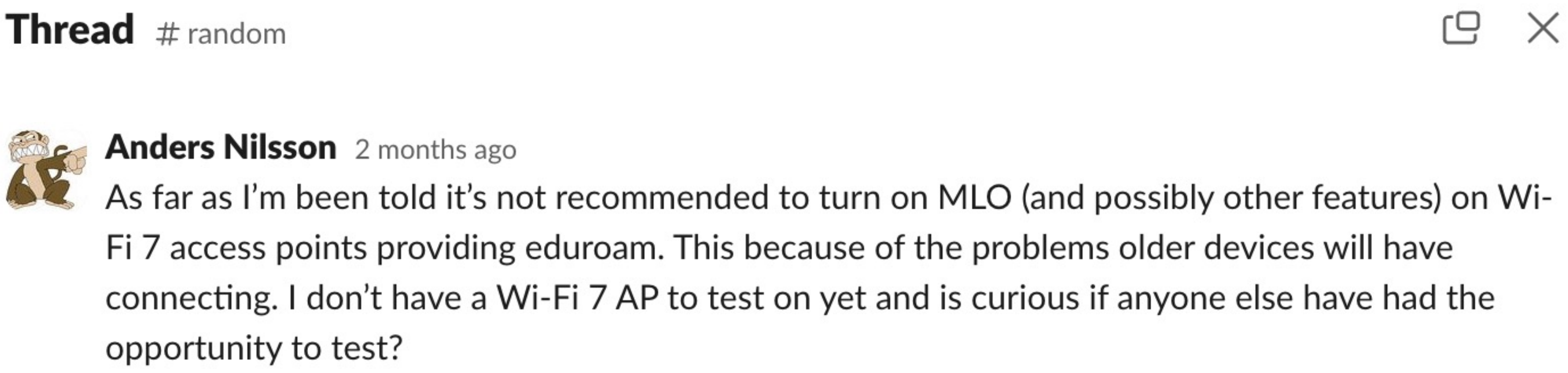
My first Wi-Fi 7

… and WPA3 CNSA

Paul Dekkers
10 Jun 2024, Mobility Day @TNC24

My First Wi-Fi 7

- I was triggered by:



Thread # random

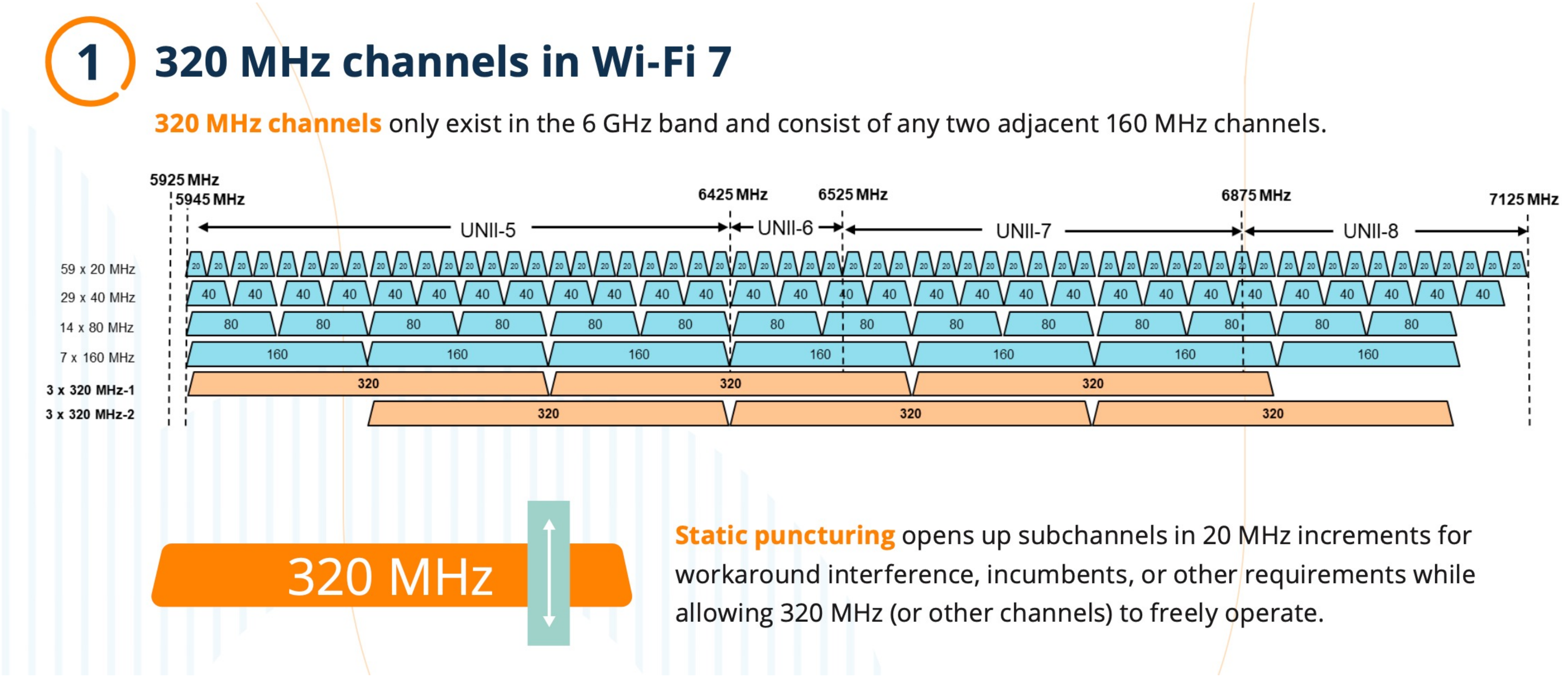
Anders Nilsson 2 months ago

As far as I'm been told it's not recommended to turn on MLO (and possibly other features) on Wi-Fi 7 access points providing eduroam. This because of the problems older devices will have connecting. I don't have a Wi-Fi 7 AP to test on yet and is curious if anyone else have had the opportunity to test?

Not impressed by speed – concerned with eduroam compatibility 🤔

- What does Wi-Fi 7 bring, what is MLO
- Does Wi-Fi 7 require WPA3 192?
- **back-of-the-envelope research**

Wi-Fi 7



1 320 MHz channels in Wi-Fi 7

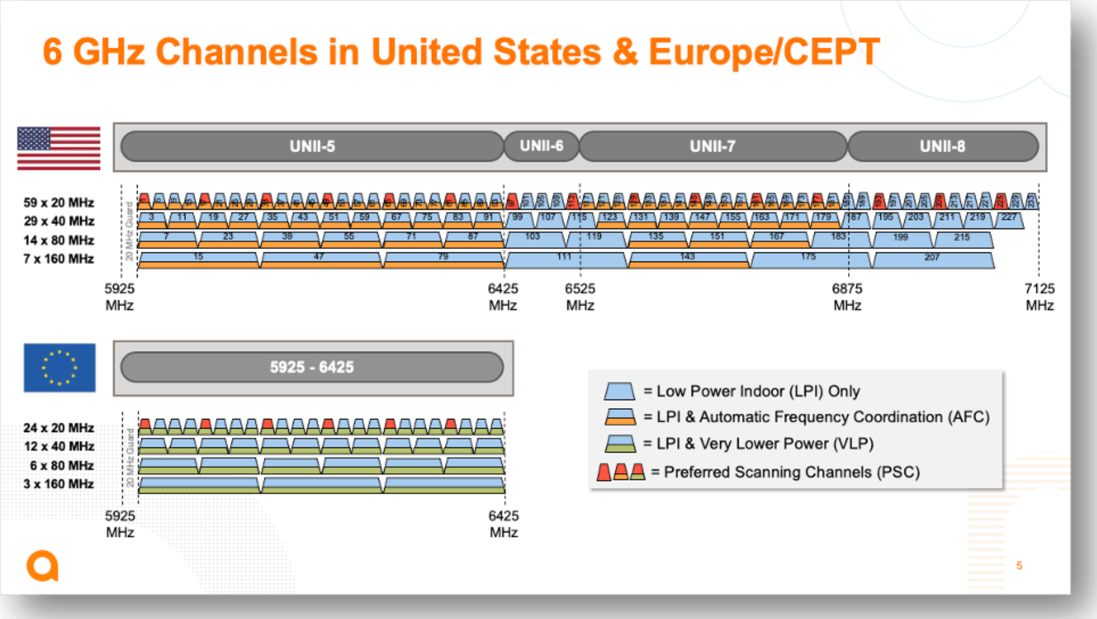
320 MHz channels only exist in the 6 GHz band and consist of any two adjacent 160 MHz channels.

Static puncturing opens up subchannels in 20 MHz increments for workaround interference, incumbents, or other requirements while allowing 320 MHz (or other channels) to freely operate.

Source: https://www.arubanetworks.com/resource/wi-fi-7-reference-guide/

Well, but Europe’s 6Ghz

Europe has only one 480Mhz



6 GHz Channels in United States & Europe/CEPT

= Low Power Indoor (LPI) Only

= LPI & Automatic Frequency Coordination (AFC)

= LPI & Very Lower Power (VLP)

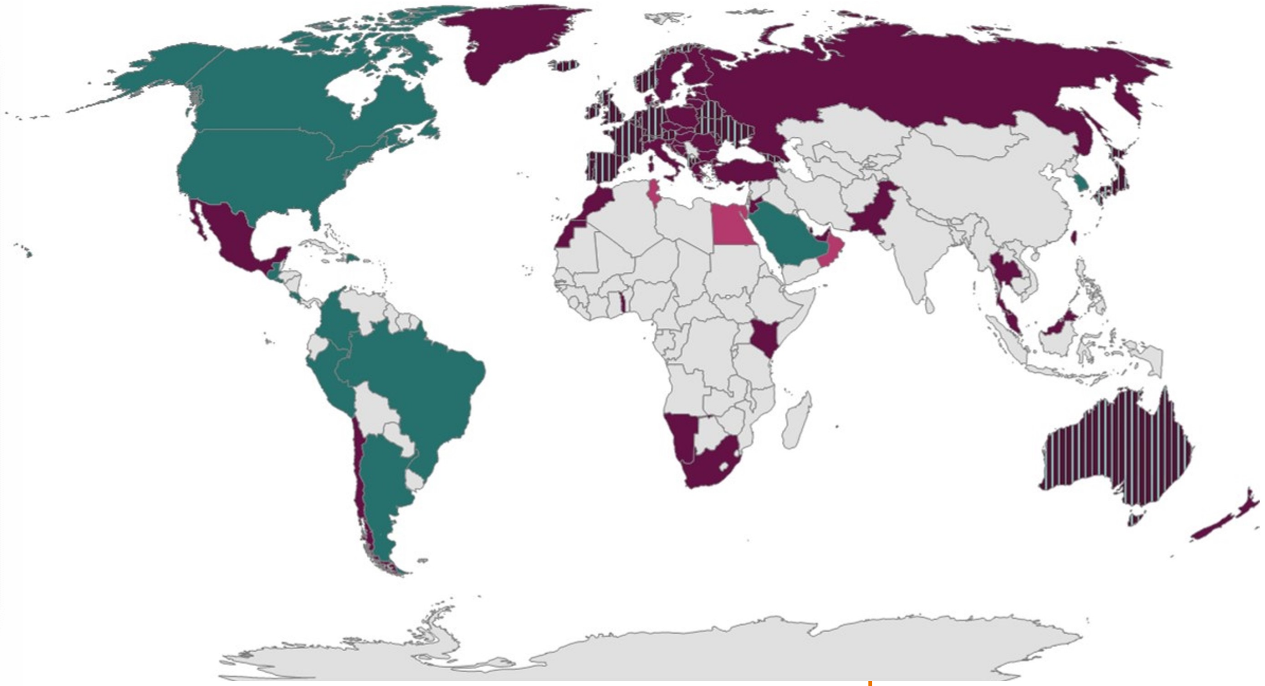
= Preferred Scanning Channels (PSC)

■ Adopted 5925-6425 MHz

■ Adopted 5925-7125 MHz

▥ Adopted 5925-6425 MHz, Considering 6425-7125 MHz

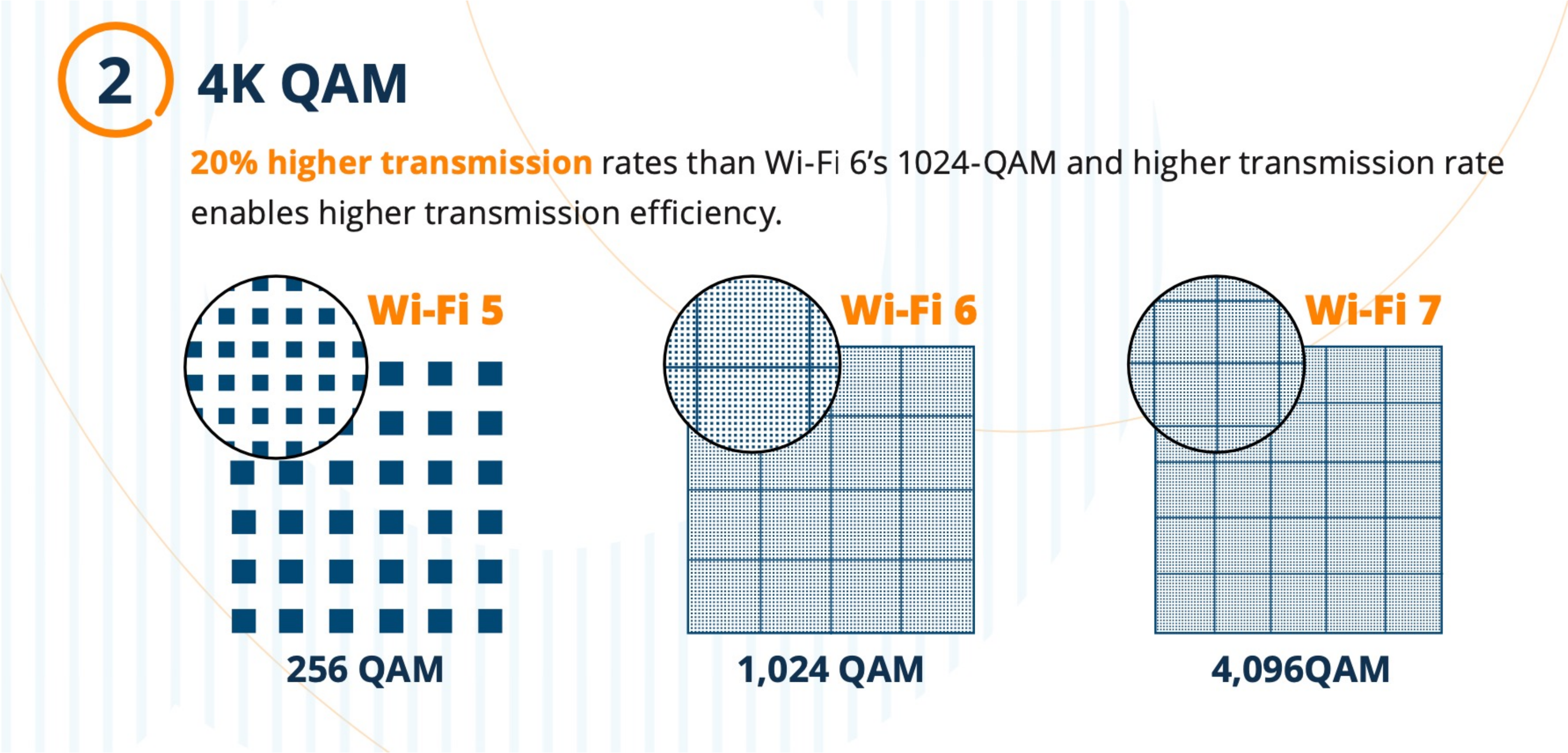
■ Considering 5925-6425 MHz



Source: https://www.wi-fi.org/regulations-enabling-6-ghz-wi-fi

Source: https://blogs.arubanetworks.com/solutions/wi-fi-6e-in-europe-frequently-asked-questions/

Wi-Fi 7

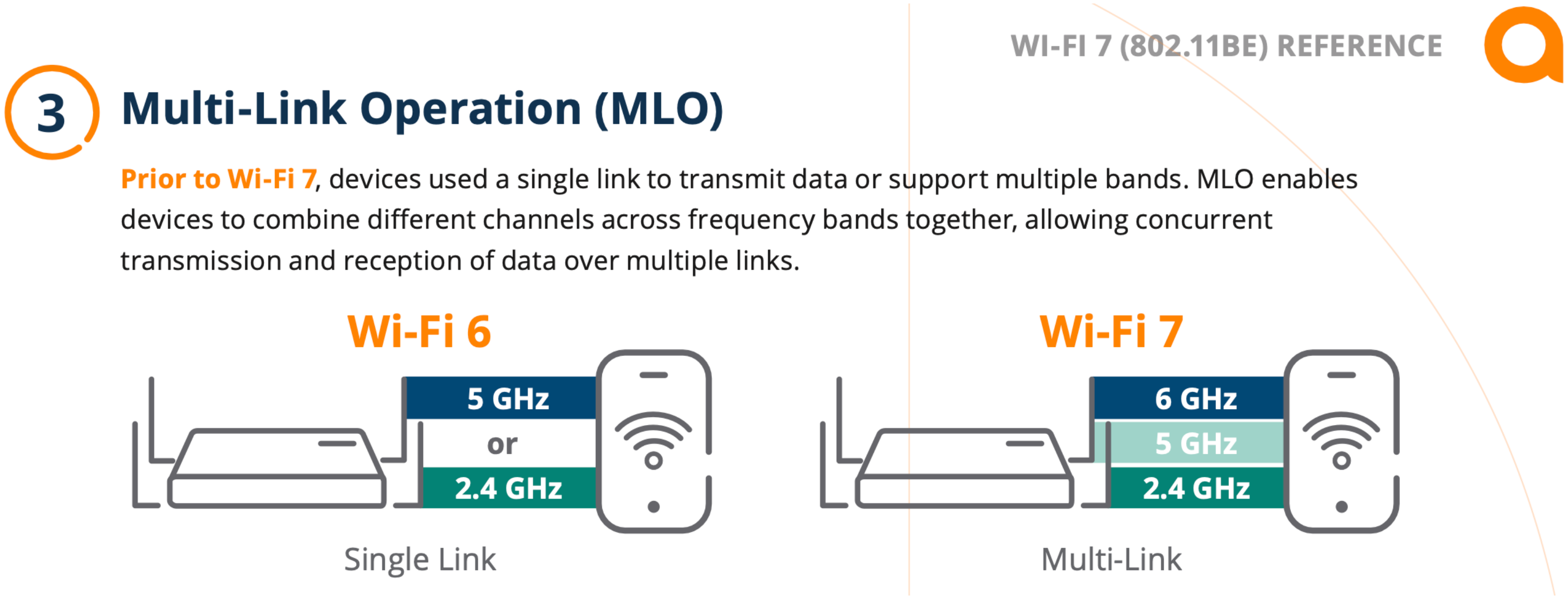


2 4K QAM

20% higher transmission rates than Wi-Fi 6’s 1024-QAM and higher transmission rate enables higher transmission efficiency.

Source: https://www.arubanetworks.com/resource/wi-fi-7-reference-guide/

Wi-Fi 7



WI-FI 7 (802.11BE) REFERENCE

3 Multi-Link Operation (MLO)

Prior to Wi-Fi 7, devices used a single link to transmit data or support multiple bands. MLO enables devices to combine different channels across frequency bands together, allowing concurrent transmission and reception of data over multiple links.

Wi-Fi 6
5 GHz
or
2.4 GHz
Single Link
Wi-Fi 7
6 GHz
5 GHz
2.4 GHz
Multi-Link

Source: https://www.arubanetworks.com/resource/wi-fi-7-reference-guide/

Wi-Fi 7 APs with MLO are still rare

- Found TP-Link EAP773 with Wi-Fi 7, MLO, and WPA-Enterprise to do my first tests

Turns out it does MLO on 5 + 6 Ghz, and does not allow AES CCNP-128 on MLO 🤦‍♂️

Wi-Fi 7 MLO types

- Multiple MLO operation modes mixing (2.4,) 5 and 6 Ghz

MLO type	
SLSR	Single-link, single-radio
(E-)MLSR	**(Enhanced) Multi-link, single-radio** (with reduced function radio to choose link)
MLMR Non-STR	Multi-link, multi-radio (concurrent) (coordinates synchronous transmission across bands)
MLMR STR	Multi-link, multi-radio (concurrent), Simultaneous Transmit and Receive (STR) (sufficient isolation between links, no interference)

- One Wi-Fi 7 device tested (S24 Ultra), unsure if it did MLO but it was faster than just 6Ghz

So… client side support

Device	SSID with 2.4 + 5 + 6 GHz	SSID with 5 + 6 GHz
Google Pixel 8	2.4 + 5 GHz MLMR STR 2.4 + 6 GHz MLMR STR	5 + 6 GHz E-MLSR
Samsung S24	2.4 + 5 GHz MLMR STR 2.4 + 6 GHz MLMR STR	**SLO**
One Plus 11	2.4 + 5 GHz MLMR STR 2.4 + 6 GHz MLMR STR	MLMR STR (Data in 6 GHz)
Intel BE200	2.4 + 5 GHz E-MLSR 2.4 + 6 GHz E-MLSR 5.0 + 6 GHz E-MLSR	5 + 6 GHz E-MLSR
Qualcomm FastConnect 7800 Wi-Fi 7 ref adapter	2.4 + 5 GHz MLMR STR 2.4 + 6 GHz MLMR STR 5.0 + 6 GHz MLMR STR	MLMR STR

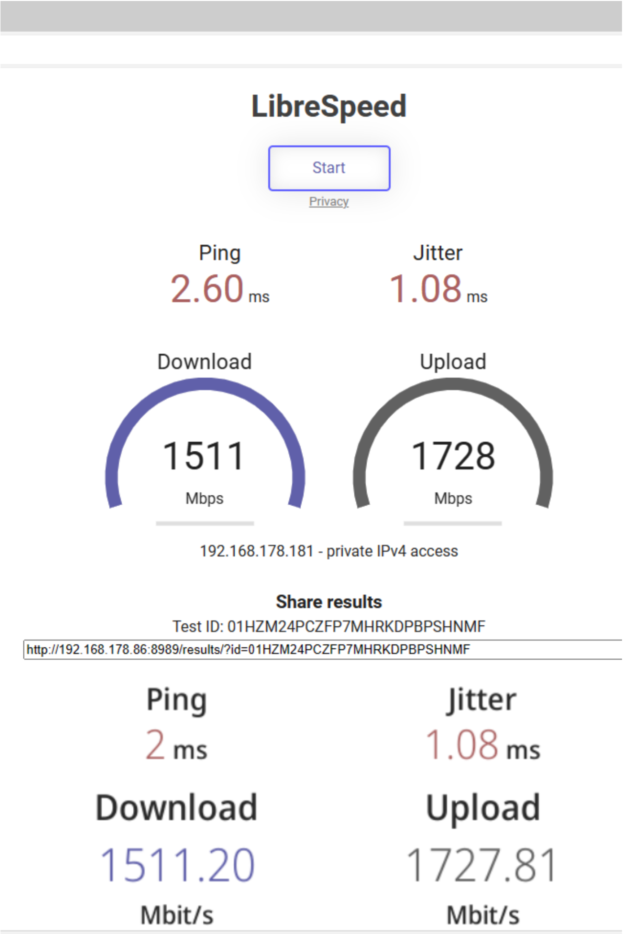
From what I could find

Ok, but – the speed?

Win 11 Wi-Fi 6 client (5 Ghz)

Intel AX201 160MHz

2401,9 Mbps rate



LibreSpeed

Start

Privacy

Ping 2.60 ms

Jitter 1.08 ms

Download 1511 Mbps

Upload 1728 Mbps

192.168.178.181 - private IPv4 access

Share results

Test ID: 01HZM24PCZFP7MHRKDPBPSHNMF

http://192.168.178.86:8989/results/?id=01HZM24PCZFP7MHRKDPBPSHNMF

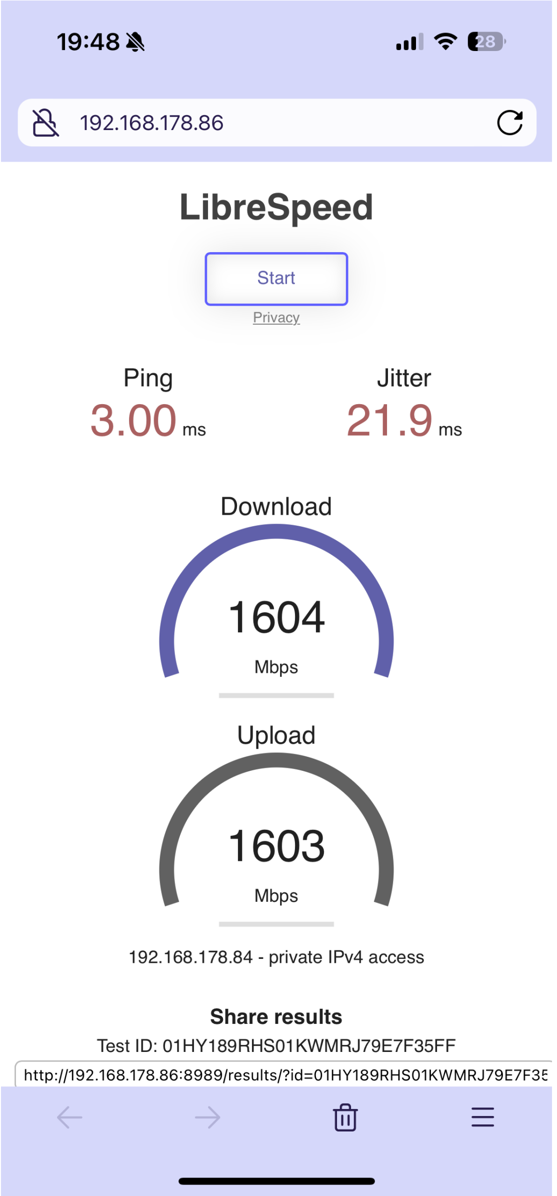
Ping 2 ms

Jitter 1.08 ms

Download 1511.20 Mbit/s

Upload 1727.81 Mbit/s

iPhone 15 Pro (6 Ghz)



19:48

192.168.178.86

LibreSpeed

Start

Privacy

Ping 3.00 ms

Jitter 21.9 ms

Download 1604 Mbps

Upload 1603 Mbps

192.168.178.84 - private IPv4 access

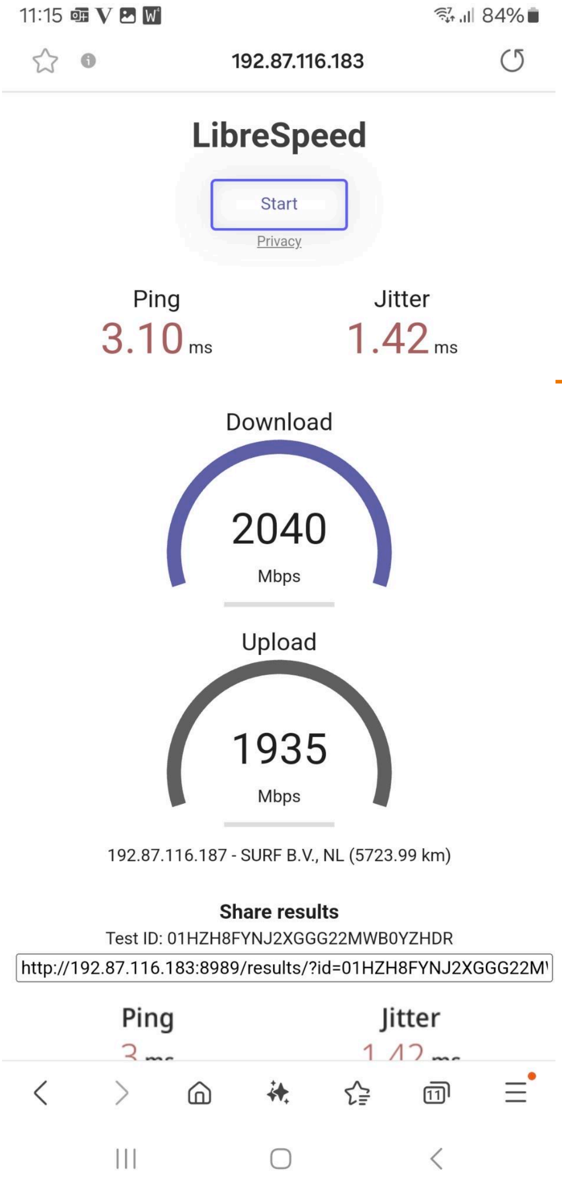
Share results

Test ID: 01HY189RHS01KWMRJ79E7F35FF

http://192.168.178.86:8989/results/?id=01HY189RHS01KWMRJ79E7F35

Samsung S24 Ultra (WiFi 7, **MLO**)

4323,6 Mbps rate



11:15 84%

192.87.116.183

LibreSpeed

Start

Privacy

Ping 3.10 ms

Jitter 1.42 ms

Download 2040 Mbps

Upload 1935 Mbps

192.87.116.187 - SURF B.V., NL (5723.99 km)

Share results

Test ID: 01HZH8FYNJ2XGGG22MWB0YZHDR

http://192.87.116.183:8989/results/?id=01HZH8FYNJ2XGGG22M

Ping 3 ms

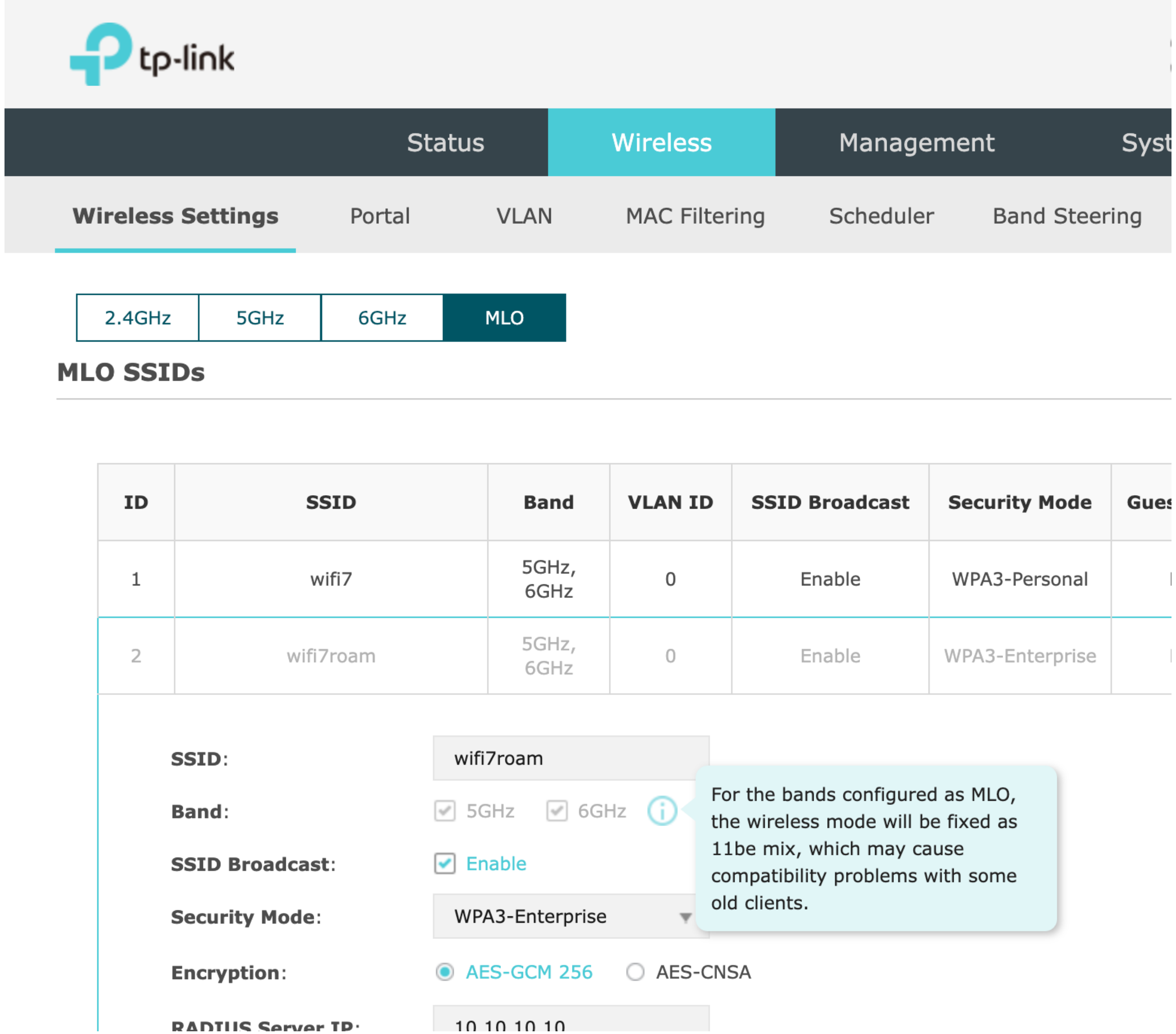
Jitter 1.42 ms

Ok, but – the speed?

- Fastest results from random (VERY unscientific) tests, all conneted to Wi-Fi 7 PSK MLO SSID offering 160 Mhz @5Ghz and 320 Mhz @6Ghz
  (tried to find optimal position/orientation)

Device	Wi-Fi ver/band/rate	Down	Up
Apple iPhone 15 Pro	**WiFi 6e, 6Ghz, 2401 / 2161 Mbps**	**1604**	**1603**
Apple iPhone 13	WiFi 6, 5Ghz, 1201 Mbps	934	542
Apple iPhone 11	WiFi 6, 5Ghz, 1201 Mbps	940	511
Apple iPhone 8	WiFi 5, 5Ghz, 866 Mbps	637	327
Surface Laptop Go 3	WiFi 6 (AX201), 5Ghz (160), 2401 Mbps	1511	1728
Dell Latitude 7430	WiFi 6 (AX211), 6Ghz (160), 2401 Mbps	1128	2017
Samsung S24 Ultra	**WiFi 7, 6Ghz (+5?), 4323,6**	**2040**	**1935**
Google Pixel 5	WiFi 5, 5Ghz, 702 Mbps	603	636
Samsung S10	WiFi 6, 5Ghz, 1201 Mbps	918	741
Acer Chromebook 314	WiFi 6, 5Ghz, 2401 Mbps	1502	1588

Problematic WPA3 support



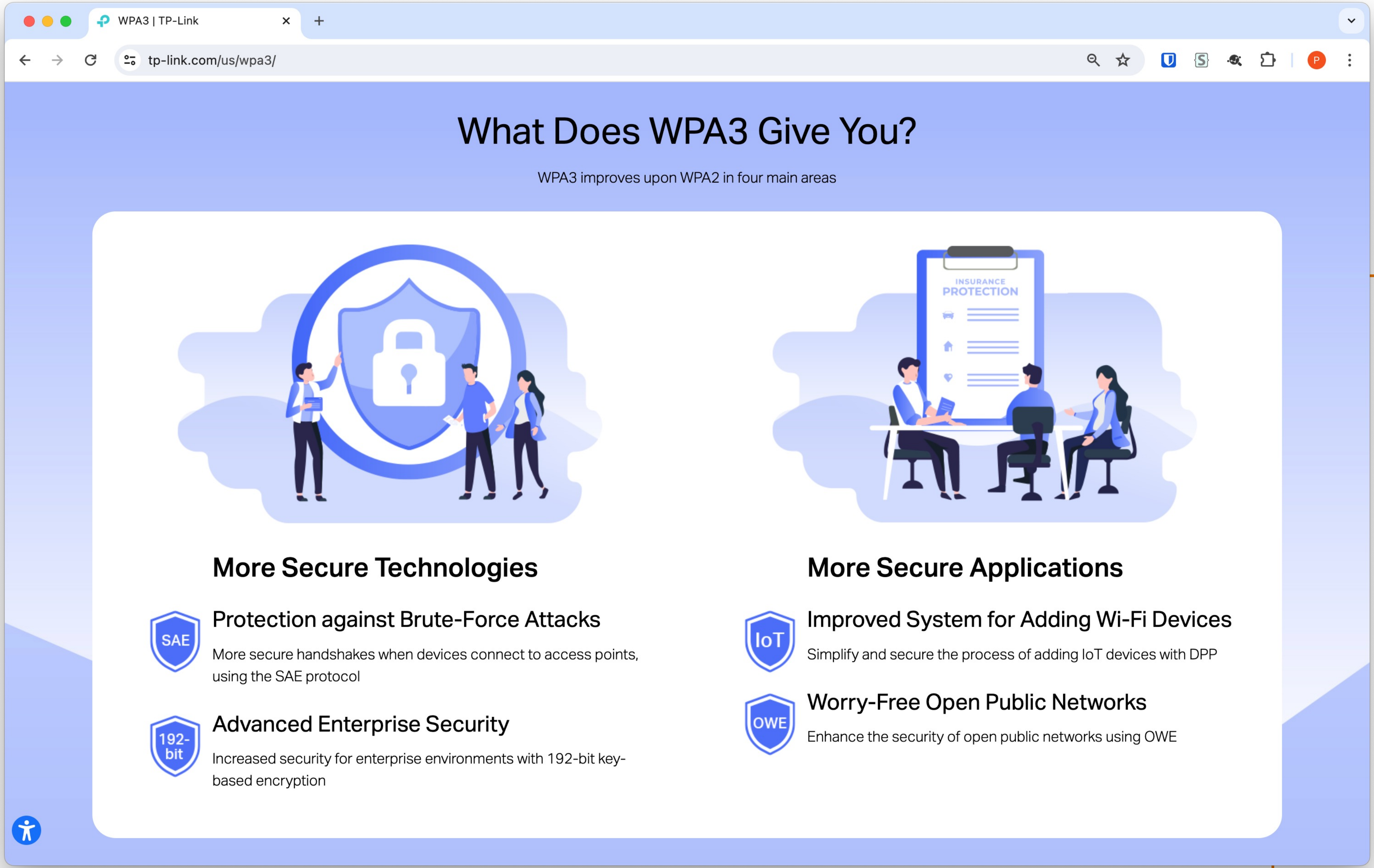
MLO SSIDs

ID	SSID	Band	VLAN ID	SSID Broadcast	Security Mode	Gues
1	wifi7	5GHz, 6GHz	0	Enable	WPA3-Personal	
2	wifi7roam	5GHz, 6GHz	0	Enable	WPA3-Enterprise	

SSID:	wifi7roam
Band:	☑ 5GHz ☑ 6GHz
SSID Broadcast:	☑ Enable
Security Mode:	WPA3-Enterprise
Encryption:	● AES-GCM 256 ○ AES-CNSA
RADIUS Server IP:	10.10.10.10

For the bands configured as MLO, the wireless mode will be fixed as 11be mix, which may cause compatibility problems with some old clients.

This is crazy (and inconsistent)



What Does WPA3 Give You?

WPA3 improves upon WPA2 in four main areas

More Secure Technologies

Protection against Brute-Force Attacks

More secure handshakes when devices connect to access points, using the SAE protocol

Advanced Enterprise Security

Increased security for enterprise environments with 192-bit key-based encryption

More Secure Applications

Improved System for Adding Wi-Fi Devices

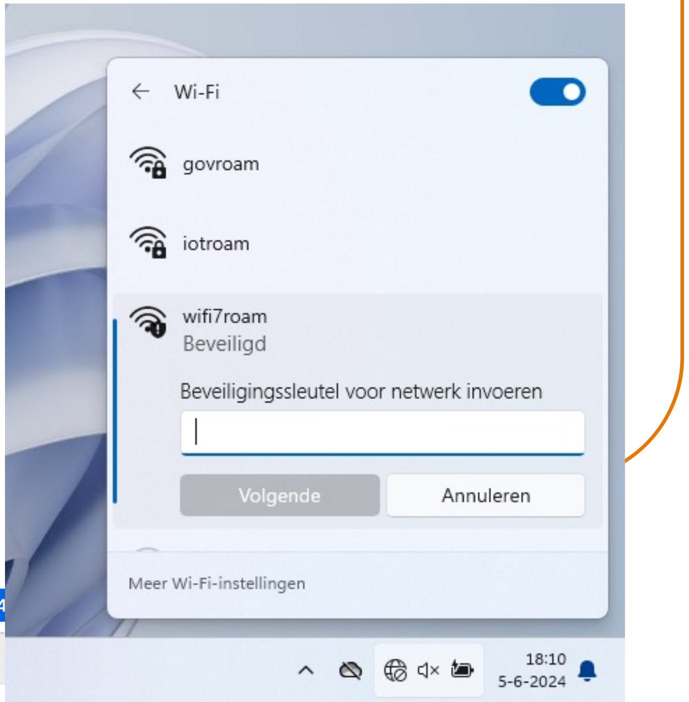
Simplify and secure the process of adding IoT devices with DPP

Worry-Free Open Public Networks

Enhance the security of open public networks using OWE

AES-GCM 256 is terrible

- Windows doesn’t even recognize it being an 802.1x network, asks PSK
- iPhone 15 Pro connected one point, after some upgrades (AP, iOS) it didn’t
- Google Pixel 5 continued to connect
- Almost all other clients didn’t



Wi-Fi

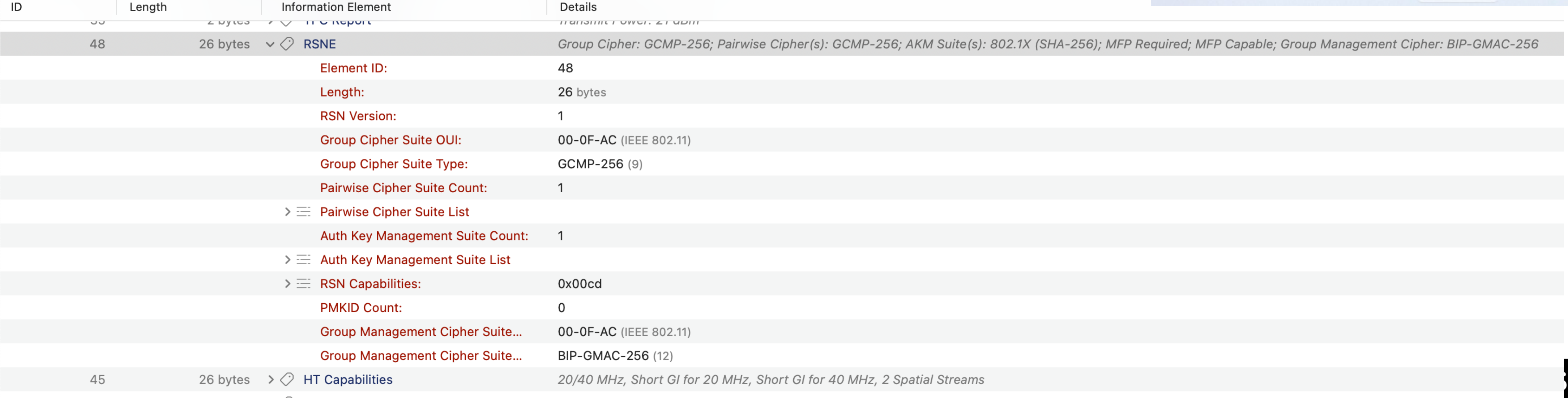
govroam

iotroam

wifi7roam
Beveiligd

Beveiligingssleutel voor netwerk invoeren

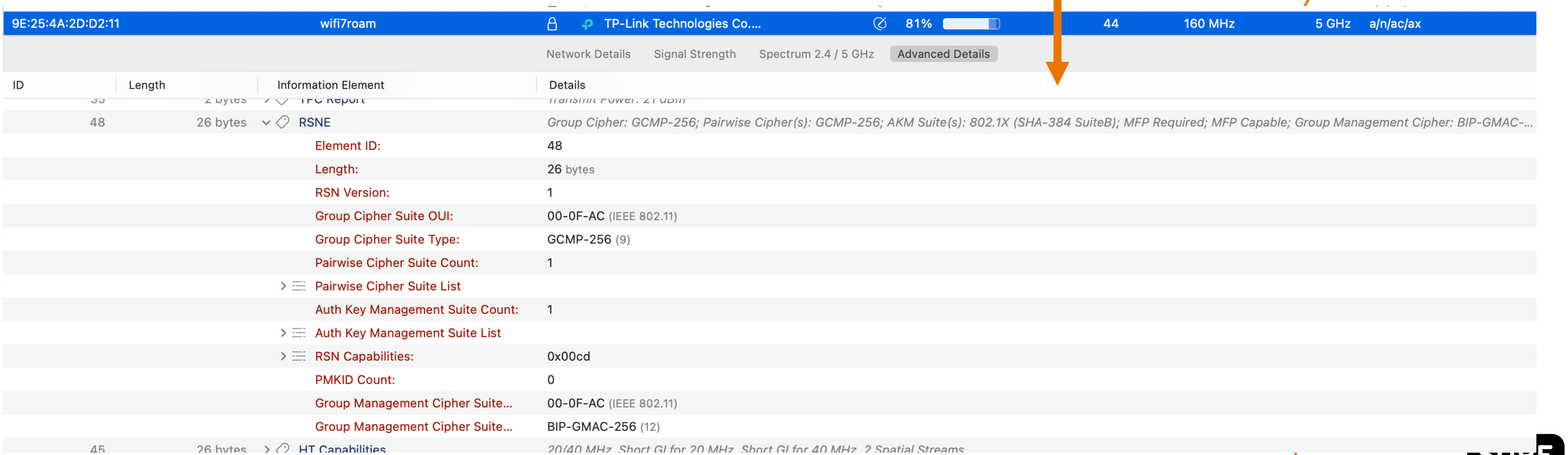
9E:25:4A:2D:D2:11 wifi7roam TP-Link Technologies Co.... 83%



ID	Length	Information Element	Details
48	26 bytes	RSNE	Group Cipher: GCMP-256; Pairwise Cipher(s): GCMP-256; AKM Suite(s): 802.1X (SHA-256); MFP Required; MFP Capable; Group Management Cipher: BIP-GMAC-256
		Element ID:	48
		Length:	26 bytes
		RSN Version:	1
		Group Cipher Suite OUI:	00-0F-AC (IEEE 802.11)
		Group Cipher Suite Type:	GCMP-256 (9)
		Pairwise Cipher Suite Count:	1
		Pairwise Cipher Suite List	
		Auth Key Management Suite Count:	1
		Auth Key Management Suite List	
		RSN Capabilities:	0x00cd
		PMKID Count:	0
		Group Management Cipher Suite...	00-0F-AC (IEEE 802.11)
		Group Management Cipher Suite...	BIP-GMAC-256 (12)
45	26 bytes	HT Capabilities	20/40 MHz, Short GI for 20 MHz, Short GI for 40 MHz, 2 Spatial Streams

AES-CNSA is (different) terrible

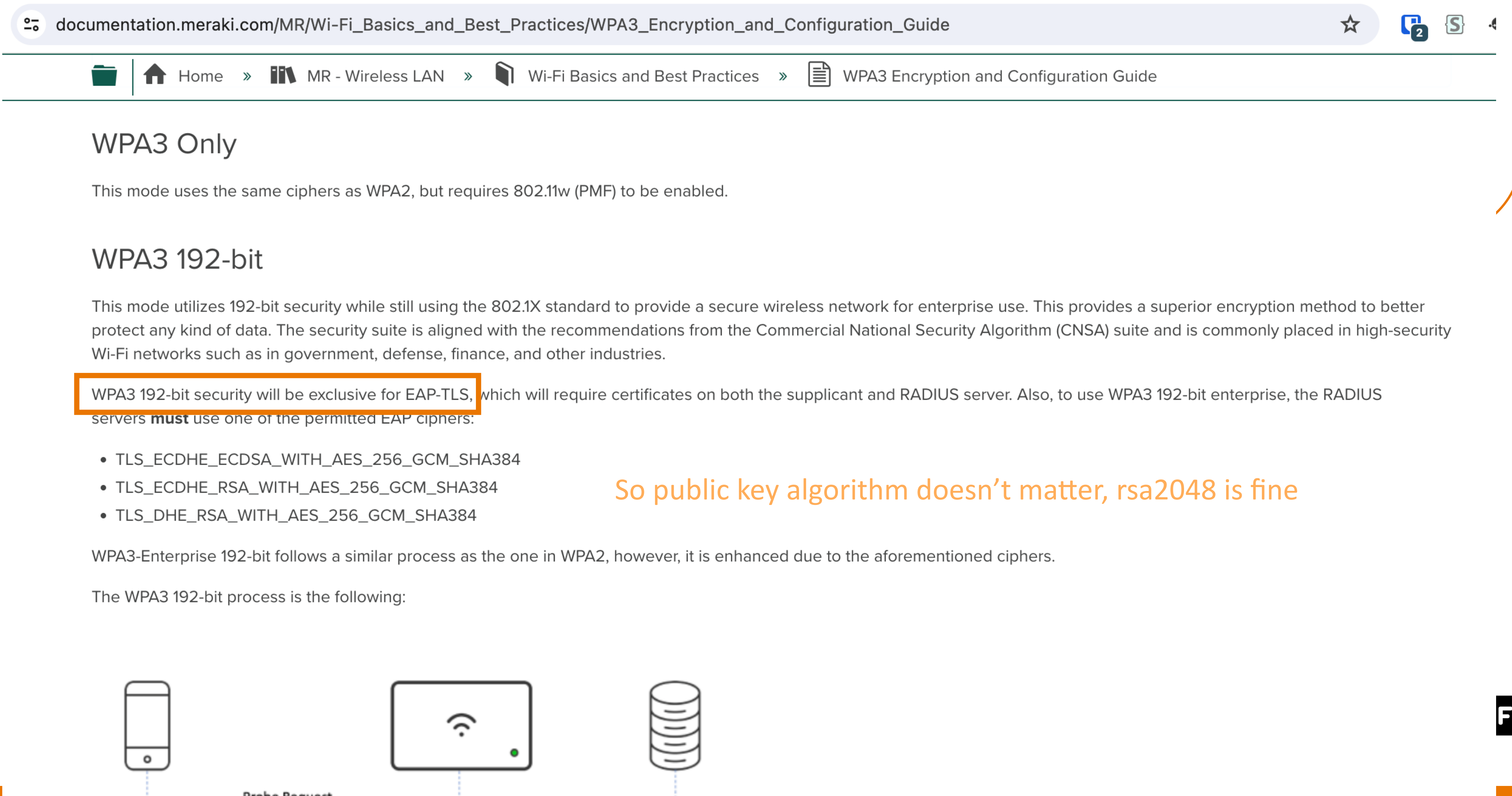
- It works on more devices
- Some clients really really want only EAP-TLS (but it’s up to the client, that’s clear)



9E:25:4A:2D:D2:11 | wifi7roam | TP-Link Technologies Co.... | 81% | 44 | 160 MHz | 5 GHz | a/n/ac/ax

ID	Length	Information Element	Details
35	2 bytes	TPC Report	Transmit Power: 21 dBm
48	26 bytes	RSNE	Group Cipher: GCMP-256; Pairwise Cipher(s): GCMP-256; AKM Suite(s): 802.1X (SHA-384 SuiteB); MFP Required; MFP Capable; Group Management Cipher: BIP-GMAC-...
		Element ID:	48
		Length:	26 bytes
		RSN Version:	1
		Group Cipher Suite OUI:	00-0F-AC (IEEE 802.11)
		Group Cipher Suite Type:	GCMP-256 (9)
		Pairwise Cipher Suite Count:	1
		Pairwise Cipher Suite List	
		Auth Key Management Suite Count:	1
		Auth Key Management Suite List	
		RSN Capabilities:	0x00cd
		PMKID Count:	0
		Group Management Cipher Suite...	00-0F-AC (IEEE 802.11)
		Group Management Cipher Suite...	BIP-GMAC-256 (12)
45	26 bytes	HT Capabilities	20/40 MHz, Short GI for 20 MHz, Short GI for 40 MHz, 2 Spatial Streams

AES-CNSA Meraki documentation



documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/WPA3_Encryption_and_Configuration_Guide

Home » MR - Wireless LAN » Wi-Fi Basics and Best Practices » WPA3 Encryption and Configuration Guide

WPA3 Only

This mode uses the same ciphers as WPA2, but requires 802.11w (PMF) to be enabled.

WPA3 192-bit

This mode utilizes 192-bit security while still using the 802.1X standard to provide a secure wireless network for enterprise use. This provides a superior encryption method to better protect any kind of data. The security suite is aligned with the recommendations from the Commercial National Security Algorithm (CNSA) suite and is commonly placed in high-security Wi-Fi networks such as in government, defense, finance, and other industries.

WPA3 192-bit security will be exclusive for EAP-TLS, which will require certificates on both the supplicant and RADIUS server. Also, to use WPA3 192-bit enterprise, the RADIUS servers **must** use one of the permitted EAP ciphers:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

WPA3-Enterprise 192-bit follows a similar process as the one in WPA2, however, it is enhanced due to the aforementioned ciphers.

The WPA3 192-bit process is the following:

So public key algorithm doesn't matter, rsa2048 is fine

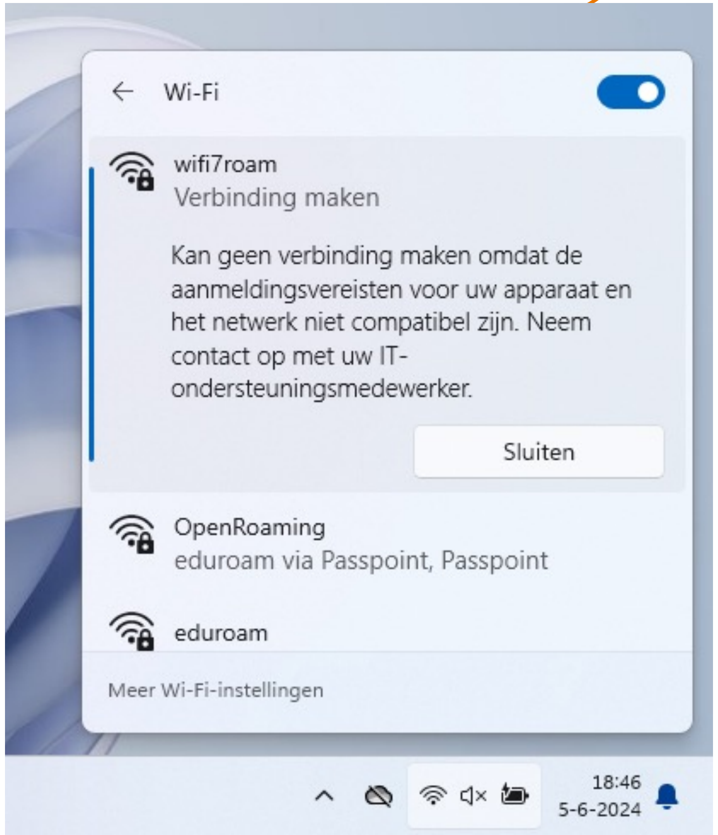
AES-CNSA is different terrible

- Windows really wants EAP-TLS

```
(11) eap: Removing EAP session with state 0xab119cc3abee8520
(11) eap: Previous EAP request found for state 0xab119cc3abee8520, released from the list
(11) eap: Peer sent packet with method EAP NAK (3)
(11) eap: Peer NAK'd indicating it is not willing to continue
(11) eap: Sending EAP Failure (code 4) ID 255 length 4
(11) eap: Failed in EAP select

DEBUG: EAP result: 1, EAP NAK 0 from peer: No proposed alternative
```

- Android insists on EAP-TLS, but on older devices it still doesn’t work



wifi7roam
Verbinding maken

Kan geen verbinding maken omdat de aanmeldingsvereisten voor uw apparaat en het netwerk niet compatibel zijn. Neem contact op met uw IT-ondersteuningsmedewerker.

OpenRoaming
eduroam via Passpoint, Passpoint

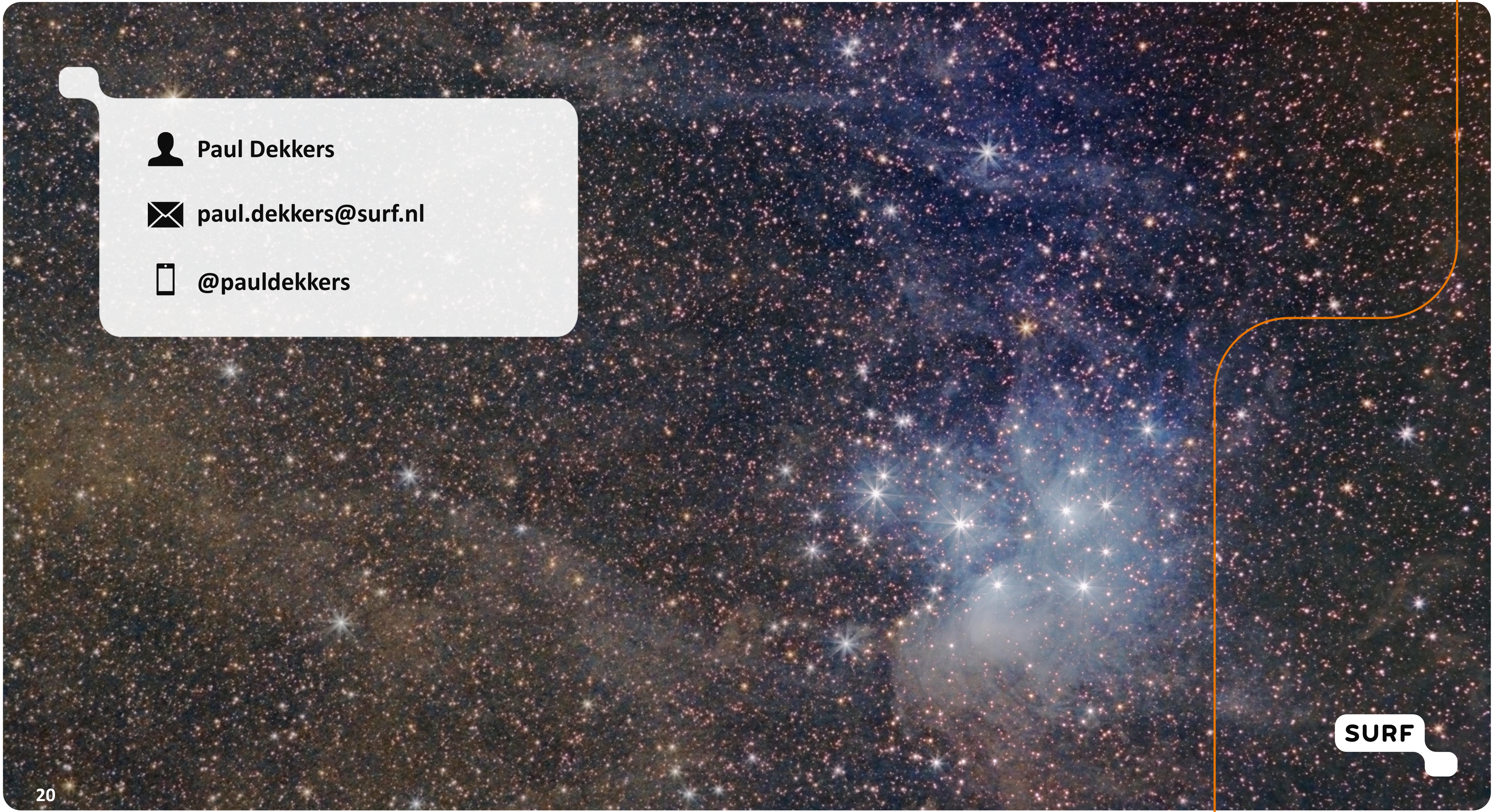
eduroam

	TP-Link EAP773			Meraki MR22
	Wi-Fi 7 MLO WPA3-SAE	Wi-Fi 7 MLO 1X AES-GCM 256	Wi-Fi 7 MLO 1X AES-CNSA	Wi-Fi 5 WPA3 CCMP-128 SHA256
iPhone 15 Pro, iOS 17.5.1	✅	✅ / ❓	✅	✅
iPhone 13, iOS 17.5.1	✅	❌	✅	✅
iPhone 11, iOS 17.5	✅	❌	✅	✅
iPad Air 2022, iOS 17.5	✅	❌	✅	✅
iPad 2018, iOS 17.4.1	✅	❌	❌	✅
iPhone 8, iOS 16.7.7	✅	❌	❌	✅
iPhone SE 2016, iOS 15.8.2	❌	❌	❌	✅
MacBook Pro 2021, Sonoma 14.4.1	✅	❌	✅	✅
iMac intel 2019, Ventura 13.6.4	✅	❌	❌	✅
Surface Go, Windows 11 Home, 22.230.0.8	✅	❌	⚠ only TLS	✅
Dell Latitude 7430, Windows 11	✅	❌	⚠ only TLS	✅
Pixel 5, Android 14	✅	✅	❌ only TLS	✅
Samsung S10, Android 12	✅	❌	❌	✅
Samsung S7, Android 8	❌	❌	❌	✅
Samsung S4, Android 11	❌	❌	❌	✅
Acer Chromebook 314	✅	❌	❌	✅

Conclusion

- WiFi 7 = 🌪️ and potential to be stable and efficient
- MLO and eduroam = 🤷‍♂️
- AES-CNSA (WPA3-E & 192bit) and eduroam = ❌

  unless 🍏👨‍💻 🤷‍♂️
- AES-GCM 256 and eduroam = ❌
- WPA3-Enterprise with CCMP-128 (SHA-256) = 👍



👤 **Paul Dekkers**

✉ **paul.dekkers@surf.nl**

📱 **@pauldekkers**