

WPA3 Personal – Compatibility Mode



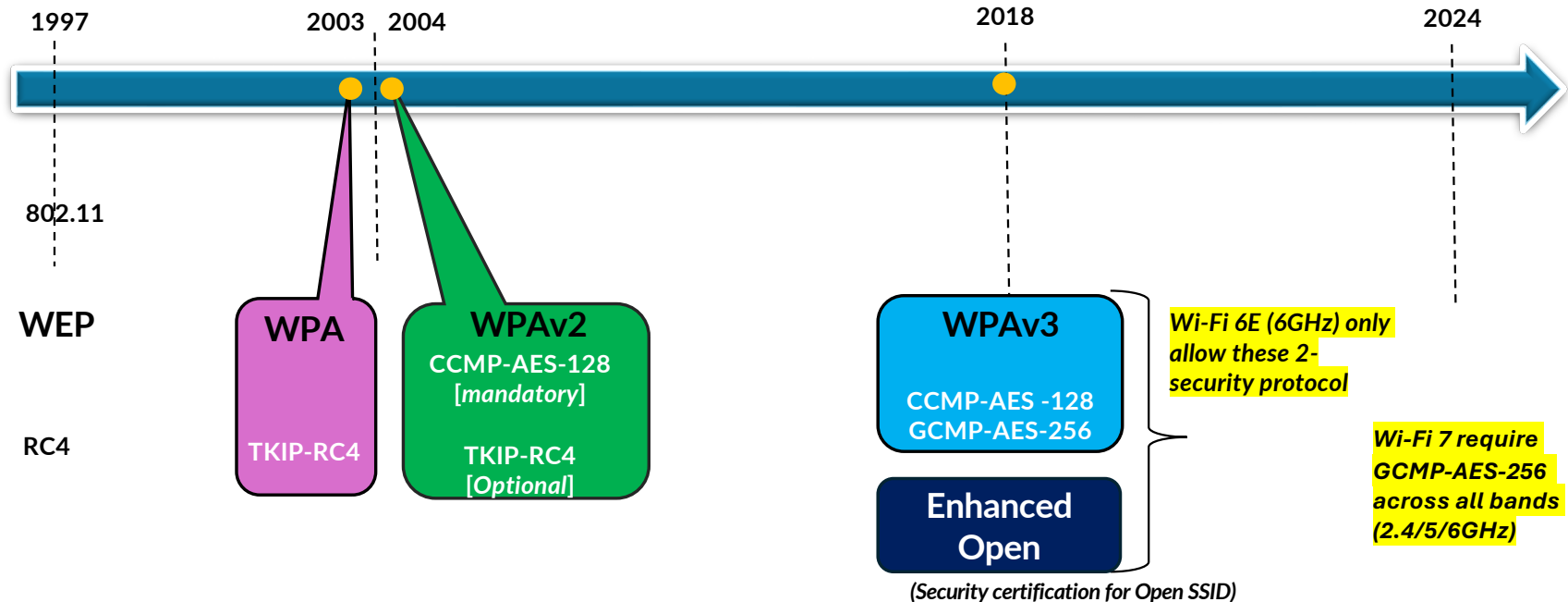
LinkedIn

by Rasika Nayanajith (@mrncciew)

Wi-Fi Security Timeline

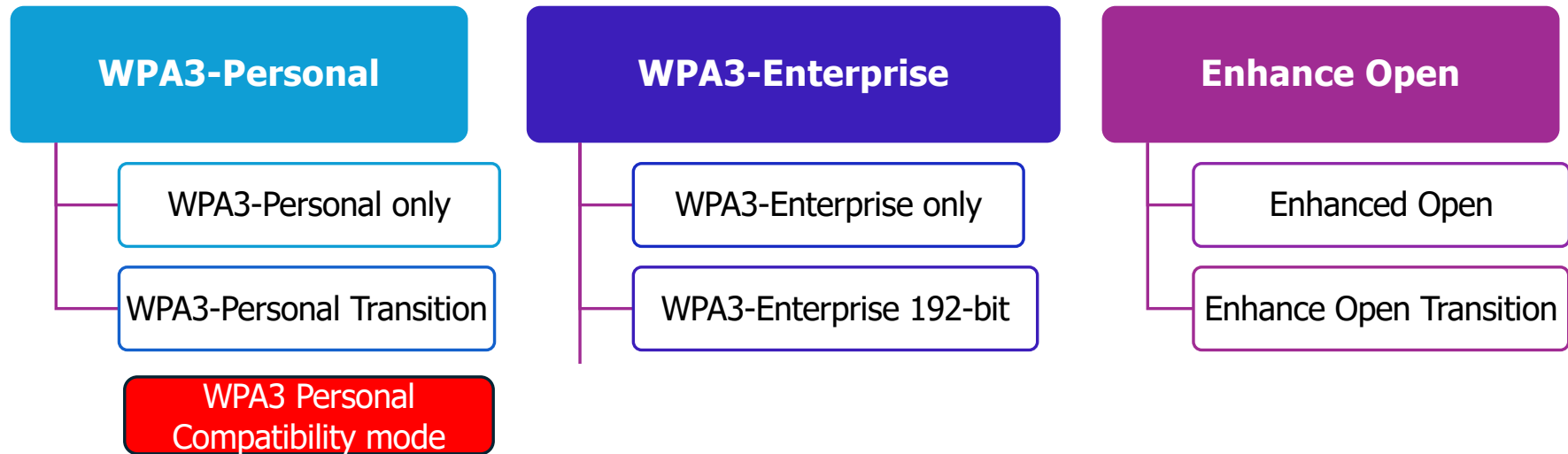


Encryption
Ciphers



- Two mode of Operation (Personal & Enterprise)
 - WPA-Personal -> WPA2-Personal -> WPA3-Personal (SAE)
 - WPA-Enterprise -> WPA2-Enterprise -> WPA3-Enterprise
- “Enhanced Open” to replace “Open” networks

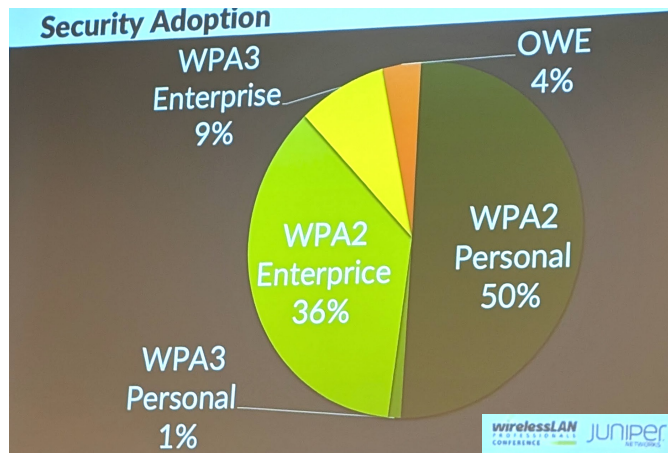
Wi-Fi Security Enhancements



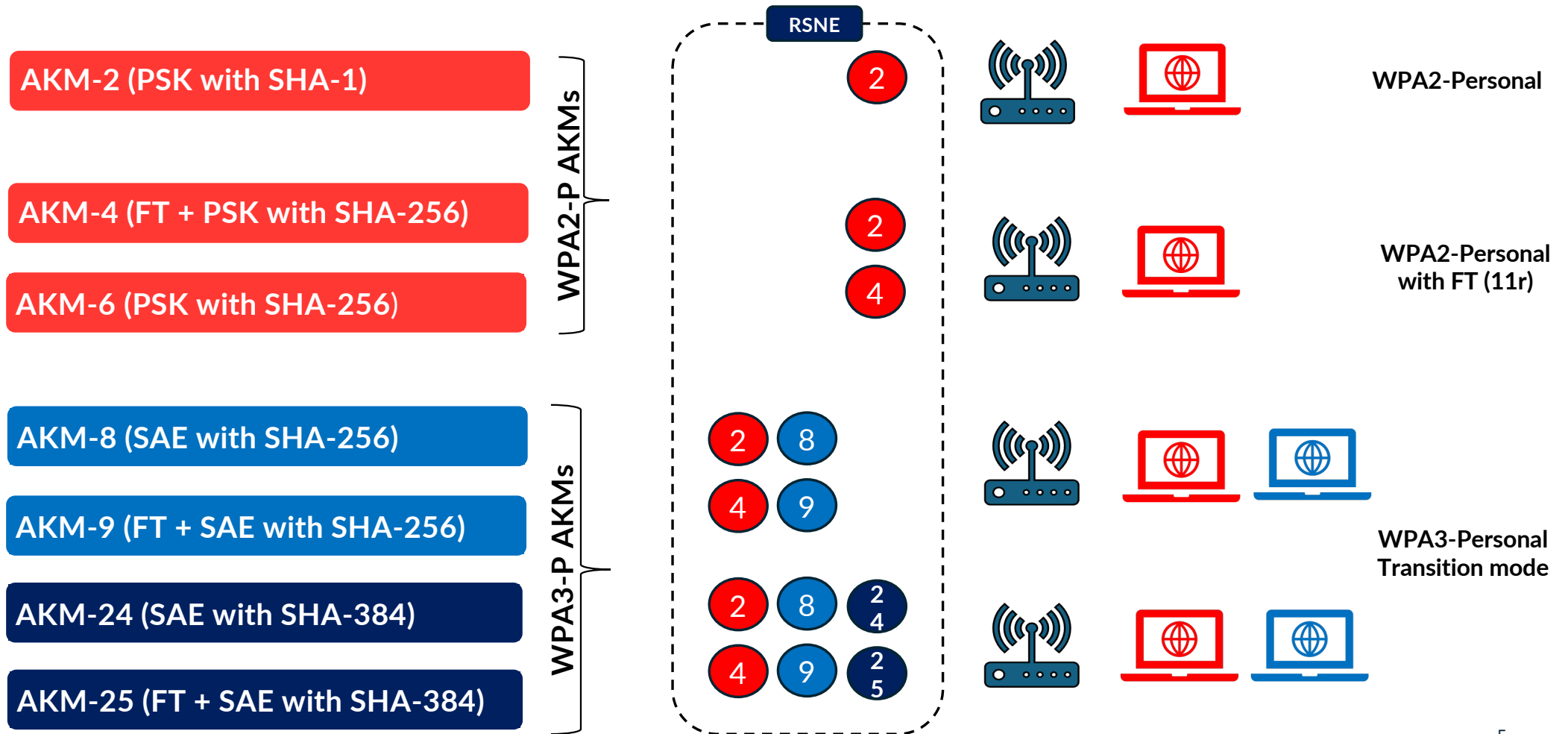
- Protected Management Frame is mandatory
- Provide Perfect Forward Secrecy (PFS)
- Resistant to offline dictionary attack (WPA3-Personal)
- minimum 192 bits key strength for higher security (256 bits strength for Quantum resistant)

Why has WPA3- Personal Adoption been Slow?

- Device compatibility issues
- Legacy WPA2 device persist
- Lack of user awareness
- Limited ISP & vendor push
- 6 GHz is still not widely deployed



Personal Security AKMs



Robust Security Network Element (RSNE)

No.	Time	Addr2 [TA]	Addr1 [RA]	Protocol	Seq No	Length	CH	RSSI	Data rate	Type/Subtype
28	0.000000	Cisco_9d:0b:ed	Broadcast	802.11	0	501	60	-53 dBm	6	Beacon frame
29	0.000000	Cisco_9d:6b:ee	Broadcast	802.11	0	619	60	-53 dBm	6	Beacon frame
30	0.000000	Cisco_9d:6b:ef	Broadcast	802.11	0	567	60	-53 dBm	6	Beacon frame

Tag: RSN Information

- Tag Number: RSN Information (48)
- Tag length: 30
- 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) AES (CCM)
 - Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
 - Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
 - Pairwise Cipher Suite type: AES (CCM) (4)
- 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)
 - Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
 - Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
 - Auth Key Management (AKM) type: SAE (SHA256) (8)
 - 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)
- RSN Capabilities: 0x00e8
- PMKID Count: 0
- PMKID List
- Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
 - Group Management Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
 - Group Management Cipher Suite type: BIP (128) (6)

Tag: OBSS Load Element 802.11e CCA Version

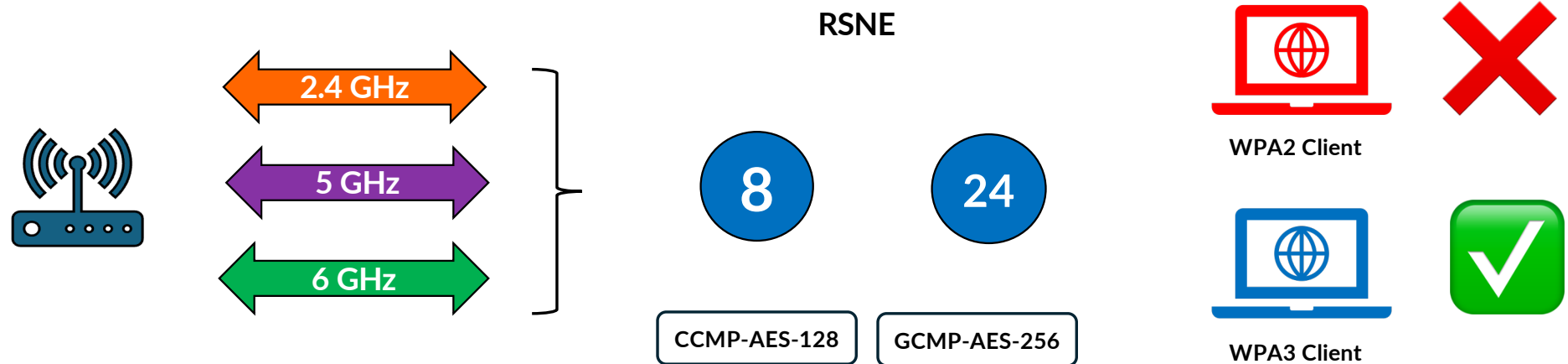
BIP – Broadcast/Multicast Integrity Protocol
SAE – Simultaneous Authentications of Equal

Deployment Option 1

WPA3 Personal only Mode

WPA3 Personal only Mode (1 of 2)

- Mandatory to enable **AKM-8** and **AKM-24** for Wi-Fi 7 APs
- Enable **AKM-8** for non-Wi-Fi 7 APs
- Recommend to enable **AKM-9** and **AKM-25** (if 802.11r support required)
- Only WPA3 capable STA can connect to WLAN



WPA3 Personal only Mode (2 of 2)

- Auth Key Management
 - AKM-8
 - AKM-24
- Unicast ciphers
 - CCMP-AES-128
 - GCMP-AES-256
- Group cipher
 - CCMP-AES-128

```

  Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 34
    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: 2
  Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) GCMP (256) 00:0f:ac (Ieee 802.11) AES (CCM)
    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)
    Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
      Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Pairwise Cipher Suite type: AES (CCM) (4)
  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)
    Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: SAE (SHA256) (8)
    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)
  RSN Capabilities: 0x00e8
    PMKID Count: 0
    PMKID List
  Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
  Tag: QBSS Load Element 802.11e CCA Version
  Tag: RM Enabled Capabilities (5 octets)

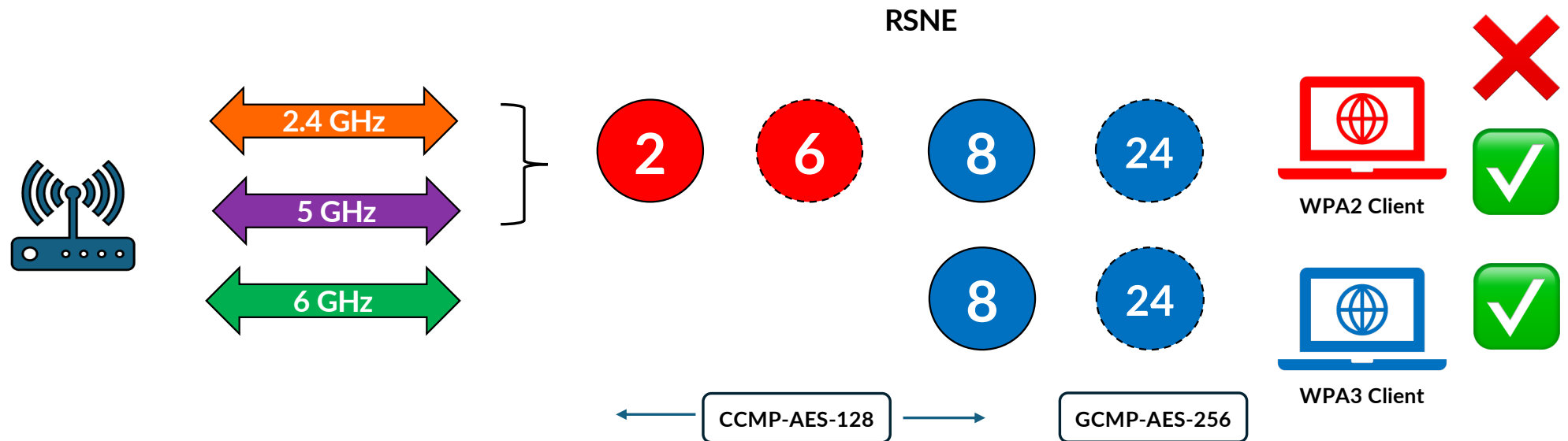
```

Deployment Option 2

WPA3 Personal – Transition Mode

WPA3 Personal – Transition Mode (1 of 2)

- Enable **AKM-2** and **AKM-8** (mandatory)
- Enable **AKM-6** and **AKM-24** (recommended)
- **Legacy** WPA2 clients may experience issues



WPA3 Personal – Transition Mode (2 of 2)

- Auth Key Management
 - AKM-2 and AKM-6 for WPA2
 - AKM-8 and AKM-24 for WPA3
- Unicast ciphers
 - CCMP-AES-128
 - GCMP-AES-256 (not in this PCAP)
- Group cipher
 - CCMP-AES-128

```
34 0.100730 Cisco_af:62:6e Broadcast 802.11 2996 537 52 -70 dBm 12 Beacon frame
  Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 38
    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) AES (CCM)
    Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
    Pairwise Cipher Suite type: AES (CCM) (4)
    Auth Key Management (AKM) Suite Count: 4
    Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK 00:0f:ac (Ieee 802.11) PSK (SHA256) 00:0f:ac (Ieee 802.11)
    Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
    Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
    Auth Key Management (AKM) type: PSK (2)
    Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK (SHA256)
    Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
    Auth Key Management (AKM) type: PSK (SHA256) (6)
    Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
    Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
    Auth Key Management (AKM) type: SAE (SHA256) (8)
    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)
    RSN Capabilities: 0x00a8
    PMKID Count: 0
    PMKID List
    Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
    Tag: QBSS Load Element 802.11e CCA Version
```

Legacy WPA2 Client Issues

- STA is not supporting more than 1 AKM in RSN
- STA is not supporting more than 2 AKM advertised by AP
- STA is not supporting more than 1 cipher suites advertised by AP
- STA copies fields from AP's RSNE
- STA is not supporting RSNXE in EAPoL

CCMP-AES-128 [4]

GCMP-AES-256 [9]

Cipher Suites

AKM-2 (PSK with SHA-1)

AKM-4 (FT + PSK with SHA-256)

AKM-6 (PSK with SHA-256)

WPA2-P AKMs

AKM-8 (SAE with SHA-256)

AKM-9 (FT + SAE with SHA-256)

AKM-24 (SAE with SHA-384)

AKM-25 (FT + SAE with SHA-384)

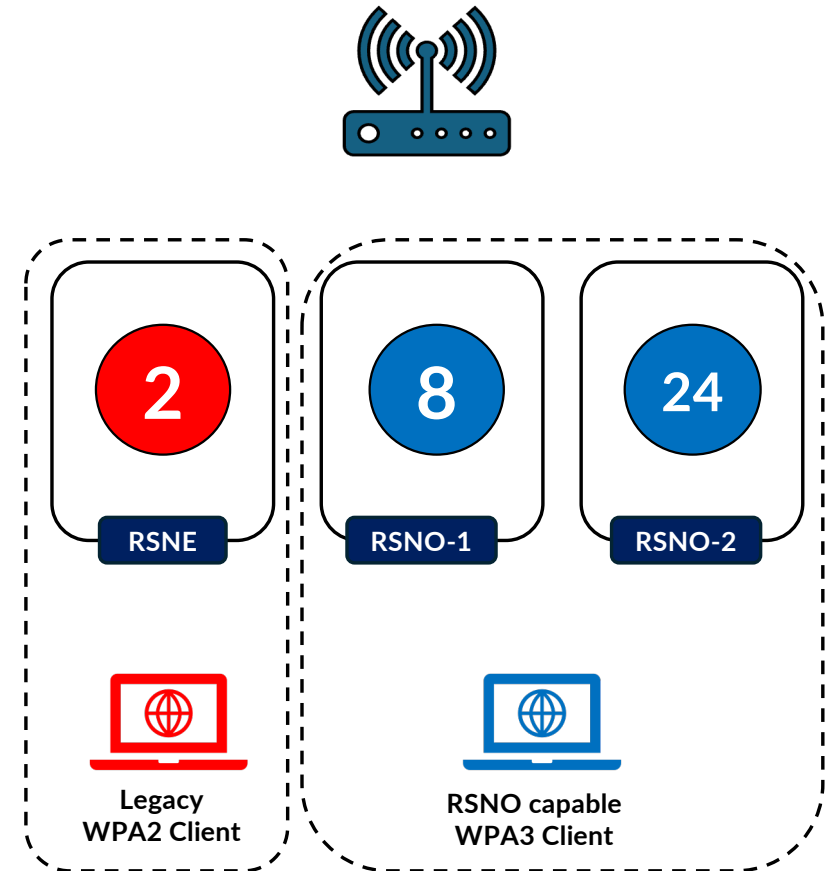
WPA3-P AKMs

Deployment Option 3

WPA3 Personal – Compatibility Mode

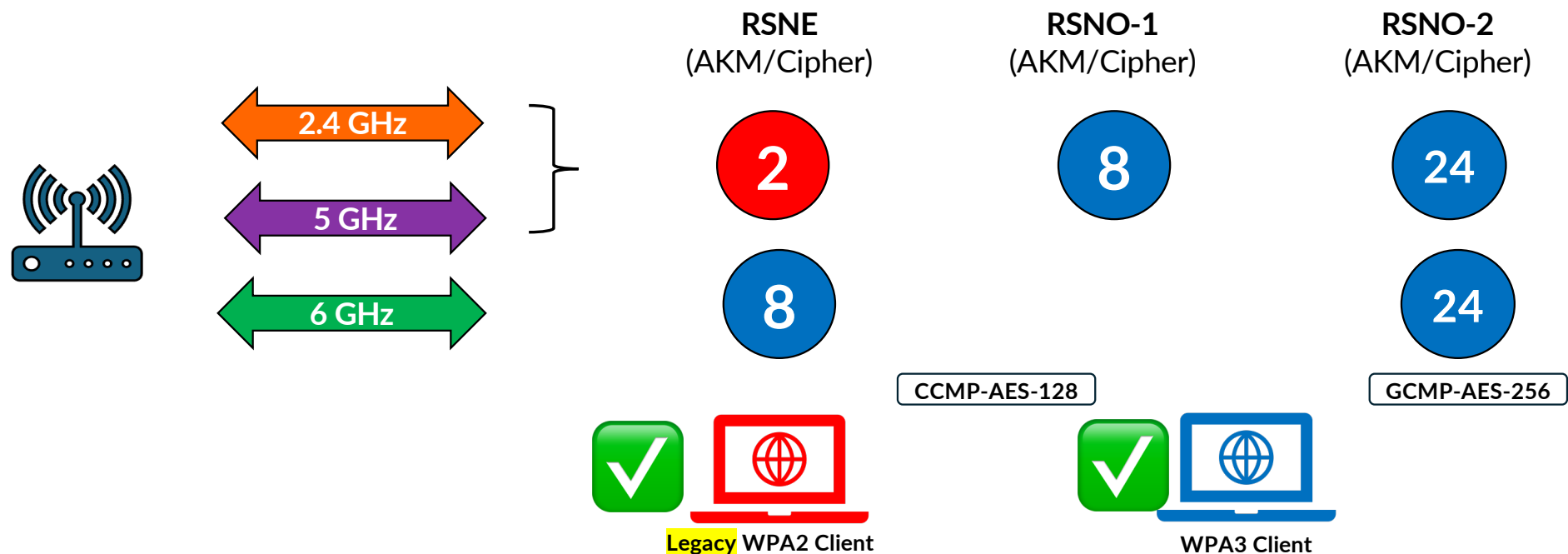
RSN Override

- Introduced in IEEE 802.11-2024 update
- AP advertise limited parameters in
 - RSNE
 - RSNXE
- Extended parameters advertised in
 - RSN Override -1
 - RSN Override -2
- Legacy clients ignore new elements
- WPA3 clients to use RSN Override element info
- WPA3-Specification 3.4 introduced WPA3-Compatibility mode



WPA3 Personal – Compatibility Mode (1 of 2)

- AP only advertise **AKM-2** in 2.4/5 GHz RSNE
- AP only advertise **AKM-8** in 6 GHz RSNE
- AP advertise **AKM-8** in RSNO-1 (2.4/5 GHz)
- AP advertise **AKM-24** in RSNO-2
- WPA3 STA supports RSNO -> WPA3
- **WPA3 STA does not support RSNO -> WPA2**



WPA3 Personal – Compatibility Mode (2 of 2)

- Single AKM [2] in RSNE
- Single Cipher suite [4] in RSNE
- WPA3-AKM [8] in RSNO-1
- WPA3-AKM [24] in RSNO-2
- Legacy clients not confused
- WPA3 clients suppose to understand RSNO ?
 - If not -> WPA2 security

> Frame 14: 593 bytes on wire (4744 bits), 593 bytes captured (4744 B) on interface 0

> Radiotap Header v0, Length 48

> 802.11 radio information

> IEEE 802.11 Beacon frame, Flags:C

▼ IEEE 802.11 Wireless Management

> Fixed parameters (12 bytes)

▼ Tagged parameters (505 bytes)

> Tag: SSID parameter set: "TESTING_5G"

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

> Tag: Traffic Indication Map (TIM): DTIM 2 of 3 bitmap

> Tag: Country Information: Country Code US, Environment Global

> Tag: Power Constraint: 0

> Tag: TPC Report Transmit Power: 26 dBm

> Tag: RSN Information

> Tag: QBSS Load Element 802.11e CCA Version

> Tag: AP Channel Report: Operating Class 134, Channel List : 6

> Tag: RM Enabled Capabilities (5 octets)

> Tag: Supported Operating Classes

> Tag: HT Capabilities

> Tag: HT Operation

> Tag: Extended Capabilities (11 octets)

> Tag: Interworking

> Tag: Advertisement Protocol

> 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: Reduced Neighbor Report

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

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

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

> Tag: Vendor Specific: Apple, Inc. (Data: 01)

> Tag: Vendor Specific: Wi-Fi Alliance: Unknown

> Tag: Vendor Specific: Wi-Fi Alliance: RSN Element Override

> Tag: Vendor Specific: Wi-Fi Alliance: RSN Element Override 2

> Tag: Vendor Specific: Wi-Fi Alliance: RSN Extension Element Override

▼ Tag: Vendor Specific: Wi-Fi Alliance: RSN Element Override

Tag Number: Vendor Specific (221)

Tag length: 24

OUI: 50:6f:9a (Wi-Fi Alliance)

Vendor Specific OUI Type: 41

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) AES (CCM)

▼ Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)

Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)

Pairwise Cipher Suite type: AES (CCM) (4)

Auth Key Management (AKM) Suite Count: 1

▼ Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) SAE (SHA256)

▼ Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)

Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)

Auth Key Management (AKM) type: SAE (SHA256) (8)

> RSN Capabilities: 0x00cc

> Tag: Vendor Specific: Wi-Fi Alliance: RSN Element Override 2

▼ Tag: Vendor Specific: Wi-Fi Alliance: RSN Element Override

Tag Number: Vendor Specific (221)

Tag length: 24

OUI: 50:6f:9a (Wi-Fi Alliance)

Vendor Specific OUI Type: 42

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)

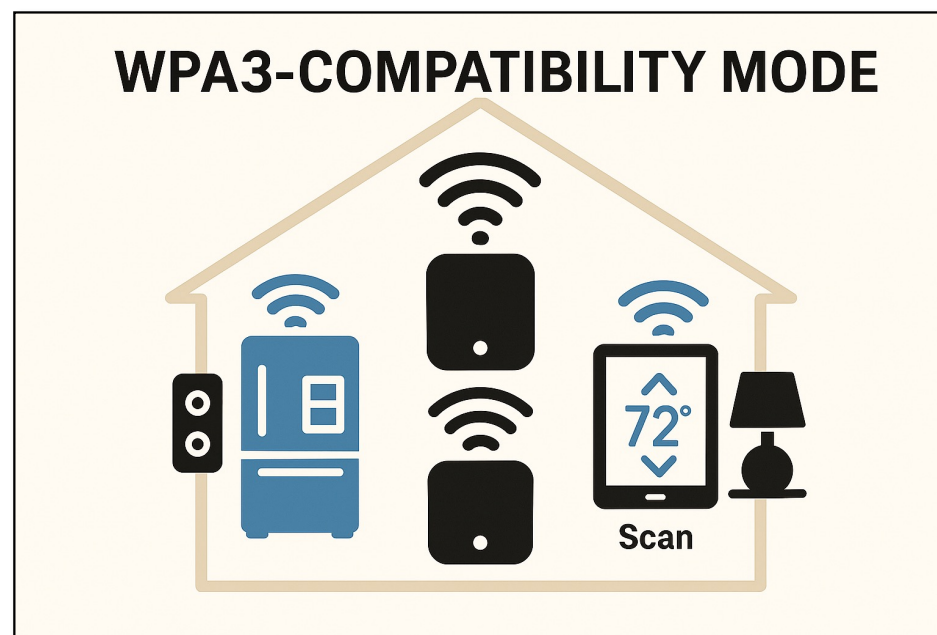
> RSN Capabilities: 0x00cc

> Tag: Vendor Specific: Wi-Fi Alliance: RSN Extension Element Override

WPA3 Personal – Compatibility Mode Challenges

Compatibility Mode Use Cases

- Only if limited success with WPA3-Transition mode
- Persistency of legacy WPA2 clients



Compatibility Mode - Challenges

- Vendor adoption ?
- WPA3 clients may not support RSNO
- Devices may not follow WFA certification/guidelines



Compatibility Mode Support



- ☐ WPA3™-Personal
 - ☐ Active Scan
 - ☐ AKM 24
 - ☐ AKM 25
 - ☐ ANQP
 - ☐ Beacon Protection
 - ☐ Fast Transition OTA on WPA3-Personal
 - ☐ Fast Transition OTA on WPA3-Personal transition mode
 - ☐ Fast Transition OTDS on WPA3-Personal
 - ☐ Operating Channel Validation
 - ☐ Privacy Extensions
 - ☐ RSNO
 - ☐ SAE-Public Key
 - ☒ WPA3-Personal compatibility mode

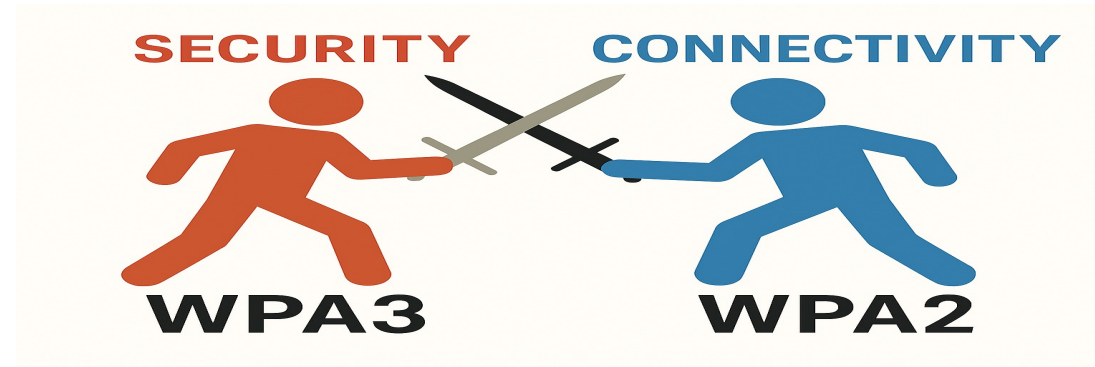
Sort By: Date Certified: New

 Product Name: AP-745 Model Number: AP-745 Total Variants: 1 (1 result) Brand: Hewlett Packard Enterprise Category: Routers Last Certified Date: 2025-08-11 	 Product Name: AT-TQ7613 Model Number: AT-TQ7613 Total Variants: 1 (1 result) Brand: Allied Telesis Holdings K.K. Category: Routers Last Certified Date: 2025-08-04 
 Product Name: MediaTek 2x2 WiFi 7 - MT7990NIC Model Number: MediaTek 2x2 WiFi 7 - MT7990NIC Total Variants: 3 (1 result) Brand: MediaTek Inc. Category: Other Last Certified Date: 2025-07-31	 Product Name: Boost Wi-Fi 7 Model Number: B30A Total Variants: 1 (1 result) Brand: TELUS Communications Category: Routers Last Certified Date: 2025-07-10 
 Product Name: Qualcomm FastConnect 7800 Mobile Connectivity system Model Number: WCN7850 Total Variants: 4 (1 result) Brand: Qualcomm Category: Computers & Accessories Last Certified Date: 2025-07-02	 Product Name: Qualcomm Networking Pro Tri-Band Wi-Fi 7 Platform Model Number: IPQ9574 Total Variants: 5 (2 results) Brand: Qualcomm Category: Other Last Certified Date: 2025-01-09

Reference: <https://www.wi-fi.org/product-finder>

Transition or Compatibility Mode ?

Scenario	WPA3-Personal Transition Mode	WPA3-Personal Compatibility Mode
WPA2 Clients	Legacy WPA2 clients may not be able to connect	Seamless association with WPA2
WPA3 clients with RSNO support	Seamless association with WPA3	Seamless association with WPA3
WPA3 clients without RSNO support	Seamless association with WPA3	WPA3 client associate with WPA2



Technical References

WPA3™ deployment options



Driving widespread adoption of WPA3

Wi-Fi Alliance® is committed to ensuring the long-term migration and broadest possible use of Wi-Fi CERTIFIED® devices. WPA3 support has been required in all new Wi-Fi CERTIFIED devices since 2018. WPA3 is mandatory in the 6 GHz band. Wi-Fi Alliance strongly recommends that deployers and users configure networks for WPA3 whenever possible.



Technical Note: Achieving secure network connectivity for all devices

Version 1.0
February 25 , 2025



WPA3™ Specification Version 3.5

