Unlocking Wi-Fi 7:
The Real-World State of Client Security

Introduction

In Wi-Fi 7, the use of Extremely High Throughput (EHT) physical layer and multiple links in the MLO mode requires new security mechanisms to be complied with across all the bands (2.4/5/6 GHz). Arista Access Points (AP) support all the mandatory security requirements of Wi-Fi 7. However, the security mechanisms can only be put into force when the clients also support them. In this white paper, we present the test results of the support for these mandatory security features by the popular Wi-Fi 7 clients in the market. Additionally, we present the test results on WPA3 support in a few legacy clients.

Wi-Fi 7 security enhancements

Wi-Fi 7 mandates the use of WPA3 on all the bands for enhanced security. It introduces enhanced authentication, encryption and protection mechanisms to ensure secure and reliable communication between a client and the Access Point (AP). The RSN (Robust Security Network) element in a Wi-Fi 7 association frame is an Information Element (IE) in which the AP and the client advertise their security capabilities. We examine this IE for the security capabilities of the client devices, an example of the same is illustrated in Fig.1. It is important to note that the individual PHY links carry unique MAC addresses that differ from the MLD MAC address (client MAC address).

```
Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 26
    RSN Version: 1
    Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
        Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
        Group Cipher Suite type: AES (CCM) (4)
    Pairwise Cipher Suite Count: 1
    Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) GCMP (256)
        Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) GCMP (256)
            Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
            Pairwise Cipher Suite type: GCMP (256) (9)
    Auth Key Management (AKM) Suite Count: 1
    Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) SAE (GROUP-DEPEND)
        Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (GROUP-DEPEND)
            Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
            Auth Key Management (AKM) type: SAE (GROUP-DEPEND) (24)
```

Fig.1: RSN Information Element in the client's association request frame

New SAE AKMs

WPA3 introduced the Simultaneous Authentication of Equals (SAE) mechanism of authentication. SAE uses an Elliptic-Curve-Diffie-Hellman to generate the Pair Wise Master Key. In this process, the client and AP mutually authenticate each other. More information on SAE can be found here. New AKMs 24 and 25 were introduced in the 802.11be standard to provide per-MLD (Multi-Link Device) authentication. For details on the significance of the new AKMs, refer to this Arista white paper.

New Pair-wise cipher key

The 802.11be standard introduced the use of the Galois/Counter Mode Protocol with 256-bit keys (GCMP-256) as the pair-wise cipher suite, in the place of AES CCMP-128. With GCMP-256, Wi-Fi 7 clients enjoy better data confidentiality, authentication, integrity, and replay protection.

```
Ext Tag Number: Multi-Link (802.11be D3.0) (107)
Multi-Link Control: 0x0180 Basic
    .... .... .... .000 = Type: Basic (0)
    .... .... .... 0... = Reserved: 0x0
    .... .... ...0 .... = Link ID Info Present: False
    .... .... ..0. .... = BSS Parameters Change Count Present: False
    .... .... .0.. .... = Medium Synchronization Delay Info Present: False
    .... .... 1... .... = EML Capabilities Present: True
    .... ...1 .... .... = MLD 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: Intel_69:d1:47 (10:5f:ad:69:d1:47)
    EML Capabilities: 0x0033, EMLSR Support
        .... .... .... ...1 = EMLSR Support: True
        .... .... .... 001. = EMLSR Padding Delay: 1
        .... .... .011 .... = EMLSR Transition Delay: 3
        .... .... 0... .... = EMLMR Support: False
        .... .000 .... .... = EMLMR Delay: 0
        .000 0... .... .... = Transition Timeout: 0
        0... .... .... .... = Reserved: 0x0
    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
```

Fig. 2: Protected Frame capabilities highlighted in the RSN element.

Protected Management frames

Sensitive management frames like deauthentication and dissociation frames were often sent unencrypted prior to the introduction of Protected Management Frames (PMF) in 802.11w. These frames could be exploited to launch Man-in-the-Middle (MITM) or Denial-of-Service (DoS) attacks. While Wi-Fi 7 does not explicitly improve upon the security of PMF's, it mandates use of PMF in single link as well as multi-link operation.

The support for Protected Management Frames is indicated in the RSN IE by setting both Management Frame Protection Required and Management Frame Protection Capable fields. Fig. 2 highlights the PMF capabilities in the RSN element.

Beacon Protection

Unprotected beacons are susceptible to attackers misusing them especially in replay attacks to spoof clients, altering the Beacon frame IEs to adversely affect the client devices by redirecting them to a wrong channel, lowering their data rates or even disconnecting the clients. Beacon frames are protected in Wi-Fi 7 against such malicious attacks.

```
Extended Capabilities: 0x10 (octet 11)
    .... ...0 = Complete List of NonTxBSSID Profiles: False
    .... ..0. = SAE Password Identifiers In Use: False
    .... .0.. = SAE Passwords Used Exclusively: False
    .... 0... = Enhanced Multi-BSSID Advertisement Support: False
    ...1 .... = Beacon Protection Enabled: True
    ..0. .... = Mirrored SCS: False
    .0.. .... = OCT: False
    0... .... = Local MAC Address Policy: False
```

Fig. 3: Beacon protection capabilities highlighted in the Extended Capabilities of the association frame.

With Beacon Protection, the AP shares a Beacon Integrity Group Temporal Key (BIGTK) with the client during the WPA3's 4-way handshake and adds a message integrity check (MIC) element to Beacon frames. The MIC allows the client to verify the Beacon frame integrity, and identify active attacks. MFP is a prerequisite for enabling Beacon Protection.

Beacon protection capabilities can be found in Extended Capabilities octet 11 in the RSN IE :
EHT Capabilities > Extended Capabilities > Beacon Protection Enabled

(See Fig. 3 for an illustrated example).

Security in Multi-Link Operation

In MLO, association takes place only on one link, and the security capabilities are advertised by the client in the association request on this link. The link that the client device chooses to associate is specific to the client implementation. In order to identify the link on which the client associates, it is required to capture packets on all the three operating bands (2.4/5/6 GHz) simultaneously. All the participating links in MLO will use the same security keys exchanged in the 4-way handshake of the associating link. The client security capabilities can be extracted from the RSN IE present in the association request frame. The MLO capabilities of a client can be found under *Common Info > MLD Capabilities> Maximum Number of simultaneous Links*. Remember increment this value by 1 to find the number of participating links in MLO. Fig 4 shows an illustration of how to check the MLO capabilities in an association frame.

More information about the working of MLO in Wi-Fi 7 can be found here.

```
Tag Number: RSN Information (48)
Tag length: 28
RSN Version: 1
> Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
Pairwise Cipher Suite Count: 2
> Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) GCMP (256) 00:0f:ac (Ieee 802.11) AES (CCM)
Auth Key Management (AKM) Suite Count: 2
> Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) SAE (SHA256) 00:0f:ac (Ieee 802.11) SAE (GROUP-DEPEND)
v RSN Capabilities: 0x00cc
    .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
    .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneou
    .... .... .... 11.. = RSN PTKSA Replay Counter capabilities: 16 replay counters per PTKSA/GTKSA/STAKeySA
    .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKeySA (0
    .... .... .1.. .... = Management Frame Protection Required: True
    .... .... 1... .... = Management Frame Protection Capable: True
    .... ...0 .... .... = Joint Multi-band RSNA: False
    .... ..0. .... .... = PeerKey Enabled: False
    ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
    .0.. .... .... .... = OCVC: False
```

Fig. 4: Multi Link capabilities highlighted in the Common Information of the association frame.

If the client is EMLSR (e.g. Intel BE-200), we may verify this by checking the following fields in the Multi-link Control element in the association frame (see Fig. 5).

```
Ext Tag: Multi-Link (802.11be D3.0)
    Ext Tag length: 117 (Tag len: 118)
    Ext Tag Number: Multi-Link (802.11be D3.0) (107)
    Multi-Link Control: 0x0180 Basic
        .... .... .... .000 = Type: Basic (0)
        .... .... .... 0... = Reserved: 0x0
        .... .... ...0 .... = Link ID Info Present: False
        .... .... ..0. .... = BSS Parameters Change Count Present: False
        .... .... .0.. .... = Medium Synchronization Delay Info Present: False
        .... .... 1... .... = EML Capabilities Present: True
        .... ...1 .... .... = MLD 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: Intel_69:d1:47 (10:5f:ad:69:d1:47)
        EML Capabilities: 0x0033, EMLSR Support
            .... .... .... ...1 = EMLSR Support: True
            .... .... .... 001. = EMLSR Padding Delay: 1
            .... .... .011 .... = EMLSR Transition Delay: 3
            .... .... 0... .... = EMLMR Support: False
            .... .000 .... .... = EMLMR Delay: 0
            .000 0... .... .... = Transition Timeout: 0
            0... .... .... .... = Reserved: 0x0
```

Fig. 5: EMLSR capabilities of a client.

Security performance of real world clients

We tested the support of the advanced security capabilities across a wide variety of Wi-Fi clients. The clients are associated with the state of the art Arista enterprise grade WiFi 7 AP. We use a multi-band sniffer capable of sniffing across all the 3 bands (2.4/5/6 GHz) simultaneously. Table 1 summarizes the results from the testing. While the client list is not exhaustive, it gives a good representation of the clients in the market and their security capabilities.

The Google Pixels and iPhones associated on the 6 GHz band. The rest of the clients associated on either 2.4 GHz or 5 GHz bands. All tested Wi-Fi 7 clients provide support for the 802.11be mandated AKM suites (24, 25) and the Pairwise Cipher suite (GCMP-256). Management Frame Protection is also widely supported. Most clients do not seem to support Beacon Protection, except for the iPhone family. In addition to Wi-Fi 7 clients, we tested two Wi-Fi 6E and one Wi-Fi 5 clients. These clients associated with AKM suites 8 & 9, as expected demonstrating seamless backward compatibility of the AP.

Client	Associated Band	Wi-Fi version	Multi-Link Mode	RSN Information			Protected Management Frame		Beacon Protection* (True | False | No)
				Group Cipher Suite	Pairwise Cipher Suite	AKM	Required	Capable	
Samsung S25	2.4/5 GHz	Wi-Fi 7	STR-MLMR	CCMP-128	GCMP-256	24	Required	Capable	No
iPhone 17	2.4/5/6GHz	Wi-Fi 7	STR-MLMR	CCMP-128	GCMP-256	24	Required	Capable	True
iPhone 16 Pro	2.4/5 GHz	Wi-Fi 7	STR-MLMR	CCMP-128	GCMP-256	24	Required	Capable	No
MacBook M5 Pro	2.4/5/6GHz	Wi-Fi 7	STR-MLMR (3 Links)	CCMP-128	GCMP-256	24	Required	Capable	True
Asus ROG 7	2.4/5 GHz	Wi-Fi 7	STR-MLMR	CCMP-128	GCMP-256	24	Required	Capable	No
Samsung S24	2.4 GHz	Wi-Fi 7	STR-MLMR	CCMP-128	GCMP-256	24	Required	Capable	No
Pixel 9	2.4/5 GHz	Wi-Fi 7	STR-MLMR	CCMP-128	GCMP-256	24	Required	Capable	No
Pixel 8	2.4/6 GHz	Wi-Fi 7	STR-MLMR	CCMP-128	GCMP-256	24	Required	Capable	No
Intel BE-200	2.4/5 GHz	Wi-Fi 7	EMLSR	CCMP-128	GCMP-256	24	Required	Capable	False
One Plus 11	2.4/5 GHz	Wi-Fi 7	STR-MLMR	CCMP-128	GCMP-256	24	Required	Capable	No
MediaTek MT7925	2.4/5GHz	Wi-Fi 7	MLSR	CCMP-128	GCMP-256	24	Required	Capable	False
Pixel-9 Pro Fold	2.4/5 GHz	Wi-Fi 7	STR-MLMR	CCMP-128	GCMP-256	24	Required	Capable	No
Pixel 7	2.4/5 GHz	Wi-Fi 6E	N/A	CCMP-128	GCMP-256	8	Required	Capable	N/A
Samsung 23	2.4/5 GHz	Wi-Fi 6E	N/A	CCMP-128	GCMP-256	8	Required	Capable	N/A
Intel AX 211	5 GHz	Wi-Fi 6E	N/A	CCMP-128	CCMP-128	8	Required	Capable	N/A
iPhone 15 Pro	2.4/5 GHz	Wi-Fi 6E	N/A	CCMP-128	GCMP-256	8	Required	Capable	N/A
iPhone 14 Pro	2.4/5 GHz	Wi-Fi 6E	N/A	CCMP-128	GCMP-256	8	Required	Capable	N/A
MacBook Pro M4	2.4/5 GHz	Wi-Fi 6E	N/A	CCMP-128	GCMP-256	8	Required	Capable	N/A
Macbook Pro (Intel)	2.4/5 GHz	Wi-Fi 5	N/A	CCMP-128	CCMP-128	8	Required	Capable	N/A

Table 1: Security & Multi-link capabilities of clients.

The meaning of various fields of beacon protection is explained below:

Beacon Protection*	Description
True	The device is capable and has enabled Beacon Protection
False	The device is capable but doesn't enable the Beacon Protection.
No	The device doesn't support beacon protection (in some cases the extended capabilities are not even present in the packet capture).
N/A	Not Applicable

Conclusions

WPA3 is a leap towards better security, improving resilience against a multitude of security threats. Wi-Fi 7 APs and clients are mandated to support WPA3 on all the three bands (2.4/5/6 GHz). In this white paper, we investigated the status of adoption of advanced Wi-Fi 7 security features outlined in the IEEE 802.11be standard in popular Wi-Fi 7 clients. While this is not an exhaustive list by any means, it does reflect on the status of WPA3 adoption in the real world.

The security features mandated in the Wi-Fi 7 standard are applicable when the AP and the client use the EHT PHY and/or MLO. Clients that do not support the new security features can still associate with a Wi-Fi 7 AP, but will not be able to benefit from the advanced data rates offered by EHT PHY and MLO. They will have to fall back to using older Wi-Fi protocols e.g., 802.11ax.

Clients	OS	Kernel version/Baseband Driver	Model Number	Year of manufacturing
Samsung S25	Android 16	6.6.77-android15-8-31998796 / s931bxxs8bzb5	SM-S931B/DS	June - 2025
iPhone 17	IOS 26.0.1	N/A / 1.00.05	MG6K4HN/A	July - 2025
MacBook M5 Pro	macOS 26.3.0	DARWIIN 25.3.0 / [REV 72.11.260N1B1 devFused=0]	MGEC4HN/A	2026
iPhone 16 Pro	iOS 26.3.1	N/A / 2.40.01	MYNF3HN/A	2024
Pixel 9	Android 16	6.1.134-android14-11/g5400c-250605-251024-B-14326965	GUR25	2024
Pixel 8	Android 16	6.1.145-andriod14-11-gc1de4747ac59 / g5300i-250909-2501-B-14326967	G9BQD	2023
Asus Rog 7	Android 15	5.15.167-android13-8-00020-g8713724d3081-ab13744575	ASUS-AI2205_D	N/A
Intel BE 200	Windows 11	Build 26200 / 24.20.0.4	Latitude 5430	
Pixel 9 Pro Fold	Android 16	6.1.145-android14-gfa1d6308d1fe / g5400c-251201-B-14784805	GGH2X	2025
Oneplus 11	Android 15	5.15.149-android13-8-o-01130-gfff5e3d854	CPH2451	2023
Samsung S24	Android 16	6.1.138-android14-11/S921BXXSDCZB2	SM-S921B/DS	2024

Table 2: Client drivers & OS versions

Clients	OS	Kernel version/Baseband Driver	Model Number	Year of manufacturing
Samsung S23	Android 15	5.15.153-android13-8-30958972 / S911BXXS8DYI3	SM-S911B/DS	2023
Pixel 7	Android 16	6.1.134-andriod14-11-g66e758f7d0c0 / g5300q-250605-B-14327462	GVUGC	2022
Intel AX 211	Windows 11	build 22361 / 23.170.0.1	Thinkpad X1 Carbon	2023
iPhone 15 Pro	iOS 26.3.1 (a)	N/A / 3.40.01	MTUX3HN/A	2023
iPhone 14 Pro	iOS 18.5	N/A / 3.60.02	MPXV3HN/A	2022
Macbook Pro (intel)	macOS 15.6.1	DARWIN 24.6.0 / 9.30.514.0.32.5.94	C02D1EF2ML7H	2020
Dell (MediaTek MT7925)	Windows 11	Build 26200 / 5.7.0.5115	Dell 13 Pro	2025
Macbook Pro M4	macOS 26.2	DARWIN 25.02 23.41.7.0.41.51.2000	MX2H3HN/A	2025

Table 2: Client drivers & OS versions

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A & B, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062