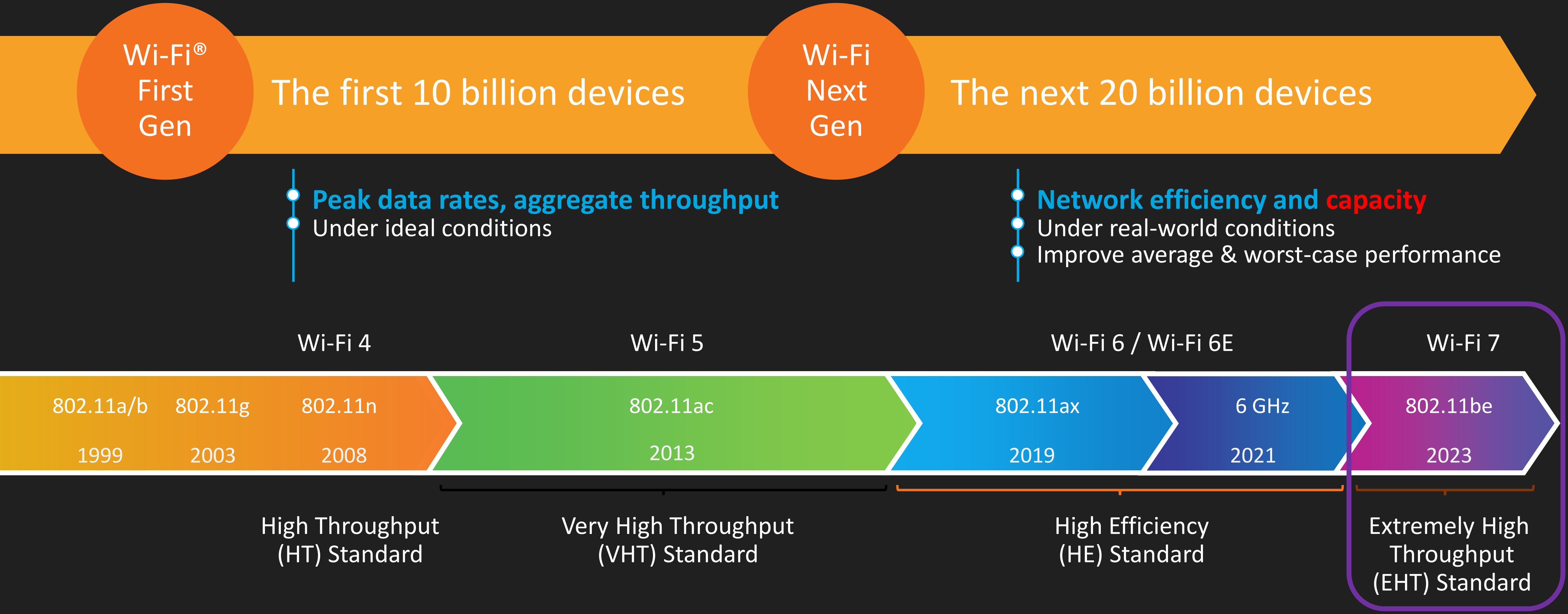
Wi-Fi 7的資安強化與挑戰

蘇俊銘 Kevin Su

RUCKUS Taiwan Sales Team

技術顧問

Wi-Fi的進程



Wi-Fi® First Gen

The first 10 billion devices

Wi-Fi Next Gen

The next 20 billion devices

- **Peak data rates, aggregate throughput**
- Under ideal conditions

- **Network efficiency and capacity**
- Under real-world conditions
- Improve average & worst-case performance

Wi-Fi 4			Wi-Fi 5	Wi-Fi 6 / Wi-Fi 6E		Wi-Fi 7
802.11a/b	802.11g	802.11n	802.11ac	802.11ax	6 GHz	802.11be
1999	2003	2008	2013	2019	2021	2023

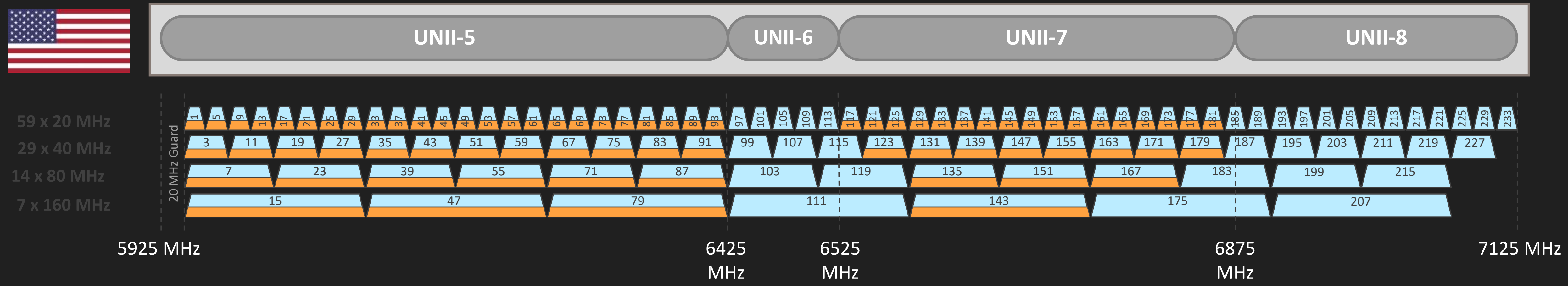
High Throughput (HT) Standard

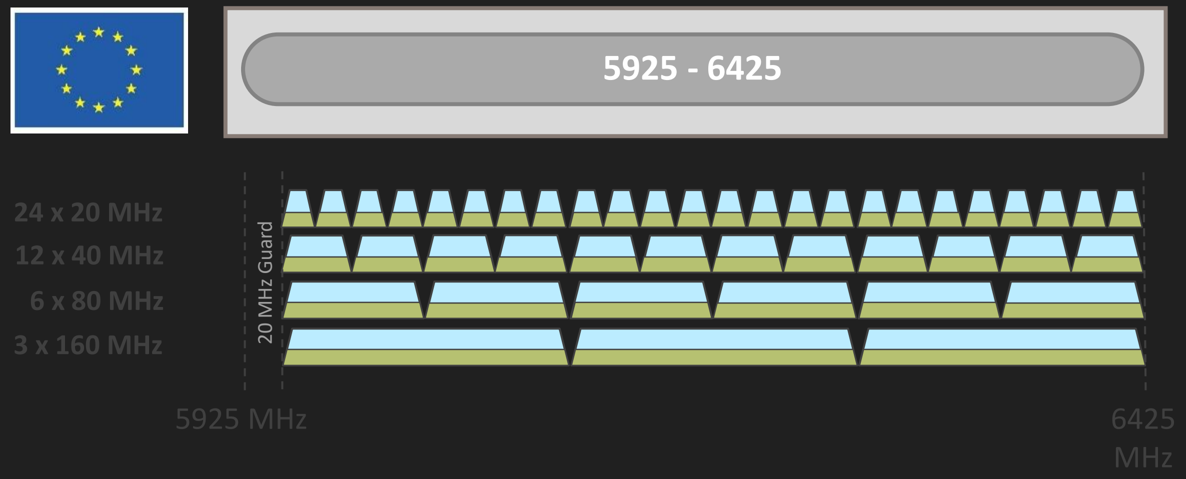
Very High Throughput (VHT) Standard

High Efficiency (HE) Standard

Extremely High Throughput (EHT) Standard

6 GHz 頻道





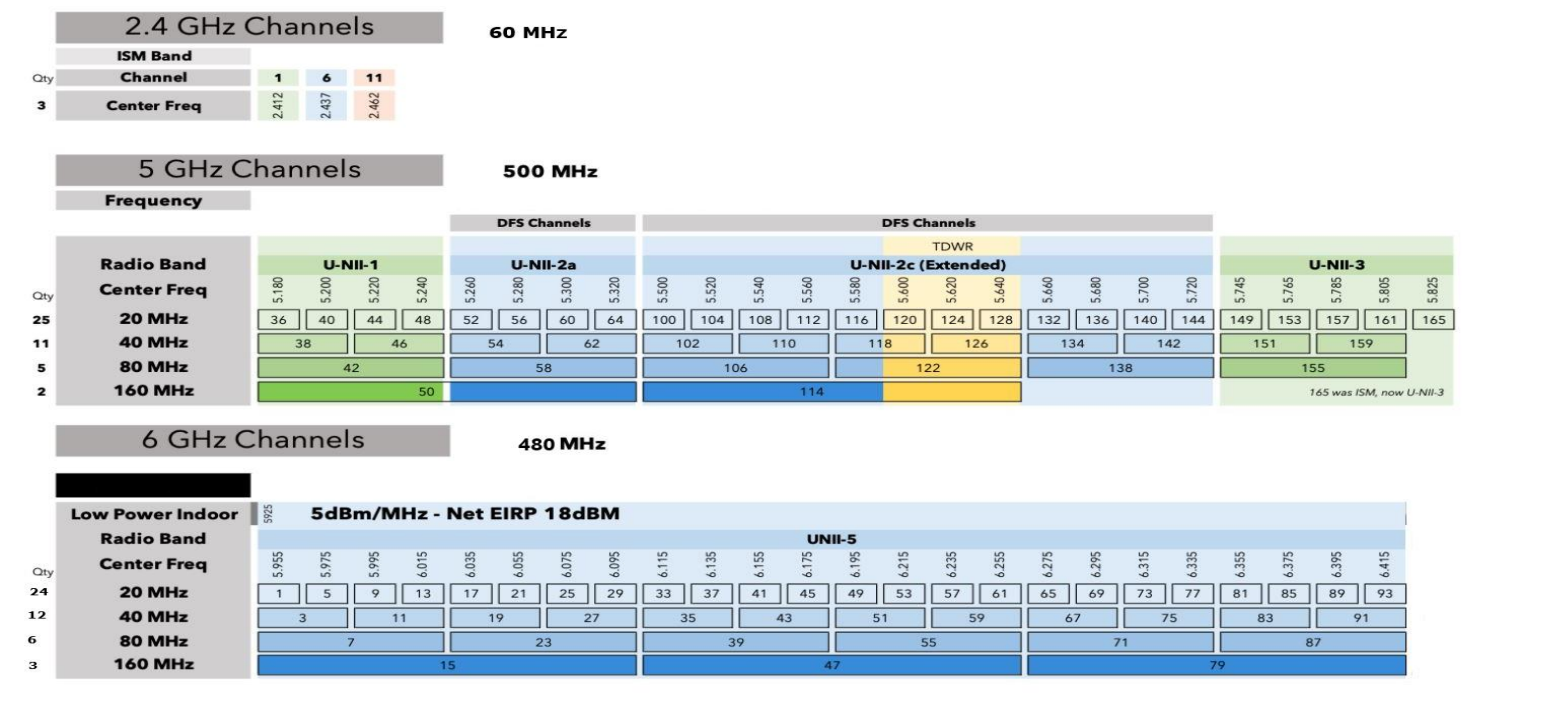
🟦 = Low Power Indoor (LPI) Only

🟧 = LPI & Automatic Frequency Coordination (AFC)

🟩 = LPI & Very Lower Power (VLP)

Source: IEEE Standards Overview

台灣可使用的Wi-Fi頻道列表



2.4 GHz Channels

60 MHz

Qty	ISM Band			
	Channel	1	6	11
3	Center Freq	2.412	2.437	2.462

5 GHz Channels

500 MHz

Frequency

						DFS Channels				DFS Channels																
															TDWR											
	Radio Band	U-NII-1				U-NII-2a				U-NII-2c (Extended)												U-NII-3				
Qty	Center Freq	5.180	5.200	5.220	5.240	5.260	5.280	5.300	5.320	5.500	5.520	5.540	5.560	5.580	5.600	5.620	5.640	5.660	5.680	5.700	5.720	5.745	5.765	5.785	5.805	5.825
25	20 MHz	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	144	149	153	157	161	165
11	40 MHz	38		46		54		62		102		110		118		126		134		142		151		159		
5	80 MHz	42				58				106				122				138				155				
2	160 MHz	50								114												*165 was ISM, now U-NII-3*				

6 GHz Channels

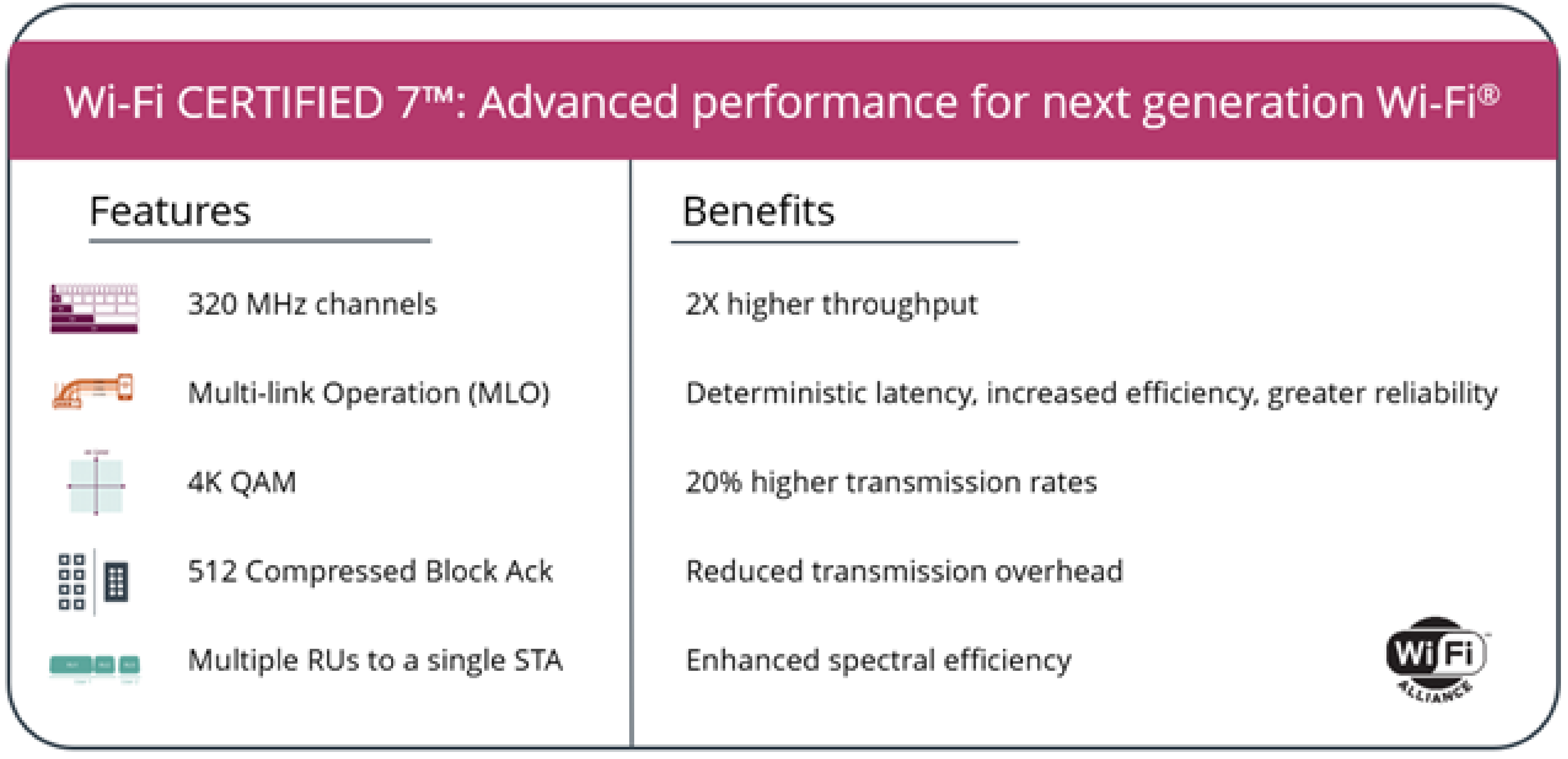
480 MHz

[redacted]

	Low Power Indoor	5925	5dBm/MHz - Net EIRP 18dBM																						
	Radio Band	UNII-5																							
Qty	Center Freq	5.955	5.975	5.995	6.015	6.035	6.055	6.075	6.095	6.115	6.135	6.155	6.175	6.195	6.215	6.235	6.255	6.275	6.295	6.315	6.335	6.355	6.375	6.395	6.415
24	20 MHz	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61	65	69	73	77	81	85	89	93
12	40 MHz	3		11		19		27		35		43		51		59		67		75		83		91	
6	80 MHz	7				23				39				55				71				87			
3	160 MHz	15								47								79							

友訊代理 必屬專業

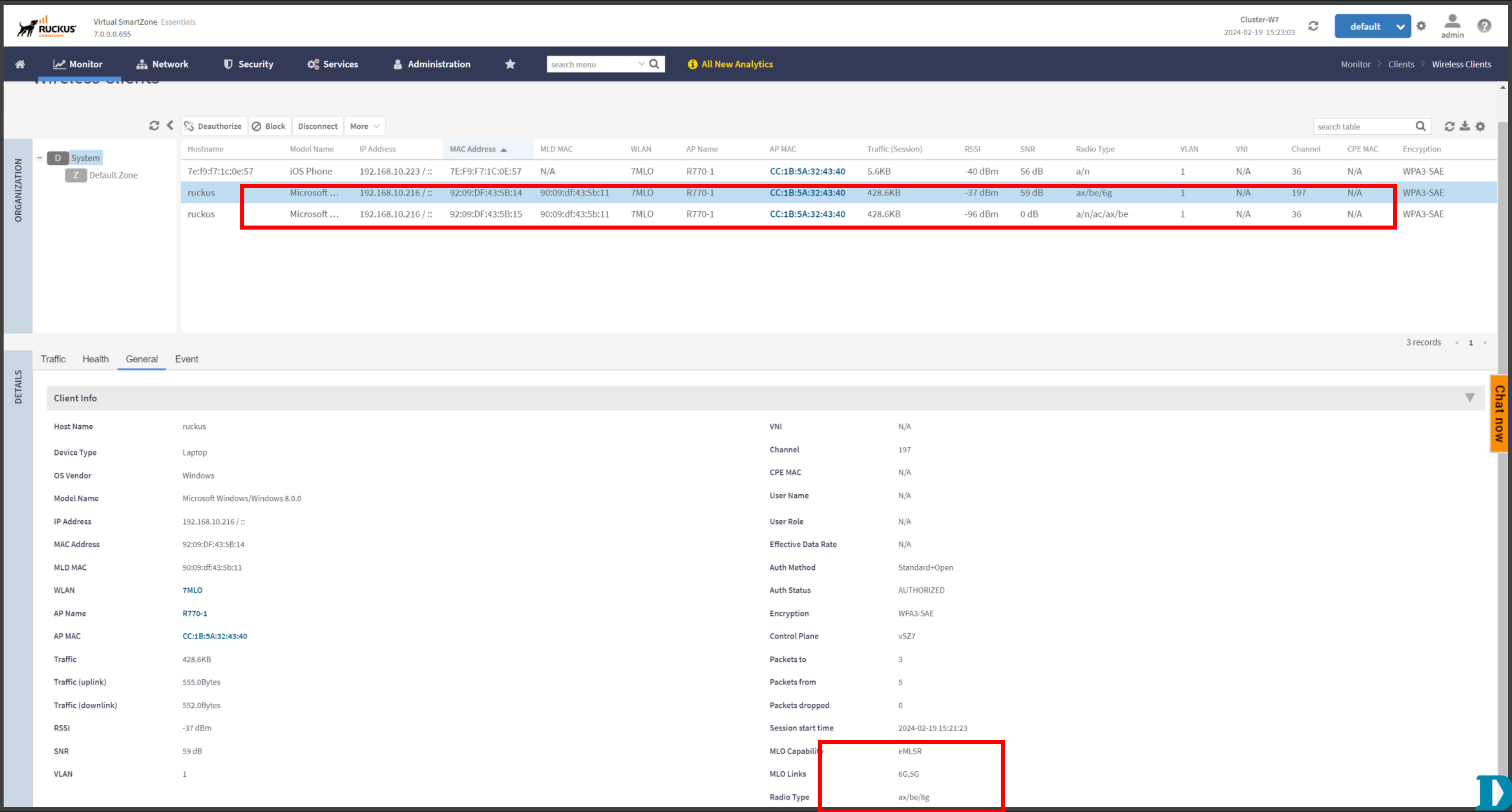
Wi-Fi 7 主要的進階功能



Wi-Fi CERTIFIED 7™: Advanced performance for next generation Wi-Fi®

Features	Benefits
320 MHz channels	2X higher throughput
Multi-link Operation (MLO)	Deterministic latency, increased efficiency, greater reliability
4K QAM	20% higher transmission rates
512 Compressed Block Ack	Reduced transmission overhead
Multiple RUs to a single STA	Enhanced spectral efficiency

MLO



Virtual SmartZone Essentials
7.0.0.0.655

Cluster-W7
2024-02-19 15:23:03

Hostname	Model Name	IP Address	MAC Address ▲	MLD MAC	WLAN	AP Name	AP MAC	Traffic (Session)	RSSI	SNR	Radio Type	VLAN	VNI	Channel	CPE MAC	Encryption
7e:f9:f7:1c:0e:57	iOS Phone	192.168.10.223 / ::	7E:F9:F7:1C:0E:57	N/A	7MLO	R770-1	CC:1B:5A:32:43:40	5.6KB	-40 dBm	56 dB	a/n	1	N/A	36	N/A	WPA3-SAE
ruckus	Microsoft ...	192.168.10.216 / ::	92:09:DF:43:5B:14	90:09:df:43:5b:11	7MLO	R770-1	CC:1B:5A:32:43:40	428.6KB	-37 dBm	59 dB	ax/be/6g	1	N/A	197	N/A	WPA3-SAE
ruckus	Microsoft ...	192.168.10.216 / ::	92:09:DF:43:5B:15	90:09:df:43:5b:11	7MLO	R770-1	CC:1B:5A:32:43:40	428.6KB	-96 dBm	0 dB	a/n/ac/ax/be	1	N/A	36	N/A	WPA3-SAE

3 records « 1 »

Traffic | Health | General | Event

Client Info

Host Name	ruckus	VNI	N/A
Device Type	Laptop	Channel	197
OS Vendor	Windows	CPE MAC	N/A
Model Name	Microsoft Windows/Windows 8.0.0	User Name	N/A
IP Address	192.168.10.216 / ::	User Role	N/A
MAC Address	92:09:DF:43:5B:14	Effective Data Rate	N/A
MLD MAC	90:09:df:43:5b:11	Auth Method	Standard+Open
WLAN	7MLO	Auth Status	AUTHORIZED
AP Name	R770-1	Encryption	WPA3-SAE
AP MAC	CC:1B:5A:32:43:40	Control Plane	vSZ7
Traffic	428.6KB	Packets to	3
Traffic (uplink)	555.0Bytes	Packets from	5
Traffic (downlink)	552.0Bytes	Packets dropped	0
RSSI	-37 dBm	Session start time	2024-02-19 15:21:23
SNR	59 dB	MLO Capability	eMLSR
VLAN	1	MLO Links	6G,5G
		Radio Type	ax/be/6g

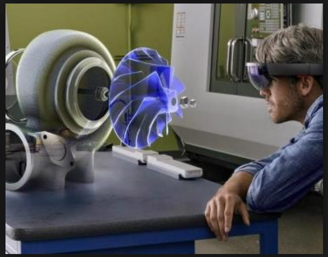
友訊代理 必屬專業

Wi-Fi 7應用案例

- Extended reality (AR/VR)
- Post pandemic Video Conferencing explosion
- Social Gaming & e-Sports
- 8K Streaming
- IoT/Operational Technology

Remote Research

Collaborative 3D design



Arena gaming

Operational Technology - IoT

Operational Technology - Manufacturing

網路需求：

- **Low latency -** affected by:
  - Distance
  - Speed
  - Media Contention
- **High Reliability**
- **High speed**

支援 Wi-Fi 6E 行動裝置

- Apple iPad Pro M2
- Apple iPhone 15

- ASUS ROG Phone 5
- ASUS Zenfone 8 and 8 Flip
- ASUS ROG Phone 5 Ultimate

- Google Pixel 6 and 6 Pro
- Google Pixel 6a
- Google Pixel 7 & Pixel 7 Pro

- Motorola Edge 2022
- Motorola X30 Pro
- Samsung Galaxy Tab S8+ and Tab S8 Ultra
- Samsung Galaxy S21 Ultra
- Samsung Galaxy Z Fold 3 5G
- Samsung Galaxy S22 Plus and S22 Ultra
- Samsung Galaxy S23 & S23 Plus
- Samsung Galaxy S23 Ultra
- Samsung Galaxy Z Fold 4 5G
- Xiaomi Mi 11
- Xiaomi Mi 11 Ultra
- Xiaomi 13 Ultra

支援 Wi-Fi 7 行動裝置

- ASUS ROG Phone 8 & phone 8 pro
- Google Pixel 8 & Pixel 8 Pro
- Samsung Galaxy S24 Ultra
- Xiaomi 13 pro
- Xiaomi 14 & 14 pro
- Oppo Find X7 Ultra & X7

支援 Wi-Fi 6E/7 電腦/筆電

Wi-Fi 6E

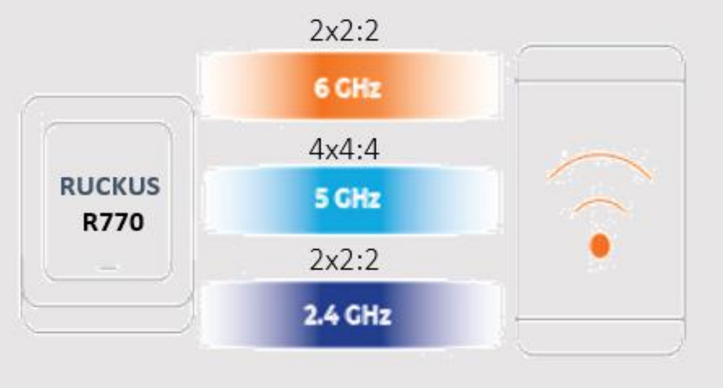
- Apple MacBook Pro (2023)
- Apple Mac Mini M2 (2023)
- Intel AX210 or newer NIC (6GHz is only support on Windows 11)

Wi-Fi 7

- Intel BE200 or newer NIC
- Media Tek MT-7925 or newer NIC
- Qualcomm QCN6274 or QCN9274

RUCKUS R770

High-Density Tri-Band Wi-Fi 7 Indoor Wireless AP with 10 Gigabit Ethernet Backhaul



2.4GHz :	2x2:2 802.11b/g/n/ax/be	689 Mbps
5GHz :	4x4:4 802.11a/n/ac/ax/be	5765 Mbps
6GHz :	2x2:2 802.11ax/be	5765 Mbps.

Max Total Throughput: 12.22 Gbps

Key capabilities

Tri-band (2+5+6): 2x2 (2.4GHz) + 4x4 (5GHz) + 2x2 (6GHz)

- Support Wi-Fi 7 in all three frequency bands
- Max PHY Data Rate: **12.218 Gbps**

Dual-band (2+5): 2x2 (2.4GHz) + 4x4 (5GHz)

- Support Wi-Fi 7 in both frequency bands
- Max PHY Data Rate: **6.454 Gbps**

6GHz Band: LPI, SP and AFC; Indoor geolocation with GPS, 802.11mc, and Mobile App

RUCKUS Advantage: Tx BeamFlex in all three frequency bands; PD-MRC; Smart Mesh

Two Ethernet Ports: 1x 100M/1G/2.5G/5G/10Gbps PoE-In Port and 1x 10M/100M/1Gbps Port

Power Supply: PoE-in (802.3bt) on the 10G Ethernet port & 48V external DC power

IoT: Onboard new IoT Radio: BLE or Zigbee selectable with "Matter“ and “Thread” capable; one USB 2.0 port for additional IoT radio

Security: TPM 2.0; Secure Boot; DPSK3; FIPS 140-3

LED: Single multi-color LED

Environmental: Operating Temperature -10 – 50 C

Dimension: 232.7 mm x 232.7 mm x 59.3 mm

Control & Management :
RUCKUS SmartZone 7.0; RUCKUS One; RUCKUS Unleashed

D-Link
友訊代理 必屬專業

6GHz的無線網路對安全性的提升

新的頻道並沒有將安全性排除在外，任何支援 6GHz 的新設備將被要求在新頻段「僅」支援以下安全標準：

- WPA3：這強制執行強制受保護管理訊框 (PMF/802.11w)
- 機會性密鑰加密 (OWE)：這取代了「開放 SSID」的概念，並允許跨裝置加密，無需任何身份驗證
- 對等實體同時驗證 (SAE)：這發揮了 PSK（Personal）身份驗證方法的作用，但透過改進的加密演算法使其能夠抵抗離線密碼攻擊

無線網路安全面面觀

目的	保護資料		保護網路	保障效能		
方式	使用更安全的認證和加密機制	定位和移除可輕鬆存取無線網路的終端設備	保護您的網路免受簡單或惡意的攻擊	規劃正確的SSID	使用不會降低網路速度的加密機制	找出並移除RF干擾源
哪些方法	Open、Enhanced Open、WEP、WPA、WPA2、WPA3 Personal or Enterprise、Captive Portal。	透過網管或是WIPS機制找出為什麼網路中有這些裝置？必要與否？	啟動受保護的訊框管理機制(PMF)	所有的頻道(2.4/5/6 GHz)都使用相同的SSID?	TKIP or AES	為什麼有干擾在我的網路？如何找出它們？
考量	終端是否支援？	無法移除該裝置時能否套用防火牆規則？	確認終端是否支援？能否正常連線？	6 GHz必須執行WPA3，終端是否支援？	舊設備汰換	需有頻譜分析設備

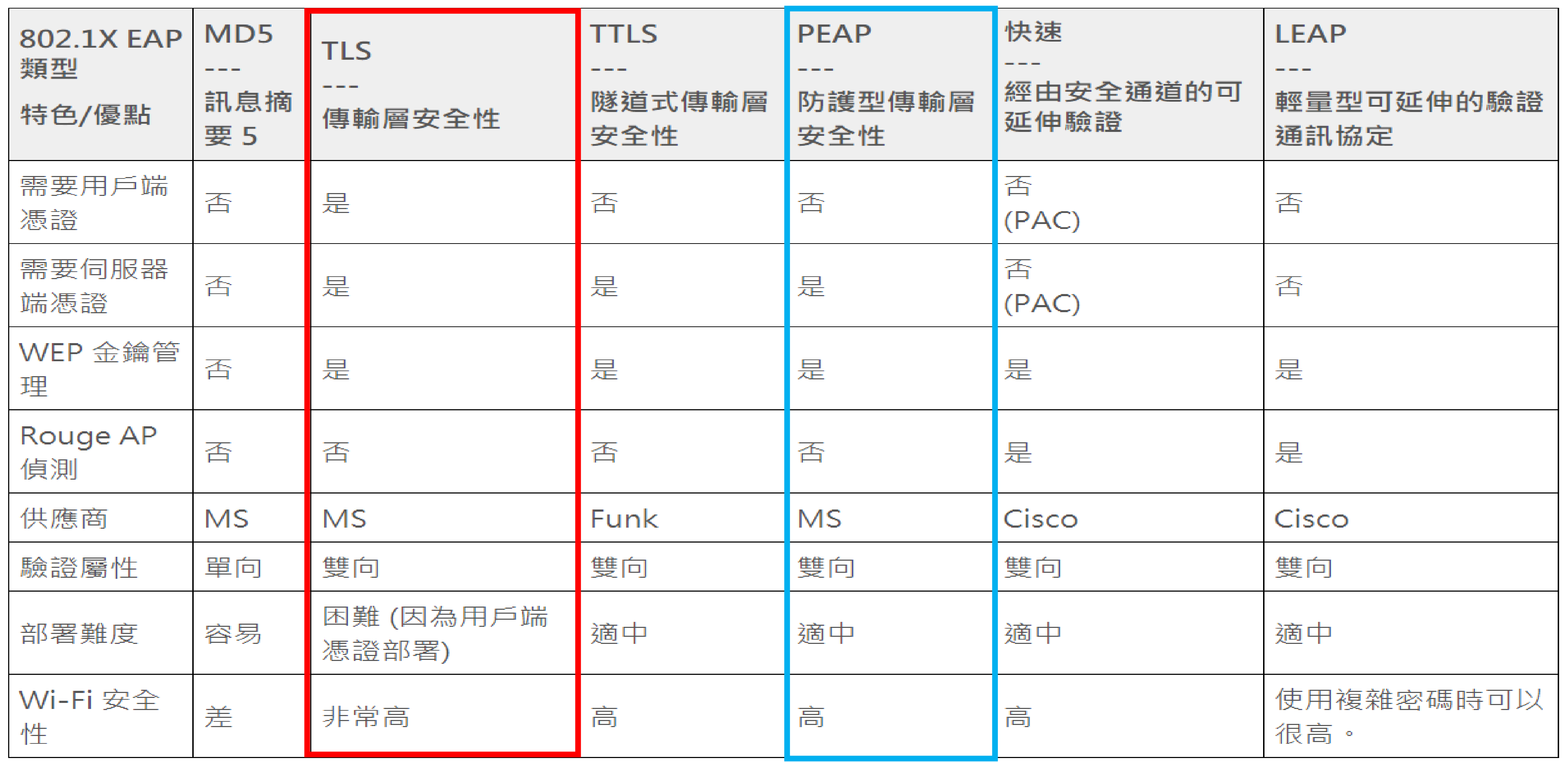
無線加密機制

機制	Open	WEP	WPA	WPA2	Enhanced Open	WPA3
認證	No	Shared Key	Personal：PSK Enterprise：802.1X	Personal：PSK Enterprise：802.1X	No	Personal：SAE Enterprise：802.1X
加密	No	RC4	TKIP/RC4	CCMP/AES (預設) TKIP/RC4 (選項)	OWE	CCMP/AES GCMP/AES
應用	通常結合Captive Portal給訪客使用	已淘汰不建議使用	僅支援802.11 a/b/g 資料率(最高54Mbps) 被WPA2取代，不建議使用	企業網路 使用CCMP/AES，它修正了TKIP/RC4的缺點	提供加密的訪客網路 6GHz強制使用	企業網路 PMF必須啟動 6GHz強制使用

無線認證項目比較

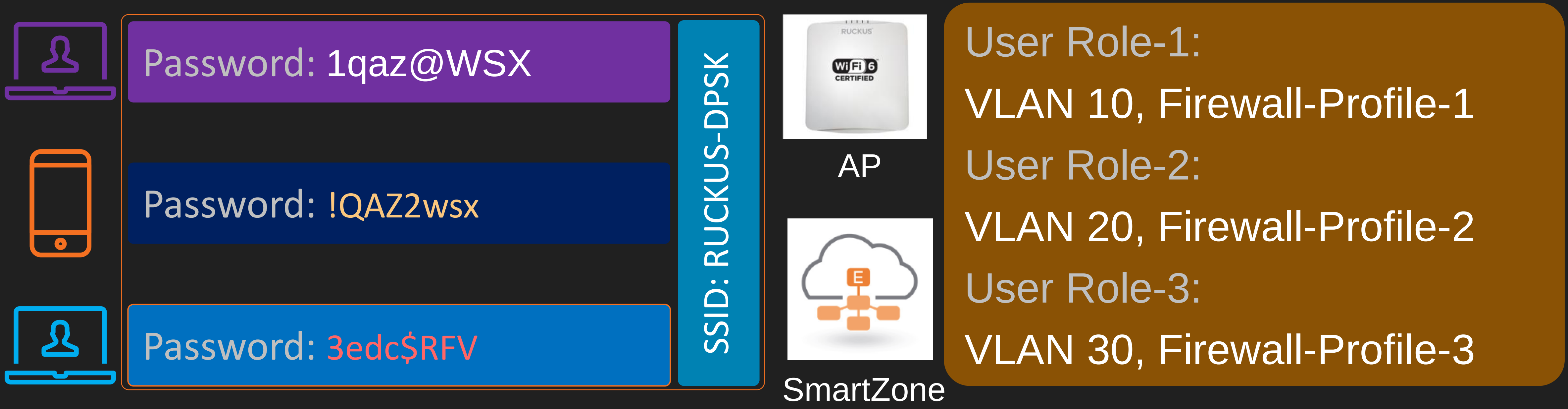
項目	802.1X 認證	MAC地址認證	網頁認證	WPA2/3-DPSK
適用情境	用戶集中且對資訊安全性要求極高的網路	適用於非用戶端裝置的認證，例如印表機和傳真機	訪客或協力廠商存取，並獲取其登入的身分資訊	對資訊安全性要求高的網路，且希望簡單配置
用戶端程式	需要	不需要	瀏覽器	不需要
優點	高安全性	容易設定、無須安裝終端	彈性佈署	容易設定、無須安裝終端程式，可以一組金鑰綁定一個MAC或一組金鑰綁定多組MAC
缺點	佈署不易	管理MAC地址麻煩，不適合大規模佈署，MAC地址容易偽冒不安全	低安全性，如使用HTTPS因憑證因素有無法重導顯示認證網頁的問題	需無線控制器支援或透過外部認證伺服器達成

802.1X 認證類型



802.1X EAP 類型 特色/優點	MD5 --- 訊息摘要 5	TLS --- 傳輸層安全性	TTLS --- 隧道式傳輸層安全性	PEAP --- 防護型傳輸層安全性	快速 --- 經由安全通道的可延伸驗證	LEAP --- 輕量型可延伸的驗證通訊協定
需要用戶端憑證	否	是	否	否	否 (PAC)	否
需要伺服器端憑證	否	是	是	是	否 (PAC)	否
WEP 金鑰管理	否	是	是	是	是	是
Rouge AP 偵測	否	否	否	否	是	是
供應商	MS	MS	Funk	MS	Cisco	Cisco
驗證屬性	單向	雙向	雙向	雙向	雙向	雙向
部署難度	容易	困難 (因為用戶端憑證部署)	適中	適中	適中	適中
Wi-Fi 安全性	差	非常高	高	高	高	使用複雜密碼時可以很高。

動態金鑰 – Dynamic Pre-Shared Key (DPSK) WPA2/WPA3



Password: 1qaz@WSX

Password: !QAZ2wsx

Password: 3edc$RFV

SSID: RUCKUS-DPSK

AP

SmartZone

User Role-1:
VLAN 10, Firewall-Profile-1

User Role-2:
VLAN 20, Firewall-Profile-2

User Role-3:
VLAN 30, Firewall-Profile-3

- 每個使用者都有獨一無二的DPSK
- 當使用者離職或遺失裝置，可以隨時取消該DPSK
- 同一個SSID可以擁有多個User-Role
- DPSK可以用於一群裝置或是綁定特定的裝置MAC
- 可應用於訪客、物聯網設備、Wi-Fi Printer、Wireless IPCAM等

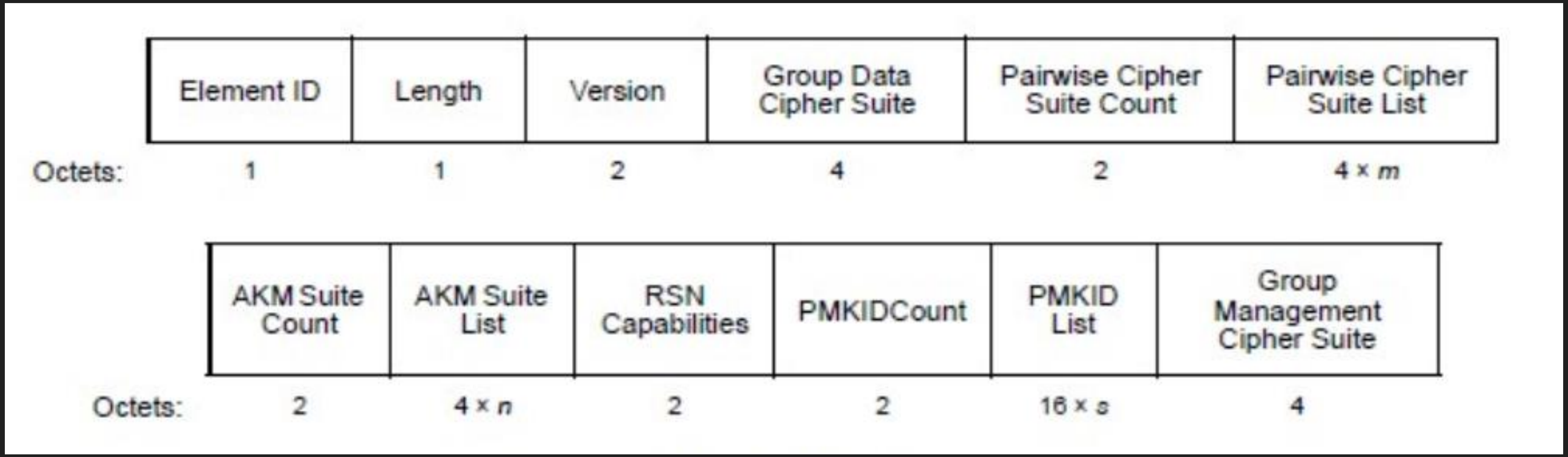
802.11i RSN IE

802.11i Protocol Operation

- WPA2 replaced WPA in 2004, implements the mandatory elements of IEEE 802.11i.
- This standard specifies security mechanisms for wireless networks.
- IEEE 802.11i enhances by providing a Robust Security Network (RSN) with two new protocols.

  -> The four-way handshake
  -> The group key handshake

RSN Information Element



	Element ID	Length	Version	Group Data Cipher Suite	Pairwise Cipher Suite Count	Pairwise Cipher Suite List
Octets:	1	1	2	4	2	4 × *m*

	AKM Suite Count	AKM Suite List	RSN Capabilities	PMKIDCount	PMKID List	Group Management Cipher Suite
Octets:	2	4 × *n*	2	2	16 × *s*	4

- The RSN element has an element ID of 48 & present in below different management frames

  1. Beacon frames.(send by AP)

  2. Probe Response frames.(send by AP)

  3. Association Request frames.(send by Client)

  4. Reassociation Request frames (Send by client)

RSN Information Element

Element ID – 48

Length – provides the number of bytes in the RSN Information element

Version – RSN version number – set to 1

Group Cipher Suite – it contains the Organizational Unique Identifier and the type of encryption selected. Default OUI is 00-0F-AC

Pairwise Cipher suite count – indicates the number of pairwise cipher suites supported

Pairwise Cipher suite list – list of different pairwise cipher suites supported

AKM Count – number of Authentication Key Management Suites supported

AKM Suite list – list of Authentication Key Management Suites

RSN Capabilities – provides additional capabilities supported

PMKID Count – The PMKID Count is used in the re-association request frame/FT authentication sequence frames only. It defines the number of Pairwise Master Key Security Association Identifiers in the PMKID List

PMKID List – List of PMKIDs

Group Management Cipher suite – cipher suite selected to protect group addressed robust management frames

Security Issues

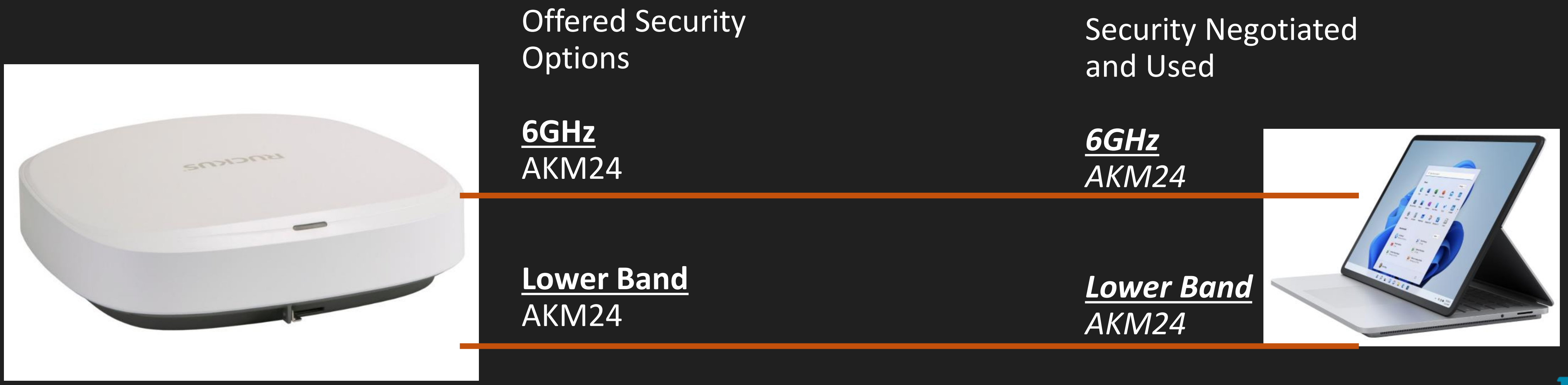
AKMs對照表

AKM values->	AKM2	AKM6	AKM8	AKM24
Security Protocol	WPA/WPA2	WPA2	WPA3	WPA3
SAE Groups	Not used	Not used	Group 19,20	Group 19,20,21
Pairwise cipher	AES-CCMP-128	AES-CCMP-128	AES-CCMP-128, GCMP-256	GCMP-256
Group Data Cipher	AES-CCMP-128	AES-CCMP-128	CCMP-128, GCMP-256	GCMP-256
Group Management Cipher	-	-	BIP-CMAC-128, BIP-GMAC-256	BIP-GMAC-256
MFP Required	No	No	Mandatory	Mandatory
MFP Capable	No	Yes	Mandatory	Mandatory
Hashed Element	NA	NA	Optional, can be 0-hunt n peck, 1- H2E, 2-both	Mandatory

友訊代理 必屬專業

Wi-Fi 7 Configuration – when network is only Wi-Fi 7

- Wi-Fi 7 Certified Devices ***must*** connect using AKM24 on all links.
- Note AKM24 even higher security than legacy WPA3.
- Microsoft insists on this. During MS interop had to support AKM24.
- No Legacy Clients can connect



Offered Security Options

6GHz
AKM24

Lower Band
AKM24

Security Negotiated and Used

6GHz
AKM24

Lower Band
AKM24

Wi-Fi 7 Configuration – with Legacy Devices ideal

- Offer all the security options that legacy devices might need.
- 6GHz Band can only offer WPA3

Offered Security Options

6GHz
AKM8, AKM24

Lower Band
AKM2, AKM8, AKM24

6GHz
AKM8

Wi-Fi 6E Certified Client

Wi-Fi 7 Certified Client

6GHz
AKM24

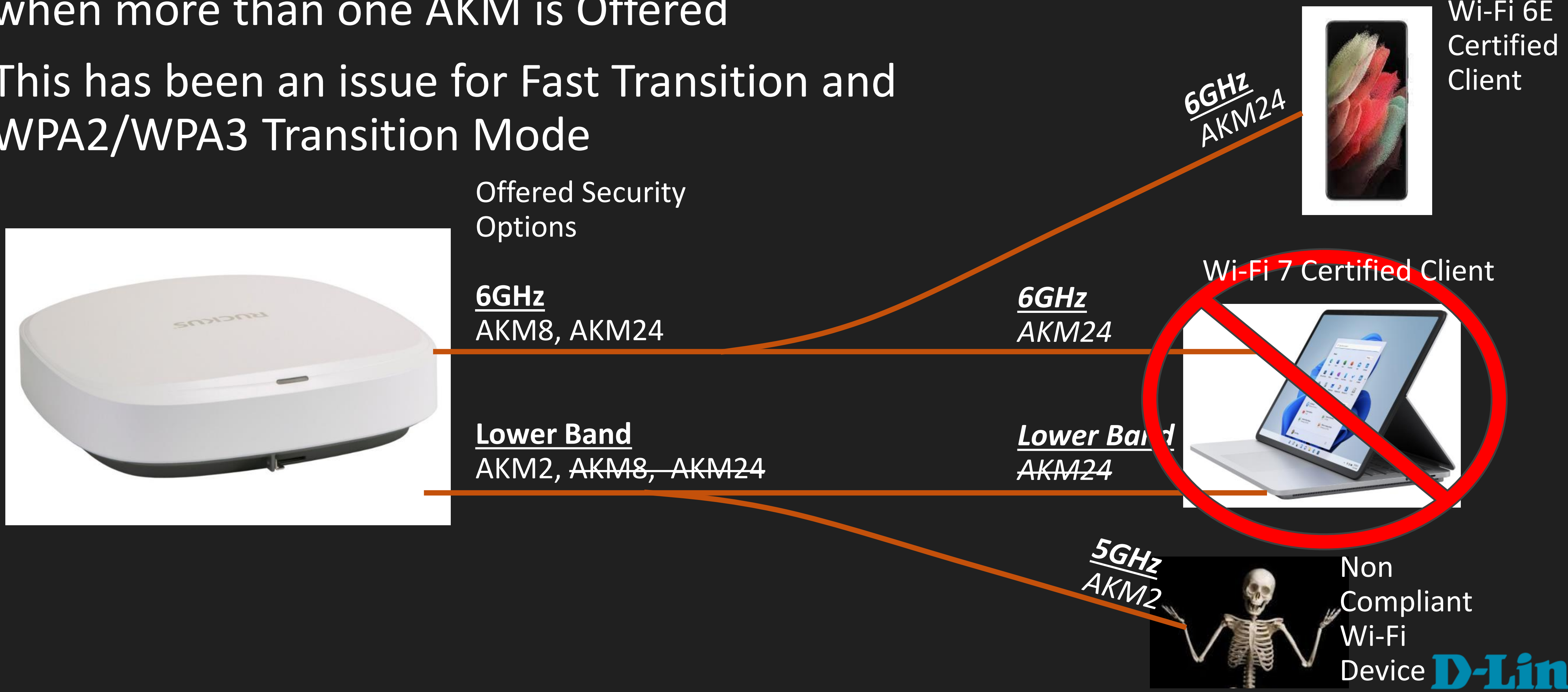
Lower Band
AKM24

5GHz
AKM2

Legacy Wi-Fi Client

Wi-Fi 7 Configuration – with Legacy Devices reality

- Certain non-Compliant Legacy devices cannot connect when more than one AKM is Offered
- This has been an issue for Fast Transition and WPA2/WPA3 Transition Mode



Offered Security Options

6GHz
AKM8, AKM24

Lower Band
AKM2, ~~AKM8, AKM24~~

6GHz
AKM24

Wi-Fi 6E Certified Client

6GHz
AKM24

Wi-Fi 7 Certified Client

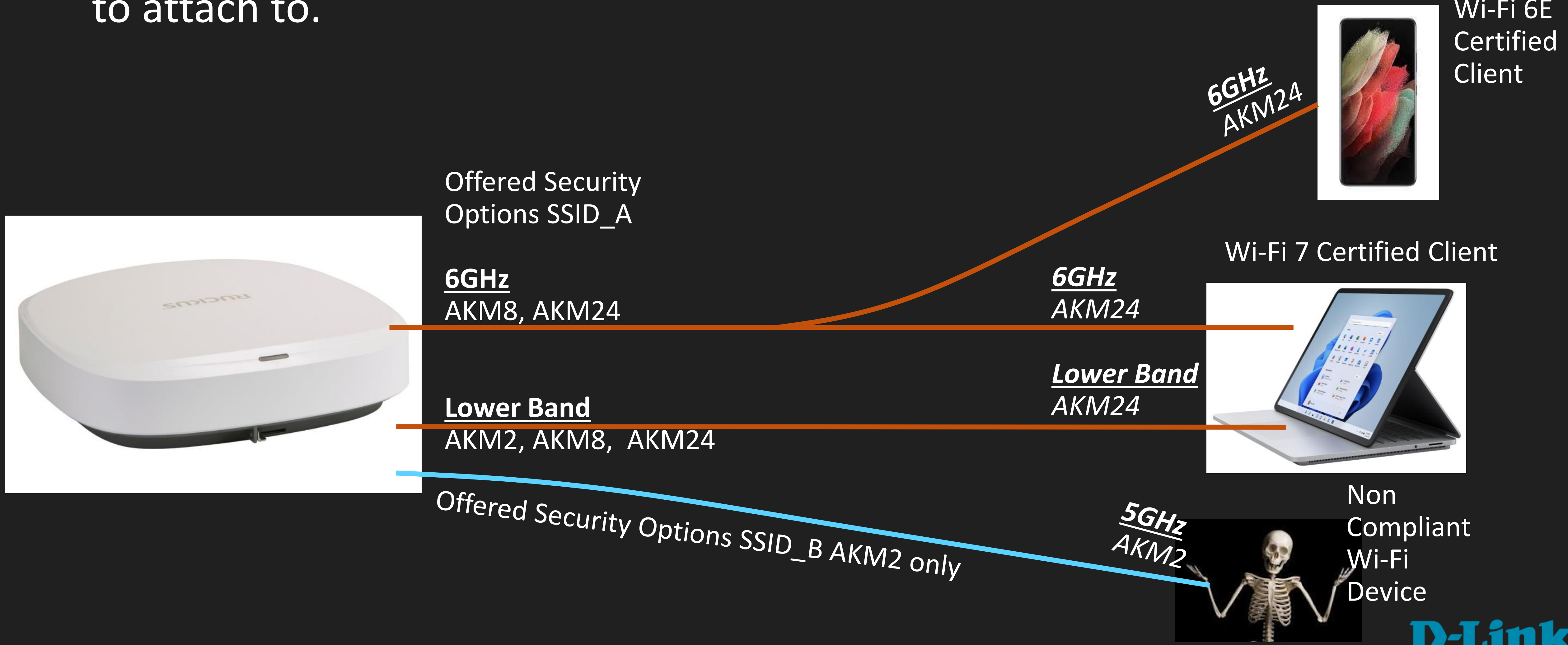
Lower Band
~~*AKM24*~~

5GHz
AKM2

Non Compliant Wi-Fi Device

Wi-Fi 7 Configuration – Multiple SSID Solution

- Create an SSID just for Non-compliant Legacy devices to attach to.



Wi-Fi 6E Certified Client

6GHz
AKM24

Offered Security Options SSID_A

6GHz
AKM8, AKM24

Lower Band
AKM2, AKM8, AKM24

Wi-Fi 7 Certified Client

6GHz
AKM24

Lower Band
AKM24

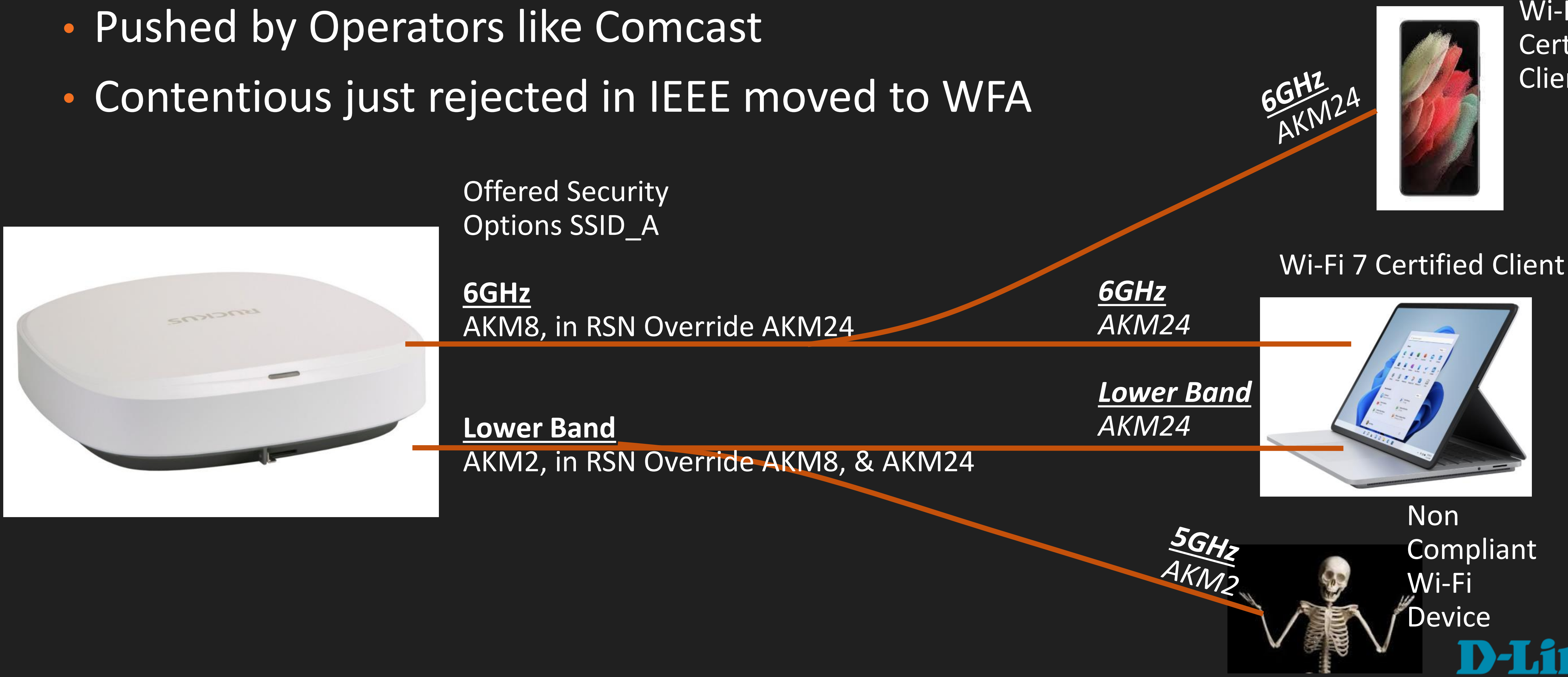
Offered Security Options SSID_B AKM2 only

5GHz
AKM2

Non Compliant Wi-Fi Device

Wi-Fi 7 Configuration – Solution RSN Override IE

- Additional security options appear in RSN Override IE
- Pushed by Operators like Comcast
- Contentious just rejected in IEEE moved to WFA



Offered Security
Options SSID_A

6GHz
AKM8, in RSN Override AKM24

Lower Band
AKM2, in RSN Override AKM8, & AKM24

6GHz
AKM24

Wi-Fi 6E
Certified
Client

Wi-Fi 7 Certified Client

6GHz
AKM24

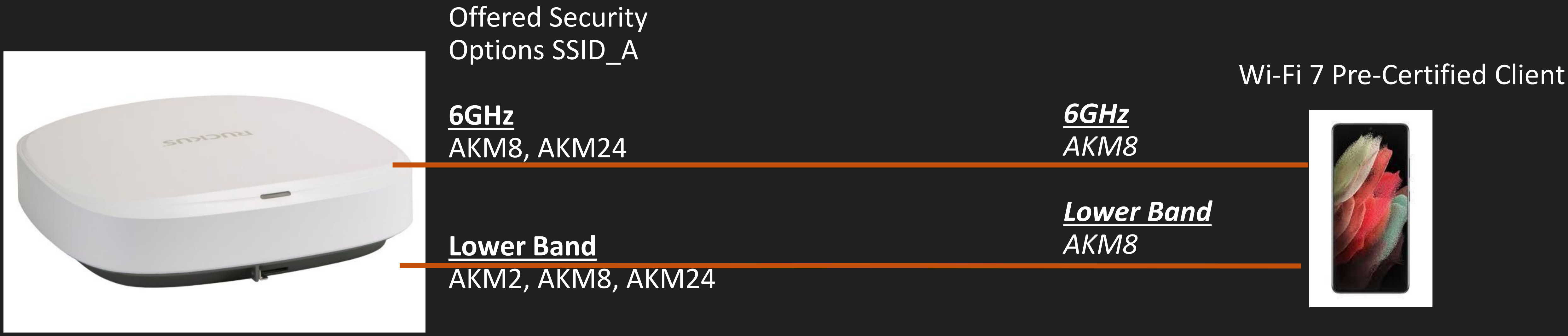
Lower Band
AKM24

5GHz
AKM2

Non
Compliant
Wi-Fi
Device

Wi-Fi 7 Configuration – Pre-cert Wi-Fi 7 Devices

- Passed Wi-Fi 6 Certification which should have negative test for unknown 2nd AKM.
- Released before AKM 24 required, must be upgraded but should support AKM8.
- Not sure whether MLO will be supported



Offered Security Options SSID_A

6GHz
AKM8, AKM24

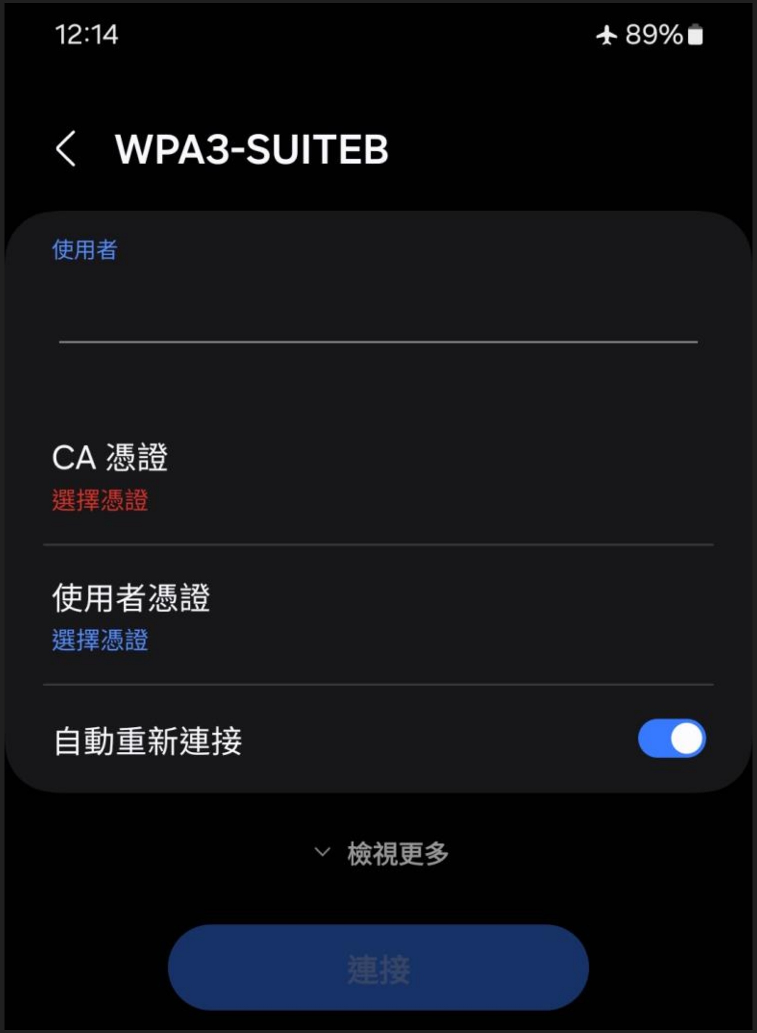
Lower Band
AKM2, AKM8, AKM24

Wi-Fi 7 Pre-Certified Client

6GHz
AKM8

Lower Band
AKM8

WPA3-SuiteB



12:14 ✈ 89%

WPA3-SUITEB

使用者

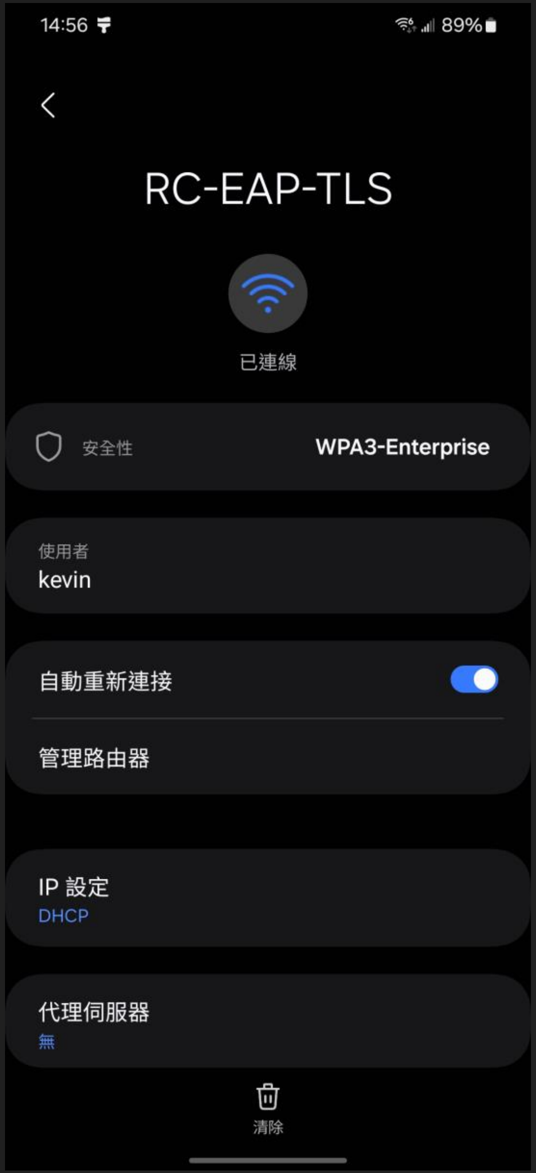
CA 憑證
選擇憑證

使用者憑證
選擇憑證

自動重新連接

檢視更多

連接



14:56 89%

RC-EAP-TLS

已連線

安全性 WPA3-Enterprise

使用者
kevin

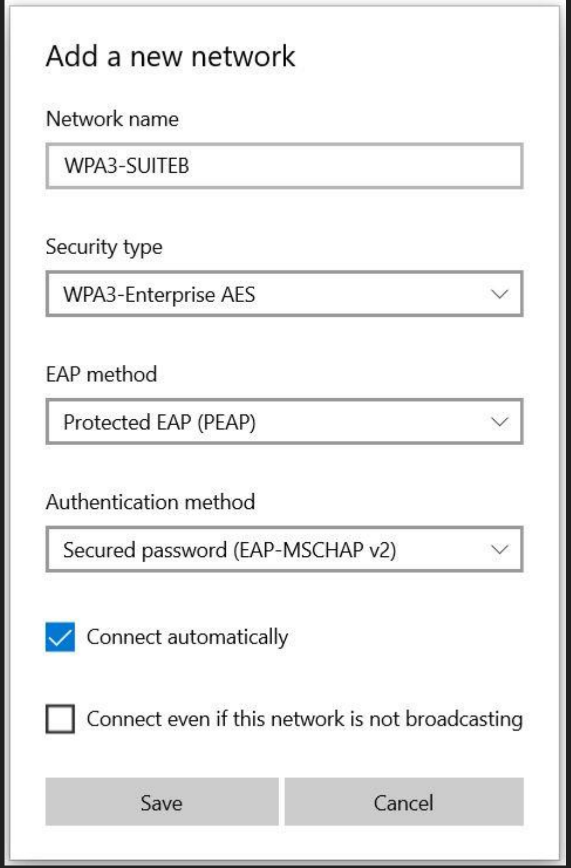
自動重新連接

管理路由器

IP 設定
DHCP

代理伺服器
無

清除



Add a new network

Network name: WPA3-SUITEB

Security type: WPA3-Enterprise AES

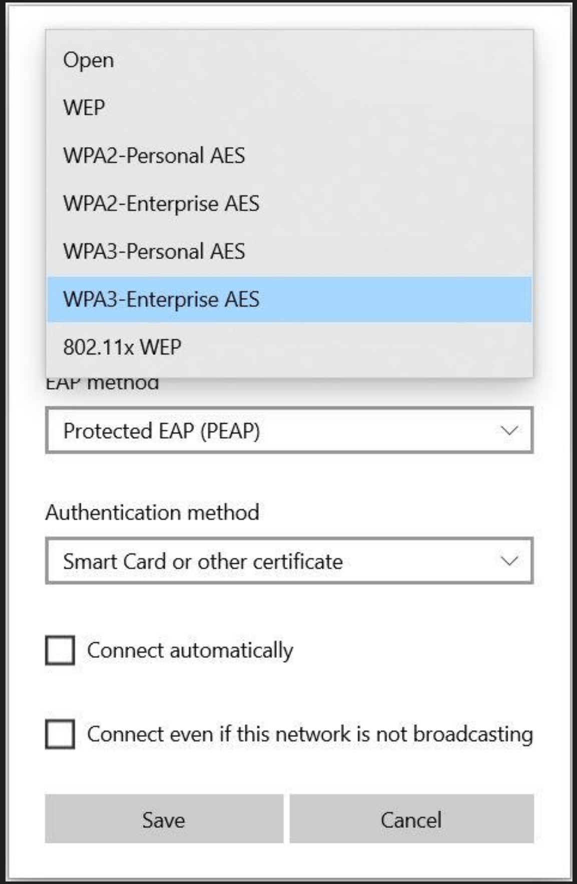
EAP method: Protected EAP (PEAP)

Authentication method: Secured password (EAP-MSCHAP v2)

☑ Connect automatically

□ Connect even if this network is not broadcasting

Save Cancel



EAP method: Protected EAP (PEAP)

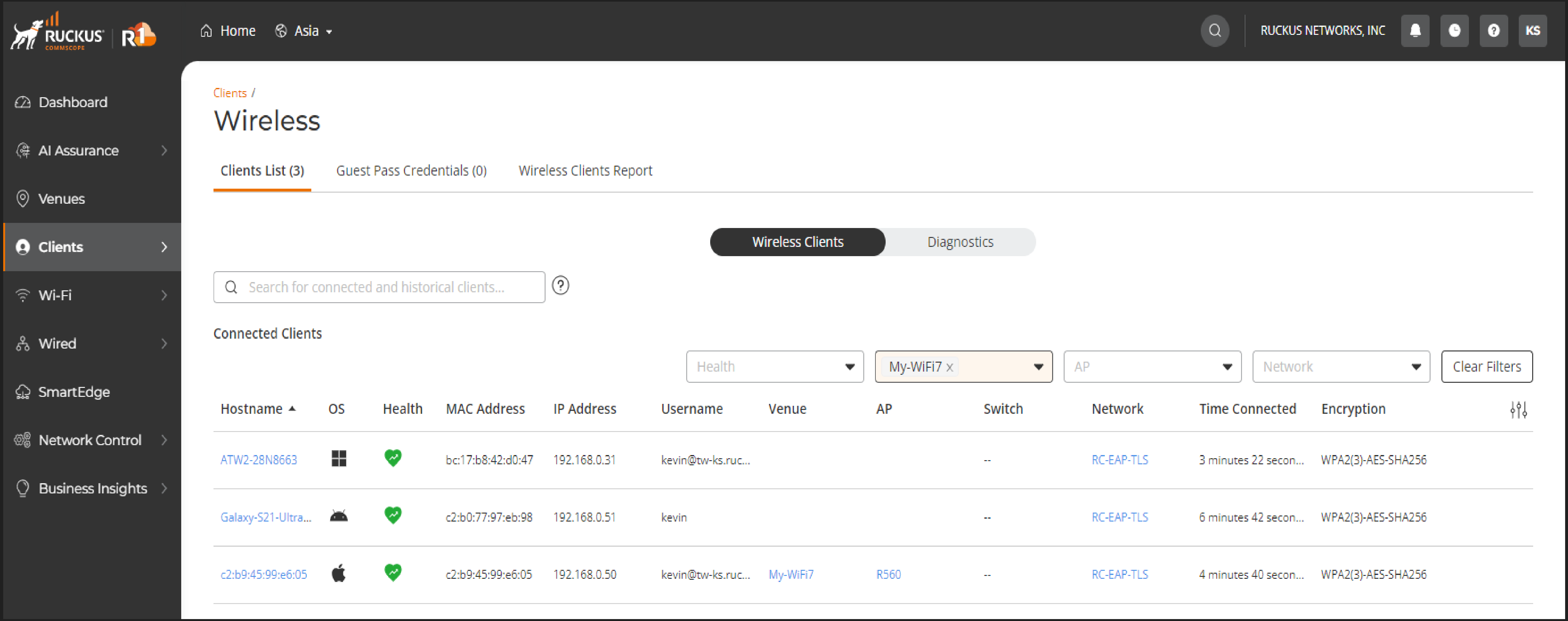
Authentication method: Smart Card or other certificate

□ Connect automatically

□ Connect even if this network is not broadcasting

Save Cancel

WPA3-Enterprise



Clients /

Wireless

Clients List (3)
Guest Pass Credentials (0)
Wireless Clients Report
Wireless Clients
Diagnostics
Search for connected and historical clients...

Connected Clients

Hostname ▲	OS	Health	MAC Address	IP Address	Username	Venue	AP	Switch	Network	Time Connected	Encryption
ATW2-28N8663	⊞	♥	bc:17:b8:42:d0:47	192.168.0.31	kevin@tw-ks.ruc...			--	RC-EAP-TLS	3 minutes 22 secon...	WPA2(3)-AES-SHA256
Galaxy-S21-Ultra...		♥	c2:b0:77:97:eb:98	192.168.0.51	kevin			--	RC-EAP-TLS	6 minutes 42 secon...	WPA2(3)-AES-SHA256
c2:b9:45:99:e6:05		♥	c2:b9:45:99:e6:05	192.168.0.50	kevin@tw-ks.ruc...	My-WiFi7	R560	--	RC-EAP-TLS	4 minutes 40 secon...	WPA2(3)-AES-SHA256

Wi-Fi 7 brings challenges to Connection Security

- A significant new flavor of WPA3, AKM24 goes beyond AKM8

- Forcing Industry to deal with legacy device forward compatibility issues.
  - Introducing more future proofing tests
  - Even proposed solutions have significant flaws

- Even modern devices have compatibility issues.

- There will be headaches, but progress to better security is happening.

RUCKUS Wi-Fi 7 R770 限量優惠體驗活動

RUCKUS首款企業級Wi-Fi 7 R770 已經開賣了!!

- 體驗登記方式:
- 1.請至RUCKUS 現場攤位，填寫您的聯絡資訊
- 2.請掃下方QR Code，填寫您的聯絡資訊

將由RUCKUS代理商 D-link 安排專人聯繫您。

D-Link 友訊代理 必屬專業

RUCKUS®
COMMSCOPE

D-Link®
友訊代理 必屬專業