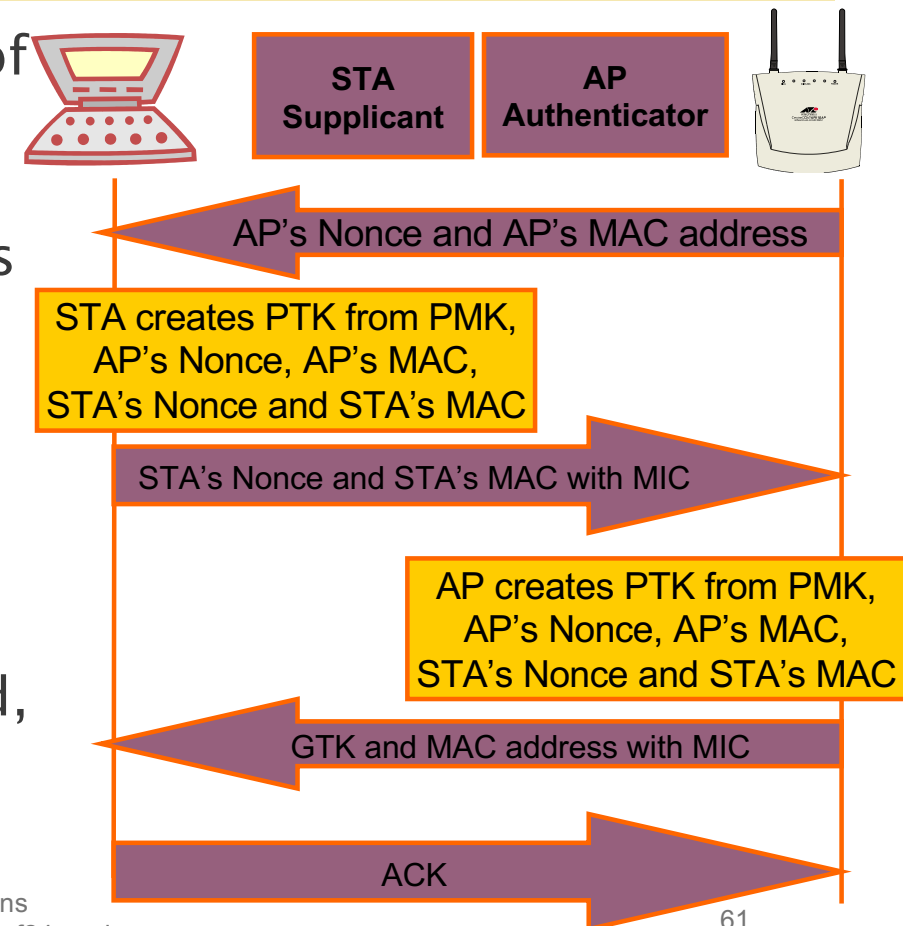
SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



10	0.116657	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:b8	Intel_27:3d:0f	-56 ...	6	✓	QoS Data	Key (Message 1 of 4)
11	0.124976	802.11a (OFDM)	85	6375MHz	Intel_27:3d:0f	Buffalo_45:1d:b8	-75 ...	6		QoS Data	Key (Message 2 of 4)
12	0.129949	802.11a (OFDM)	85	6375MHz	Buffalo_45:1d:b8	Intel_27:3d:0f	-56 ...	6		QoS Data	Key (Message 3 of 4)
13	0.130826	802.11a (OFDM)	85	6375MHz	Intel_27:3d:0f	Buffalo_45:1d:b8	-75 ...	6		QoS Data	Key (Message 4 of 4)

- The frame #10~#14 are 4 way Handshake of EAPOL of WPA1/2/3

1. Message1 contains AP's Nonce and MAC
2. STA creates PTK from PMK, AP's Nonce, AP's MAC, STA's Nonce and STA's MAC
Message2 contains STA's Nonce and MAC with MIC (Message Integrity Code), hash value using sending MIC key, part of PTK.
3. AP creates PTK from PMK, AP's Nonce, AP's MAC, STA's Nonce and STA's MAC
and confirm MIC value using receiving MIC key, part of PTK, if the MIC value is matched, Message3 contains GTK and MAC with MIC
4. Message4 contains Confirm value of MIC



#10 #11 #12 #13 4 way handshake of EAPOL

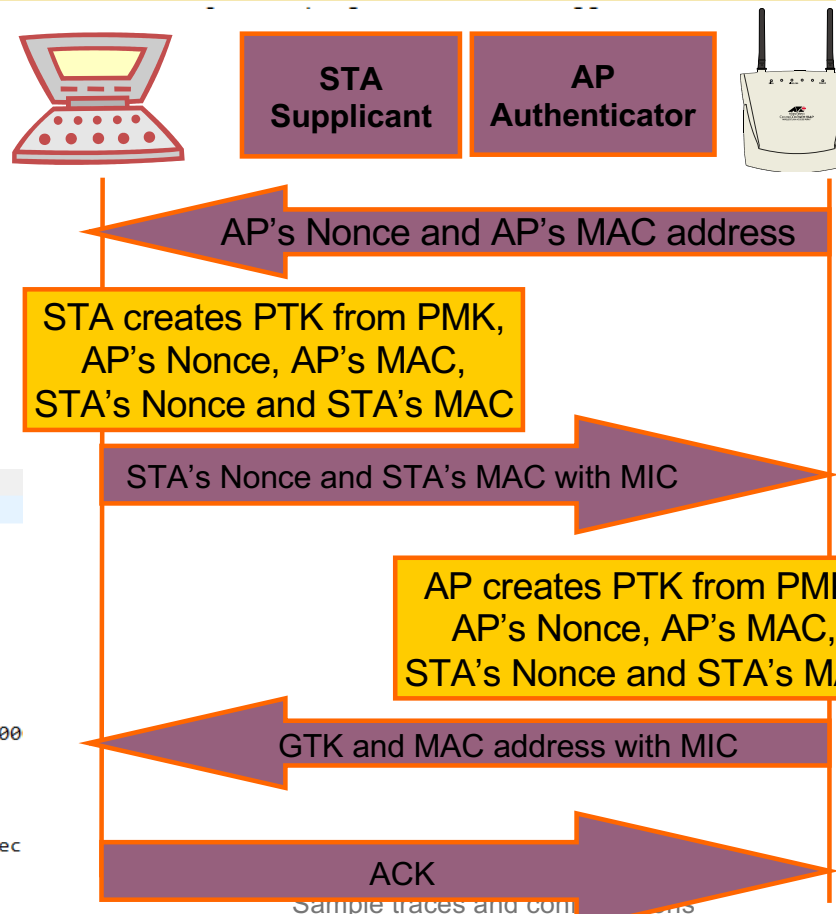
SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



10	0.116657	802.11a (OFDM)	85	6375MHz Buffalo_45:1d:b8 Intel_27:3d:0f	-56 ...	6	✓	QoS Data	Key (Message 1 of 4)
11	0.124976	802.11a (OFDM)	85	6375MHz Intel_27:3d:0f Buffalo_45:1d:b8	-75 ...	6		QoS Data	Key (Message 2 of 4)
12	0.129949	802.11a (OFDM)	85	6375MHz Buffalo_45:1d:b8 Intel_27:3d:0f	-56 ...	6		QoS Data	Key (Message 3 of 4)
13	0.130826	802.11a (OFDM)	85	6375MHz Intel_27:3d:0f Buffalo_45:1d:b8	-75 ...	6		QoS Data	Key (Message 4 of 4)

▼ 802.1X Authentication
Version: 802.1X-2001 (1)
Type: Key (3)
Length: 127
Key Descriptor Type: EAPOL RSN Key (2)
[Message number: 2]
> Key Information: 0x0108
Key Length: 0
Replay Counter: 1
WPA Key Nonce: 86479ba98e5933920149b6d441f1c2:
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000
WPA Key ID: 0000000000000000
WPA Key MIC: 141e67db406cb28e3c454ca36248d4bc
WPA Key Data Length: 32
> WPA Key Data: 301a010000fac040100000fac040100

▼ 802.1X Authentication
Version: 802.1X-2001 (1)
Type: Key (3)
Length: 95
Key Descriptor Type: EAPOL RSN Key (2)
[Message number: 4]
> Key Information: 0x0308
Key Length: 0
Replay Counter: 2
WPA Key Nonce: 00000000000000000000000000000000
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000
WPA Key ID: 0000000000000000
WPA Key MIC: 70e6f63ab3ea2ae1132683c35a2e12ec
WPA Key Data Length: 0



▼ 802.1X Authentication
Version: 802.1X-2004 (2)
Type: Key (3)
Length: 95
Key Descriptor Type: EAPOL RSN Key (2)
[Message number: 1]
> Key Information: 0x0088
Key Length: 16
Replay Counter: 1
WPA Key Nonce: 9a292b453a98b9be3922e849ed772b
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000
WPA Key ID: 0000000000000000
WPA Key MIC: 00000000000000000000000000000000
WPA Key Data Length: 0

▼ 802.1X Authentication
Version: 802.1X-2004 (2)
Type: Key (3)
Length: 183
Key Descriptor Type: EAPOL RSN Key (2)
[Message number: 3]
> Key Information: 0x13c8
Key Length: 16
Replay Counter: 2
WPA Key Nonce: 9a292b453a98b9be3922e849ed772b9
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000
WPA Key ID: 0000000000000000
WPA Key MIC: d9fb391d620d889d0b82023877002cb5
WPA Key Data Length: 88
WPA Key Data: 0e10facf1d46a004e318a1eb0e3e2ba7

#14 QoS Data and the #15, #16 Data

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



- Finally, the data communication between STA and AP has begun,
- Frame #14 is QoS Data, it is truly IEEE802.11be but CommView's export dissector is not updated yet, so Wireshark shows nothing about PHY type

14	0.131610	85	6375MHz Intel_27:3d:0f	IPv6mcast_ff:05...	-67 ...	30	QoS Data	QoS Data, SN=2, FN=0, Flags=.p...
----	----------	----	------------------------	--------------------	---------	----	----------	-----------------------------------

ログビューア [20-9-2024@14-53-49-232.ncfx]

ファイル(F) 検索(S) フィルタ(R)

▼ Wireless Packet Info

- PPDU type: Multi User
- Signal level: 46%
- Signal level in dBm: -67
- Noise level in dBm: -91
- Rate type: EHT (OFDMA)
- Rate: 30.0 Mbps
- Band: 6 GHz
- Channel: 85 - 6375 MHz
- MCS index: 3 (16-QAM, 1/2)
- Streams: 2
- Guard Interval: 0.8 μ s
- Channel width: 106-tone RU
- 年月日: 20-9-2024
- 絶対時間: 14:53:32.940772
- デルタ時間: 0.000013
- フレームのサイズ: 122 バイト
- フレーム番号: 440

▼ - 802.11

番号	プロトコル	送信元MAC	送信先MAC	BSSID	絶対時間	信号強度	レート	エラー	統計
430	EAPOL	Buffalo45:1D:B8	Intel27:3D:0F	Buffalo45:1D:B8	14:53:32.925819	-56	6		EAPOL-Key (4-Way Handshake Message 1), Length = 95
431	CTRL/ACK	N/A	Buffalo45:1D:B8	Buffalo45:1D:B8	14:53:32.926014	-74	6		
432	EAPOL	Intel27:3D:0F	Buffalo45:1D:B8	Buffalo45:1D:B8	14:53:32.934138	-75	6		EAPOL-Key (4-Way Handshake Message 2), Length = 127
433	CTRL/ACK	N/A	Intel27:3D:0F	Buffalo45:1D:B8	14:53:32.934157	-56	6		
434	EAPOL	Buffalo45:1D:B8	Intel27:3D:0F	Buffalo45:1D:B8	14:53:32.939111	-56	6		EAPOL-Key (4-Way Handshake Message 3), Length = 183
435	CTRL/ACK	N/A	Buffalo45:1D:B8	Buffalo45:1D:B8	14:53:32.939130	-72	6		
436	EAPOL	Intel27:3D:0F	Buffalo45:1D:B8	Buffalo45:1D:B8	14:53:32.939988	-75	6		EAPOL-Key (4-Way Handshake Message 4), Length = 95
437	CTRL/ACK	N/A	Intel27:3D:0F	Buffalo45:1D:B8	14:53:32.940000	-56	6		
438	CTRL/RTS	Intel27:3D:0F	Buffalo45:1D:B8	Buffalo45:1D:B8	14:53:32.940743	-67	6		
439	CTRL/CTS	N/A	Intel27:3D:0F	Buffalo45:1D:B8	14:53:32.940759	-55	6		
440	ENCR. DATA	Intel27:3D:0F	33:33:FF:05:C9:B0	Buffalo45:1D:B8	14:53:32.940772	-67	30 (EHT MCS 3, SS 2, CW RU 106)		WPA: Can't decrypt
441	CTRL/ACK	N/A	Intel27:3D:0F	Buffalo45:1D:B8	14:53:32.940787	-55	24		
442	DATA/QoS NULL	Intel27:3D:0F	Buffalo45:1D:B8	Buffalo45:1D:B8	14:53:32.945769	-75	6		

▼ Wireless Packet Info

- PPDU type: Multi User
- Signal level: 46%
- Signal level in dBm: -67
- Noise level in dBm: -91
- Rate type: EHT (OFDMA)
- Rate: 30.0 Mbps
- Band: 6 GHz
- Channel: 85 - 6375 MHz
- MCS index: 3 (16-QAM, 1/2)
- Streams: 2
- Guard Interval: 0.8 μ s
- Channel width: 106-tone RU
- 年月日: 20-9-2024
- 絶対時間: 14:53:32.940772
- デルタ時間: 0.000013
- フレームのサイズ: 122 バイト
- フレーム番号: 440

▼ Radiotap Header v0, Length 32

- Header revision: 0
- Header pad: 0
- Header length: 32
- > Present flags
- MAC timestamp: 1726811612940772
- > Flags: 0x00
- Data Rate: 30.0 Mb/s
- Channel frequency: 6375 [6 GHz 85]
- > Channel flags: 0x0000
- Antenna signal: -67 dBm
- Antenna noise: -91 dBm
- Channel number: 85
- Channel frequency: 6375
- > Channel flags: 0x00000000
- ▼ 802.11 radio information
- Data rate: 30.0 Mb/s
- Channel: 85
- Frequency: 6375MHz
- Signal strength (dBm): -67 dBm
- Noise level (dBm): -91 dBm
- Signal/noise ratio (dB): 24 dB
- TSF timestamp: 1726811612940772

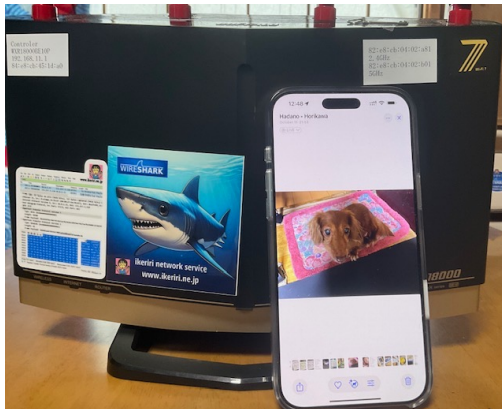
- CommView for WiFi shows “Rate type: EHT(OFDMA), Rate 30.0Mbps, Band: 6GHz, Channel:85 – 6375MHz, MCS index:3 (16-QAM, 1/2), Streams:2, Guard Interval:0.8, Channel width:106-tone RU

- #15, #16 are Data frames https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu

Sample traces and configurations



- We dissected the WiFi7 datalink by Wireshark!!
- There are bonus trace files
Appendix1: iphone-wifi7.pcapng, this trace contains WiFi7 20MHz connection between iPhone16 and Buffalo
Appendix2: setupWiFi7EasyMeshAndMLO.pcapng
WiFi7-certified EashMesh and MLO setup capture by two access points using Profitap ProfiShark1 G



Sample traces and configurations
https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu.zip

WiFi7 show time!!

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



- I bring a Buffalo WXR18000BE10P here with 10GbE NIC
- AP has a 10GbE LAN, I connected My macbook via 10GbE NIC



- SSID: ikeriri7 (only works on 6GHz)
ikeriri7mlo (MLO with 2.4/5/6GHz)
- Passphrase: wireshark
- AP's IP:192.168.11.1 6GHz BSSID:84:E8:CB:45:1D:BF
10GbE macbook's IP:192.168.11.2 MAC:00:23:A4:0D:16:B1
- Turn on iperf3 server on 192.168.11.2

Sample traces and configurations
https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu.zip

WiFi7 show time!!

SharkFest'24 EUROPE
Vienna, Austria • #sf24eu



- SSID: ikeriri7 (only works on 6GHz)
ikeriri7mlo (MLO with 2.4/5/6GHz)
- Passphrase: wireshark
- At first, I test by HE network tool of my iPhone16

```
megumitakeshita@ikeririmacbook ~ % iperf3 -s
-----
Server listening on 5201 (test #1)
-----
Accepted connection from 192.168.11.3, port 61740
[ 5] local 192.168.11.2 port 5201 connected to 192.168.11.3 port 61741
[ ID] Interval      Transfer    Bitrate
[ 5]  0.00-0.56    sec  98.8 MBytes  1.48 Gbits/sec
-----
[ ID] Interval      Transfer    Bitrate
[ 5]  0.00-0.56    sec  98.8 MBytes  1.48 Gbits/sec                               receiver
```

- **Welcome to over 1Gbps wireless**
- You can also get 192.168.11.X/24 from AP
please try “iperf3 -c 192.168.11.2” too

Sample traces and configurations
https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu.zip





USE WIRESHARK

Thank you for watching.

Please complete the survey

trace files and Wireshark profiles are here:

https://www.ikeriri.ne.jp/sharkfest/wifi7_sf24eu.zip



ikeriri network service

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

