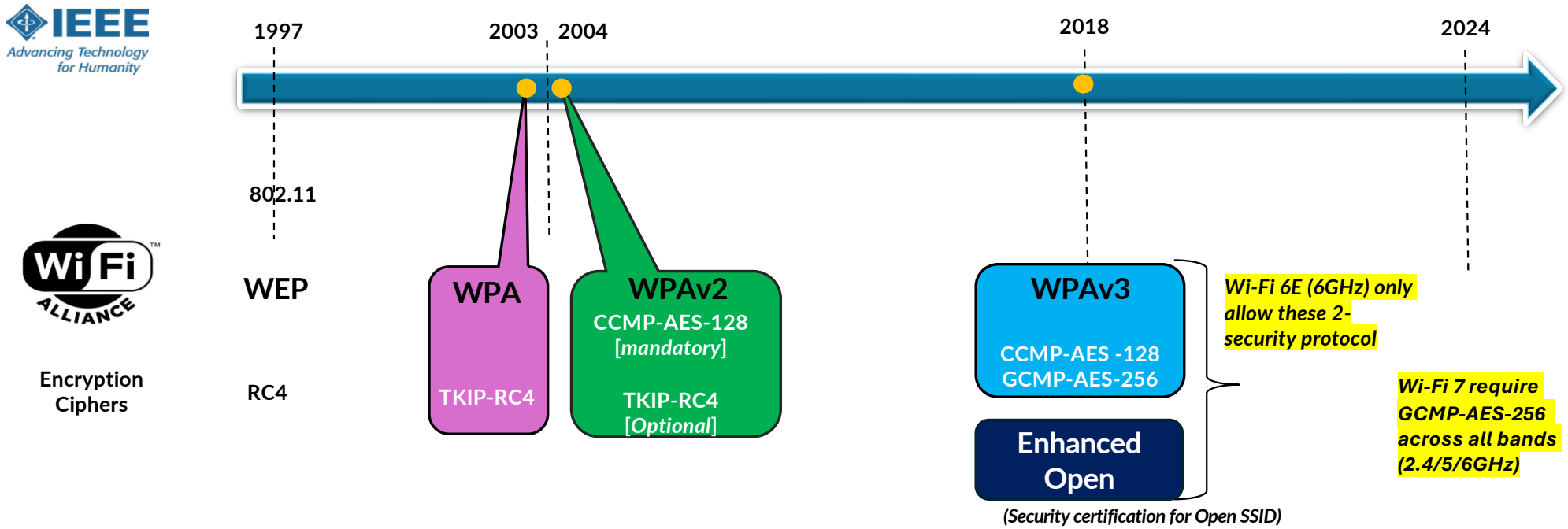
WPA3 Personal – Compatibility Mode

by Rasika Nayanajith (@mrncciew)

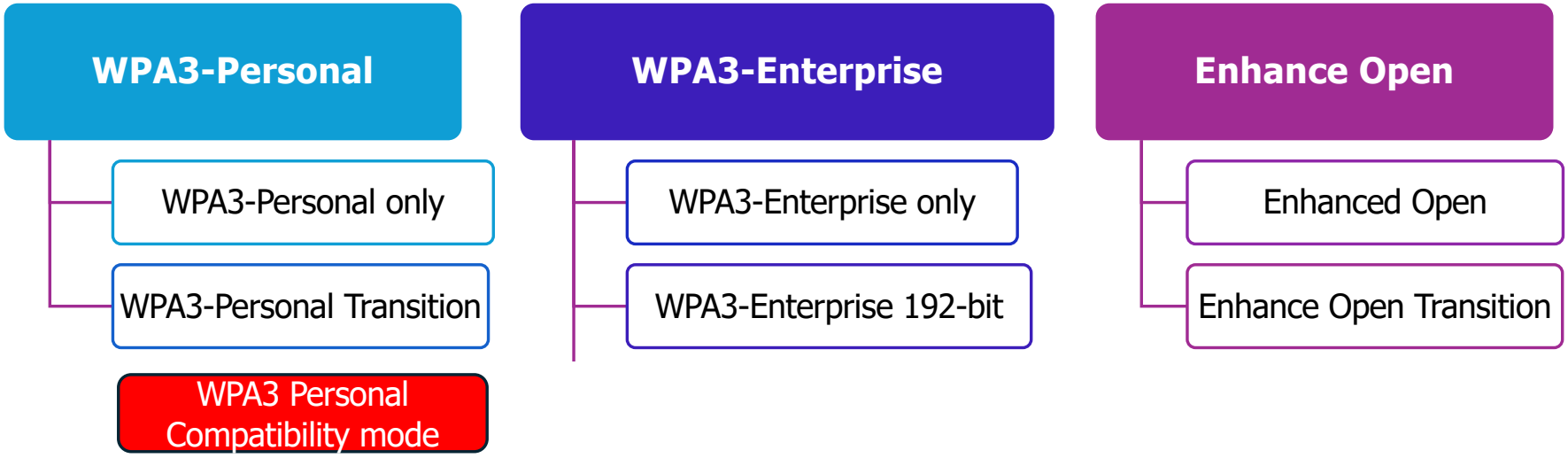
Wi-Fi Security Timeline



- 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

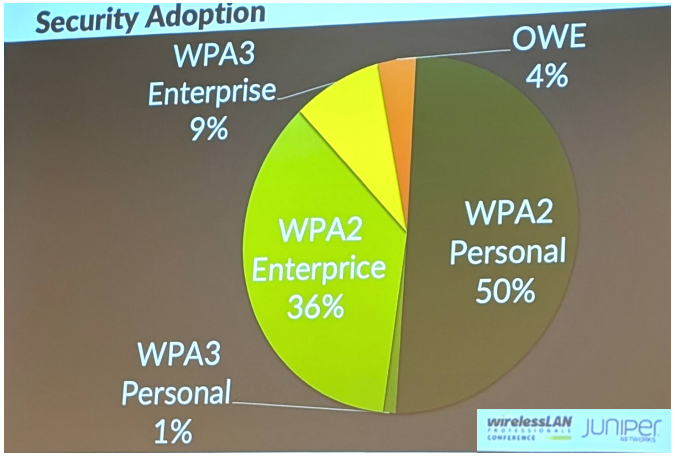


- Protected Management Frame is mandatory
- Provide Perfect Forward Secrecy (PFS)
- Resistant to offline dictionary attack (WPA3-Personal)
- minimum 192 bits key strength for higher security (256 bits strength for Quantum resistant)

Ref: Wi-Fi.org, WPA3_Specification_v3.5 – Feb 2025

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

AKM-2 (PSK with SHA-1)

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

AKM-6 (PSK with SHA-256)

AKM-8 (SAE with SHA-256)

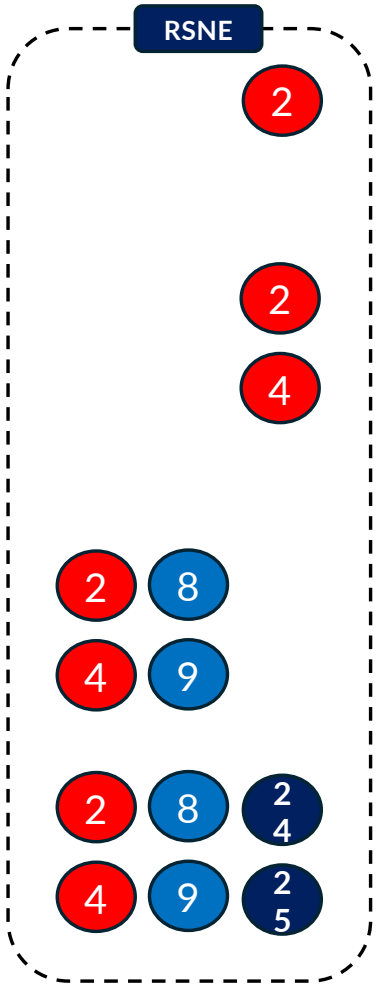
AKM-9 (FT + SAE with SHA-256)

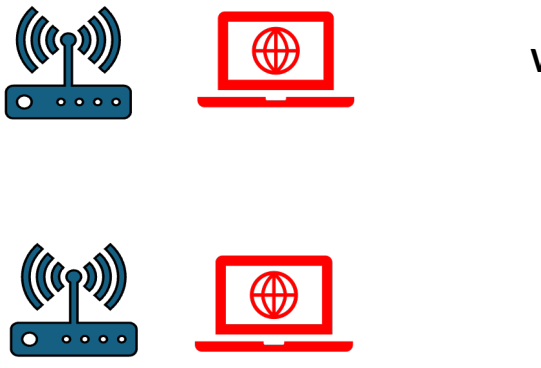
AKM-24 (SAE with SHA-384)

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

WPA2-P AKMs

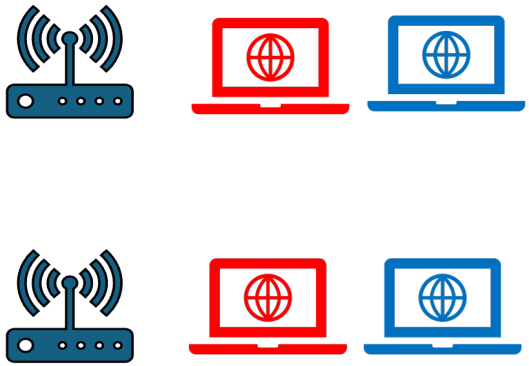
WPA3-P AKMs





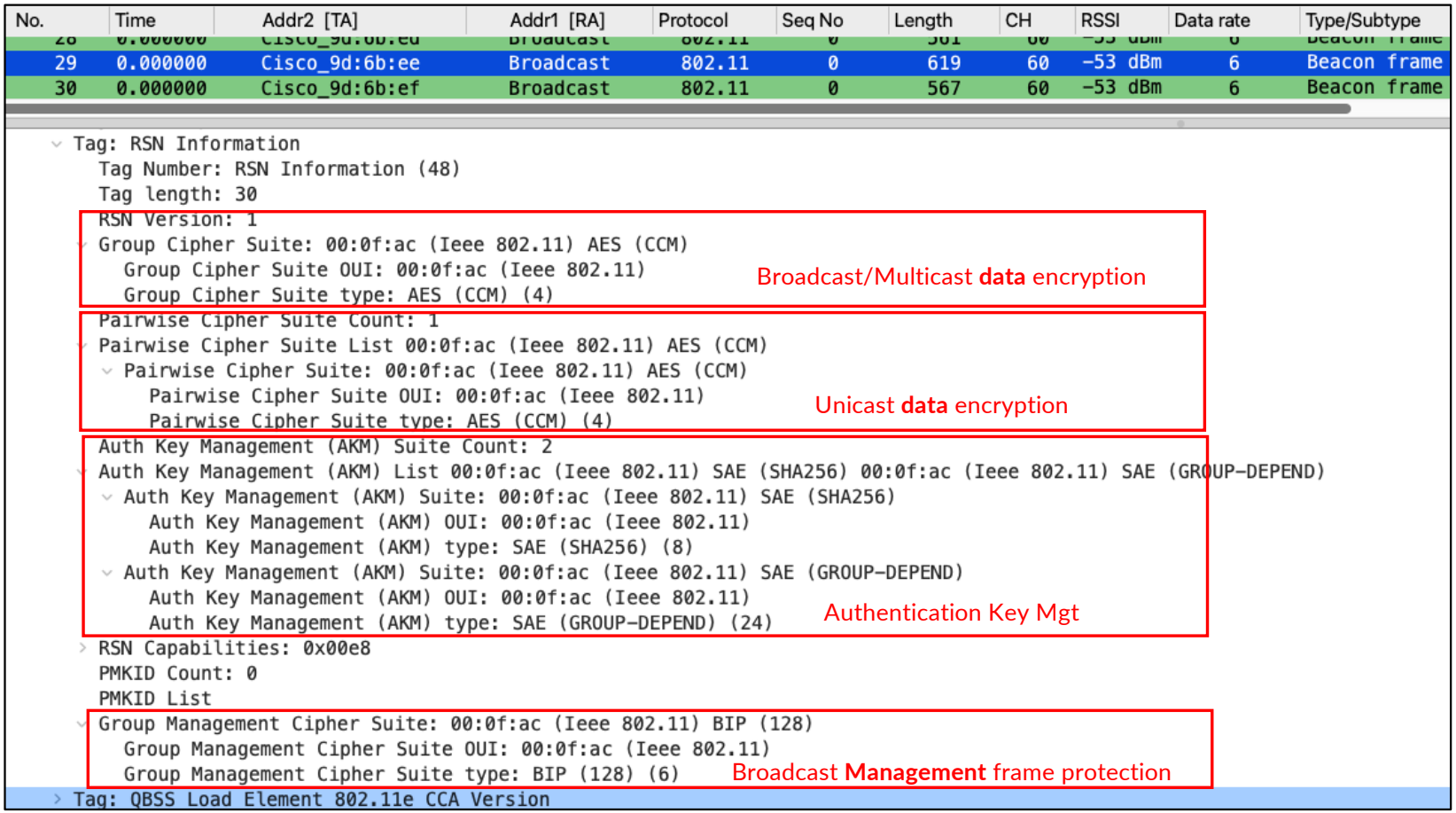
WPA2-Personal

WPA2-Personal with FT (11r)



WPA3-Personal Transition mode

Robust Security Network Element (RSNE)



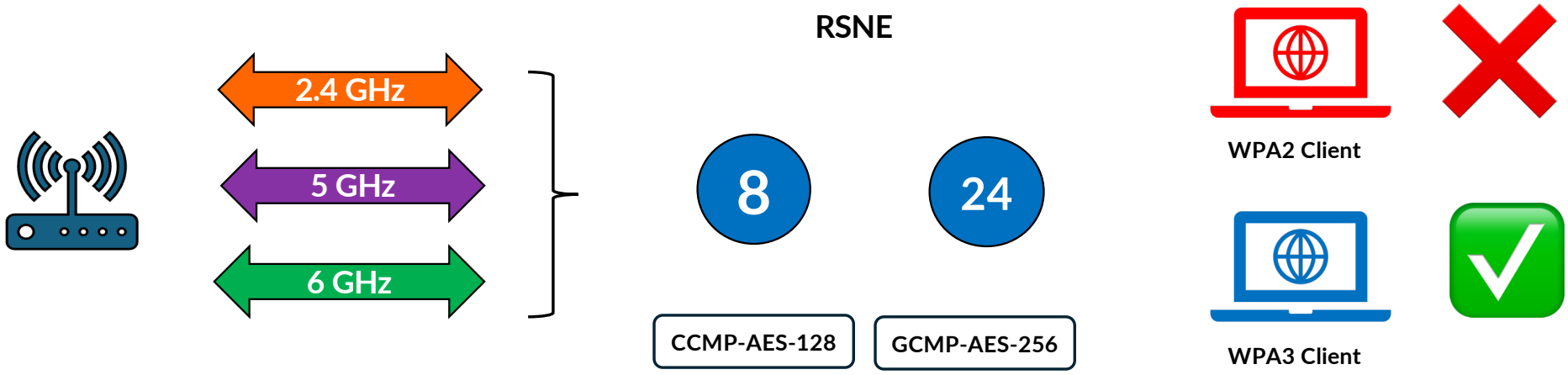
BIP – Broadcast/Multicast Integrity Protocol
SAE – Simultaneous Authentications of Equal

Deployment Option 1

WPA3 Personal only Mode

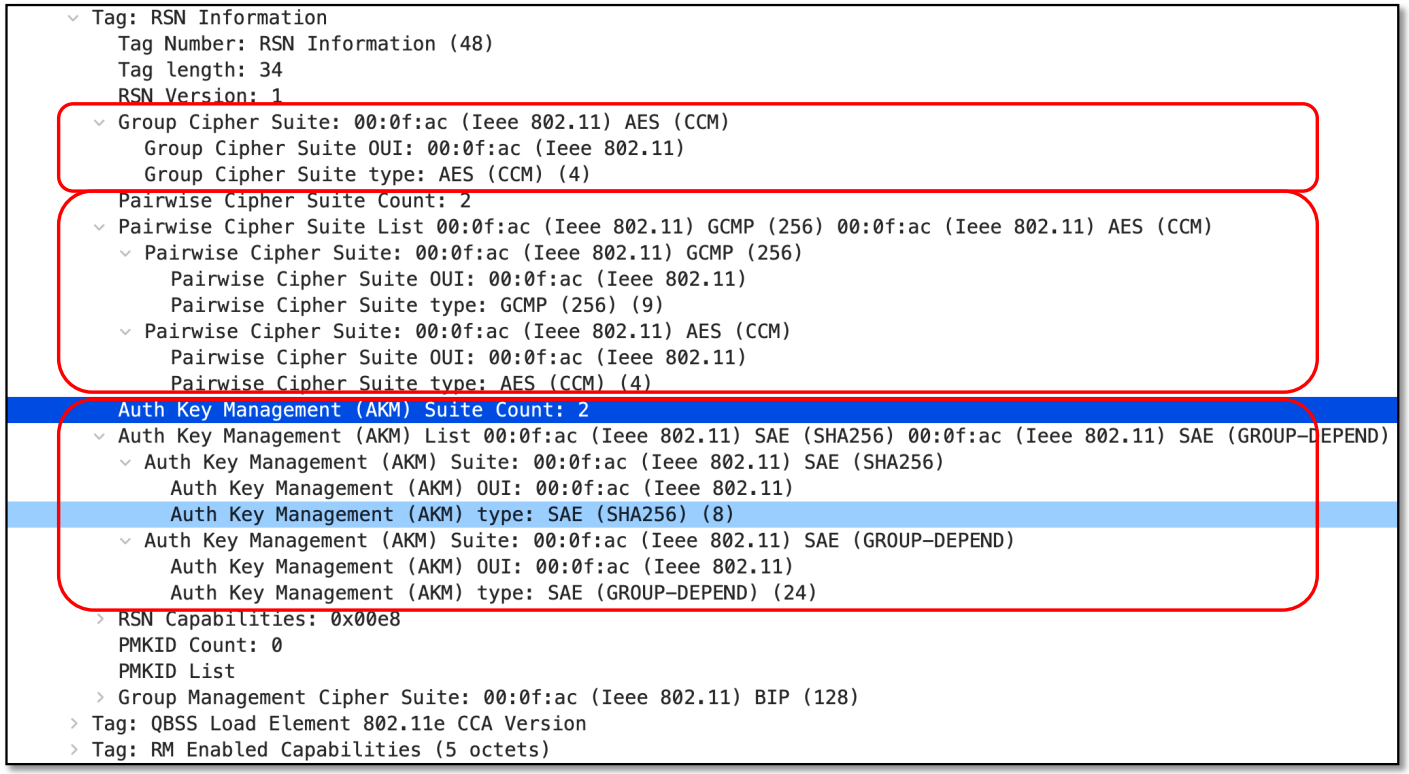
WPA3 Personal only Mode (1 of 2)

- 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

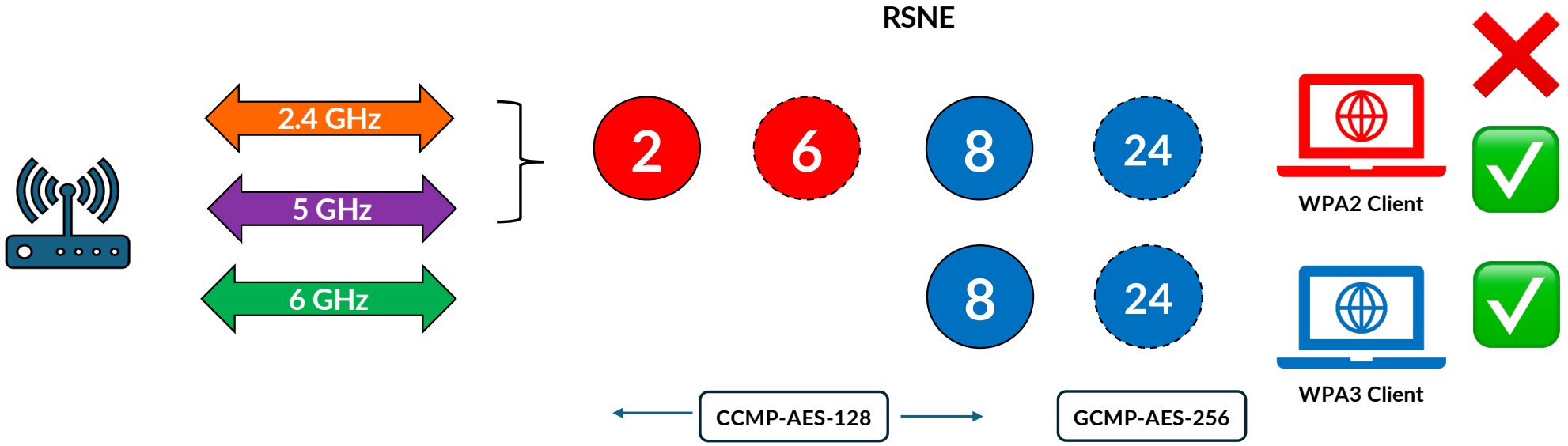


Deployment Option 2

WPA3 Personal – Transition Mode

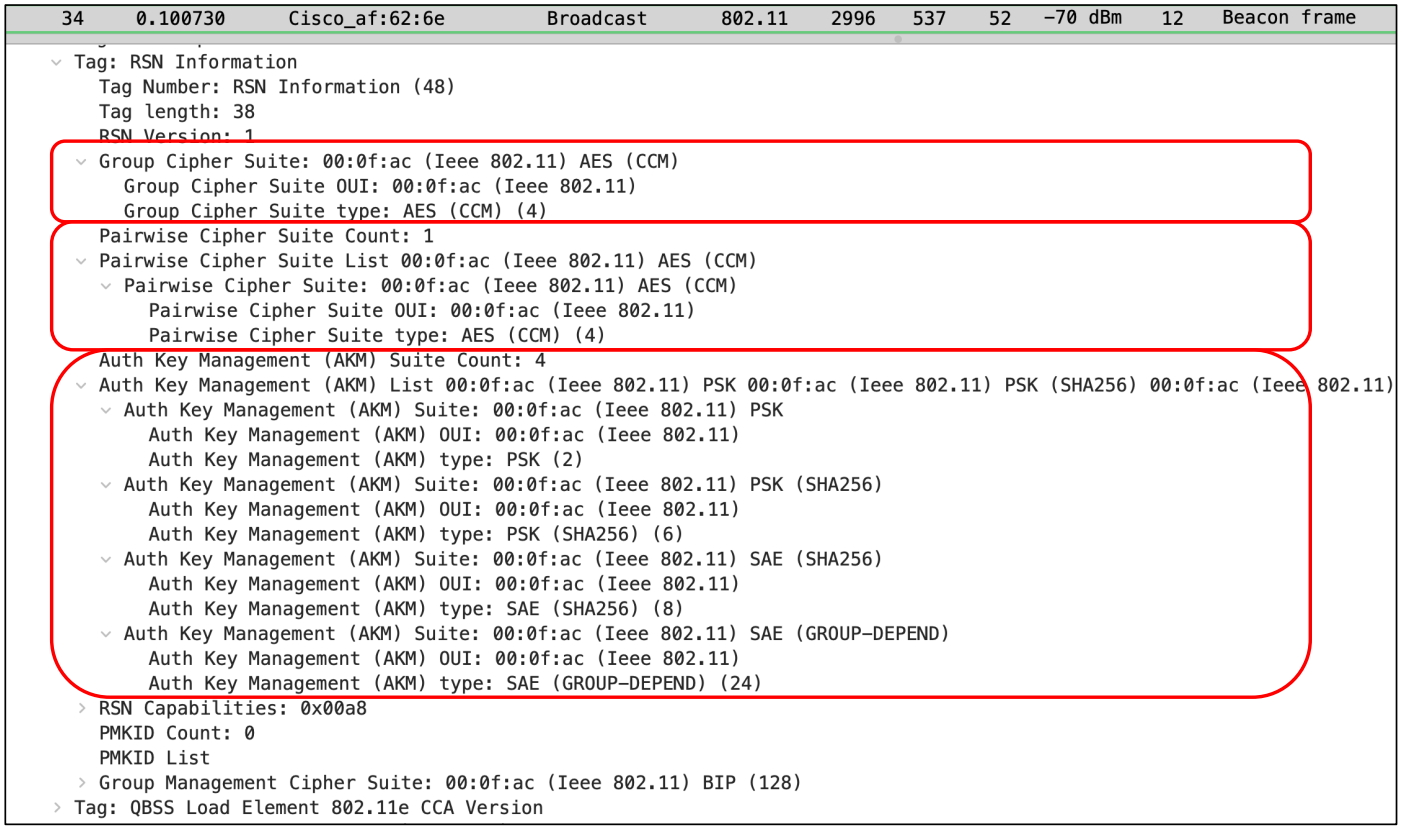
WPA3 Personal – Transition Mode (1 of 2)

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



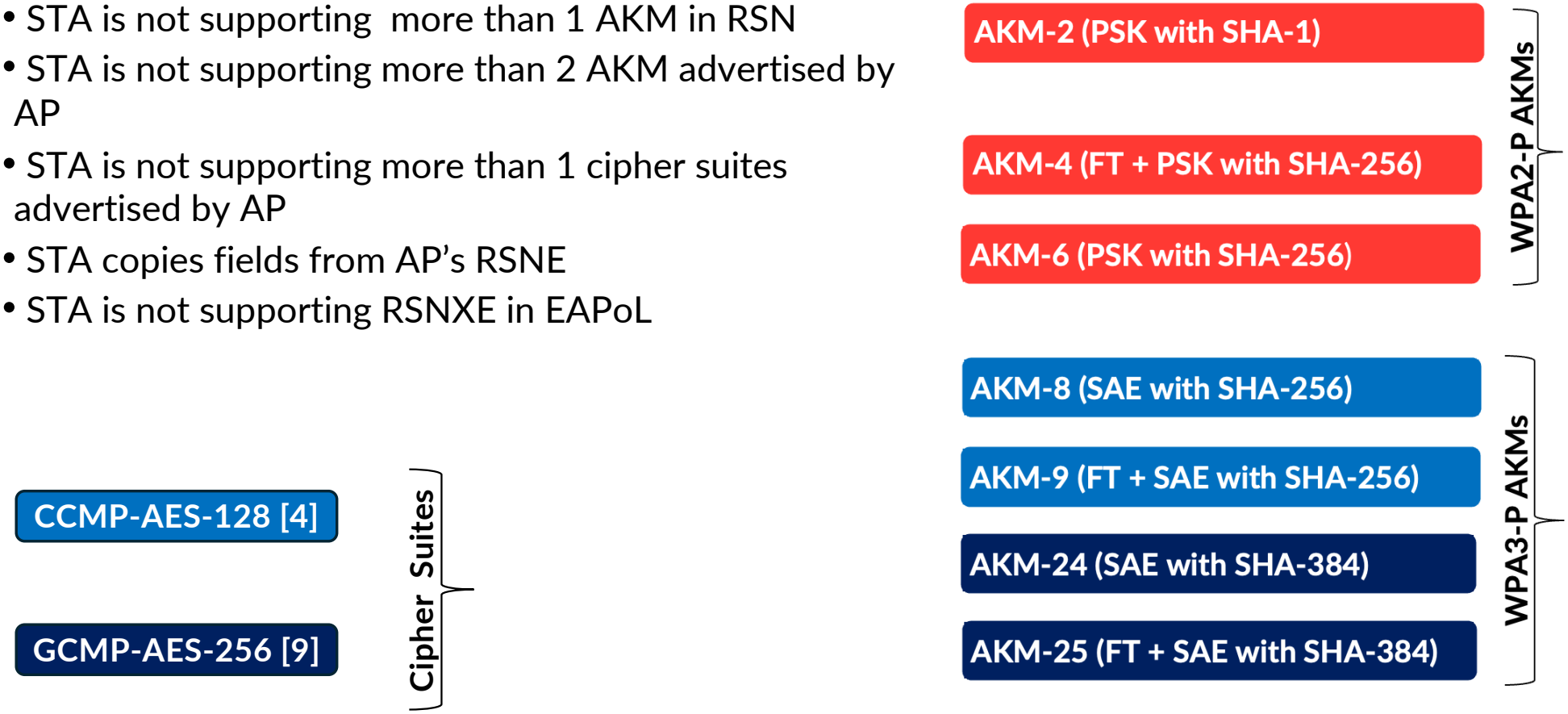
WPA3 Personal – Transition Mode (2 of 2)

- 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



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

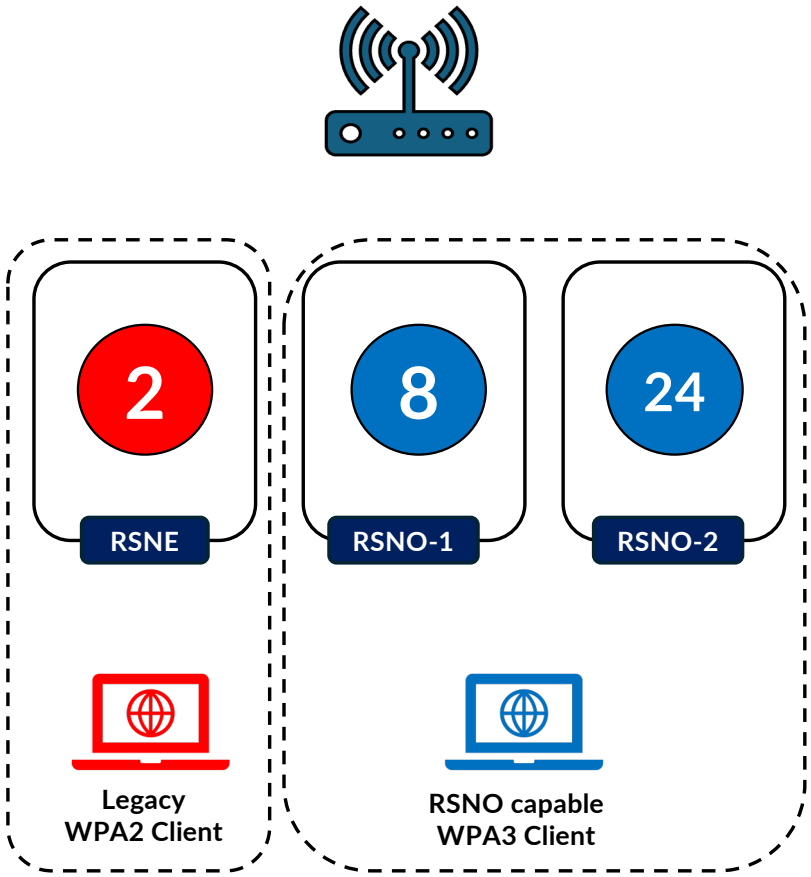


Deployment Option 3

WPA3 Personal – Compatibility Mode

RSN Override

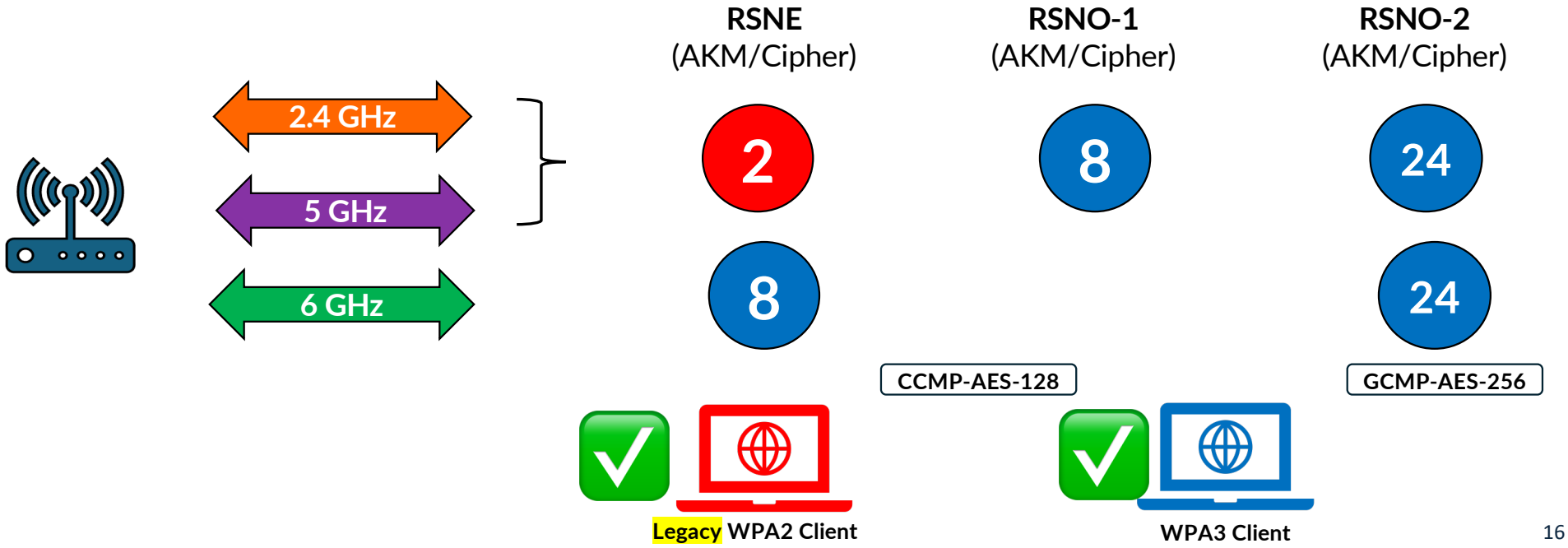
- Introduced in IEEE 802.11-2024 update
- AP advertise limited parameters in
  - RSNE
  - RSNXE
- Extended parameters advertised in
  - RSN Override -1
  - RSN Override -2
- Legacy clients ignore new elements
- WPA3 clients to use RSN Override element info
- WPA3-Specification 3.4 introduced WPA3-Compatibility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



WPA3 Personal – Compatibility Mode (1 of 2)

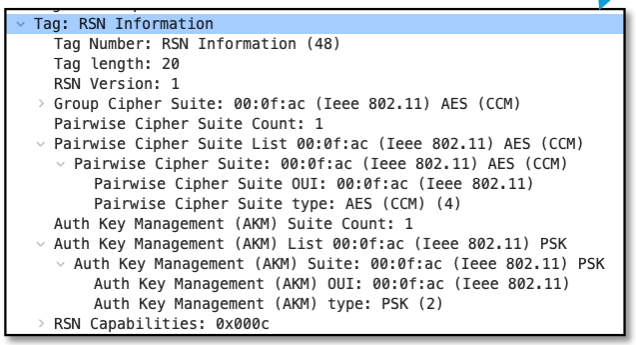
- AP only advertise **AKM-2** in 2.4/5 GHz RSNE
- AP only advertise **AKM-8** in 6 GHz RSNE
- AP advertise **AKM-8** in RSNO-1 (2.4/5 GHz)
- AP advertise **AKM-24** in RSNO-2

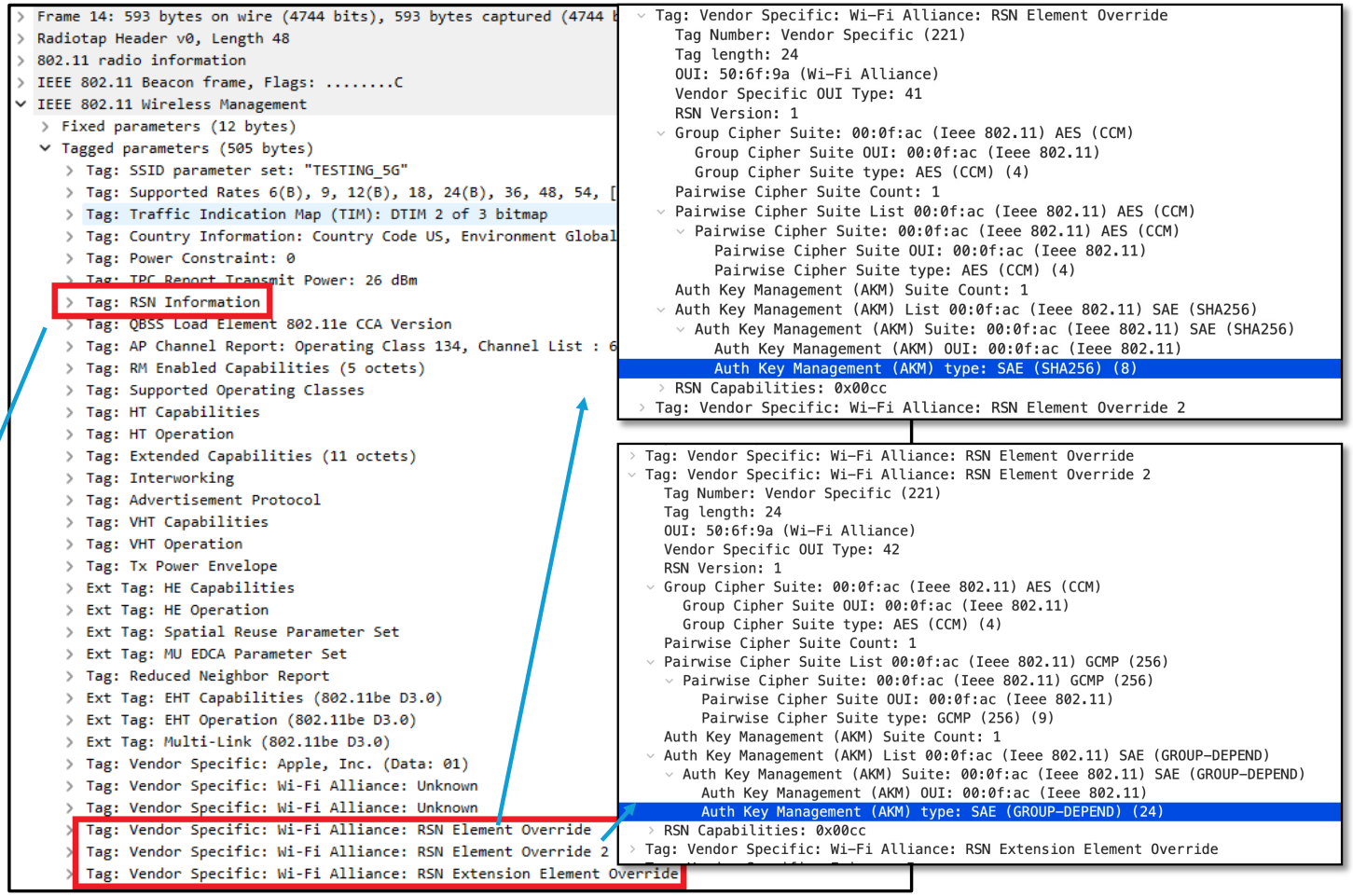
- WPA3 STA supports RSNO -> WPA3
- WPA3 STA does not support RSNO -> WPA2



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

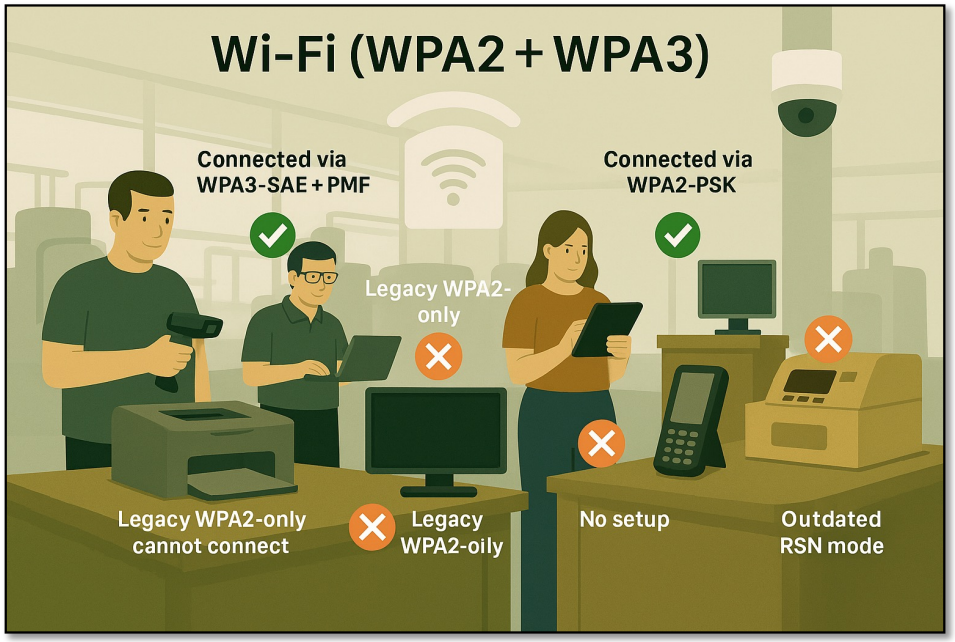


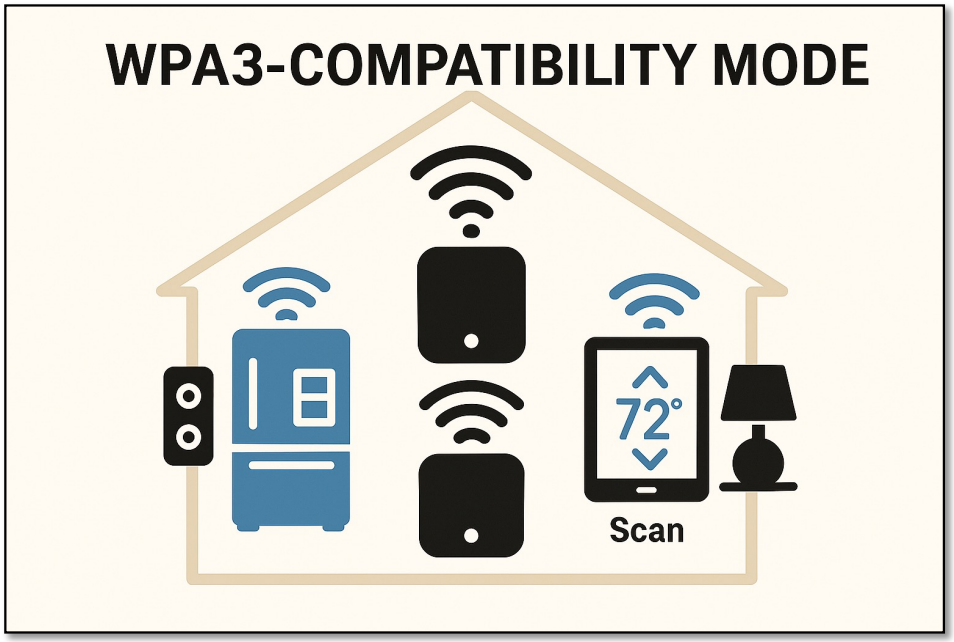


WPA3 Personal – Compatibility Mode Challenges

Compatibility Mode Use Cases

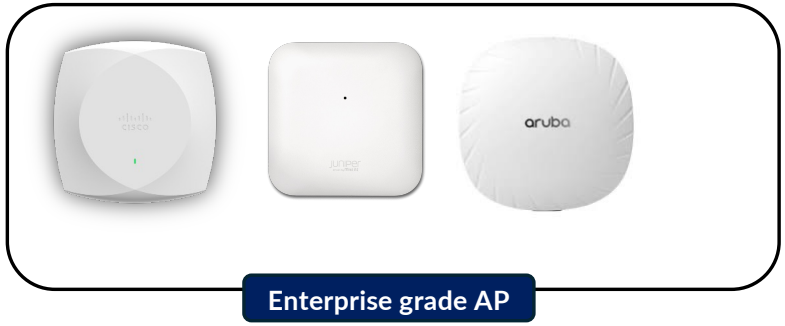
- Only if limited success with WPA3-Transition mode
- Persistency of legacy WPA2 clients



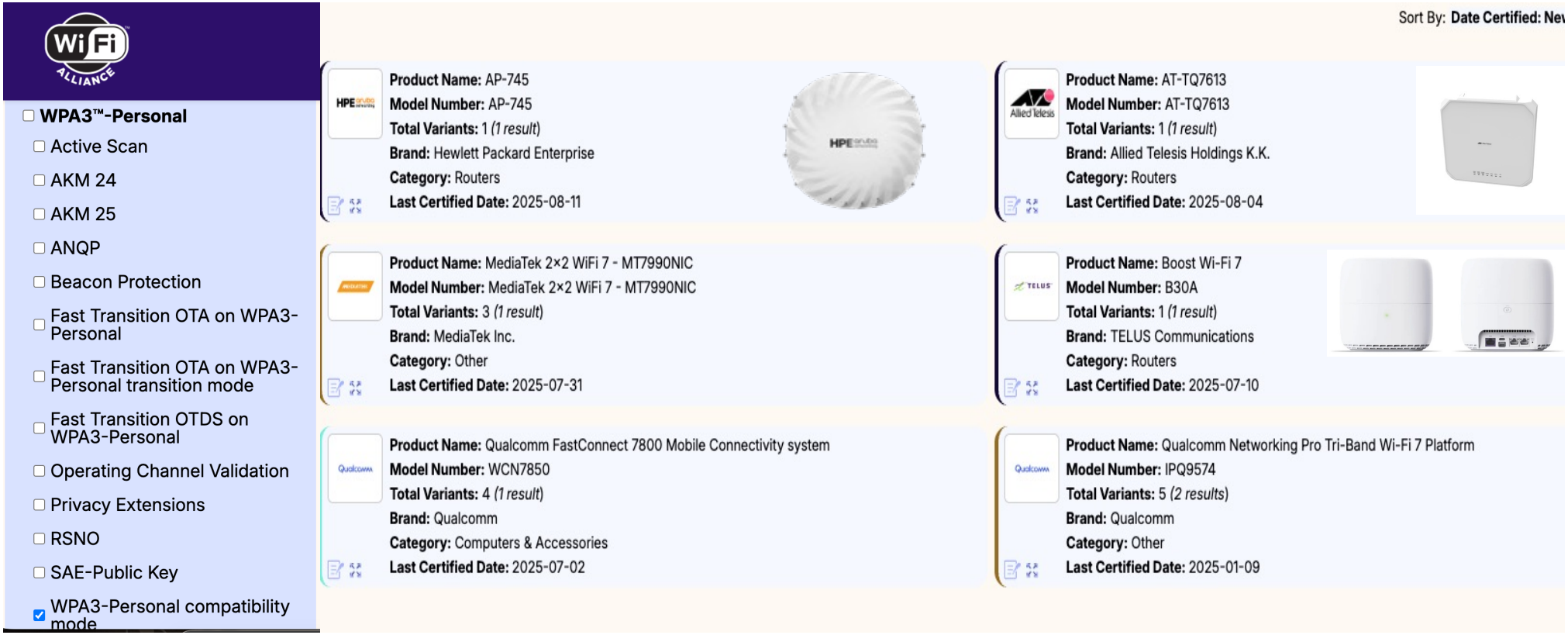


Compatibility Mode - Challenges

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



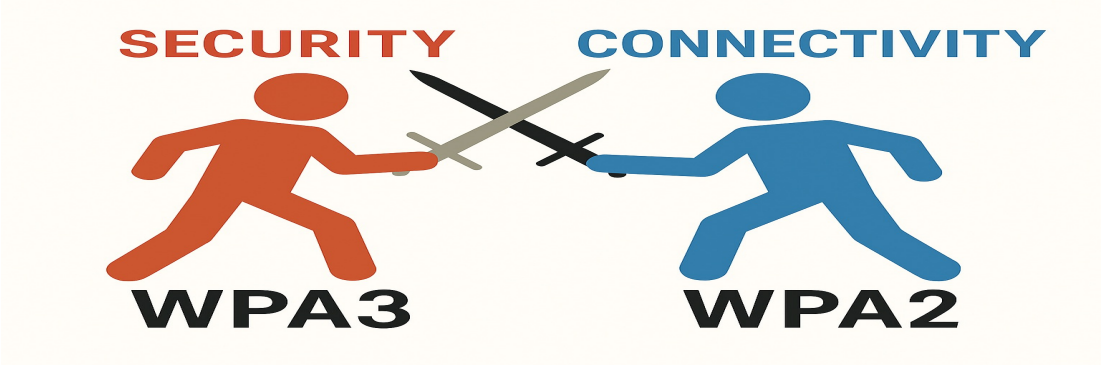
Compatibility Mode Support



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