Entender O Fluxo De Criptografia Sem Fio Oportunista

Contents

Introdução

Este documento descreve o fluxo de transição OWE e como ele funciona no Catalyst 9800 Wireless LAN Controller (WLC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Como configurar a WLC 9800, o ponto de acesso (AP) para operação básica
- Como configurar perfis de WLAN e de política.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- C9800-80, Cisco IOS® XE 17.12.4 e também testado no Cisco IOS® XE 17.9.6
- Modelo de AP: C9136I, verificado nos modos de conexão local e flexível.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Descrição

- OWE (Opportunistic Wireless Encryption) é uma extensão do IEEE 802.11 que fornece criptografia para o meio sem fio. A finalidade da autenticação baseada em OWE é evitar a conectividade sem fio aberta e não segura entre o AP e os clientes.
- O OWE usa a criptografia baseada em algoritmos Diffie-Hellman para configurar a criptografia sem fio.
- Com o OWE, o cliente e o AP executam uma troca de chave Diffie-Hellman durante o procedimento de acesso e usam o segredo resultante em pares com o handshake de 4 vias.
- O uso do OWE melhora a segurança da rede sem fio para implantações em que redes abertas ou compartilhadas baseadas em PSK são implantadas.

Etapas

1. Configure uma WLAN ABERTA sem qualquer criptografia/segurança e habilite a transmissão.
2. Configure outro SSID com configurações de segurança OWE e mapeie o número de ID de WLAN OPEN no modo de transição-wlan-id. Desabilite a opção de SSID de transmissão neste SSID de transição OWE.
3. Mapeie o número de ID da WLAN de transição OWE no campo OPEN WLAN "transition-mode-wlan-id".

Detalhes do Lab Repro

- Nome do SSID aberto: OPEN-OWE

- Nome do SSID de transição OWE: Transição OWE
- BSSID de OPEN-OWE: 40:ce:24:dd:2e:87
- BSSID de OWE-Transition: 40:ce:24:dd:2e:8f

FLUXO DE DÉBITO

1. Os beacons podem ser transmitidos para o SSID ABERTO. Você pode vê-lo por seu nome SSID no AIR PCAP.
2. Também podemos ver o SSID habilitado para segurança oculta com o nome "Curinga" em vez de seu próprio nome SSID no AIR PCAP.
3. Quando os clientes receberem o quadro beacon para o SSID ABERTO, se ele tiver ou suportar o OWE, ele poderá começar a enviar a solicitação de sondagem para o SSID de transição do OWE (que é o SSID com segurança ativada em vez do SSID ABERTO).
4. Os clientes compatíveis com OWE podem obter resposta de sondagem do SSID de transição.
5. A autenticação OPEN pode ocorrer entre o cliente e o AP.
6. O cliente pode enviar uma solicitação de associação ao AP com detalhes de troca de chave DH e usar o segredo resultante em pares para o handshake de 4 vias.
7. O AP pode enviar a resposta da associação.
8. O handshake de quatro vias pode acontecer entre o AP e o dispositivo do cliente.
9. Após o gerenciamento bem-sucedido de chaves, a L2 PSK pode ser bem-sucedida.
10. O cliente pode obter o IP de DHCP, ARP, etc.
11. O cliente pode ir para o estado EXECUTAR.
12. Se os dispositivos cliente não estiverem suportando OWE, ele poderá enviar a solicitação de sondagem para o próprio SSID OPEN e poderá obter diretamente o IP do que poderá ir para o estado RUN.

Quadro original de beacon

- Aqui, AIR PCAP mostra isso, o SSID "OPEN-OWE" broadcast (Quadro de Beacon). Que contém detalhes do SSID de transição e é chamado de "OWE-Transition".

Imagem-1: Quadro de beacon do SSID ABERTO

Beacons de SSID ocultos

- De acordo com a configuração da WLAN, a "transmissão" está desabilitada para esse SSID de "transição OWE". No entanto, você pode ver beacons de SSID ocultos no AIR PCAP que contêm o nome de SSID "Curinga". No entanto, se você verificar esse pacote, ele conterá detalhes de OWE-Transition.
- Obtenha o BSSID do SSID oculto usando este pacote, como "40:ce:24:dd:2e:8f" e pesquise-o na captura de pacotes.
- Nesse pacote, ele mostra que o SSID está "ausente" e contém seu SSID de transição como "OPEN-OWE" e seu BSSID "40:ce:24:dd:2e:87".

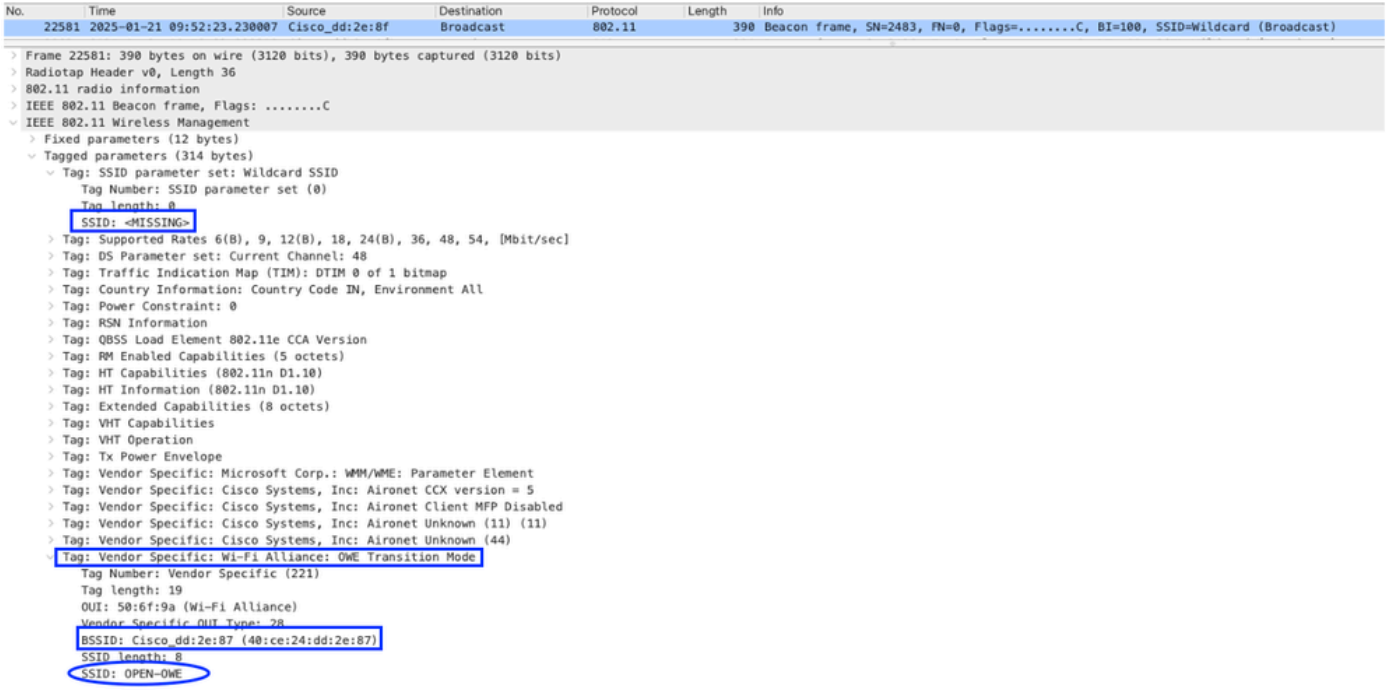

Imagem-2: SSID oculto - Transição OWE

Solicitação de Investigação enviada do cliente para o SSID de Transição OWE

- Com base no quadro de beacon SSID "OPEN-OWE", o cliente passa a conhecer os outros detalhes do SSID que precisa conectar; nesse cenário, é "OWE-Transition". Se o cliente for capaz de suportar a criptografia OWE, ele poderá enviar a solicitação de sondagem para o SSID "OWE-Transition" e obter uma resposta.
- Solicitação de sondagem enviada para OWE-Transition BSSID "40:ce:24:dd:2e:8f" e obteve uma resposta. Dentro desse pacote de resposta de sondagem também, você pode ver detalhes do SSID OPEN-OWE.

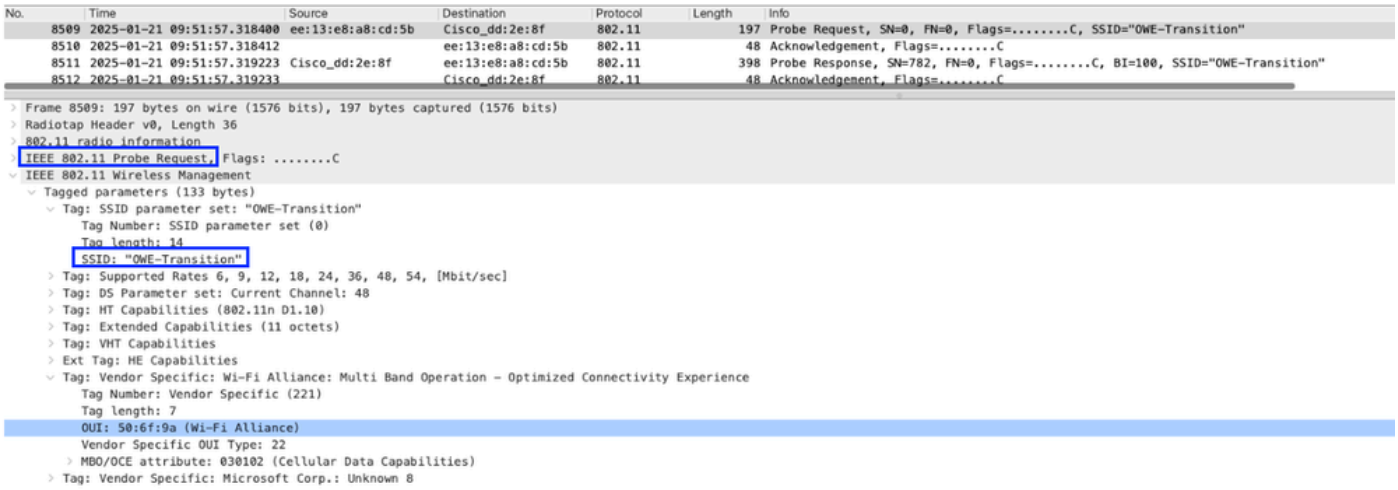

Imagem 3: Solicitação de Sondagem

Resposta de sondagem enviada do AP para o cliente

- O cliente recebeu uma resposta de sondagem para o SSID "OWE-Transition", no entanto, ele tem seus detalhes de SSID originais "OPEN-OWE" na WiFi Alliance.

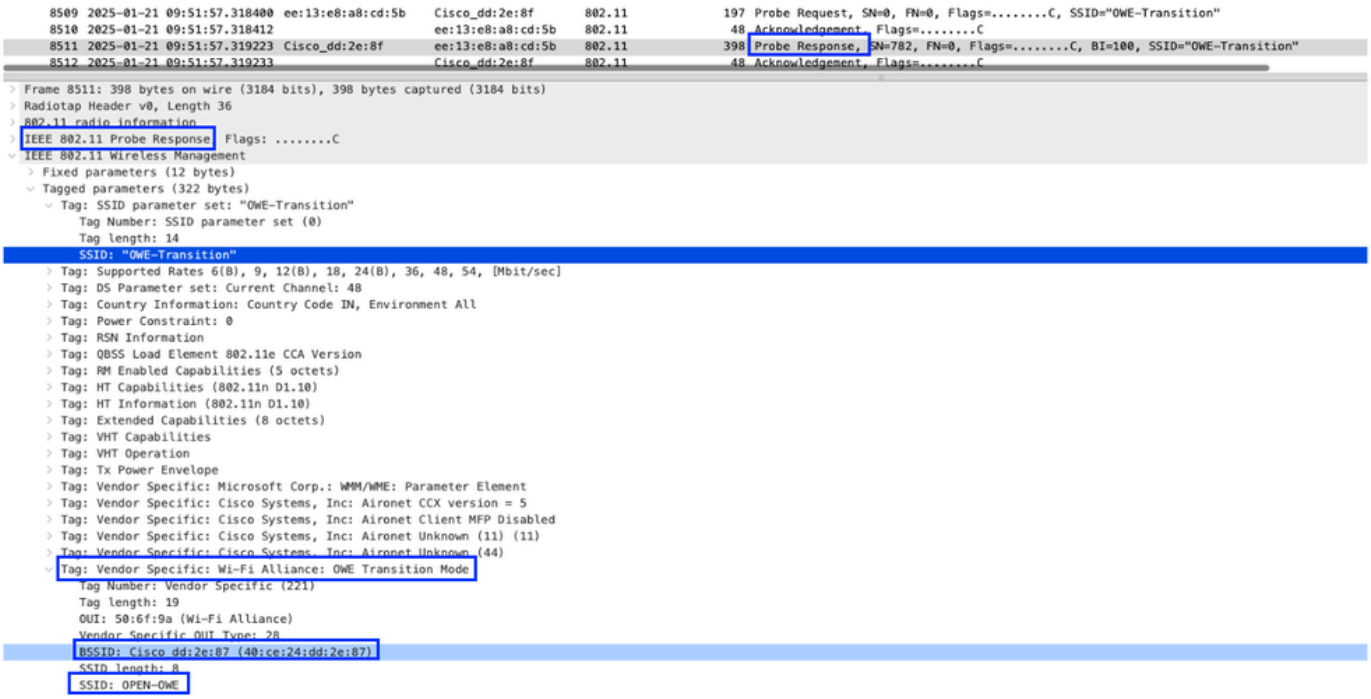

Imagem-4: Resposta da Sondagem

autenticação OPEN

- Depois de obter a resposta da sonda, a autenticação OPEN pode acontecer entre o cliente e o AP para verificar os detalhes/capacidades wifi dos clientes, antes da associação.

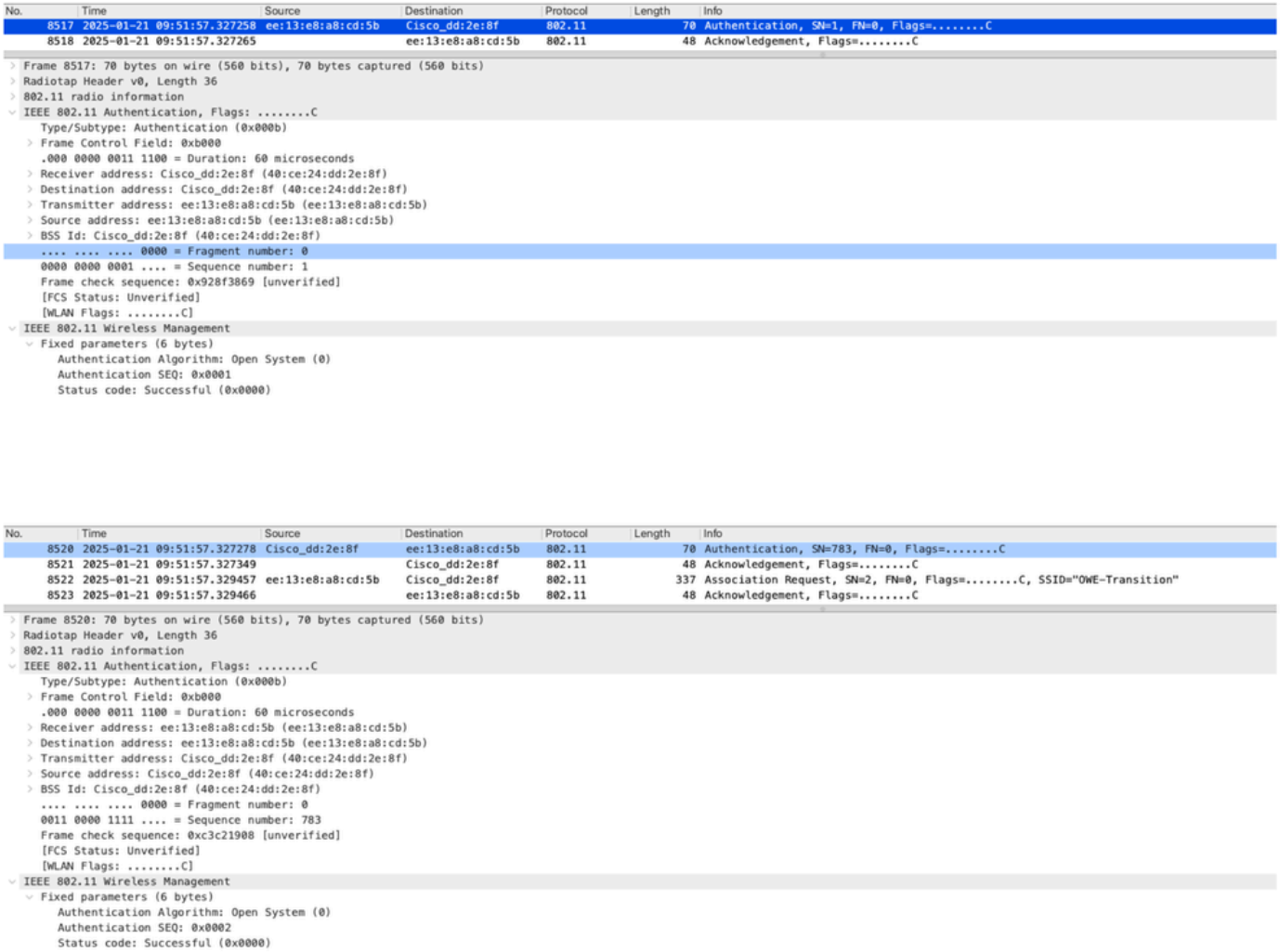

Imagem 5: ABRIR autenticação após investigação bem-sucedida

Solicitação de Associação do cliente para o AP

- Neste pacote, observe que o cliente pode estar anexando o valor do parâmetro Diffie-Hellman para criptografia.

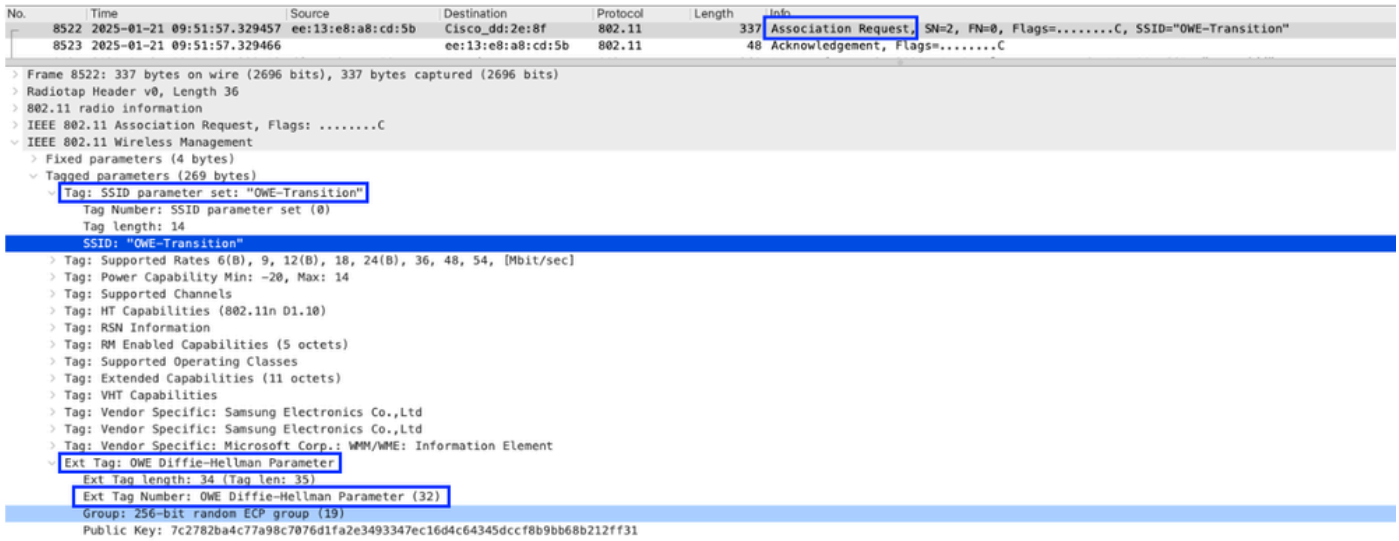

Imagem-6: Solicitação de Associação

- No rastreamento de RA, você pode começar a ver os logs de cliente da fase de Associação,

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

Resposta de associação enviada do AP para o cliente

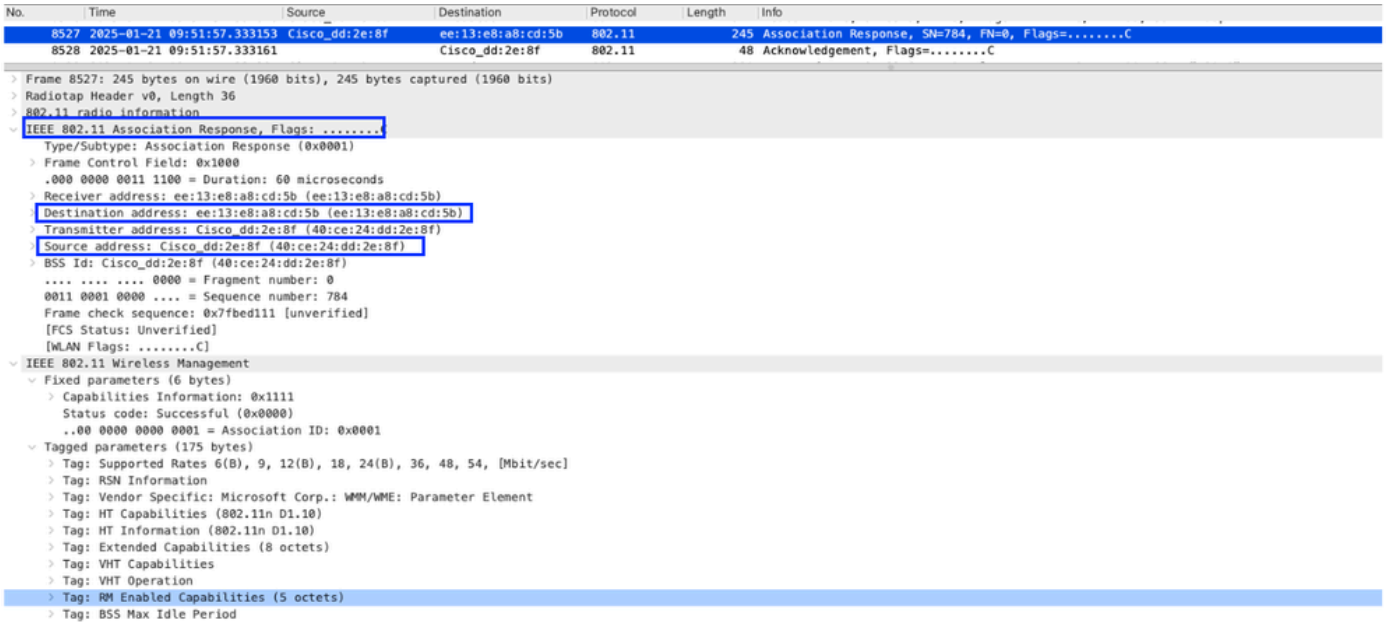

Imagem-7: Resposta da associação

```
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
```

Intercâmbio de chave

O handshake de 4 vias pode acontecer entre o AP e o dispositivo do cliente.

Key-1 enviado por AP

Key-2 enviada pelo cliente

Key-3 enviada pelo AP

Key-4 enviado pelo cliente

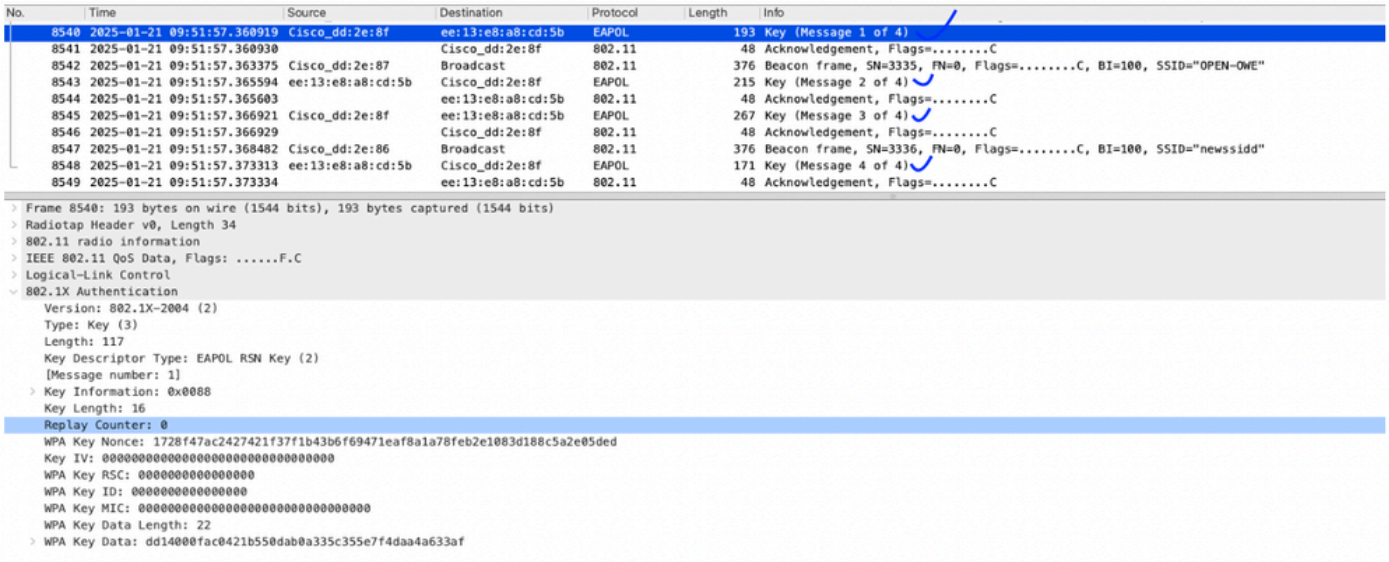

Imagem-8: Handshake em quatro vias

```
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
```

Autenticação L2 Bem-sucedida

```
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
```

Estado de aprendizagem 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
```

Cliente no estado EXECUTAR

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

Clientes sem suporte para criptografia OWE

- Ao revisar um quadro beacon em si, os clientes ficam sabendo se eles são capazes de suportar esse método de criptografia ou não. Se não for suportado, ele pode simplesmente enviar uma solicitação de sondagem para abrir o SSID "OPEN-OWE" e pode fazer uma autenticação aberta normal, obter o endereço IP e, em seguida, passar para o estado 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
```

Informações sobre a transição rápida

- Podemos configurar o OWE apenas na autenticação OPEN ou em Webauth (CWA/LWA/EWA).
- O FT não é suportado na transição OWE.
- Se você habilitar o FT, receberá esta mensagem de erro,

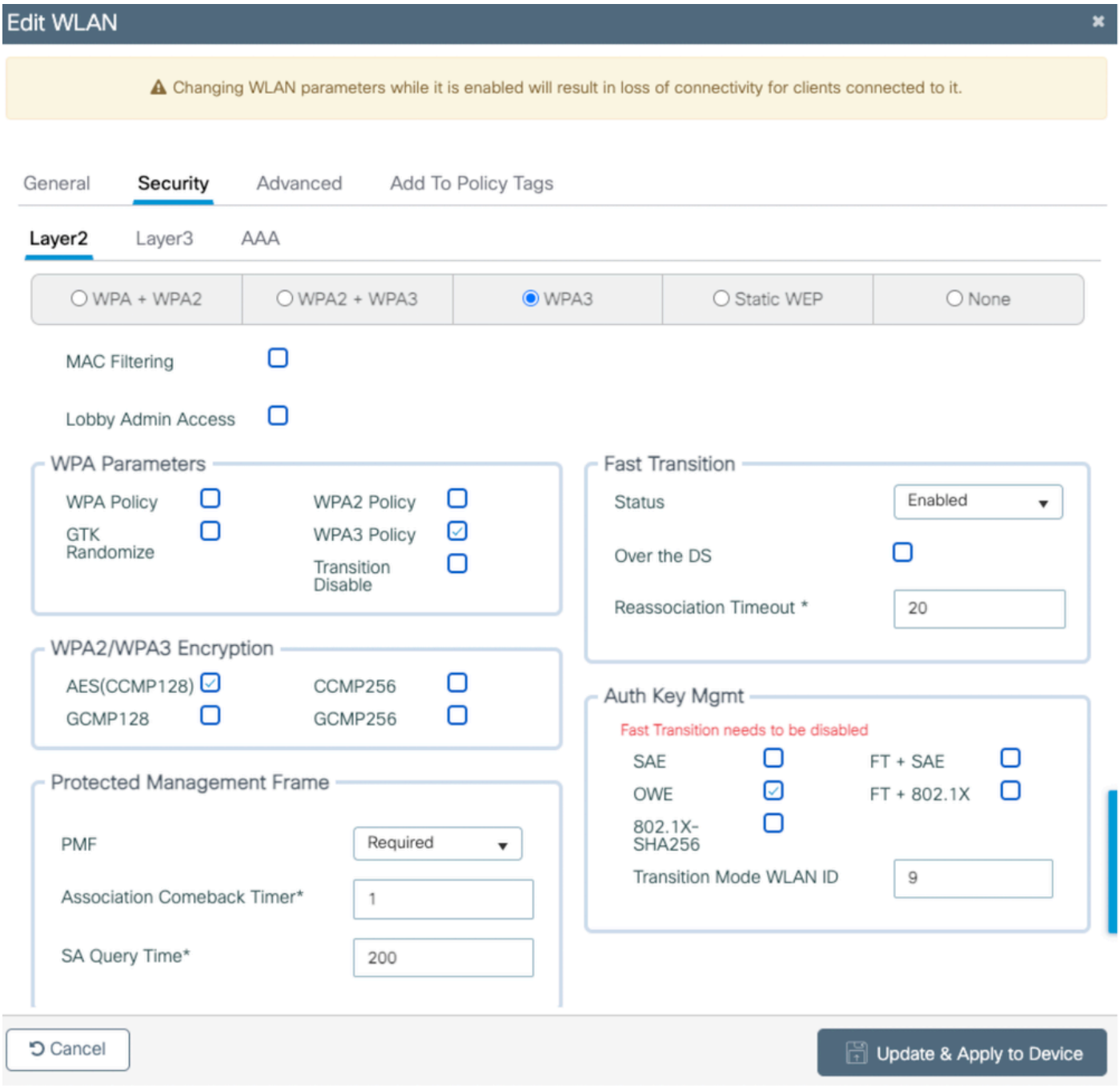

Imagem-9: Mensagem de erro quando habilitamos FT no SSID de transição OWE

OWE não é suportado com PSK/dot1x

Não podemos habilitar o OWE nessas combinações,

1. 802.1x ou FT+802.1x

2. PSK ou FT+PSK ou PSK-SHA256

3. SAE ou FT+SAE

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

Se você tentar ativar qualquer um desses métodos, receberá a mensagem de erro,

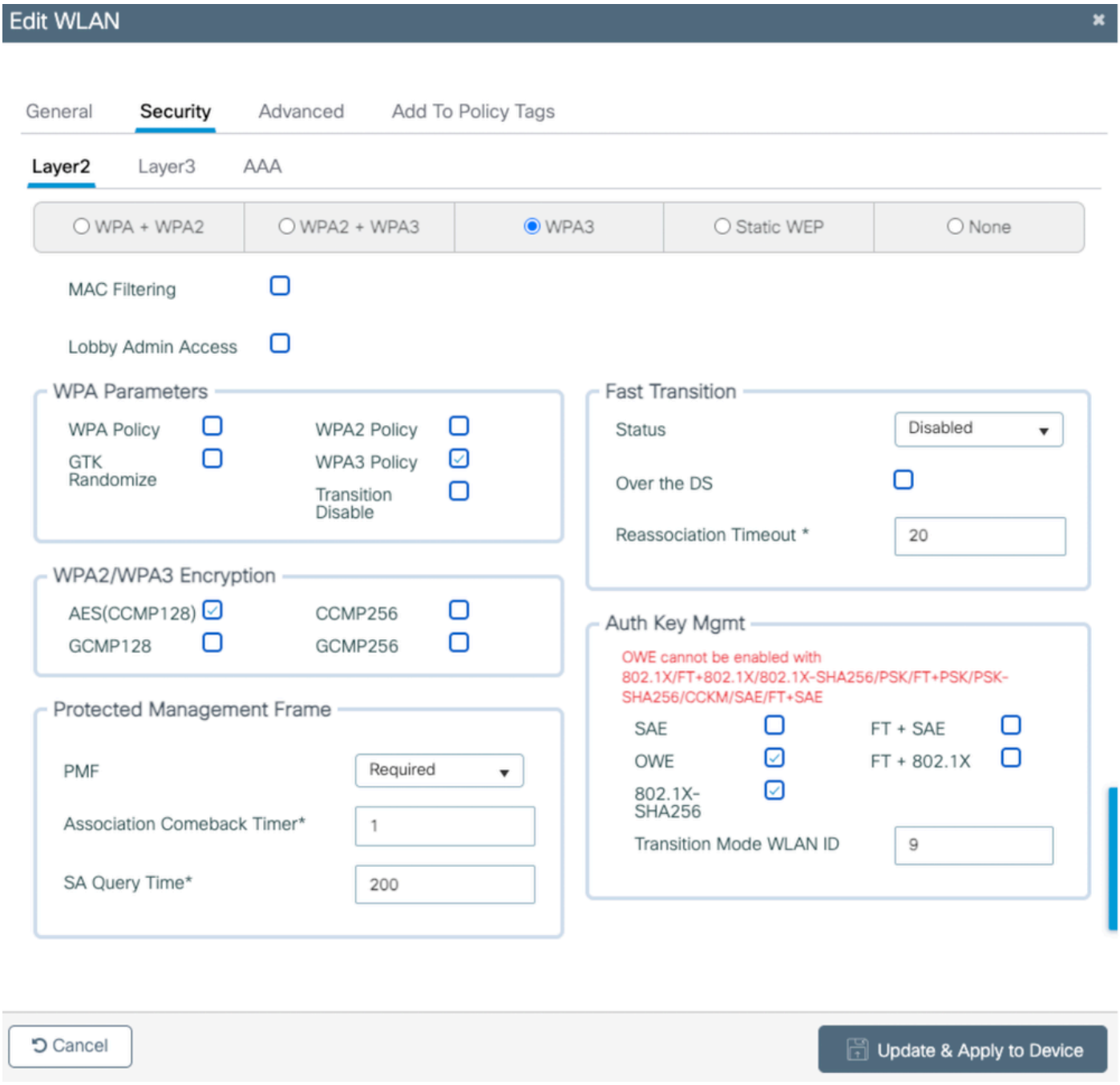

Imagem-10: Mensagem de erro ao obter ao habilitar outros métodos de autenticação no SSID OWE

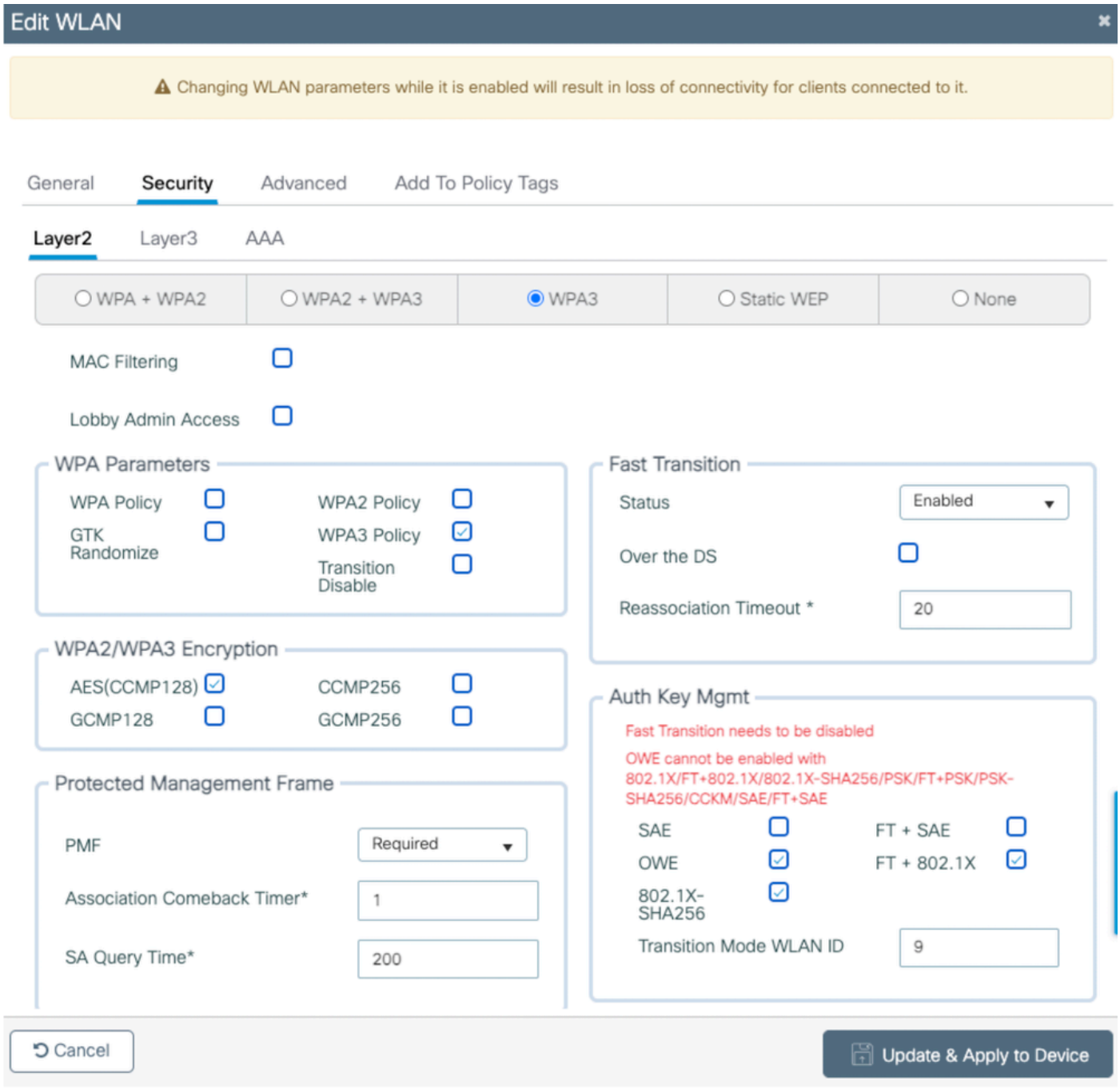

Imagem-11: Mensagem de erro ao habilitar o AKM

- Na versão IOS do Cisco IOS® XE 17.9.6, você pode ver a opção "OWE" no AKM quando seleciona "WPA2+WPA3". No entanto, você pode obter a mensagem de erro, você não pode usar OWE com essa combinação.

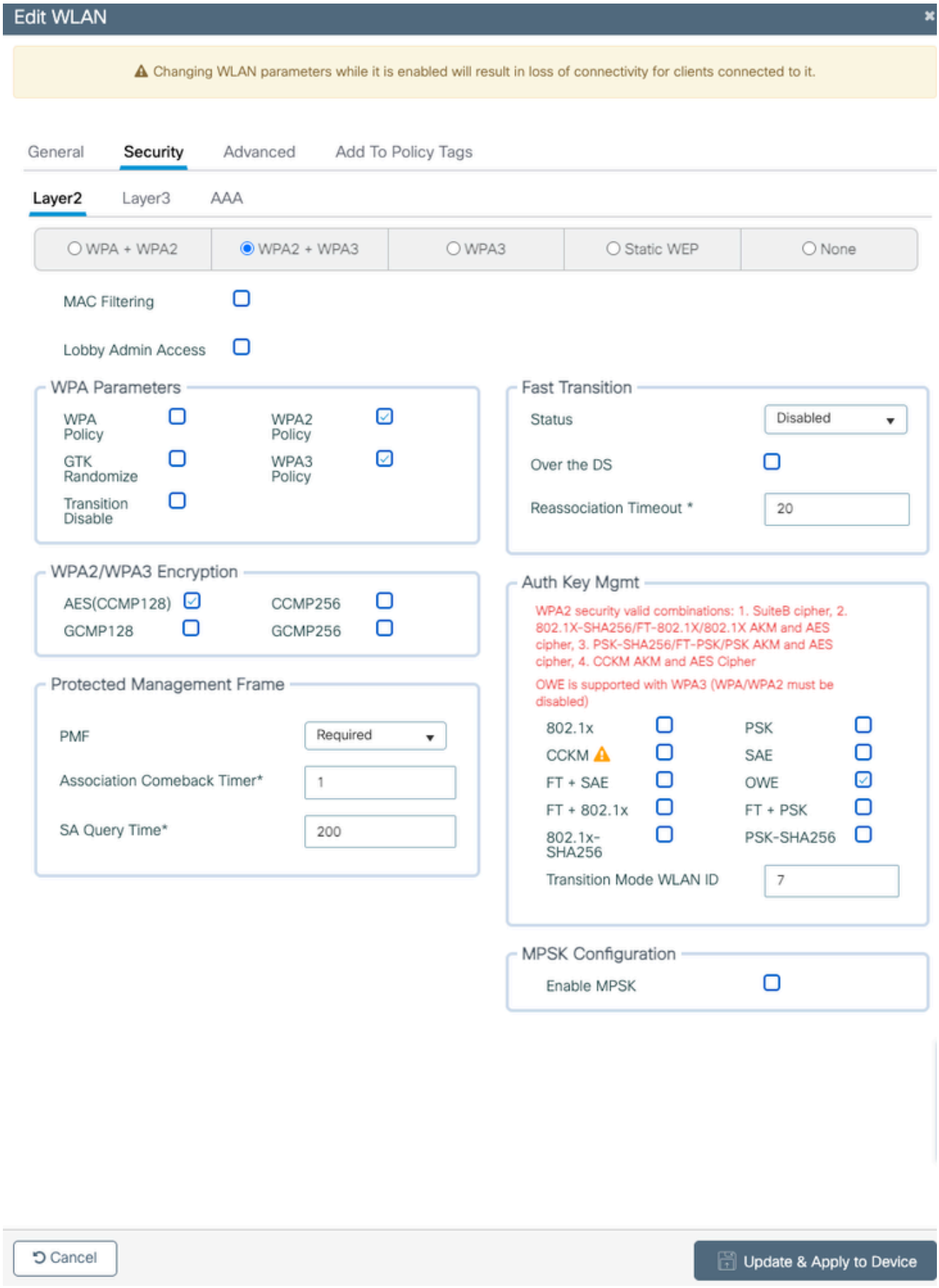

Imagem-12: Mensagem de erro ao escolher WPA2+WPA3

- No Cisco IOS® XE versão 17.12.4, quando você escolhe "WPA2+WPA3", você não pode

obter a opção "OWE" no AKM,

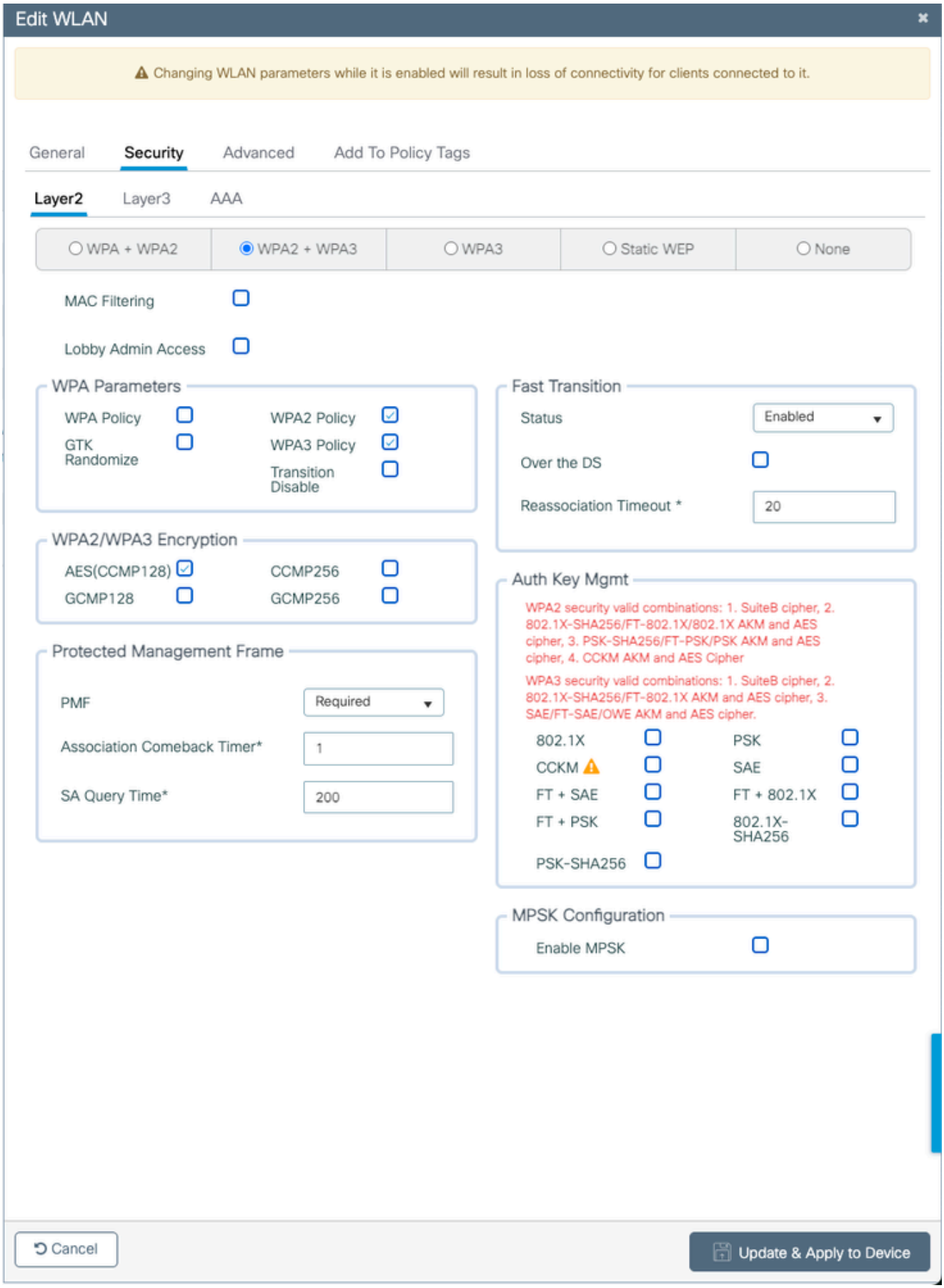

Imagem-13: Mensagem de erro - Não obtendo a opção OWE no AKM

Troubleshooting

1. Verifique as configurações nas duas WLANs, no SSID ABERTO e no SSID de transição OWE, para que o ID da WLAN de transição seja mapeado.
2. A opção de difusão deve ser desabilitada no SSID de transição OWE; ela deve ser habilitada somente no SSID OPEN.
3. Verifique os métodos de autenticação/criptografia/FT suportados descritos neste artigo.
4. Se as configurações estiverem corretas na extremidade da WLC, colete os logs e as saídas necessários para restringir o problema.

RA Trace e EPC (Captura de PAcket Incorporada)

Login to WLC GUI -> Troubleshooting -> Radioative Trace -> Add client wifi MAC address -> Clique na caixa de seleção desse cliente -> Start

Faça login na GUI da WLC -> Solução de problemas -> Captura de pacotes -> Adicione um novo nome de arquivo -> Escolha a interface de uplink e a VLAN/Interface da WMI -> Iniciar.

Da Máquina Cliente: Se possível, você pode instalar o aplicativo wireshark e coletar a captura de pacotes escolhendo a interface 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

AIR PCAP

Você pode coletá-lo usando o laptop MAC ou configurando um dos AP no modo farejador, consulte estes links,

Do laptop MAC:

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

Do AP farejador:

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

Conecte um laptop (servidor wireshark) à porta do switch e ele deve ter um aplicativo wireshark instalado. Esse servidor wireshark deve ter acessibilidade para a interface WMI da WLC. É necessário permitir o protocolo "5555, 5000 ou 5556" no firewall se ele estiver entre o WLC e o servidor do Wireshark.

Verifique se há algum "gscaler" instalado no PC em que o Wireshark está instalado, se for o que, por favor, "desligue" e tente, se houver qualquer firewall como o Windows Defender ou qualquer coisa presente nele, desabilite-os e tente coletar o PCAP.

Roaming

Quando o cliente faz roaming de um AP para outro, ele precisa executar estas etapas,

- Necessidade de enviar reassociação/associação - Depende da solicitação do cliente.
- É necessário enviar detalhes DH (Diffie-Helman) na solicitação de associação.
- O cliente pode obter detalhes de DH na resposta de associação do AP, com base nas obtenções de PMK geradas no cliente e no AP.
- O handshake de 4 vias pode acontecer entre o AP e o cliente.
- No OWE, você não consegue habilitar a FT, portanto, o 802.11r não é possível.
- Cada vez, quando o cliente faz roaming, ele precisa fazer um handshake de 4 vias após a troca de DH em associação.
- Cliente e AP que usam seu próprio PMKID, é exclusivo para cada AP e clientes.
- Se o cliente se conectar ao mesmo AP, ele poderá usar o mesmo PMKID. Em algum cenário, se o cliente foi excluído do que o AP pode gerar um novo PMKID, no entanto, o cliente usa o mesmo PMKID para handshake de 4 vias.

Exemplo:

Se o cliente se conectar ao mesmo AP, você poderá ver o mesmo PMKID tanto na solicitação de associação quanto na resposta de associação. Na resposta de Associação, você não poderá ver detalhes de DH se ele usar o mesmo PMKID.

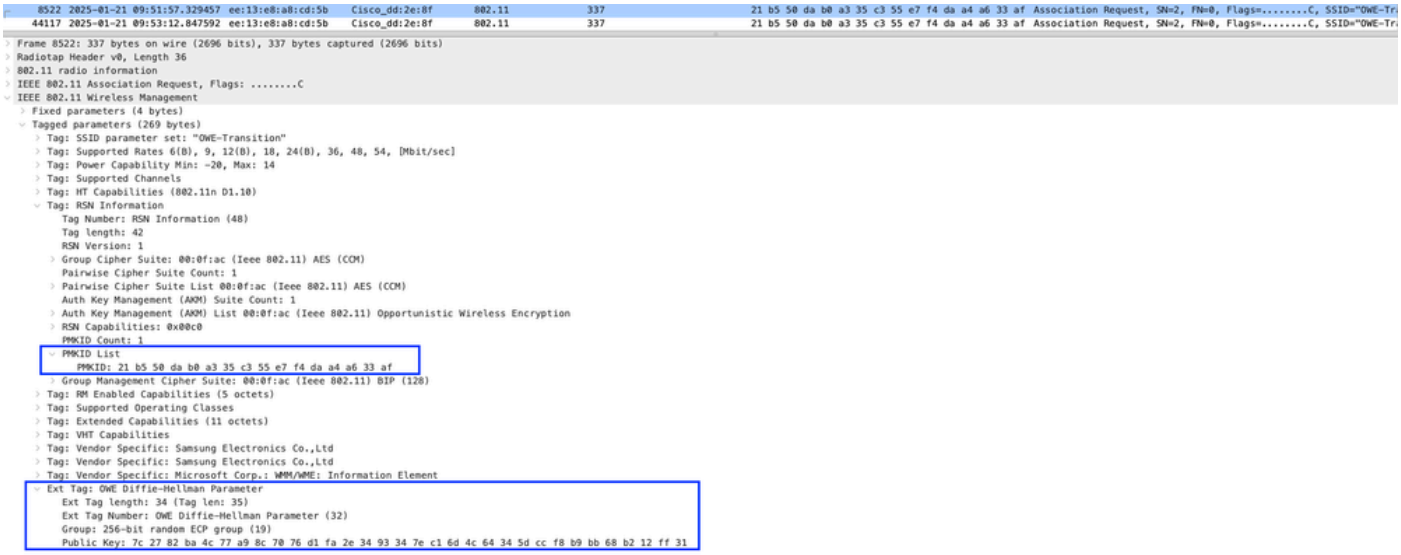

Imagem-14: Usando o mesmo PMKID

Imagem-15: Resposta de Associação com o mesmo PMKID

Para testes, excluiu manualmente esse cliente da WLC e ele foi associado novamente ao mesmo AP, nesse momento, o cliente envia um mesmo PMKID, mas o AP envia detalhes de DH na resposta de associação.

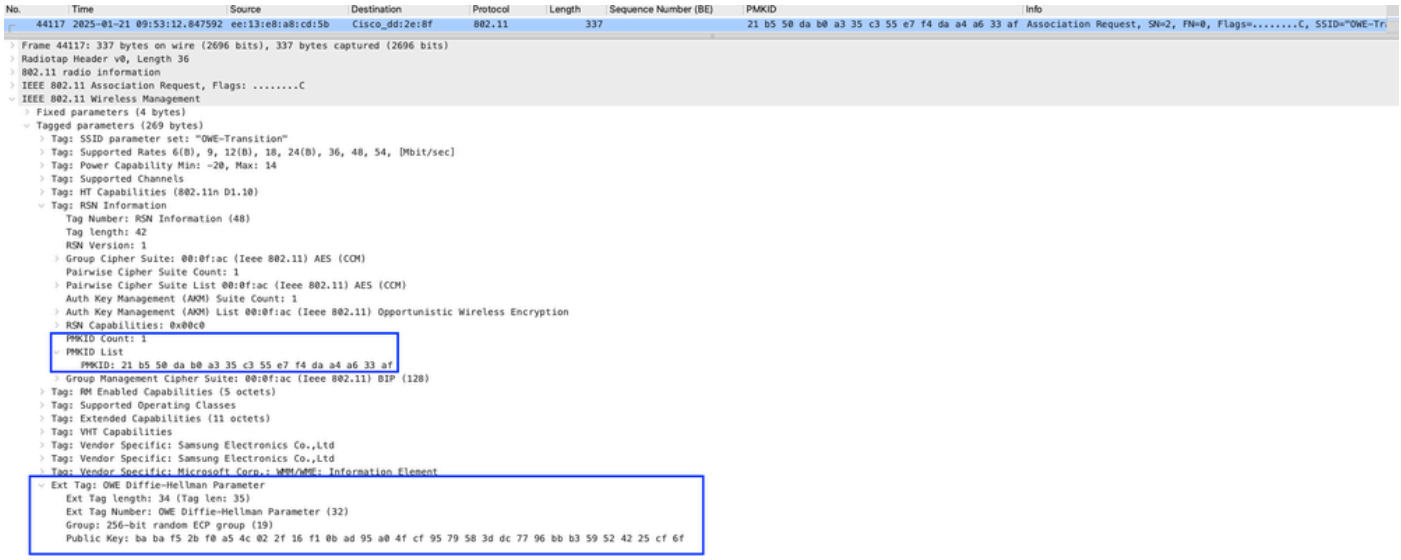

Imagem-16: Após a exclusão, o cliente enviou a mesma PMKID com detalhes de DH

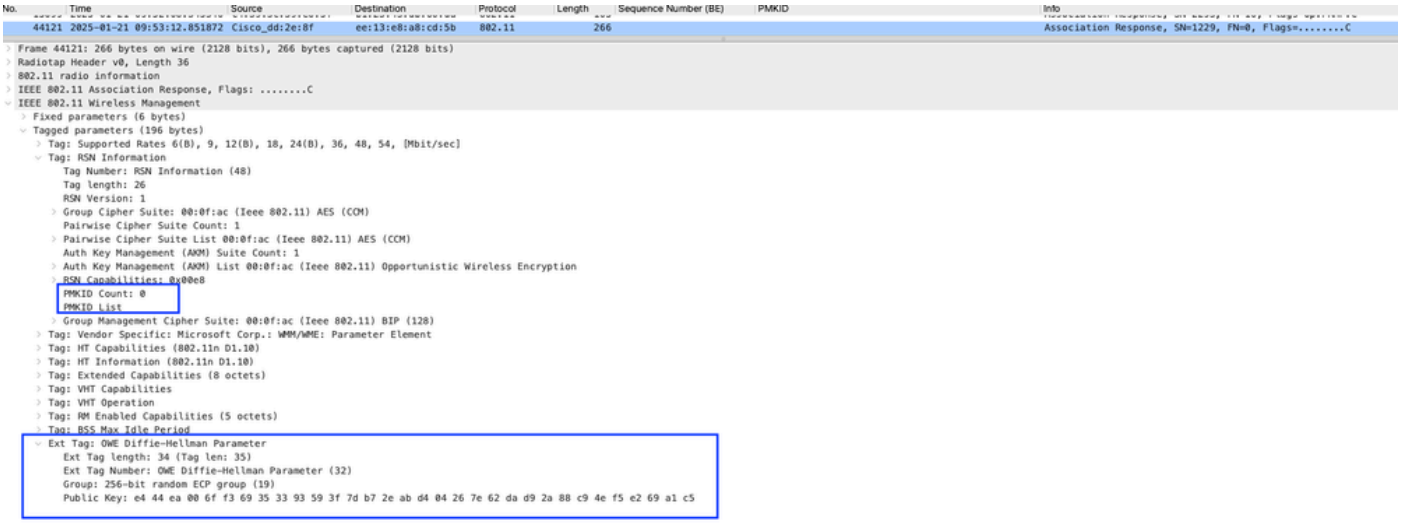

Imagem-17: O AP usa valores DH para gerar seu novo PMKID

Neste exemplo: Tanto o AP como o cliente usam o mesmo PMKID ao fazer handshake de 4 vias, verifique as mensagens "M1 e em M2".

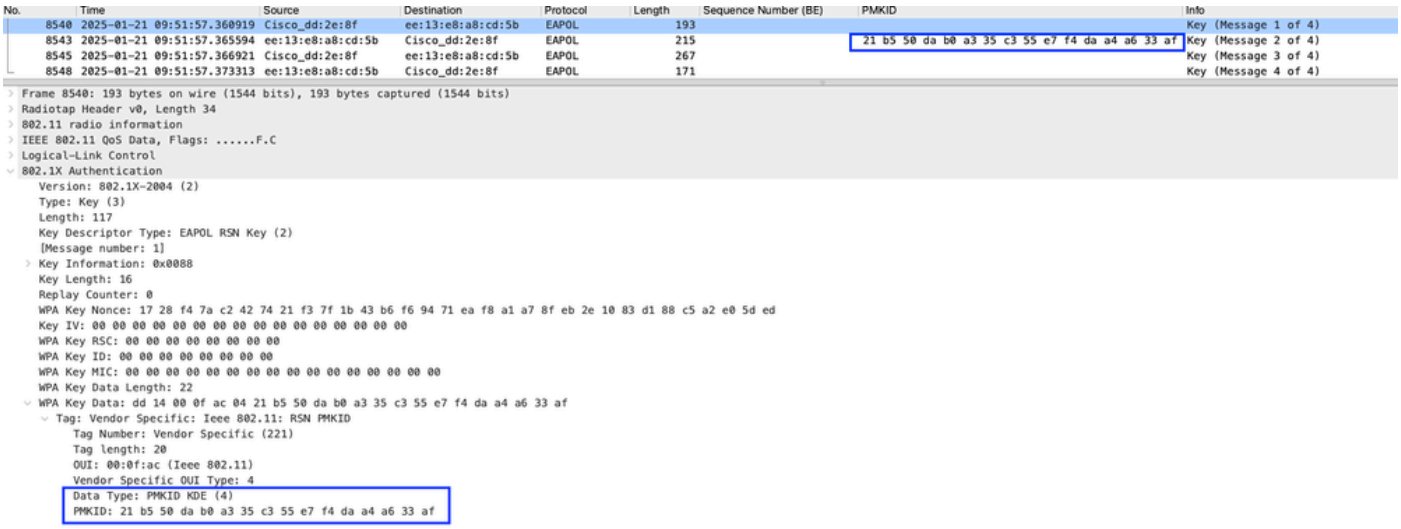

Imagem- 18: AP e cliente usando o mesmo PMKID

Neste exemplo: O cliente que usa o mesmo PMKID, mas o AP que usa um PMKID diferente que ele gerou depois que o cliente foi excluído, verifique as mensagens "M1 e M2".

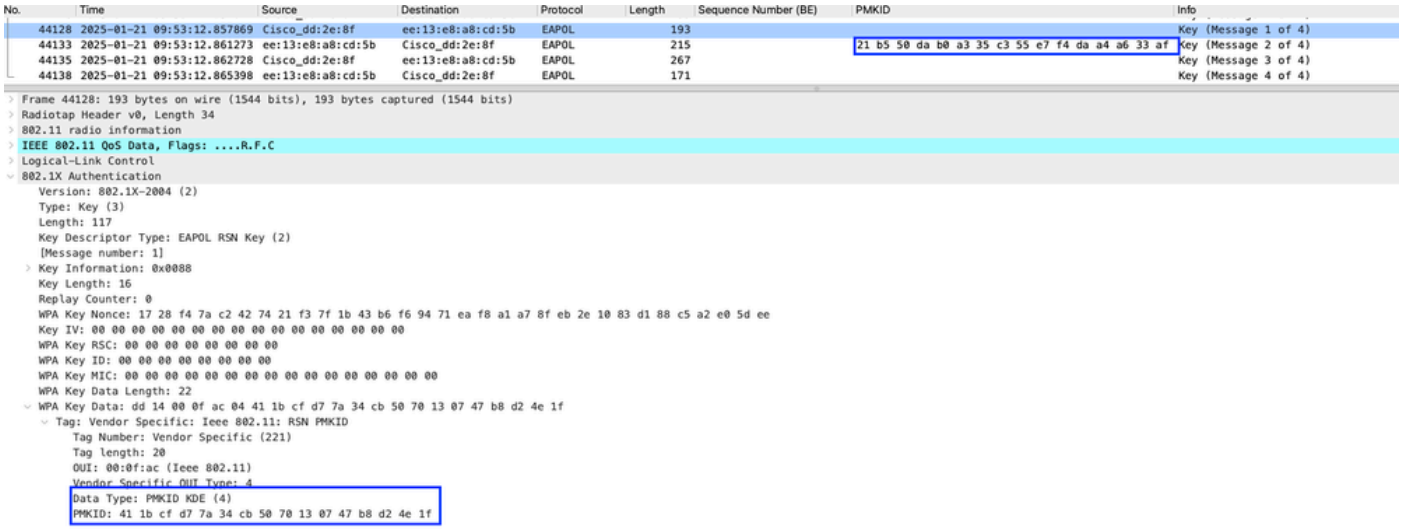

Imagem-19: AP e cliente usando PMKID diferente

Do rastreamento RA interno:

Neste exemplo: O cliente enviou parâmetros DH na solicitação de associação e o AP processou mais do que gerou a 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
```

Depois disso, o mesmo cliente se conectando ao mesmo AP, neste momento, o AP não gerou o novo 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
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.