Comprendere il flusso della crittografia wireless

Sommario

Introduzione

Questo documento descrive il flusso di transizione OWE e il suo funzionamento sul controller WLC (Wireless LAN Controller) Catalyst 9800.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Come configurare il WLC 9800, il punto di accesso (AP) per le operazioni di base
- Come configurare i profili WLAN e criteri.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- C9800-80, Cisco IOS® XE 17.12.4 e testato anche in Cisco IOS® XE 17.9.6
- Modello AP: C9136I, controllato sia in modalità locale che in modalità flex connect.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Descrizione

- OWE (Opportunistic Wireless Encryption) è un'estensione di IEEE 802.11 che fornisce la crittografia per il supporto wireless. Lo scopo dell'autenticazione basata su OWE è quello di evitare la connettività wireless aperta non protetta tra i punti di accesso e i client.
- Per impostare la crittografia wireless, OWE utilizza la crittografia basata sugli algoritmi Diffie-Hellman.
- Con OWE, il client e l'access point eseguono uno scambio di chiavi Diffie-Hellman durante la procedura di accesso e utilizzano il segreto pairwise risultante con l'handshake a 4 vie.
- L'utilizzo di OWE migliora la sicurezza delle reti wireless per le installazioni in cui vengono installate reti aperte o condivise basate su PSK.

Passi

1. Configurare una WLAN APERTA senza crittografia/sicurezza e abilitare la trasmissione.
2. Configurare un altro SSID con le impostazioni di sicurezza OWE ed eseguire il mapping del numero ID OPEN WLAN in modalità di transizione wlan-id. Disabilitare l'opzione SSID broadcast in questo SSID di transizione OWE.
3. Mappare il numero ID della WLAN di transizione OWE nel campo OPEN WLAN "transition-mode-wlan-id" (WLAN aperta, modalità di transizione: id-wlan).

Dettagli di Lab Repro

- Apri nome SSID: OPEN-OWE
- Nome SSID transizione OWE: OWE-Transition
- BSSID di OPEN-OWE: 40:ce:24:gg:2e:87

- BSSID della transizione verso il basso: 40:ce:24:gg:2e:8f

FLUSSO DEL DEBITO

1. I beacon possono essere trasmessi per OPEN SSID. È possibile visualizzarli tramite il relativo nome SSID in AIR PCAP.
2. In AIR PCAP è inoltre possibile visualizzare l'SSID protetto nascosto con il nome "Wildcard" anziché il nome SSID.
3. Dopo aver ricevuto il frame beacon per OPEN SSID, se dispone o supporta OWE, i client possono iniziare a inviare la richiesta di probe a OWE SSID di transizione (ovvero SSID abilitato per la sicurezza anziché OPEN SSID).
4. I client supportati da OWE possono ottenere la risposta del probe da SSID di transizione.
5. L'autenticazione OPEN può avvenire tra client e punto di accesso.
6. Il client può inviare la richiesta di associazione all'access point con i dettagli di scambio chiave DH e utilizzare il segreto pairwise risultante per l'handshake a 4 vie.
7. Il punto di accesso può inviare una risposta di associazione.
8. L'handshake a quattro vie può essere eseguito tra il punto di accesso e il dispositivo client.
9. Una volta completata la gestione delle chiavi, la chiave primaria di secondo livello può avere esito positivo.
10. Il client può ottenere IP da DHCP, ARP, ecc.
11. Il client può passare allo stato RUN.
12. Se i dispositivi client non supportano OWE, può inviare una richiesta di sonda a OPEN SSID e può ottenere direttamente l'indirizzo IP prima di passare allo stato RUN.

Cornice beacon originale

- Qui, AIR PCAP lo mostra, la trasmissione SSID "OPEN-OWE" (Beacon Frame). che contiene i dettagli SSID della transizione e viene denominata "OWE-Transition".

Image-1 Frame beacon di OPEN SSID

Beacon SSID nascosti

- In base alla configurazione WLAN, "broadcasting" è disabilitato per questo SSID "OWE-Transition". Tuttavia, è possibile visualizzare i beacon SSID nascosti in AIR PCAP che contengono il nome SSID "Wildcard". Tuttavia, se si controlla tale pacchetto, esso contiene i dettagli OWE-Transition.
- Ottenere il BSSID del SSID nascosto utilizzando questo pacchetto, ad esempio "40:ce:24:dd:2e:8f" ed eseguirne la ricerca nell'acquisizione del pacchetto.
- In questo pacchetto, viene mostrato che SSID "Missing" (Mancante) e che contiene il SSID di transizione "OPEN-OWE" e il BSSID "40:ce:24:dd:2e:87".

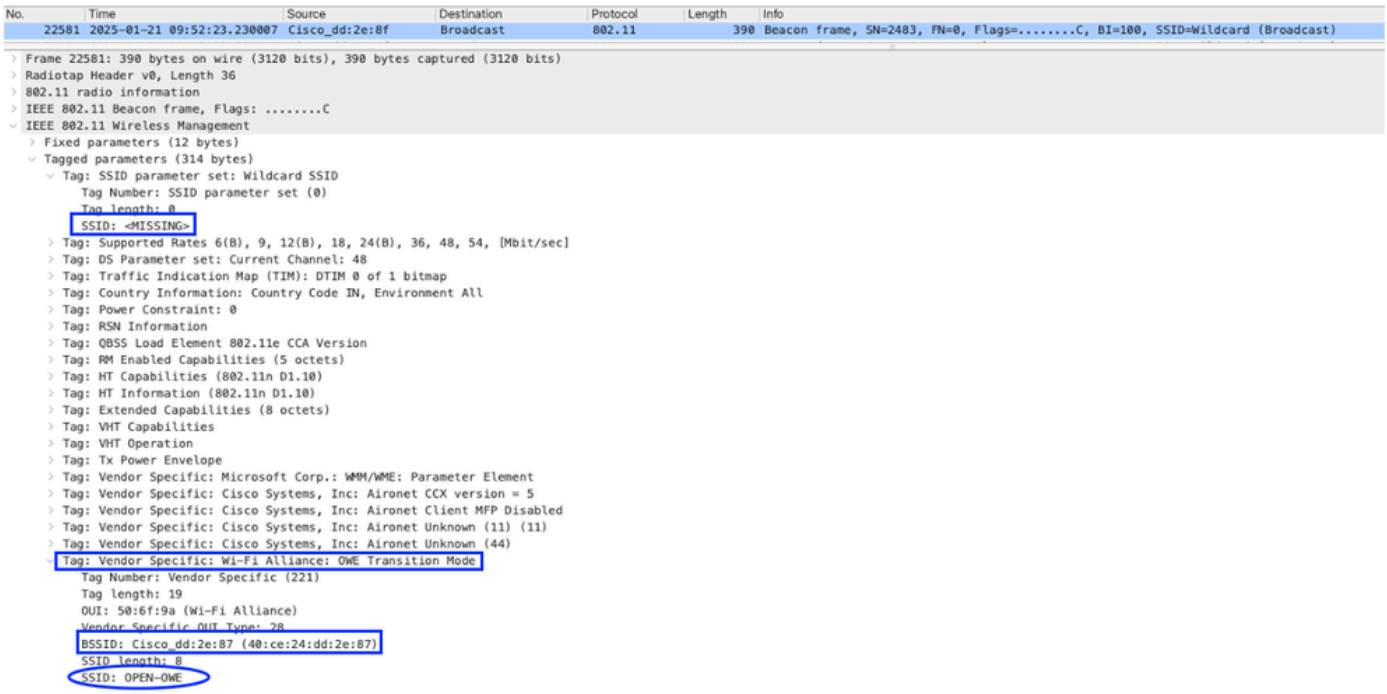

Image-2 SSID nascosto - transizione OWE

Richiesta di verifica inviata dal client all'SSID di transizione OWE

- In base all'SSID "OPEN-OWE" del frame del beacon, il client viene a conoscenza degli altri dettagli SSID necessari per la connessione, in questo scenario è "OWE-Transition". Se il client è in grado di supportare la crittografia OWE, può inviare la richiesta di probe all'SSID "OWE-Transition" e ottenere una risposta.
- La richiesta di sonda è stata inviata a OWE-Transition BSSID "40:ce:24:dd:2e:8f" e ha ricevuto una risposta. Anche all'interno di questo pacchetto di risposta della sonda è possibile visualizzare i dettagli di OPEN-OWE SSID.

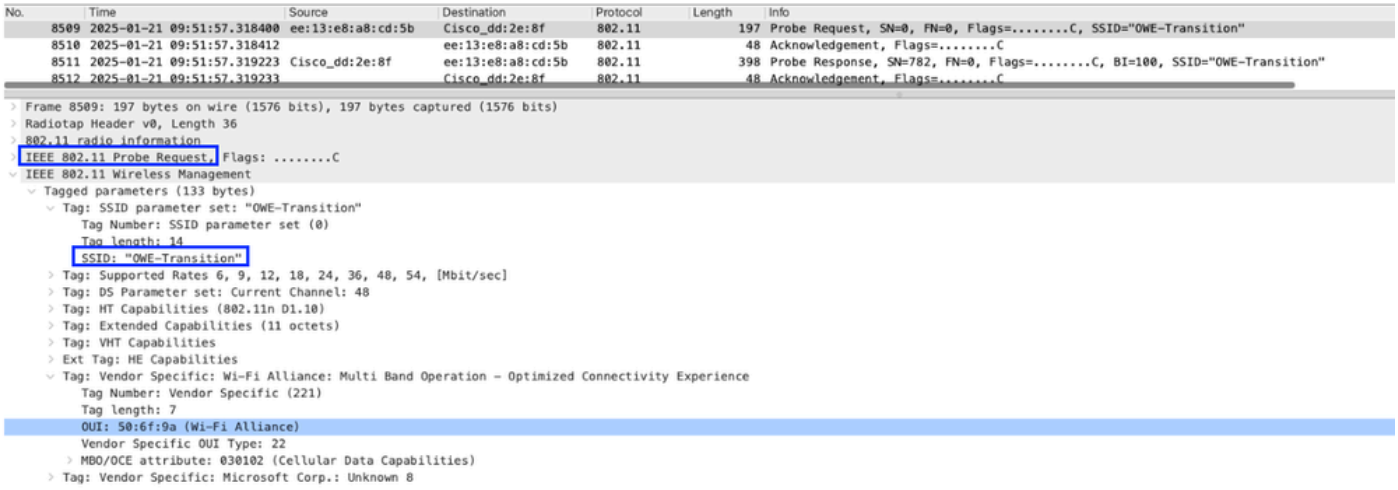

Image-3 Richiesta probe

Risposta probe inviata dal punto di accesso al client

- Il client ha ricevuto una risposta di richiesta per l'SSID "OWE-Transition", ma ha i suoi dettagli SSID originali "OPEN-OWE" in WiFi Alliance.

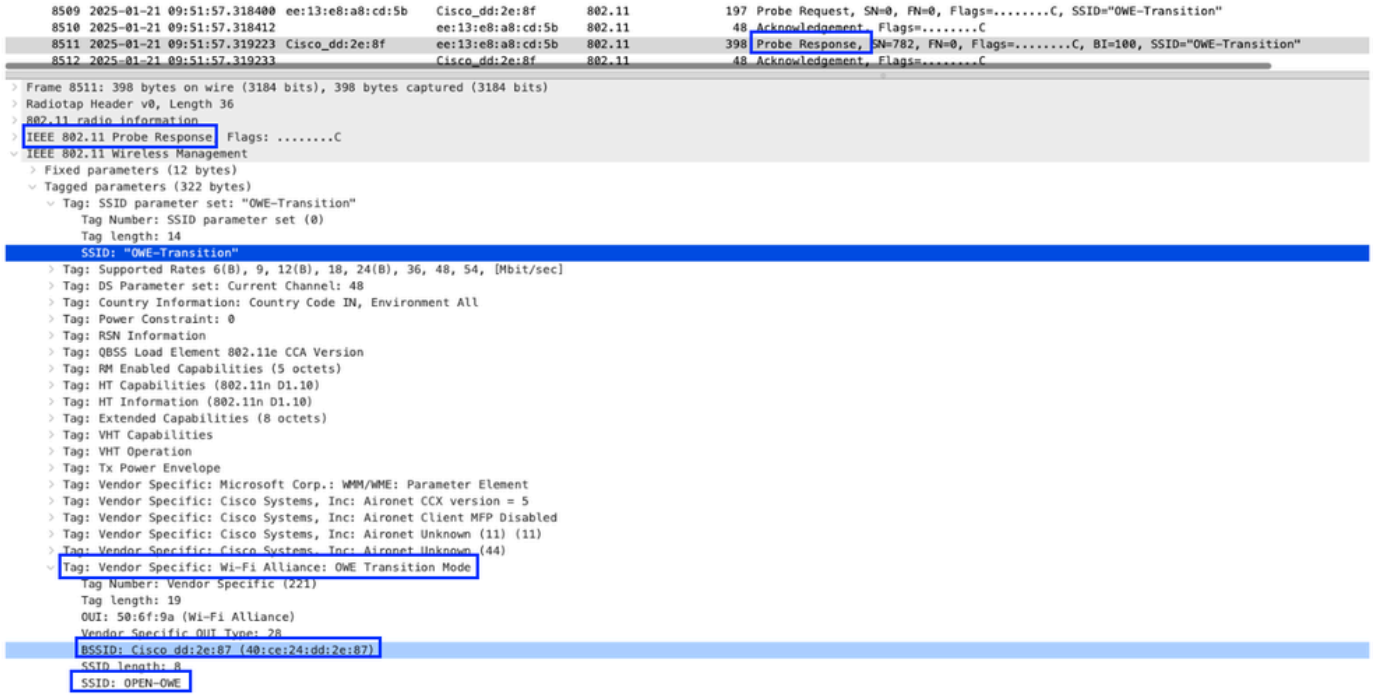

Image-4 Risposta probe

autenticazione OPEN

- Dopo aver ricevuto la risposta della sonda, l'autenticazione OPEN può avvenire tra il client e l'access point per controllare i dettagli/le funzionalità wifi dei client, prima dell'associazione.

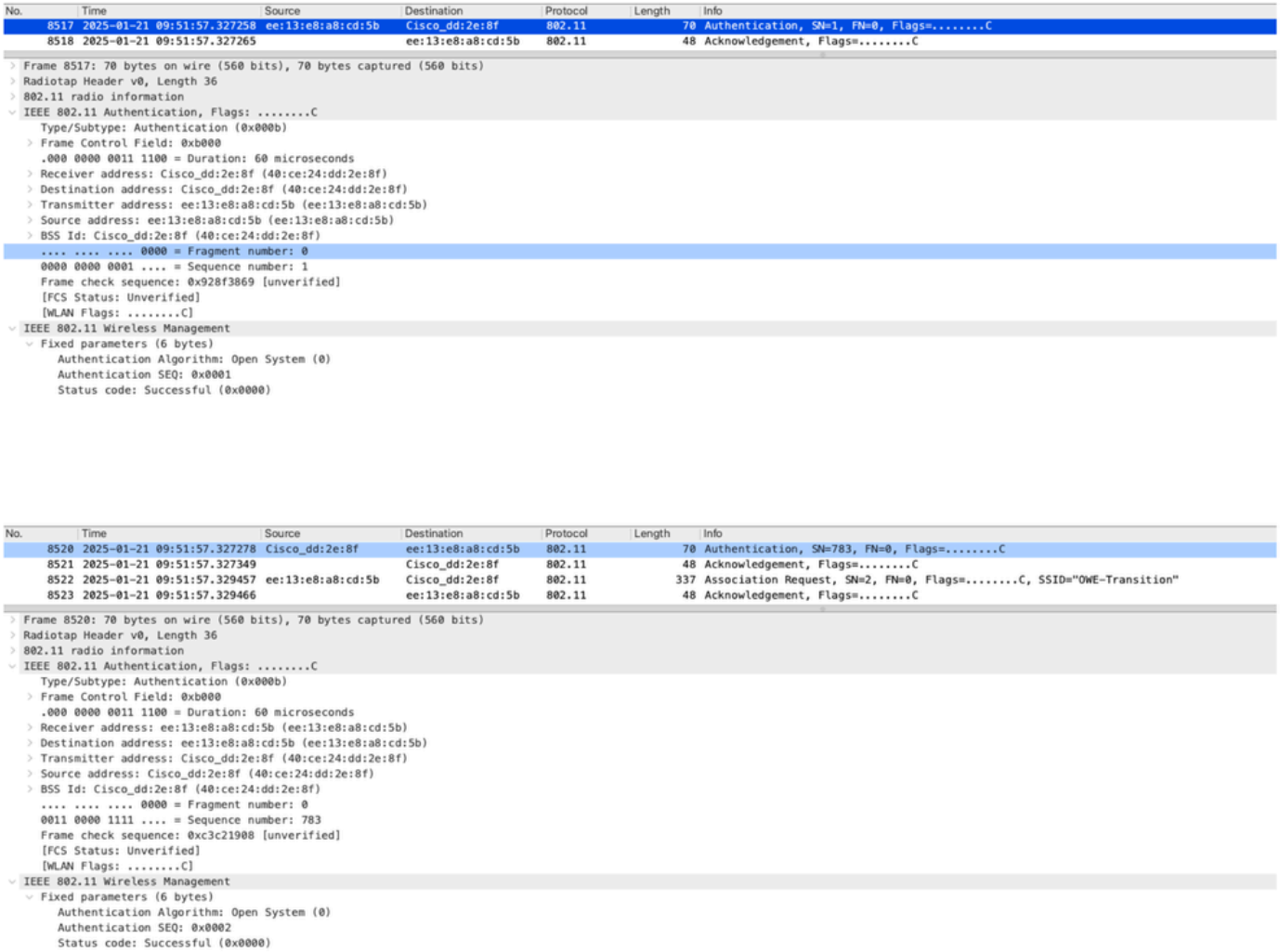

Image-5 Autenticazione OPEN dopo il completamento del probe

Richiesta di associazione dal client al punto di accesso

- In questo pacchetto, il client può allegare il valore del parametro Diffie-Hellman per la crittografia.

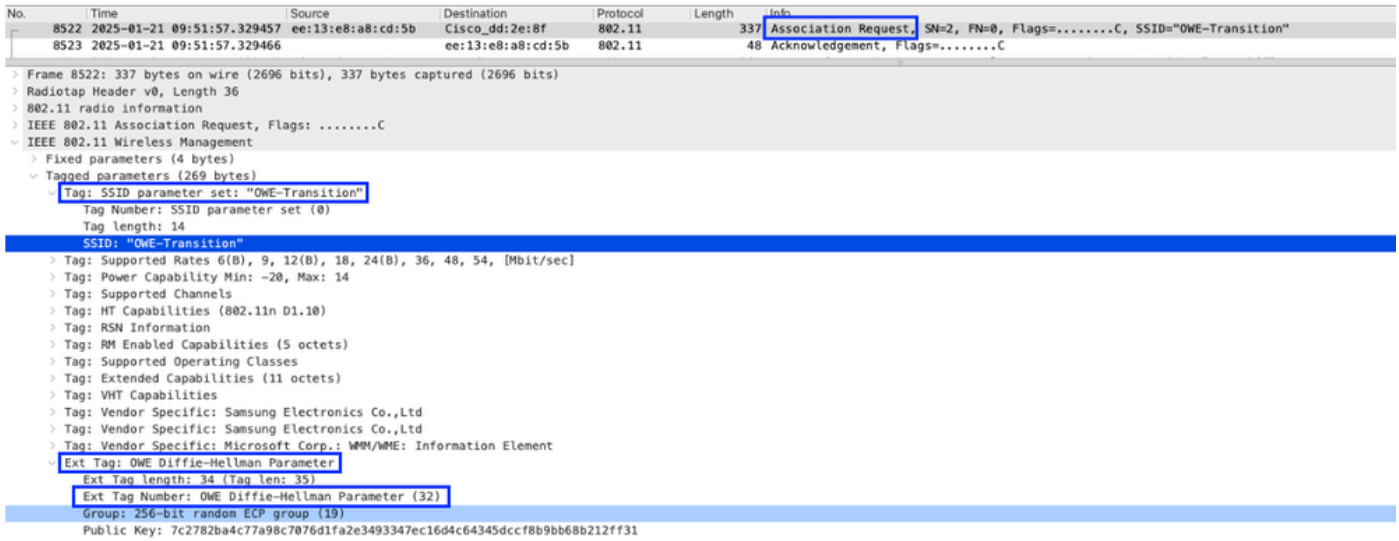

Image-6 Richiesta associazione

- In RSA trace è possibile iniziare a visualizzare i log del client dalla fase di associazione,

```
2025/01/21 15:21:57.391071821 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (note): MAC: ee13.e8a8.cd5b  A
2025/01/21 15:21:57.391117645 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b
```

Risposta di associazione inviata dal punto di accesso al client

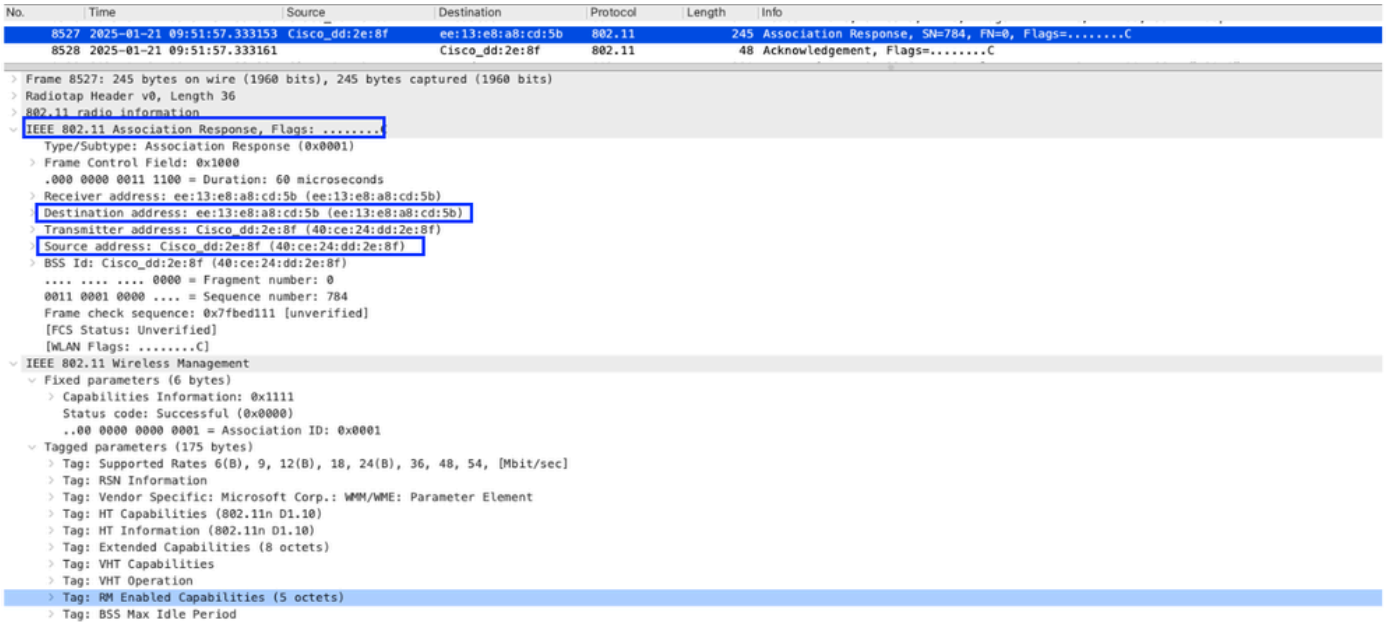

Image-7 Risposta associazione

```
2025/01/21 15:21:57.391334260 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
2025/01/21 15:21:57.392296819 {wncd_x_R0-0}{1}: [dot11] [21675]: (note): MAC: ee13.e8a8.cd5b  Associati
```

Scambio chiave

L'handshake a 4 vie può essere eseguito tra il punto di accesso e il dispositivo client.

Chiave 1 inviata dal punto di accesso

Chiave 2 inviata dal client

Chiave-3 inviata dal punto di accesso

Chiave 4 inviata dal client

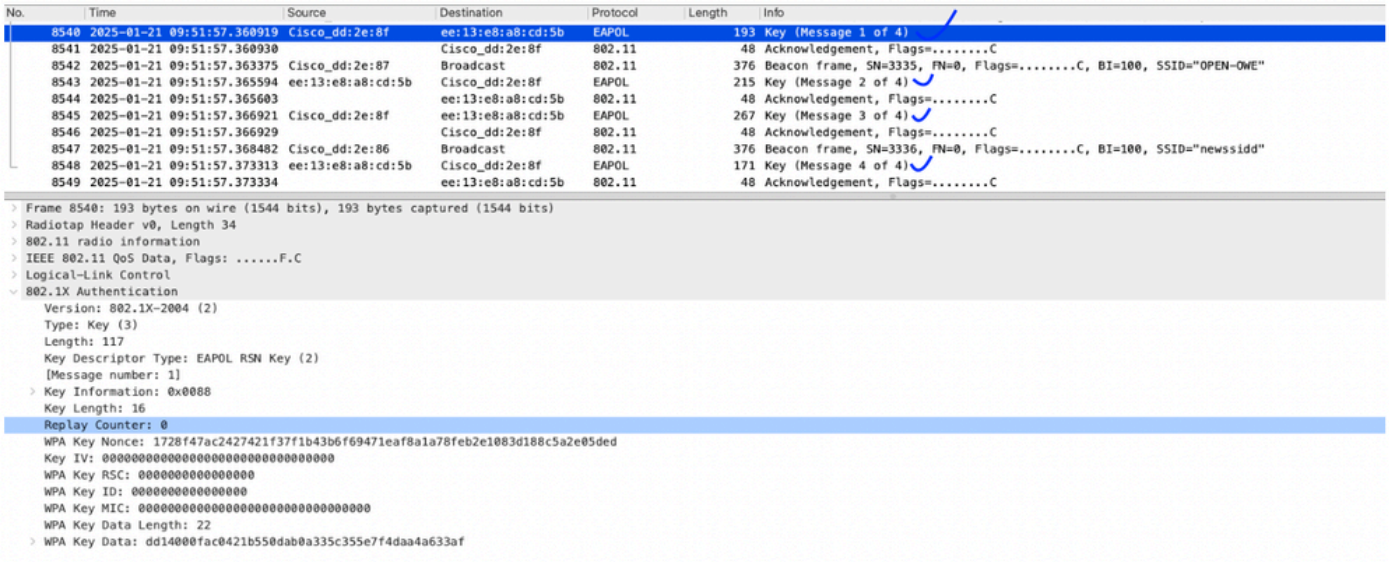

Image-8 Handshake a 4 vie

```
2025/01/21 15:21:57.392538716 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.392557538 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
2025/01/21 15:21:57.392640494 {wncd_x_R0-0}{1}: [client-auth] [21675]: (note): MAC: ee13.e8a8.cd5b  L2
2025/01/21 15:21:57.394830551 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b  Cli
2025/01/21 15:21:57.395171903 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b  Cli
2025/01/21 15:21:57.420590731 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b  Cli

2025/01/21 15:21:57.420706435 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.420775720 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.426548998 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.426725965 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.426727805 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.434078994 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.434099154 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (note): MAC: ee13.e8a8.cd5b
```

Autenticazione L2 riuscita

```
2025/01/21 15:21:57.434111288 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.434250308 {wncd_x_R0-0}{1}: [client-auth] [21675]: (note): MAC: ee13.e8a8.cd5b  L2
2025/01/21 15:21:57.434286035 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b  Cli
2025/01/21 15:21:57.434308953 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b
```

Stato di apprendimento IP

```
2025/01/21 15:21:57.434789679 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.436611026 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
2025/01/21 15:21:57.437239513 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
2025/01/21 15:21:57.437508189 {wncd_x_R0-0}{1}: [client-iplearn] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.534166453 {wncd_x_R0-0}{1}: [sisf-packet] [21675]: (info): TX: DHCPv4 from interfac
2025/01/21 15:21:57.535325325 {wncd_x_R0-0}{1}: [client-iplearn] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.535874658 {wncd_x_R0-0}{1}: [sisf-packet] [21675]: (info): TX: DHCPv4 from interfac
2025/01/21 15:21:57.536500021 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b
```

Client in stato RUN

```
2025/01/21 15:21:57.537017277 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
```

Client non supportati per la crittografia OWE

- Esaminando un frame del beacon, i client vengono a sapere se sono in grado di supportare o meno questo metodo di crittografia. Se non è supportata, può semplicemente inviare una richiesta di richiesta di verifica per aprire SSID "OPEN-OWE" e può eseguire una normale autenticazione aperta, ottenere l'indirizzo IP, quindi può passare allo stato RUN.

```
2025/01/16 15:36:06.178370757 {wncd_x_R0-2}{1}: [client-orch-sm] [17332]: (note): MAC: d037.4587.8f35
2025/01/16 15:36:06.209288788 {wncd_x_R0-2}{1}: [dot11] [17332]: (note): MAC: d037.4587.8f35  Associati
2025/01/16 15:36:06.248651191 {wncd_x_R0-2}{1}: [client-auth] [17332]: (note): MAC: d037.4587.8f35  Ope
2025/01/16 15:36:06.248751507 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
2025/01/16 15:36:06.281808554 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
2025/01/16 15:36:06.303307756 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
2025/01/16 15:36:10.305041414 {wncd_x_R0-2}{1}: [client-iplearn] [17332]: (note): MAC: d037.4587.8f35
2025/01/16 15:36:10.305777492 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
```

Informazioni sulla transizione rapida

- È possibile configurare OWE solo nell'autenticazione OPEN o in Webauth (CWA/LWA/EWA).
- FT non è supportato nella transizione OWE.
- Se si attiva FT, viene visualizzato questo messaggio di errore:

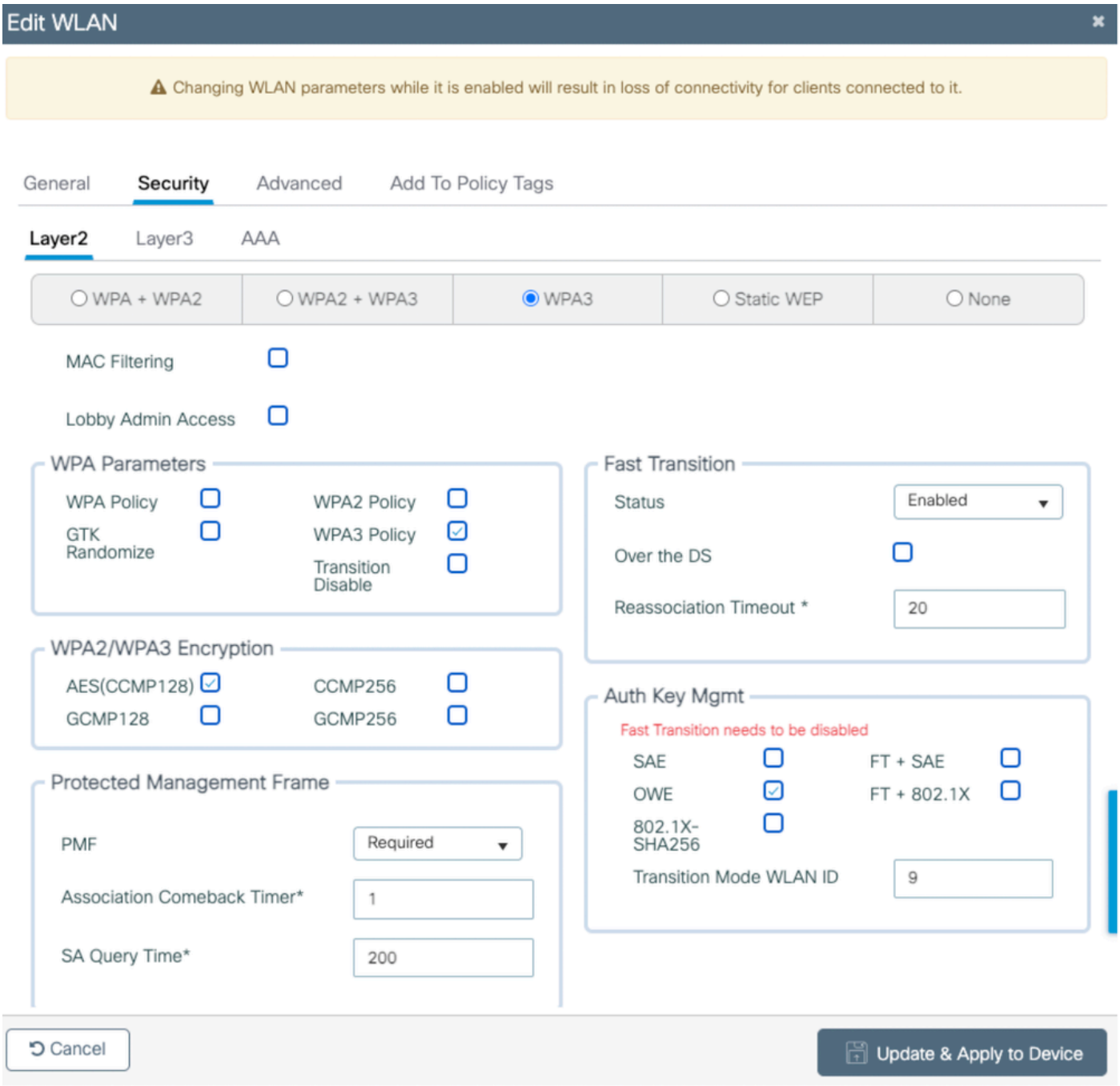

Image-9 Messaggio di errore quando viene abilitato FT in OWE Transition SSID

OWE non supportato con PSK/dot1x

Non siamo in grado di abilitare OWE in queste combinazioni,

1. 802.1x o FT+802.1x

2. PSK o FT+PSK o PSK-SHA256

3. SAE o FT+SAE

4. 802.1x-SHA256 o FT+802.1x-SHA256

Se si tenta di attivare uno di questi metodi, è possibile che venga visualizzato il messaggio di

errore

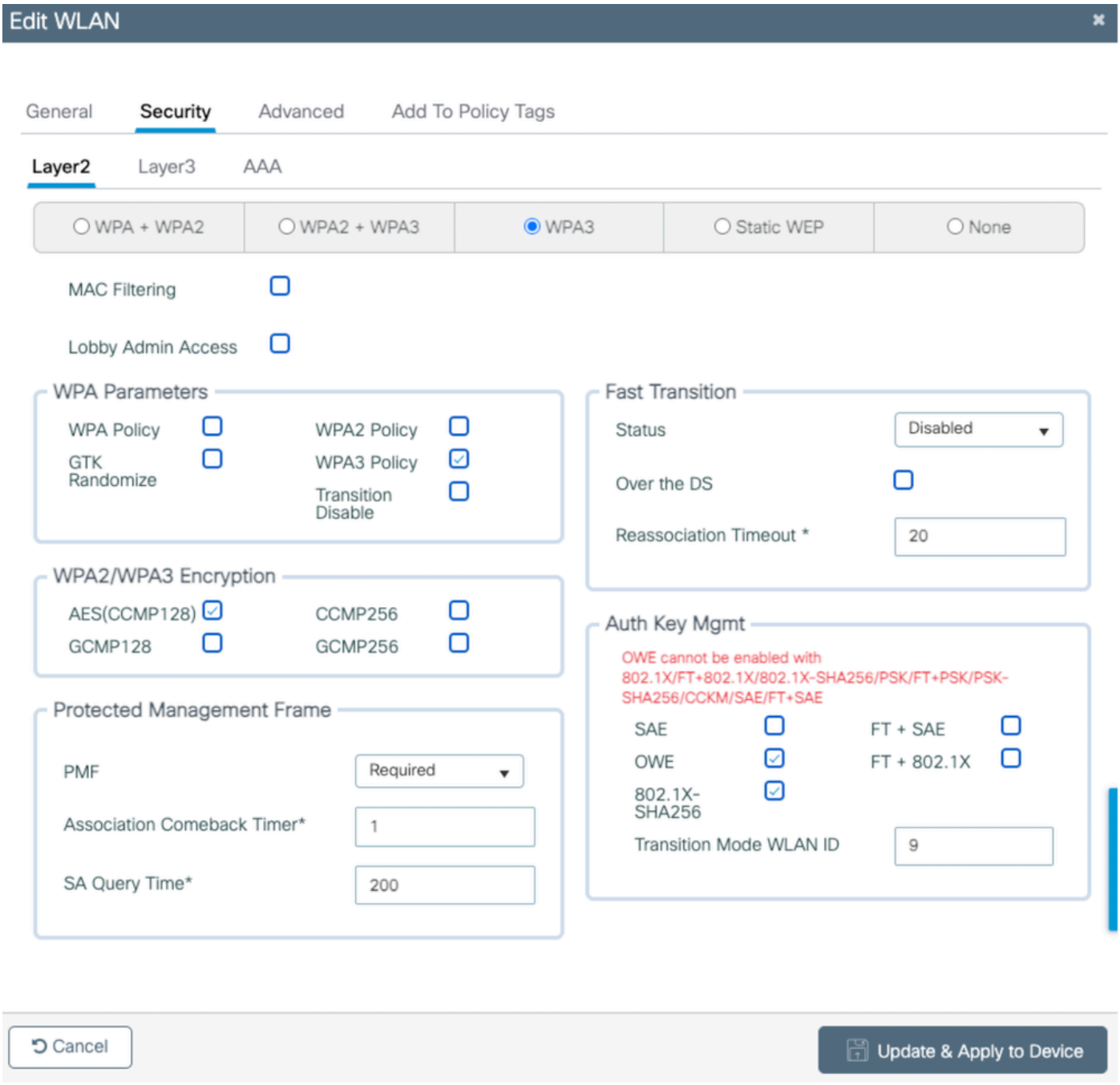

Image-10 Ricevimento del messaggio di errore durante l'abilitazione di altri metodi di autenticazione in OWE SSID

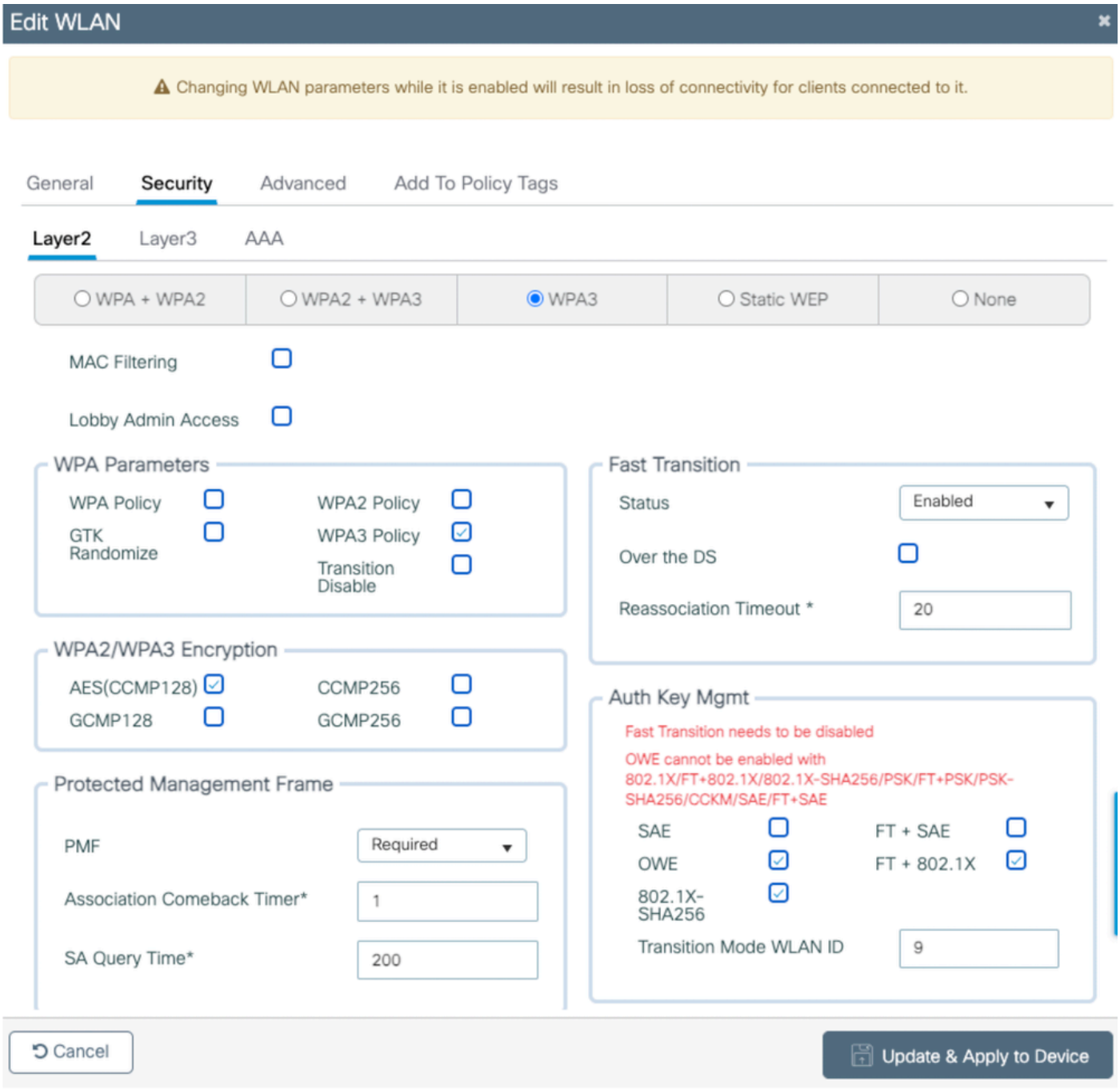

Image 11 Messaggio di errore durante l'abilitazione di AKM

- Nella versione Cisco IOS® XE 17.9.6 IOS, è possibile visualizzare l'opzione "OWE" in AKM quando si seleziona "WPA2+WPA3". Tuttavia, è possibile visualizzare il messaggio di errore e non utilizzare OWE con questa combinazione.

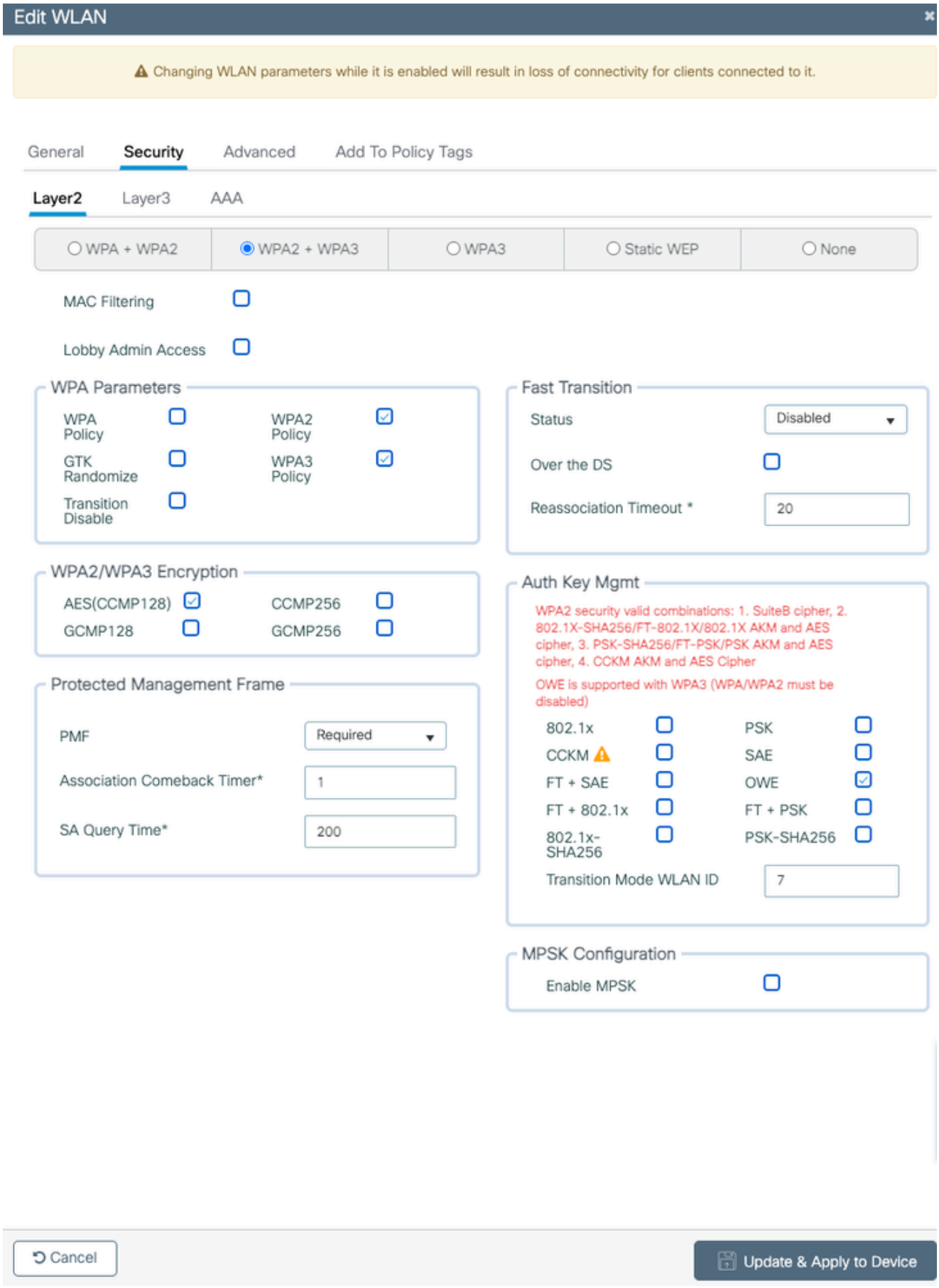

Image 12 Messaggio di errore quando si sceglie WPA2+WPA3

- Nella versione Cisco IOS® XE 17.12.4, se si sceglie "WPA2+WPA3", non è possibile

ottenere l'opzione "OWE" in AKM,

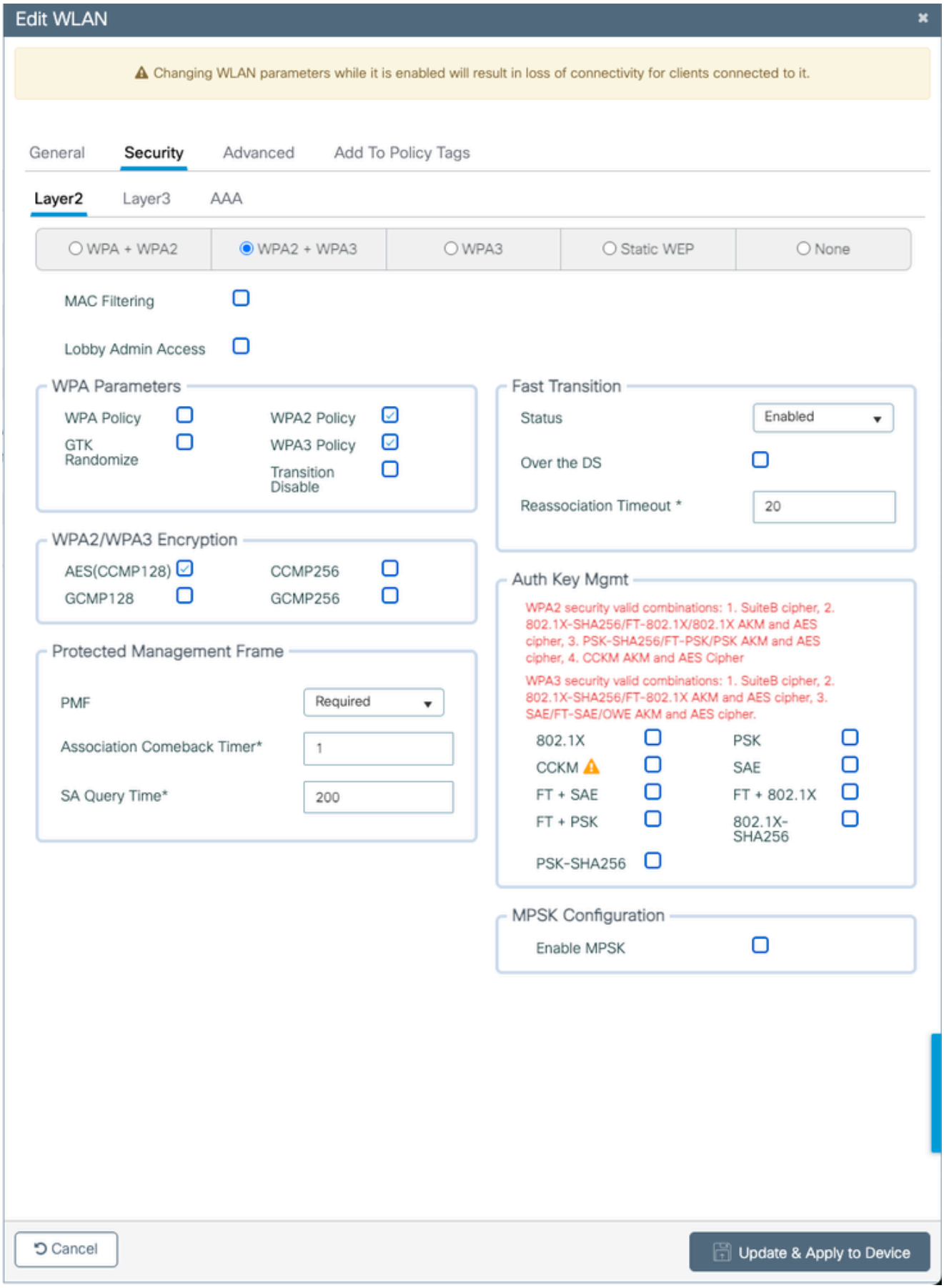

Image 13 Messaggio di errore - Opzione OWE non disponibile in AKM

Risoluzione dei problemi

1. Verificare le configurazioni sia nelle WLAN, sia nell'OPEN SSID e nell'SSID di transizione OWE se l'ID della WLAN di transizione deve essere mappato.
2. L'opzione di trasmissione deve essere disabilitata in OWE Transition SSID. Deve essere abilitata solo in OPEN SSID.
3. Verificare i metodi di autenticazione/crittografia/FT supportati descritti in questo articolo.
4. Se le configurazioni sono adatte dall'estremità del WLC, raccogliere i log e gli output necessari per ridurre il problema,

RA Trace ed EPC (Embedded Packet Capture)

Login alla GUI WLC -> Risoluzione dei problemi -> Traccia radioattiva -> Aggiungi indirizzo MAC wifi client -> Casella di controllo di client selezionati -> Avvia

Login alla GUI WLC -> Risoluzione dei problemi -> Packet Capture -> Add new file name -> Scegliere l'interfaccia uplink e WMI VLAN/Interface -> Start (Avvia).

Dal computer client: Se possibile, è possibile installare l'applicazione wireshark e raccogliere l'acquisizione del pacchetto scegliendo l'interfaccia WiFi.

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213949-wireless-debugging-and-log-collection-on.html#anc12

CAPPUCCIO

È possibile raccoglierlo utilizzando il laptop MAC o configurando uno dei punti di accesso in modalità sniffer, si prega di fare riferimento questi collegamenti,

Da laptop MAC:

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-mobility/217042-collect-packet-captures-over-the-air-on.html

Da Sniffer AP:

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/217057-configure-access-point-in-sniffer-mode-o.html

Collegare un laptop (server wireshark) alla porta dello switch e deve contenere un'applicazione wireshark. Questo server wireshark deve essere raggiungibile dall'interfaccia WMI WLC. È necessario consentire l'uso del protocollo "5555 o 5000 o 5556" nel firewall se questo è posizionato tra il WLC e il server wireshark.

Controllare se c'è qualsiasi "gscaler" installato in quel PC dove wireshark installato, se è più di "spegnere" e provare, se si tratta di un firewall come windows defender o qualsiasi cosa presente in esso, disabilitare questi e provare a raccogliere PCAP.

Roaming

Quando il client esegue il roaming da un punto di accesso a un altro, deve eseguire la procedura seguente:

- Necessità di inviare una riassociazione/associazione - A seconda della richiesta del client.
- È necessario inviare i dettagli DH (Diffie-Helman) nella richiesta di associazione.
- Il client può ottenere i dettagli DH nella risposta dell'associazione dall'access point, in base a questo PMK generato sia nel client che nell'access point.
- È possibile che l'handshake a 4 vie venga eseguito tra il punto di accesso e il client.
- In OWE non è possibile abilitare FT, quindi 802.11r non è possibile.
- Ogni volta, durante il roaming, il client deve eseguire l'handshake a 4 vie dopo lo scambio DH in associazione.
- Client e AP che utilizzano il proprio PMKID, è univoco per ogni AP e client.
- Se il client si connette allo stesso punto di accesso, può utilizzare lo stesso PMKID. In alcuni scenari, se il client è stato eliminato rispetto a AP può generare un nuovo PMKID, tuttavia il client utilizza lo stesso PMKID per l'handshake a 4 vie.

Esempio:

Se il client si connette allo stesso punto di accesso, è possibile visualizzare lo stesso PMKID sia in Association-Request che in Association-Response. Nella risposta Association non è possibile visualizzare i dettagli DH se viene utilizzato lo stesso PMKID.

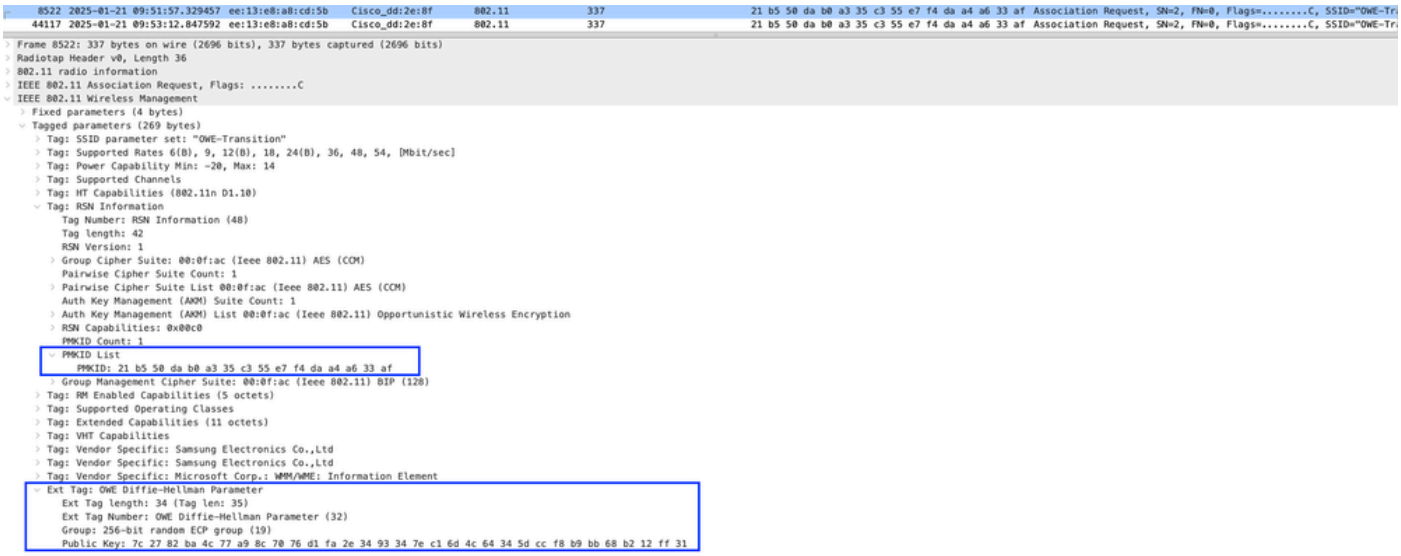

Image 14 Utilizzo dello stesso PMKID

Image 15 Risposta di associazione con lo stesso PMKID

Per il test, il client è stato eliminato manualmente dal WLC e associato di nuovo allo stesso AP. In questo momento, il client invia lo stesso PMKID, ma l'AP invia i dettagli DH nella risposta dell'associazione.

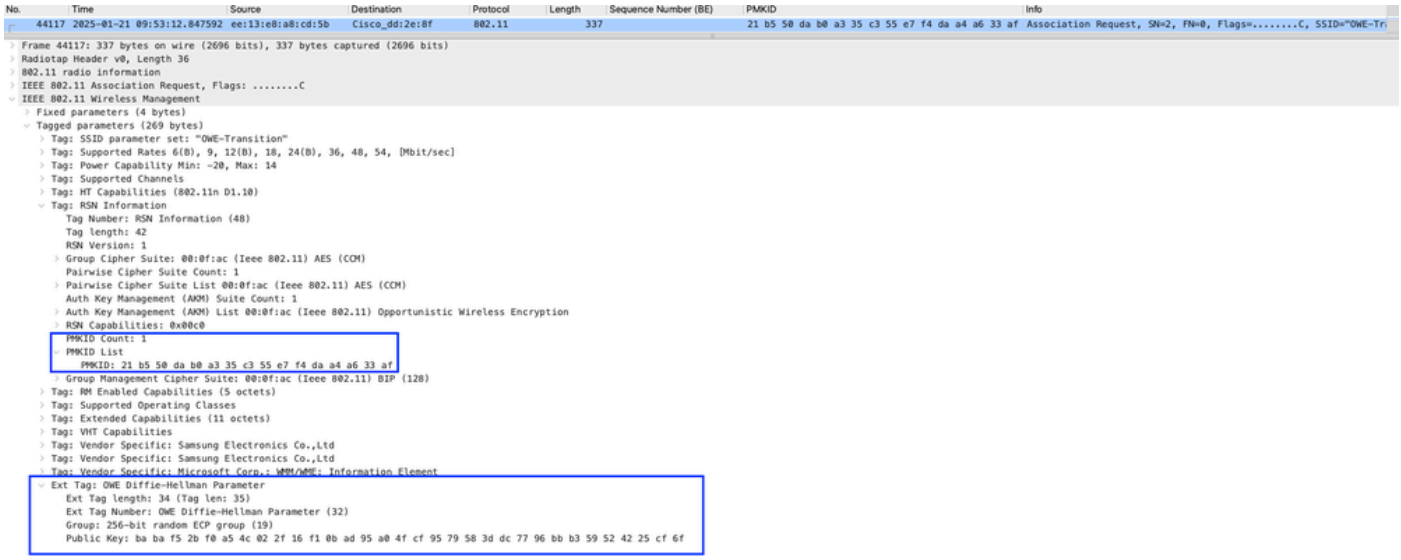

Image 16 Dopo l'eliminazione, il client ha inviato lo stesso PMKID con i dettagli DH

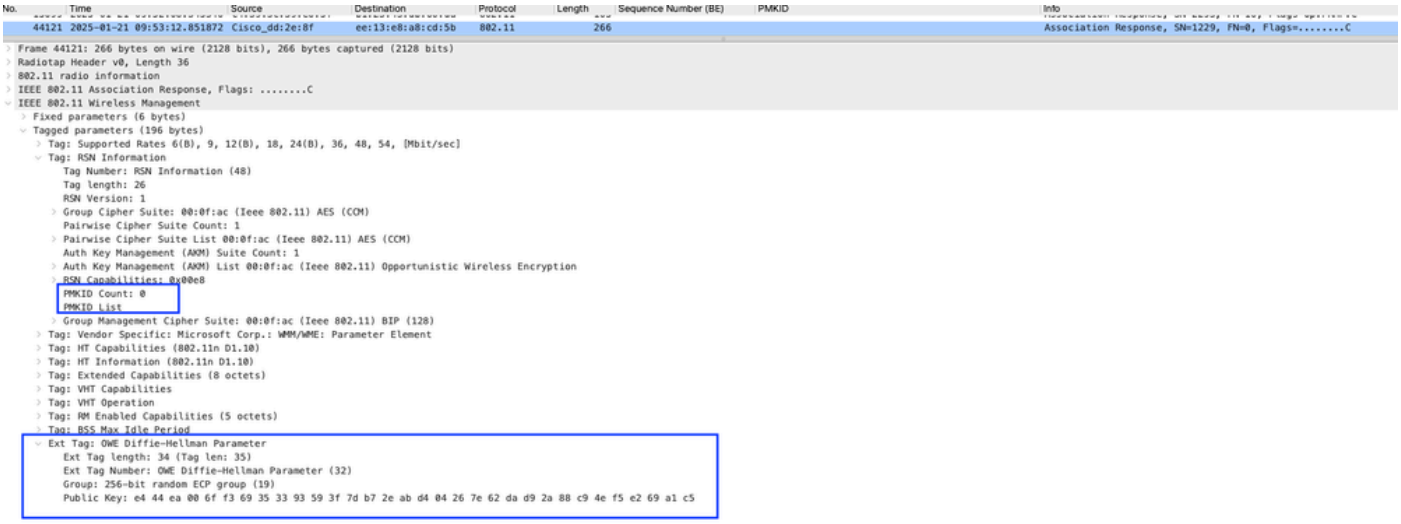

Image 17 AP utilizza i valori DH per generare il nuovo PMKID

In questo esempio: Sia AP che client utilizzano lo stesso PMKID durante l'handshake a 4 vie. Archiviare i messaggi "M1 e M2".

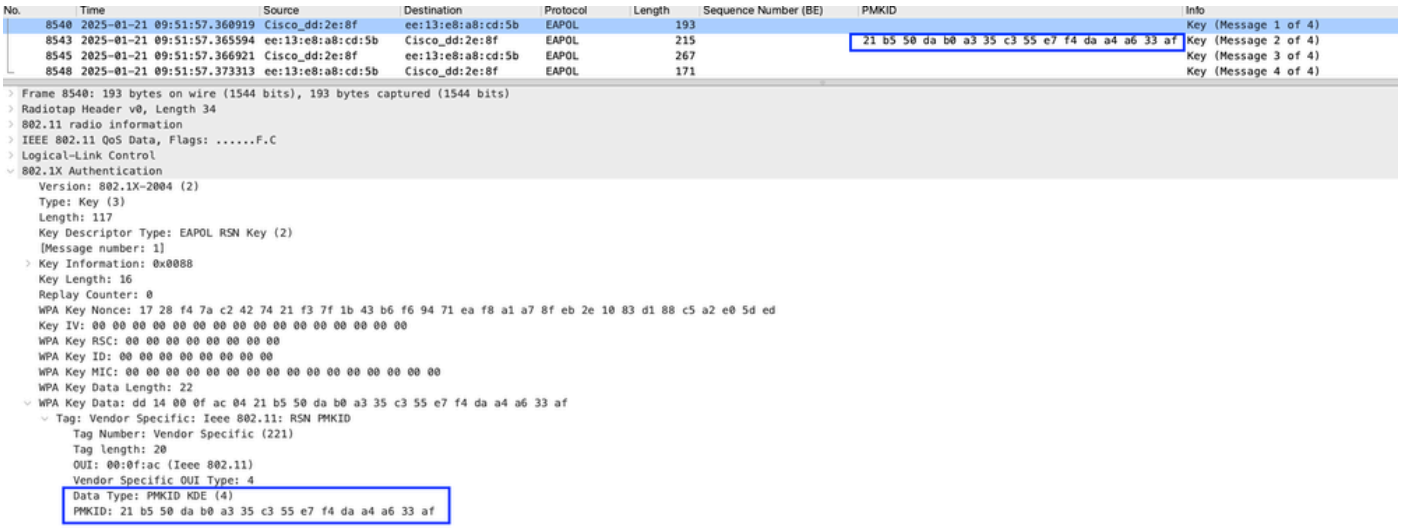

Immagine - 18: AP e client che utilizzano lo stesso PMKID

In questo esempio: Il client utilizza lo stesso PMKID ma il punto di accesso utilizza un PMKID diverso generato dopo l'eliminazione del client. Controllare i messaggi "M1 e M2".

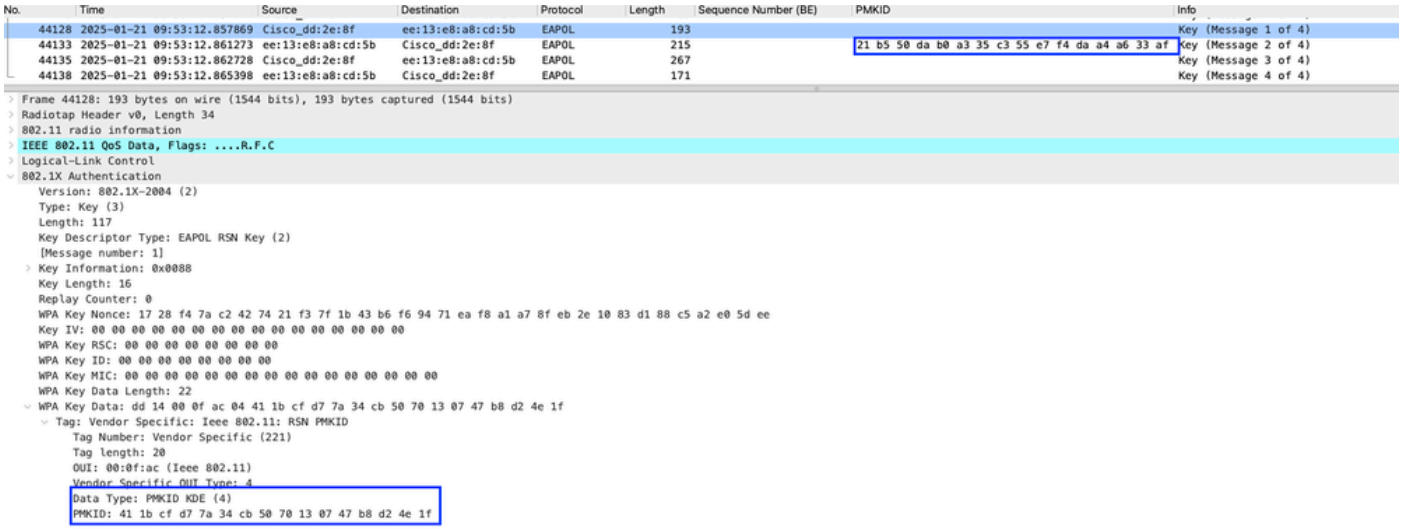

Image 19 AP e client che utilizzano un PMKID diverso

Da traccia RA interna:

In questo esempio: Il client ha inviato i parametri DH nella richiesta di associazione e l'access point è stato elaborato prima della generazione della chiave PMK.

```
2025/01/21 15:18:50.157081690 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157082294 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157523328 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157531792 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157532236 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157532538 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157841380 {wncd_x_R0-0}{1}: [dot11-frame] [21675]: (debug): MAC: ee13.e8a8.cd5b  OW
```

In seguito, lo stesso client che si connette allo stesso punto di accesso, in questo momento, non ha generato un nuovo PMKID,

```
2025/01/21 15:21:57.391898613 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391903915 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391906073 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391906329 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).