Interoperability Insights

2026 Multi-Vendor Testing: Findings and Lessons

Gaurav Jain, Wi-Fi Alliance

October 2026

| © Wi-Fi Alliance

Real-World Interoperability Insights at Ecosystem Scale

4
Event Locations

5
Multi-Vendor Interop Events

50+
Participating Companies

300+
Commercial Devices

US . Shanghai . Beijing . Taipei

Broad Wi-Fi ecosystem participation

Chipset & Device vendors . OEMs & ODMs . Service Providers . OS vendors . Enterprise & Residential . IOT

Four Interoperability Challenges in Focus

1. **When management frames get too large**
   IoT device interoperability
2. **When more security choices challenge connectivity**
   Legacy clients and multiple AKMs/pairwise ciphers
3. **When Wi-Fi 7 client meets enterprise security**
   WPA3-Enterprise client interoperability
4. **Getting 6 GHz implementation right**
   Spectrum stewardship and opportunities for improvement

- What we observed
- Why it happened
- Why it matters
- What should be done.

1 When management frames get too large

IoT device interoperability

What we observed

- Several commercial **IoT client devices, including smartplugs, smart LED bulbs,** unable to discover or connect to the network
- In all affected cases, the device did not properly detect the SSID, resulting in connection failure at discovery/association
- The issue was observed when the AP transmitted larger Beacon and Probe Response management frames

Why it happened

- Several IoT clients appeared unable to properly process larger management frames during network discovery, for example, due to **management RX buffer too small**
- Exact root cause vary across implementations

Why it matters

- As Wi-Fi generations evolve, Beacon frames are expected to grow in length due to additional capabilities and IEs
- This is not just a point failure in one setup, but a Forward Compatibility issue
- For users, this can show up as intermittent discovery issues, onboarding failures, or inability to connect to newer AP deployments

What should be done.

- Harden client implementations around management frame reception, parsing
- **Wi-Fi CERTIFIED®**. Wi-Fi Alliance testing covers robustness to larger management frames to support forward compatibility

```
> Frame 15984: 574 bytes on wire (4592 bits), 574 bytes captured
> Radiotap Header v0, Length 48
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (486 bytes)
    > Tag: SSID parameter set: "Multi-AP-MLD-1"
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36,
    > Tag: DS Parameter set: Current Channel: 6
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    > Tag: Country Information: Country Code US, Environment Glc
    > Tag: Power Constraint: 0
    > Tag: TPC Report Transmit Power: 36, Link Margin: 0
    > Tag: Tx Power Envelope
    > Tag: RM Enabled Capabilities (5 octets)
    > Tag: AP Channel Report: Operating Class 81, Channel List :
    > Tag: ERP Information
    > Tag: Extended Supported Rates 6, 12, 24, 48, [Mbit/sec]
    > Tag: RSN Information
    > Tag: Vendor Specific: Microsoft Corp.: WPS
    > Tag: QBSS Load Element 802.11e CCA Version
    > Tag: Interworking
    > Tag: Advertisement Protocol
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: HT Information (802.11n D1.10)
    > Tag: Vendor Specific: Wi-Fi Alliance: Unknown
    > Tag: Extended Capabilities (11 octets)
    > Ext Tag: HE Capabilities
    > Ext Tag: HE Operation
    > Ext Tag: Spatial Reuse Parameter Set
    > Ext Tag: MU EDCA Parameter Set
    > Tag: Vendor Specific: Wi-Fi Alliance: Multi Band Operatior
    > Tag: FILS Indication
    > Tag: RSN eXtension (1 octet)
    > Tag: Reduced Neighbor Report
    > Ext Tag: Multi-Link (802.11be D3.0)
    > Ext Tag: EHT Capabilities (802.11be D3.0)
    > Ext Tag: EHT Operation (802.11be D3.0)
    > Tag: Vendor Specific: MediaTek Inc.
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter
    > Tag: Management MIC
```

```
> Frame 16947: 1552 bytes on wire (12416 bits), 1552 bytes captured
> Radiotap Header v0, Length 48
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  > Tagged parameters (1464 bytes)
```

2 When more security choices challenge connectivity

Legacy clients and multiple AKMs/pairwise ciphers

What we observed

- Several commercial clients, including IoT devices, tablets, phones, still fail to connect when the AP advertise **multiple pairwise cipher suites: CCMP-128 and GCMP-256 and multiple AKMs: 2 (PSK), 8, 24 (SAE)**
- **For a Wi-Fi 7 AP deployment, WPA3-Personal transition mode** with multiple AKMs and pairwise ciphers remains a prevalent security profile configuration

Why it happened

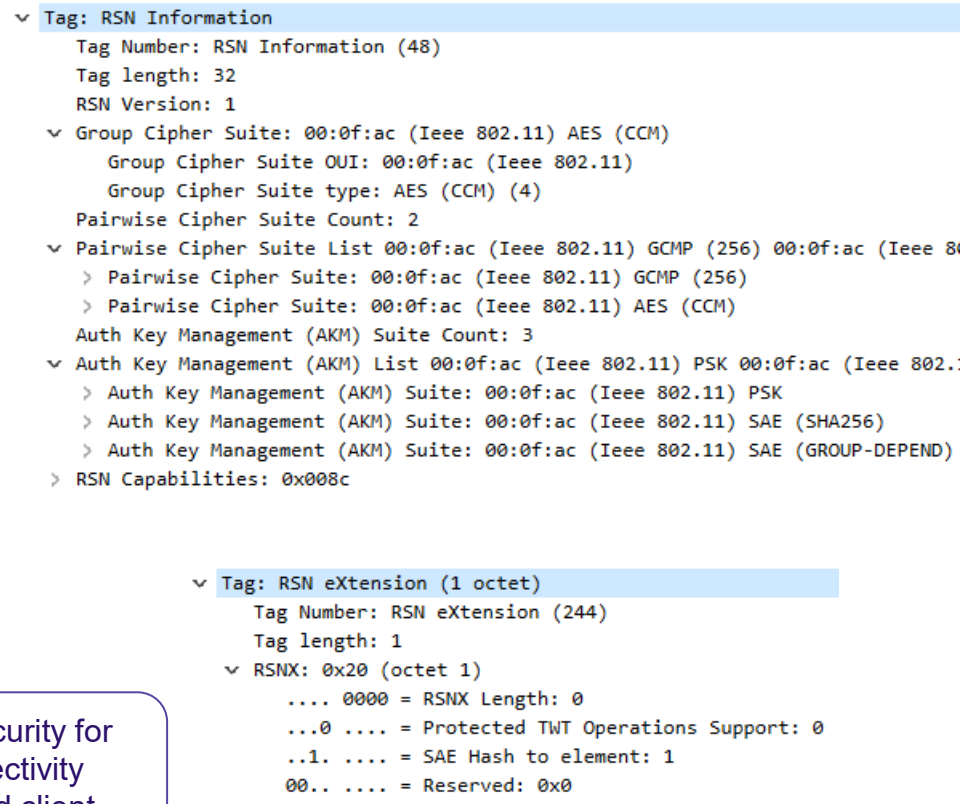
- **Cipher selection may not account for driver/hardware support:** the host supplicant can select an AP-advertised cipher that the Wi-Fi driver or hardware cannot use
- **Network profile settings may depend on the initial scan:** enabled ciphers and AKMs may reflect the AP first discovered, creating compatibility gaps when other APs in the ESS advertise different security options

Why it matters

- Advertising **multiple cipher suites and AKMs** supports legacy clients while enabling stronger security for newer devices, but gaps between host security selection and driver capabilities can prevent connectivity
- **WPA3-Personal compatibility mode offers a viable mitigation**, although support across AP and client implementations is ramping up

What should be done.

- A recommended read for implementers and deployers - **Wi-Fi Alliance Technical Note: Achieving secure network connectivity for all devices**
- **Wi-Fi CERTIFIED®.** Wi-Fi Alliance conformance tests provides comprehensive coverage for these compatibility scenarios



3 When Wi-Fi 7 client meets enterprise security

WPA3-Enterprise client interoperability

What we observed

- Multiple commercial Wi-Fi 7 smartphones failed **802.1X authentication** with WPA3-Enterprise enabled Wi-Fi 7 networks
- The failure occurred when the **affiliated AP's link MAC address (BSSID) differed from the AP MLD MAC address**.

Why it happened

- Affected clients used the AP's link-specific BSSID as the destination address, instead of the AP MLD MAC address required for a Wi-Fi 7 ML connection
- The AP driver dropped the incorrectly addressed EAP frames; 802.1X auth failed

Why it matters

- Affected clients fail connectivity to existing or new enterprise networks when Wi-Fi 7 ML is enabled (IF the AP implementation has different link and MLD MAC)
- A client-side implementation bug: This was confirmed in wpa_supplicant v2.11 (July 2024); **Fix commit - https://git.w1.fi/cgit/hostap/commit/?id=bc43e75b2b9ca3f66587f53bd0a7d4e3dcd5df5c**

What should be done.

- Wi-Fi Alliance is extending Wi-Fi CERTIFIED testing to cover such enterprise authentication scenarios
- **An upstream fix won't ensure a deployed fix:** affected products remain subject to this interoperability issue until vendors integrate and distribute the correction

```
▾ Ext Tag: Multi-Link (802.11be D3.0)
    Ext Tag length: 15 (Tag len: 16)
    Ext Tag Number: Multi-Link (802.11be D3.0) (107)
  ▸ Multi-Link Control: 0x01b0 Basic
  ▾ Common Info
      Common Info Length: 13
      MLD MAC Address: ee:f4:0c:c7:23:70 (ee:f4:0c:c7:23:70)
    ▸ Link ID subfield: 0x01
      BSS Parameters Change Count: 3
    ▸ EML Capabilities: 0x4001, EMLSR Support
    ▸ MLD Capabilities: 0x0022
    Basic STA Profile Count: 0
```

No.	Source	Destination	Protocol	Info
3663	Cisco_c7:23:6f	Broadcast	802.11	Beacon frame, SN=1535,

No.	Source	Destination	Protocol	Info
3679	06:2e:4e:53:e5:e2	Cisco_c7:23:6f	802.11	Association Request,
3684	Cisco_c7:23:6f	06:2e:4e:53:e5:e2	802.11	Association Response
4399	ee:f4:0c:c7:23:70	06:2e:4e:53:e5:e2	EAP	Request, Identity
4403	06:2e:4e:53:e5:e2	Cisco_c7:23:6f	EAP	Response, Identity
5980	Cisco_c7:23:6f	06:2e:4e:53:e5:e2	802.11	Deauthentication, SN

4 Getting 6 GHz implementation right

Spectrum stewardship and opportunities for improvement

What we observed

TPC reporting

Some commercial residential APs reported incorrect transmit power (ranging from 20 to 30 dBm) in Beacons sent on the primary 20 MHz channel, without indicating **non-HT duplicate transmission** in the Duplicate Beacon subfield

TPE reporting

- One residential LPI AP advertised 40 dBm EIRP across all bandwidths
- Two residential LPI APs advertised client PSD of 11 and 14 dBm/MHz resp. (US limit: −1 dBm/MHz)
- 6 AP models tested in LPI mode, advertised a fixed 24 dBm client EIRP across bandwidths (20/40/80/160 MHz)

Regulatory signaling

A commercial residential AP implementation set the Regulatory Info subfield in the Beacon's 6 GHz Operation Information field to **1 (Standard Power)** while operating in the **U-NII-8 sub-band**, where Standard Power operation is not permitted in the US

PSC channel selection

High concentration of consumer AP implementations appeared to select the **first available PSC (37),** and leaving the broader 6 GHz spectrum underused

Why it happened

Bad implementation!

Why it matters and what should be done.

- These issues require prompt attention. Wi-Fi Alliance has contacted the affected AP vendors, but also strongly encourages all implementers to review their 6 GHz AP behavior and make corrections where applicable
- **Get Wi-Fi CERTIFIED.** Compliance testing for these issues has been part of Wi-Fi Alliance's **6 GHz test suite for some time now.**

Wi-Fi Alliance® and Bluetooth-SIG initiate joint work to advance coexistence

Critical work is underway at Wi-Fi Alliance to protect Wi-Fi's equitable access to shared spectrum

- Safeguard deployed Wi-Fi device ecosystem as shared-spectrum use evolves
- Preserve Wi-Fi performance for current and future Wi-Fi technology applications
- Evaluate fair coexistence through collaborative technical work

Read the joint Press Release here - https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-and-bluetooth-sig-initiate-joint-work-advance-coexistence

Call for contribution and collaboration



Wi-Fi Alliance invites WLPC community to collaborate in shaping the next phase of interoperability evolution – informed by real-world deployment insights.



Your deployment insights and field data are vital to strengthening interoperability assurances and ensuring Wi-Fi delivers consistent, reliable performance for every user and environment.

Thank you!

Gaurav Jain

VP of Technology, Wi-Fi Alliance

www.wi-fi.org



FOLLOW US:

/wi-fi-alliance /wifialliance @wifialliance WiFiAlliance

Proprietary | © Wi-Fi Alliance