

Companion-BSSID Assisted PSK Discovery: Enabling WPA3-SAE in Multi-PSK (ePSK / MPSK / DPSK / iPSK) Community-Wide Wi-Fi Deployments

Azif Abdul Salam Kolisam beevi¹; Anil Kumar Reddy²

¹Director of Enterprise Solutions Engineering, San Jose, CA, USA

²Principal Engineer, Bangalore, Karnataka, India

Publication Date: 2026/10/08

Abstract

Multi-family residential communities, student housing, senior living and hospitality venues increasingly deploy a single community-wide SSID in which every resident is issued a unique pre-shared key (PSK) that is bound to a dedicated VLAN. Vendors market this capability under several names, including Enterprise PSK (ePSK), Multiple PSK (MPSK), Dynamic PSK (DPSK) and Identity PSK (iPSK), but all implementations rely on the same mechanism: the access point (AP) identifies the resident's key by performing a reverse lookup of the Message Integrity Code (MIC) contained in message 2 of the WPA2 four-way handshake against every PSK provisioned for the SSID. The Simultaneous Authentication of Equals (SAE) exchange mandated by WPA3-Personal is, by design, resistant to offline dictionary attacks, and therefore removes exactly the property on which MIC-based key identification depends. Furthermore, the 6 GHz band admits only WPA3-SAE, so multi-PSK networks cannot be extended to Wi-Fi 6E/7 clients without a new identification mechanism. This paper proposes a Companion-BSSID Assisted PSK Discovery (CAPD) algorithm that combines (i) a broadcast WPA2-PSK-only companion BSSID used exclusively for first-time onboarding and PSK discovery, (ii) a hidden primary BSSID with the same SSID operating in WPA2/WPA3 transition mode, (iii) a per-station PSK binding cache, and (iv) IEEE 802.11v BSS Transition Management (BTM) to steer the onboarded client to the primary BSSID, where SAE is executed using the already-learned PSK. The approach requires no client software change, no SAE password identifier support and no modification to the SAE protocol. The design, algorithm, complexity and security properties are presented, and an experimental evaluation across a broad range of commercial client devices demonstrates seamless transition with per-resident VLAN isolation preserved.

Keywords: WPA3, SAE, Multiple PSK, ePSK, DPSK, iPSK, MPSK, IEEE 802.11v, BSS Transition Management, 6 GHz, Multi-Dwelling Unit, Wi-Fi Security, VLAN Isolation.

I. INTRODUCTION

Wireless connectivity has become a core utility in multi-dwelling unit (MDU) properties such as apartment complexes, condominiums, student housing and assisted-living communities. Operators increasingly replace per-unit consumer routers with a managed, property-wide Wi-Fi network. The preferred user experience is a single community-wide SSID that residents can use anywhere on the property: in their unit, in the gym, at the pool or in the leasing office. At the same time, each resident expects the privacy of a home network: their smart TV, printer and personal devices must not be visible to neighbours.

The industry answer has been to issue each resident a unique PSK on the shared SSID and to map that PSK to a dedicated VLAN (or equivalent per-resident network segment). The AP determines which resident is connecting by identifying which PSK the client used, and places the client's traffic into the corresponding VLAN. Vendors refer to the feature as Enterprise PSK (ePSK), Multiple PSK (MPSK), Dynamic PSK (DPSK), Identity PSK (iPSK) or Private PSK (PPSK); functionally these implementations are equivalent, and in this paper we refer to them collectively as *multi-PSK*.

Under WPA2-Personal, multi-PSK works because the four-way handshake exposes enough material for the

AP to test every candidate PSK offline: after the client returns its SNonce and MIC in EAPOL-Key message 2 (M2), the AP can derive a candidate Pairwise Transient Key (PTK) for each provisioned PSK and check which one reproduces the received MIC. The disclosure of the Key Reinstallation Attacks (KRACK) in 2017 [2] and the long-standing susceptibility of WPA2-PSK to offline dictionary attacks accelerated industry adoption of WPA3-Personal [5], which replaces PSK-based PMK derivation with the SAE password-authenticated key exchange [1], [3]. SAE deliberately prevents an observer, and equally the AP itself, from testing multiple passwords against a single exchange. The MIC-based reverse lookup is therefore no longer possible.

The problem is made more pressing by spectrum regulation and certification policy. The 6 GHz band opened for unlicensed use in 2020 [9] admits only WPA3-SAE (with hash-to-element), Enhanced Open (OWE) or WPA3-Enterprise; WPA2-PSK and WPA3 transition mode are not permitted [5], [10]. A multi-PSK community network that remains on WPA2 is therefore unable to offer Wi-Fi 6E and Wi-Fi 7 capacity to its residents.

➤ *This Paper Makes the Following Contributions:*

- We formalise why MIC-based multi-PSK identification fails under WPA3-SAE and why simply configuring WPA2/WPA3 transition mode does not solve the problem for multi-PSK networks.
- We propose Companion-BSSID Assisted PSK Discovery (CAPD), a two-phase algorithm that learns a client's PSK on a WPA2-only companion BSSID and

then uses IEEE 802.11v BTM to move the client to a hidden WPA2/WPA3 primary BSSID of the same SSID, where SAE is performed with the learned PSK.

- We describe how CAPD extends multi-PSK to the 6 GHz band, handles clients without 802.11v support, and interacts with MAC address randomisation, roaming and binding expiry.
- We analyse the computational cost and the security properties of the scheme, and report an experimental evaluation across a broad set of commercial client devices demonstrating seamless onboarding and transition with per-resident VLAN isolation preserved.

The remainder of the paper is organised as follows. Section 2 reviews the relevant background. Section 3 discusses related approaches. Section 4 presents the CAPD architecture and Section 5 the algorithm. Section 6 analyses complexity and Section 7 security. Section 8 reports the experimental evaluation, Section 9 discusses limitations, and Section 10 concludes.

II. BACKGROUND

➤ *Multi-PSK and Per-Resident Network Segmentation*

In a multi-PSK deployment the network administrator provisions a database of tuples $\langle \text{PSK}_i, \text{Resident}_i, \text{VLAN}_i \rangle$, $i = 1 \dots N$, associated with a single SSID. The database may reside on the AP, on a WLAN controller, in a cloud management platform, or on a RADIUS server that returns the PSK and VLAN as vendor-specific attributes. Table 1 summarises the terminology used by the industry for this feature.

Table 1 Industry Terminology for Per-User PSK on a Shared SSID

Term	Description
ePSK -Enterprise PSK	Per-user or per-group PSKs on one SSID, each mapped to its own VLAN / policy.
MPSK -Multiple PSK	Multiple PSKs configured or returned by RADIUS for one SSID; the matching key selects the user role.
DPSK -Dynamic PSK	Unique, automatically generated PSK per user or device, commonly issued through a portal or property-management integration.
iPSK -Identity PSK	PSK bound to an identity (user or device) and delivered via RADIUS with VLAN / ACL attributes.
PPSK -Private PSK	Per-user private key on a shared SSID; used by several vendors with the same semantics.

Regardless of the name, the defining property is that the key selected by the client determines the resident identity and therefore the VLAN. Because each VLAN is a separate layer-2 broadcast domain, resident A's devices cannot discover or reach resident B's devices, while both residents enjoy property-wide roaming on one SSID.

➤ *WPA2-PSK Four-Way Handshake and MIC-Based PSK Identification*

In WPA2-Personal the Pairwise Master Key (PMK) is derived deterministically from the passphrase and SSID:

$$\text{PMK} = \text{PBKDF2-HMAC-SHA1}(\text{PSK}, \text{SSID}, 4096, 256)(1)$$

After association, the AP (authenticator, address AA) sends EAPOL-Key M1 carrying ANonce. The client

(supplicant, address SPA) chooses SNonce, derives the PTK and returns M2 containing SNonce and a MIC computed with the Key Confirmation Key (KCK) portion of the PTK:

$$\text{PTK} = \text{PRF-384}(\text{PMK}, \text{"Pairwise key expansion"}, \min(\text{AA}, \text{SPA}) \parallel \max(\text{AA}, \text{SPA}) \parallel \min(\text{ANonce}, \text{SNonce}) \parallel \max(\text{ANonce}, \text{SNonce})) \quad (2)$$

$$\text{MIC} = \text{HMAC-SHA1-128}(\text{KCK}, \text{EAPOL-Key M2}), \text{KCK} = \text{PTK}[0..127] \quad (3)$$

Because every input except the PMK is visible to the AP after receiving M2, the AP can compute Eq. (2)–(3) for each candidate PMK_i and select the unique index k for which the computed MIC equals the received MIC. The

PMK_i values can be pre-computed once per SSID, so each test costs only one PRF and one HMAC operation. This is the basis of every commercial multi-PSK implementation. The same property, however, also enables a passive eavesdropper who captures M1/M2 to mount an offline dictionary attack against the passphrase [4].

➤ *KRACK and the Transition to WPA3*

In 2017 Vanhoef and Piessens disclosed the Key Reinstallation Attacks (KRACK), which manipulate and replay handshake messages to force nonce reuse in the four-way and group-key handshakes [2]. Although KRACK was mitigated by client and AP patches, together with the offline-dictionary weakness of WPA2-PSK it motivated the Wi-Fi Alliance to introduce WPA3 in 2018 [5]. WPA3-Personal replaces PSK-derived PMKs with SAE, mandates Protected Management Frames (PMF), and defines a WPA2/WPA3 *transition mode* in which one BSS advertises both AKM 2 (PSK) and AKM 8 (SAE) so that legacy clients can continue to connect.

➤ *Simultaneous Authentication of Equals (SAE)*

SAE, specified in IEEE 802.11-2020 [1] and derived from the Dragonfly key exchange [3], [6], is a balanced password-authenticated key exchange. Both parties map the password (and, with hash-to-element, the SSID and an optional password identifier) to a group element PWE. Each party then chooses secret values *rand* and *mask* and exchanges an SAE Commit message containing:

$$scalar = (rand + mask) \bmod r, element = -mask \cdot PWE \quad (4)$$

and computes the shared secret

$$K = rand \cdot (scalar_{peer} \cdot PWE + element_{peer}), k = F(K) \quad (5)$$

SAE Confirm messages then prove knowledge of *k*, and the resulting PMK is used in a subsequent four-way handshake. The critical property for this work is that each SAE exchange tests exactly one password. The AP must commit to a PWE, and therefore to a specific password, *before* it can compute *K*; if it commits to the wrong password the exchange simply fails, and the transcript gives neither party any information that allows other candidate passwords to be tested offline. This is precisely the offline-dictionary resistance that makes SAE attractive [7], and it makes MIC-style reverse lookup across *N* PSKs impossible. An AP could only discover the correct key by running up to *N* complete online SAE exchanges with the client, which clients do not tolerate (they abort after a failed Confirm and typically blacklist the BSS temporarily).

Configuring the community SSID in WPA2/WPA3 transition mode does not solve the problem either: WPA3-capable clients will prefer AKM 8 (SAE) on the transition-mode BSS, at which point the AP again has no means to determine which of the *N* keys the client holds.

➤ *6 GHz Band Constraints*

In April 2020 the U.S. FCC opened 1200 MHz of spectrum at 5.925–7.125 GHz for unlicensed use [9], with

other regulators following. The Wi-Fi Alliance requires that 6 GHz BSSs use WPA3-Personal with SAE hash-to-element (H2E) only, OWE or WPA3-Enterprise, with PMF mandatory; WPA2-PSK and WPA3 transition mode are prohibited in 6 GHz [5], [10]. Consequently, a multi-PSK SSID can only be extended to 6 GHz if the AP can identify the resident's PSK *without* a WPA2 handshake on that band.

➤ *IEEE 802.11v BSS Transition Management*

IEEE 802.11v (Wireless Network Management), now incorporated into IEEE 802.11-2020 [1], [8], defines the BSS Transition Management (BTM) protocol. An AP sends a BTM Request frame containing a candidate list of preferred BSSIDs (Neighbor Report elements); a client that advertises BSS Transition support (Extended Capabilities, bit 19) evaluates the request and typically reassociates to the recommended BSSID, returning a BTM Response. BTM is widely supported by contemporary smartphones, laptops and tablets, and is used today for load balancing and band steering. CAPD reuses BTM as a *security-state* steering mechanism.

III. RELATED WORK AND ALTERNATIVE APPROACHES

Several alternatives exist for delivering per-resident segmentation with WPA3-level security. Table 2 compares them against the requirements of an MDU deployment.

➤ *SAE Password Identifiers*

IEEE 802.11-2020 allows a client to send a Password Identifier element in its SAE Commit, naming which password it is using [1]. This is the standards-native solution, but it requires the identifier to be configured on the client alongside the password. Mainstream consumer operating systems do not expose a user interface for SAE password identifiers, so the mechanism is not practical for resident self-provisioning today.

➤ *One SSID per Resident*

Separate SSIDs trivially map to separate VLANs but do not scale: beacon and probe overhead grows linearly with the number of SSIDs, and most APs limit the number of BSSIDs per radio (commonly 8–16).

➤ *WPA3-Enterprise (802.1X) / Passpoint*

Per-user credentials with RADIUS-assigned VLANs give strong security [11], but many residential devices (smart TVs, game consoles, streaming sticks, IoT) cannot perform 802.1X, and certificate or EAP onboarding creates a support burden unsuitable for residents.

➤ *Multi-PSK on WPA2 Only / Transition-Mode Fallback*

Keeping the SSID WPA2-only, or forcing multi-PSK clients to AKM 2 on a transition-mode BSS, preserves segmentation but forfeits WPA3 protection and excludes 6 GHz entirely.

➤ MAC-Based Pre-Registration

Binding a device MAC address to a PSK in advance avoids lookup but is defeated by MAC address

randomisation, now enabled by default on major mobile and desktop operating systems, and imposes an administrative registration step.

Table 2 Comparison of Approaches for Per-Resident Segmentation on WPA3

Approach	Single SSID	WPA3 / 6 GHz	No client config change	Works with IoT	Scales to 100s
SAE Password Identifier	Yes	Yes	No	No	Yes
SSID per resident	No	Yes	Yes	Yes	No
WPA3-Enterprise / Passpoint	Yes	Yes	No	No	Yes
WPA2 multi-PSK only	Yes	No	Yes	Yes	Yes
MAC pre-registration	Yes	Yes	Partly	Yes	Partly
CAPD (proposed)	Yes	Yes	Yes	Yes ¹	Yes

¹ IoT clients without SAE or BTM support remain on the WPA2 companion BSSID with full VLAN isolation (Section 5.5).

Our work is complementary to the SAE hardening literature [7], [12] and to research on steering via 802.11v/k/r; to the best of our knowledge, it is the first to use BTM specifically to bridge a WPA2 key-discovery phase into a WPA3-SAE association for multi-PSK networks.

IV. PROPOSED ARCHITECTURE

CAPD introduces no new frame formats and requires no client modification. It re-arranges existing IEEE 802.11 mechanisms on the AP side. Figure 1 shows the architecture.

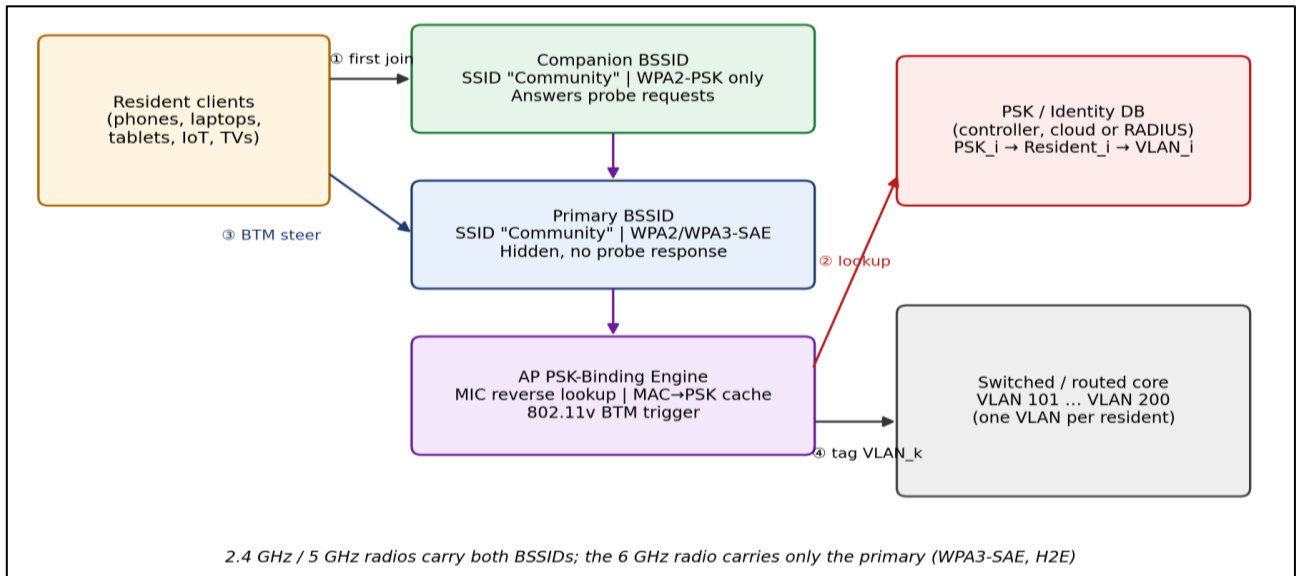


Fig 1 CAPD Architecture: Companion and Primary BSSIDs Share One SSID; the PSK-Binding Engine Links WPA2 Discovery to WPA3 Association.

➤ Components

• Companion BSSID (C-BSS)

Advertises the community SSID with WPA2-PSK (AKM 2) only. It is the *only* BSS that responds to probe requests from unknown stations and its beacons are broadcast normally. It carries all N resident PSKs and performs MIC-based reverse lookup. It is configured on the 2.4 GHz and 5 GHz radios.

• Primary BSSID (P-BSS)

Uses the *same SSID string*, configured in WPA2/WPA3 transition mode (AKM 2 + AKM 8, PMF capable) on 2.4/5 GHz and WPA3-SAE-H2E only (PMF required) on 6 GHz. It is hidden: the SSID is suppressed in beacons and the BSS does not answer probe requests from stations without a valid binding. It never performs a PSK search; it only uses a PSK already bound to the station.

• PSK Binding Table (B)

A table keyed by station MAC address, storing (PSK_k, Resident_k, VLAN_k, timestamp, TTL). It is populated after a successful WPA2 lookup on the C-BSS and consulted when the station starts SAE on the P-BSS. In multi-AP deployments it is synchronised through the controller or cloud so that bindings follow the client when it roams.

• Steering Agent

Issues an 802.11v BTM Request to the station immediately after the WPA2 handshake on the C-BSS completes, nominating the P-BSS (and, where available, its co-located 6 GHz BSSID via a Neighbor Report) as the preferred candidate.

Table 3 Recommended WLAN Profile Configuration

Parameter	Companion BSSID	Primary BSSID
SSID string	Community (same)	Community (same)
Security (2.4 / 5 GHz)	WPA2-PSK (AKM 2) only	WPA2/WPA3 transition (AKM 2 + 8)
Security (6 GHz)	Not configured	WPA3-SAE, H2E only (AKM 8/24)
PMF (802.11w)	Optional	Capable (2.4/5); Required (6 GHz)
SSID broadcast	Yes	Hidden
Probe response	All stations	Only stations with valid binding
802.11v BTM	Enabled (sender)	Enabled
PSK source	Full resident PSK database	Binding table only
VLAN assignment	VLAN_k from lookup	VLAN_k from binding

Using the same SSID string on both BSSIDs is a deliberate design choice. Modern operating systems derive randomised ("private") MAC addresses per SSID, so the client presents the same MAC address on the companion and primary BSSIDs. This allows the binding learned in phase 1 to be found in phase 2 without any pre-registration, and it means that the client stores a single network profile, "Community", with a single passphrase.

V. THE CAPD ALGORITHM

CAPD operates in two phases: an onboarding and PSK-discovery phase on the companion BSSID, followed by a steady-state WPA3-SAE phase on the primary BSSID. Figure 2 shows the message sequence and Figure 3 the AP-side decision logic.

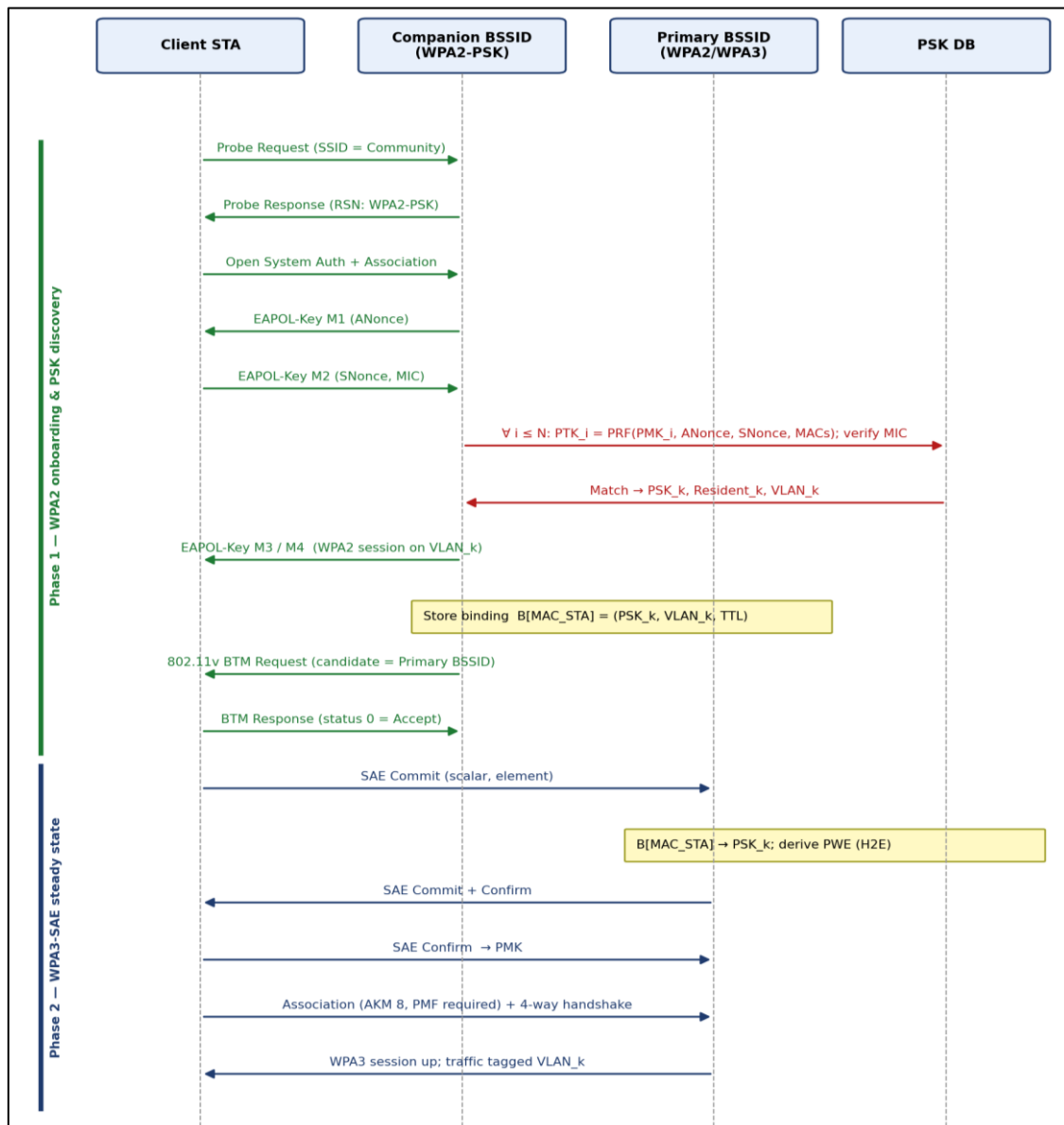


Fig 2 CAPD Message Sequence: WPA2 Onboarding with MIC Reverse Lookup, 802.11v Steering, and WPA3-SAE Association Using the Learned PSK.

➤ Phase 1: WPA2 Onboarding and PSK Discovery

- A new client scans for the community SSID. Because the primary BSSID is hidden and suppresses probe responses, only the companion BSSID is discovered, advertising WPA2-PSK.
- The client performs open-system authentication and association with the companion BSSID, then the AP sends EAPOL-Key M1 containing ANonce.
- The client, configured with the resident's passphrase, returns M2 containing SNonce and the MIC.
- The AP iterates over the pre-computed PMK_1 ... PMK_N, deriving PTK_i by Eq. (2) and testing the MIC by Eq. (3). On a match at index k, the AP completes M3/M4, places the client on VLAN_k and records the binding B[MAC_STA] = (PSK_k, VLAN_k, TTL). If no PSK matches, the AP deauthenticates the client (reason code 15, 4-way handshake timeout) and applies rate limiting to that MAC address.
- If the client advertises BSS Transition support and WPA3/SAE capability (inferred from its RSN capabilities in probe/association frames and its supported-bands information), the AP sends a BTM Request with the primary BSSID as the preferred

candidate. For 6 GHz-capable clients the 6 GHz primary BSSID is listed with the highest preference.

➤ Phase 2: WPA3-SAE Association on the Primary BSSID

- The client accepts the BTM Request and initiates SAE authentication with the primary BSSID, using the *same* passphrase it holds for the "Community" profile.
- On receipt of the SAE Commit, the AP looks up B[MAC_STA]. If a valid binding exists, the AP derives PWE from PSK_k (hunting-and-pecking or H2E, as negotiated) and completes a standard SAE exchange. Because the client used the same passphrase, the exchange succeeds on the first attempt.
- The client associates using AKM 8 (or AKM 24 for SAE-EXT-KEY), PMF is negotiated, and the four-way handshake installs keys derived from the SAE PMK. Traffic is tagged with VLAN_k, exactly as in phase 1.
- If no valid binding exists (e.g., the binding has expired or the client connected directly to the hidden BSSID from a stale profile), the AP rejects the SAE authentication. The client re-scans, discovers the companion BSSID and re-enters phase 1, which re-establishes the binding transparently.

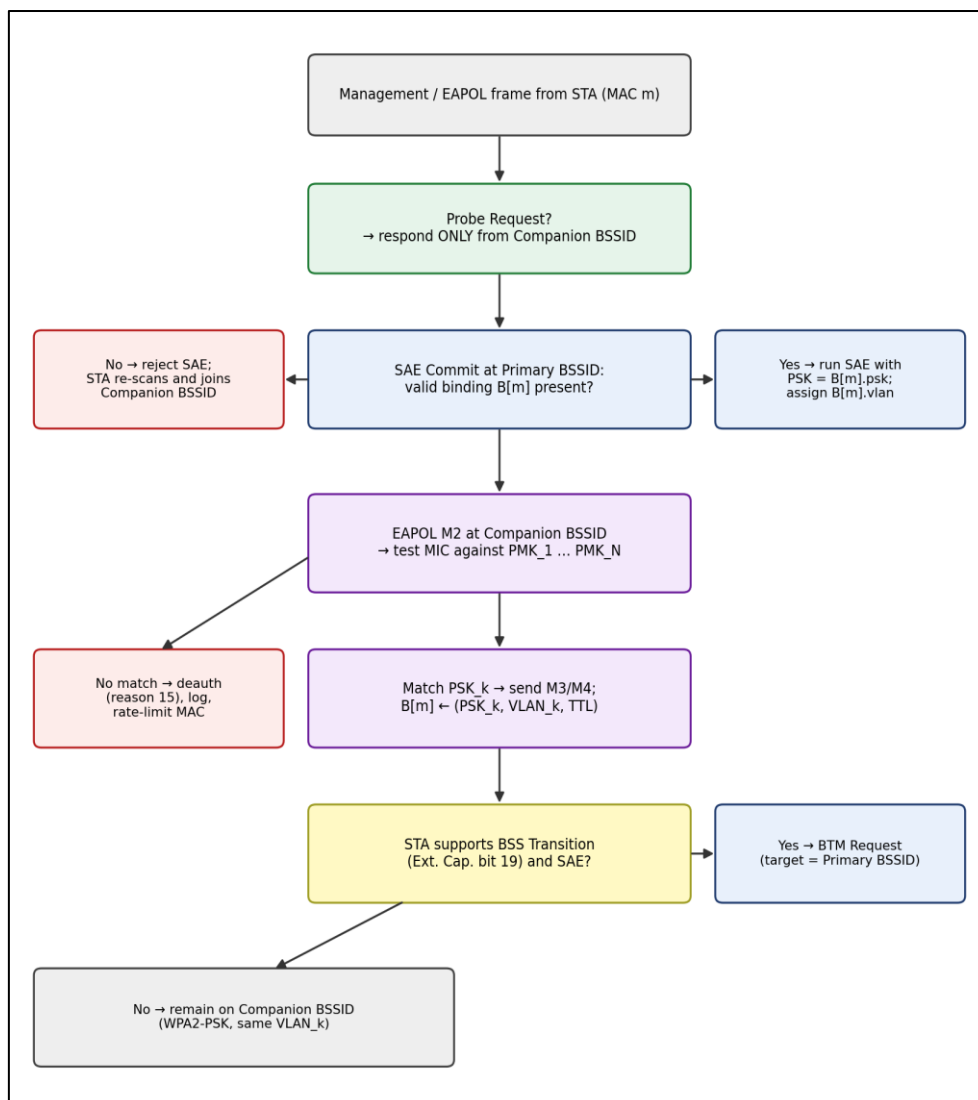


Fig 3 AP-Side Decision Flow for CAPD.

➤ Algorithm Specification

• Algorithm 1. Companion-BSSID Assisted PSK Discovery (AP Side)

Input : SSID S; resident DB D = {(PSK_i, R_i, VLAN_i)}, i = 1..N

companion BSSID C (WPA2-PSK), primary BSSID P (WPA2/WPA3, hidden)
State : binding table B : MAC → (psk, vlan, expiry)

Init : for i in 1..N: PMK[i] ← PBKDF2(PSK_i, S, 4096, 256)

on ProbeRequest(m, S) at radio r:

 respond from C // P never answers unsolicited probes
 if B[m] valid: also allow P response // optional, for fast reconnect

on EAPOL_M2(m, ANonce, SNonce, MIC) at C:

 for i in 1..N:
 PTK ← PRF384(PMK[i], AA, m, ANonce, SNonce)

 if HMAC_SHA1_128(PTK.KCK, M2) == MIC:
 send M3; await M4
 assign VLAN_i to m
 B[m] ← (PSK_i, VLAN_i, now + TTL); sync B[m] to controller
 if BTM_capable(m) and SAE_capable(m):
 send BTM_Request(m, candidates = [P_6GHz, P_5GHz, P_2.4GHz])
 return
 deauth(m, reason = 15); rate_limit(m)

on SAE_Commit(m, scalar, element) at P:

 if B[m] invalid: reject_auth(m); return // client falls back to C
 PWE ← derive_PWE(B[m].psk, S, H2E?)
 run standard SAE (Commit/Confirm) with PWE
 on success: associate(m, AKM 8/24, PMF); assign B[m].vlan;
 refresh B[m].expiry

on BTM_Response(m, status != Accept) or no SAE within T_{steer}:

 keep m on C (WPA2) with VLAN B[m].vlan; retry BTM after backoff

➤ Roaming and Multi-AP Operation

Community networks comprise tens to hundreds of APs. The binding table is therefore maintained centrally (controller or cloud) and pushed, or fetched on demand, by each AP. When a client roams from one AP to another, it performs SAE with the new AP's primary BSSID; the new AP retrieves B[MAC_STA] and completes SAE without any WPA2 phase. SAE PMK caching and, where supported, Fast BSS Transition (802.11r, FT-SAE) further reduce roaming latency. Because PMK caching and FT operate on the PMK derived from the correct PSK, they are unaffected by CAPD.

➤ Clients Without BTM or SAE Support

Legacy clients that do not support SAE (e.g., older IoT devices) or do not advertise BSS Transition capability are simply left on the companion BSSID. They continue to receive the same per-resident VLAN assignment and therefore the same isolation guarantees as today's WPA2 multi-PSK networks. CAPD thus degrades gracefully to the status quo and never reduces service for any device class.

➤ Binding Lifetime and MAC Randomisation

The binding TTL should exceed the typical reconnection interval of resident devices (e.g., 7–30 days, refreshed on every successful association) while bounding stale state. Operating systems that rotate private MAC addresses periodically will present a new MAC after rotation; the AP then has no binding, rejects SAE on the primary BSSID, and the client transparently repeats phase 1. Because phase 1 costs a single WPA2 association plus one BTM, rotation causes no user-visible disruption.

➤ Extending Multi-PSK to 6 GHz

The companion BSSID cannot exist on 6 GHz, but it does not need to. A tri-band client first discovers the companion BSSID on 2.4 or 5 GHz, where the PSK is learned. The BTM Request then nominates the 6 GHz primary BSSID; the client performs SAE-H2E on 6 GHz with the learned PSK. Subsequent 6 GHz reconnections and roams use the binding directly. CAPD therefore makes the full multi-PSK feature set available on Wi-Fi 6E and Wi-Fi 7 without violating the 6 GHz security requirements.

VI. COMPUTATIONAL COMPLEXITY

Let N be the number of resident PSKs on the SSID. PBKDF2 (Eq. 1) is by far the most expensive primitive (4096 iterations of HMAC-SHA1 × 2 blocks), but it depends only on the PSK and SSID, so all N PMKs are pre-computed once at provisioning time and whenever a key is added or changed. Because the companion and primary BSSIDs share the SSID string, a single PMK table serves both.

Per onboarding event, phase 1 requires at most N evaluations of PRF-384 and HMAC-SHA1-128, i.e. O(N) with a small constant (approximately 4 SHA-1 compressions for the PRF and 2–3 for the MIC per candidate). On average N/2 candidates are tested. For N = 100 this is on the order of a few hundred SHA-1 compressions, which completes in well under a millisecond on contemporary AP CPUs and is negligible compared with over-the-air handshake latency. For large properties (N in the thousands) the search can be parallelised across cores or offloaded to the controller.

Phase 2 costs exactly one SAE exchange, identical to any standard WPA3-Personal association; the binding lookup is O(1) using a hash table keyed by MAC address. CAPD therefore adds no cryptographic cost to steady-state

WPA3 operation, and its one-off onboarding cost is equal to that of today's WPA2 multi-PSK.

Table 4 Per-Client Cost Summary

Operation	When	Cost
PMK pre-computation	Provisioning / key change	$N \times \text{PBKDF2 (offline)}$
MIC reverse lookup	Phase 1 (first join, MAC change, binding expiry)	$\leq N \times (\text{PRF} + \text{HMAC}), \text{avg } N/2$
BTM Request / Response	Phase 1 $\rightarrow$ 2	2 management frames
Binding lookup	Every SAE on P-BSS	$O(1)$
SAE exchange	Every WPA3 association	1 standard SAE

VII. SECURITY ANALYSIS

We analyse CAPD against the threats relevant to a community network. Table 5 summarises the analysis.

➤ *Steady-State Protection*

Once a client is on the primary BSSID, its session is a standard WPA3-SAE session with PMF. It inherits SAE's forward secrecy and resistance to offline dictionary attacks: an attacker who records the SAE exchange cannot test candidate passphrases offline. Implementations should incorporate the post-Dragonblood mitigations [7], in particular constant-time PWE derivation and H2E, which is mandatory in 6 GHz and recommended on all bands.

➤ *Exposure During Onboarding*

Phase 1 is a WPA2-PSK handshake, so a passive attacker who captures M1/M2 during onboarding could attempt an offline dictionary attack against that resident's passphrase. This exposure is identical to -and strictly less than -that of today's WPA2 multi-PSK networks, in which every association is WPA2. It is minimised by (i) issuing high-entropy, randomly generated PSKs (e.g., ≥ 12 random characters), which is already the norm for DPSK/iPSK platforms, and (ii) the fact that phase 1 is executed only on first join, MAC rotation or binding expiry.

➤ *The Binding is Not a Credential*

An attacker might spoof a victim's MAC address to exploit an existing binding. This gains nothing: the binding

only tells the AP *which* PSK to use in SAE. To complete SAE the attacker must still know PSK_k; without it, the SAE Confirm fails. Conversely, an attacker who knows only their own PSK cannot use a victim's binding to reach the victim's VLAN. The binding table can therefore be treated as non-secret state, although it should still be integrity-protected when synchronised between APs.

➤ *Downgrade Considerations*

Because the companion BSSID remains available, a WPA3-capable client could be induced (e.g., by an attacker jamming the primary BSSID) to stay on WPA2. This is the same downgrade surface as any WPA2/WPA3 transition-mode network [7]. Operators may reduce it by monitoring the proportion of SAE-capable clients that remain on the companion BSSID, by re-issuing BTM periodically, and by restricting the companion BSSID to the 2.4/5 GHz bands. The WPA3 Transition Disable indication [5] could further lock clients to SAE, but it would prevent re-onboarding after MAC rotation or binding expiry; we therefore do not enable it by default and leave its selective use to future work.

➤ *Denial of Service*

An attacker could flood the companion BSSID with forged M2 frames to force repeated $O(N)$ searches. Standard defences apply: per-MAC rate limiting, limiting concurrent handshakes, and blacklisting MACs after repeated failures. On the primary BSSID, SAE anti-clogging tokens protect against commit flooding [1].

Table 5 Threat and Mitigation Summary

Threat	Impact Under CAPD	Mitigation
Offline dictionary attack (steady state)	Not possible (SAE)	Inherent to SAE; H2E
Offline dictionary attack (onboarding)	Possible on phase-1 capture only	High-entropy PSKs; phase 1 is infrequent
MAC spoofing of binding	SAE fails without PSK _k	Binding is not a credential
Cross-resident traffic access	Prevented	Per-resident VLAN from PSK identity
Downgrade to WPA2	Same as transition mode	Monitoring, periodic BTM, band restriction
Handshake / commit flooding	CPU load	Rate limiting; SAE anti-clogging
KRACK-class attacks	Mitigated on WPA3 sessions	Patched stacks; PMF required

VIII. EXPERIMENTAL EVALUATION

➤ *Testbed*

CAPD was implemented in the firmware of an enterprise-class tri-band access point and evaluated in a laboratory environment representative of an MDU deployment. The testbed comprised 4 APs of Cambium X7-35X model managed by cnMaestro X, with a community SSID provisioned with 1,000 resident PSKs,

each mapped to a unique VLAN (VLAN 101–1001), trunked to a layer-3 switch with inter-VLAN routing disabled between resident VLANs. Over-the-air traffic was captured with another X7-35X in a sniffer mode to verify frame sequences.

➤ Methodology

Each client device was provisioned with its resident's passphrase for the "Community" network and subjected to the following test cases:

- **TC1 First Join:**

Client discovers only the companion BSSID and completes WPA2 onboarding; correct PSK identified from 100 candidates.

- **TC2 Steering:**

BTM Request issued and accepted; client performs SAE on the primary BSSID and associates with AKM 8/24 and PMF.

- **TC3 VLAN Isolation:**

Client receives an address in its resident VLAN; ARP, ICMP and mDNS/SSDP discovery towards devices of other residents fail.

- **TC4 Reconnect:**

Wi-Fi toggled off/on and device rebooted; client reconnects directly to the primary BSSID using the stored binding.

- **TC5 Roaming:**

Client roams between APs and remains on WPA3 in the same VLAN.

- **TC6 6 GHz (6E/7 Clients Only):**

Client is steered to, and associates on, the 6 GHz primary BSSID using SAE-H2E.

- **TC7 Recovery:**

Binding manually cleared / private MAC rotated; client transparently repeats phase 1 and returns to WPA3.

➤ Results

Table 6 summarises results by client category. All tested clients completed onboarding with the correct PSK identified, accepted the BTM steering, and connected to the primary BSSID with WPA3-SAE while preserving per-resident VLAN isolation. No user interaction beyond entering the passphrase once was required, and users did not observe the transition between BSSIDs.

Table 6 Interoperability Results by Client Category

Client Category	Example Devices / OS	TC1	TC2	TC3	TC4	TC5	TC6
iOS / iPadOS	iPhone17 Pro Max(ios version 26.6.2)	Pass	Pass	Pass	Pass	Pass	NA
Android	Pixel 6 Pro(android version 15, build number AP4A.241205.013)	Pass	Pass	Pass	Pass	Pass	NA
Windows 10 / 11	Windows 11	Pass	Pass	Pass	Pass	Pass	NA
macOS	MacBook pro Tahoe version 26.4	Pass	Pass	Pass	Pass	Pass	NA
IoT (WPA2-only)	Ring video Doorbell 2	Pass	N/A ²	Pass	Pass	-	-

² WPA2-only clients remain on the companion BSSID by design (Section 5.5), with full VLAN isolation.

IX. DISCUSSION AND LIMITATIONS

➤ Dependence on 802.11v

Clients that do not advertise BSS Transition capability cannot be steered with a BTM Request. For these clients, once the WPA2 handshake has identified the PSK and the binding has been stored, the AP triggers a disconnection (deauthentication). When the client re-scans and reconnects, the AP recognises its MAC address from the binding and answers it from the primary BSSID, so the client associates to the primary BSSID with the learned PSK and its resident VLAN. BTM support is widespread among smartphones, tablets and laptops, so this disconnection path is needed only for a minority of devices and costs a single brief reconnection at first join.

➤ Additional BSSID

CAPD uses one extra BSSID per radio on 2.4/5 GHz. Because the companion BSSID replaces, rather than supplements, the legacy WPA2 multi-PSK SSID, the net airtime cost relative to the status quo is one additional beacon stream per radio; this can be reduced with multiple-BSSID beaconing where supported.

➤ Hidden-SSID Behaviour

Some clients probe for hidden networks actively; the primary BSSID must answer such probes only for stations

with a valid binding, otherwise it risks attracting new clients that it cannot authenticate.

➤ Onboarding Exposure

The first association is WPA2 and therefore inherits WPA2's offline-dictionary exposure for that single handshake. High-entropy PSKs make this impractical to exploit.

➤ Standards Path

Wider OS support for SAE password identifiers [1] would provide a native, single-BSSID solution. CAPD is complementary: it delivers WPA3 multi-PSK with today's unmodified clients and can coexist with password identifiers as client support matures.

X. CONCLUSION AND FUTURE WORK

Multi-PSK community networks, marketed as ePSK, MPSK, DPSK and iPSK, are a cornerstone of managed MDU Wi-Fi, but their key-identification mechanism is fundamentally incompatible with WPA3-SAE and therefore with the 6 GHz band. This paper presented Companion-BSSID Assisted PSK Discovery, which separates *key discovery* from *key use*: a broadcast WPA2-only companion BSSID identifies the resident's PSK by MIC reverse lookup, and IEEE 802.11v BTM steers the

client to a hidden primary BSSID of the same SSID where WPA3-SAE is performed with the learned key. The scheme requires no client modification, preserves per-resident VLAN isolation, adds no cost to steady-state WPA3 operation, and extends multi-PSK to Wi-Fi 6E and Wi-Fi 7. Experimental evaluation across a broad range of commercial clients confirmed seamless onboarding and transition.

Future work includes selective use of the WPA3 Transition Disable indication for clients with stable MAC addresses, integration with SAE password identifiers as operating-system support emerges, large-scale field measurements in occupied MDU properties, and extension of the binding concept to Multi-Link Operation (MLO) in Wi-Fi 7.

➤ Acknowledgment

Tested in the Cambium Networks lab and observed its worked.

REFERENCES

- [1]. IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11-2020, Feb. 2021.
- [2]. M. Vanhoef and F. Piessens, "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2," in *Proc. ACM SIGSAC Conf. Computer and Communications Security (CCS)*, Dallas, TX, USA, 2017, pp. 1313–1328.
- [3]. D. Harkins, "Simultaneous Authentication of Equals: A Secure, Password-Based Key Exchange for Mesh Networks," in *Proc. 2nd Int. Conf. Sensor Technologies and Applications (SENSORCOMM)*, 2008, pp. 839–844.
- [4]. C. He and J. C. Mitchell, "Security Analysis and Improvements for IEEE 802.11i," in *Proc. Network and Distributed System Security Symp. (NDSS)*, 2005.
- [5]. Wi-Fi Alliance, *WPA3 Specification*, Version 3.x. Austin, TX, USA: Wi-Fi Alliance.
- [6]. D. Harkins, Ed., "Dragonfly Key Exchange," RFC 7664, Internet Research Task Force (IRTF), Nov. 2015.
- [7]. M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd," in *Proc. IEEE Symp. Security and Privacy (S&P)*, 2020, pp. 517–533.
- [8]. IEEE Standard 802.11v-2011, Amendment 8: IEEE 802.11 Wireless Network Management, IEEE, Feb. 2011.
- [9]. Federal Communications Commission, "Unlicensed Use of the 6 GHz Band," Report and Order and Further Notice of Proposed Rulemaking, FCC 20-51, ET Docket No. 18-295, Apr. 2020.
- [10]. Wi-Fi Alliance, "Wi-Fi CERTIFIED 6 / Wi-Fi 6E security requirements (WPA3 and Enhanced Open

in 6 GHz)," Wi-Fi Alliance technical documentation.

- [11]. IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control, IEEE Std 802.1X-2020, 2020.
- [12]. M. Vanhoef, "Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation," in *Proc. 30th USENIX Security Symp.*, 2021, pp. 161–178.
- [13]. K. Moriarty, B. Kaliski, and A. Rusch, "PKCS #5: Password-Based Cryptography Specification Version 2.1," RFC 8018, IETF, Jan. 2017.
- [14]. D. Harkins and W. Kumari, "Opportunistic Wireless Encryption," RFC 8110, IETF, Mar. 2017.
- [15]. IEEE Standard 802.11ax-2021, Amendment 1: Enhancements for High-Efficiency WLAN, IEEE, 2021.