기회주의적 무선 암호화 흐름 이해

목차

```
<u>소개</u>
<u>사전 요구 사항</u>
  요구 사항
  사용되는 구성 요소
설명
단계
Lab Repro 세부 정보
OWE 플로우
  <u>원래 비컨 프레임</u>
  숨겨진 SSID 비콘
  <u>클라이언트에서 WISE 전환 SSID로 전송된 프로브 요청</u>
  <u>AP에서 클라이언트로 전송된 프로브 응답</u>
  OPEN 인증
  <u>클라이언트에서 AP로의 연결 요청</u>
  <u>AP에서 클라이언트로 보낸 연결 응답</u>
  키 교환
  <u>L2 인증 성공</u>
  <u>IP 학습 상태</u>
  <u>클라이언트 실행 상태</u>
  WISE 암호화가 지원되지 않는 클라이언트
빠른 전환 정보
WISE는 PSK/dot1x에서 지원되지 않습니다.
<u>문제 해결</u>
  RA 추적 및 EPC(임베디드 패킷 캡처)
  <u>항공 모함</u>
<u>로밍</u>
```

소개

이 문서에서는 OWE 전환 흐름과 Catalyst 9800 WLC(Wireless LAN Controller)에서 작동하는 방식에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 작동을 위해 9800 WLC, 액세스 포인트(AP)를 구성하는 방법
- WLAN 및 정책 프로필 구성 방법

사용되는 구성 요소

- 이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.
 - C9800-80, Cisco IOS® XE 17.12.4 및 Cisco IOS® XE 17.9.6에서 테스트됨
 - AP 모델: C9136I, 로컬 및 플렉스 연결 모드에서 모두 확인됨.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

설명

- OWE(Opportunistic Wireless Encryption)는 무선 매체를 위한 암호화를 제공하는 IEEE 802.11의 확장입니다. OWE 기반 인증의 목적은 AP와 클라이언트 간의 안전하지 않은 개방형 무선 연결을 방지하는 것입니다.
- OWE는 무선 암호화를 설정하기 위해 Diffie-Hellman 알고리즘 기반 암호화를 사용합니다.
- OWE를 사용하면 클라이언트와 AP는 액세스 절차 중에 Diffie-Hellman 키 교환을 수행하고 그 결과로 생성되는 페어와이즈 암호를 4방향 핸드셰이크로 사용합니다.
- OWE를 사용하면 개방형 또는 공유 PSK 기반 네트워크가 구축된 구축에서 무선 네트워크 보안이 향상됩니다.

다계

- 1. 암호화/보안 없이 하나의 OPEN WLAN을 구성하고 브로드캐스트를 활성화합니다.
- 2. OWE 보안 설정으로 다른 SSID를 구성하고 변환 모드 wlan-id에서 OPEN WLAN ID 번호 를 매핑합니다. 이 OWE 변환 SSID에서 브로드캐스트 SSID 옵션을 비활성화합니다.
- 3. OPEN WLAN "transition-mode-wlan-id" 필드에 OWE 전환 WLAN ID 번호를 매핑합니다.

Lab Repro 세부 정보

- 개방형 SSID 이름: 채무액 공개
- OWE 전환 SSID 이름: 채무 이행
- OPEN-WISE의 BSSID: 40:ce:24:dd:2e:87
- BSSID OF OWE-Transition(WISE-Transition의 BSSID): 40:ce:24:dd:2e:8f

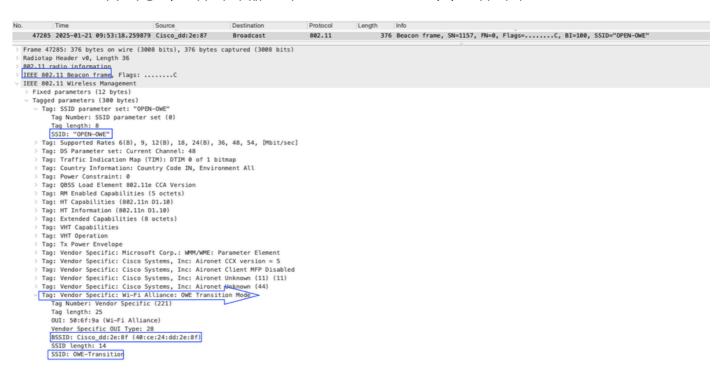
OWE 플로우

1. 신호는 OPEN SSID에 대해 브로드캐스트될 수 있습니다. AIR PCAP에서 해당 SSID 이름으로 신호를 볼 수 있습니다.

- 2. 또한 AIR PCAP에서 자체 SSID 이름 대신 "Wildcard"라는 이름의 숨겨진 보안 지원 SSID를 볼 수 있습니다.
- 3. 클라이언트가 OPEN SSID에 대한 비콘 프레임을 수신하면 WISE가 있거나 이를 지원하는 경우 WISE 전환 SSID(OPEN SSID 대신 보안이 활성화된 SSID)로 프로브 요청 전송을 시작할수 있습니다.
- 4. WISE 지원 클라이언트는 전환 SSID에서 프로브 응답을 가져올 수 있습니다.
- 5. 클라이언트와 AP 간에 OPEN 인증이 발생할 수 있습니다.
- 6. 클라이언트는 DH 키 교환 세부사항이 포함된 연결 요청을 AP에 전송하고 그 결과로 생성되는 쌍방향 암호를 4-way 핸드셰이크에 사용할 수 있습니다.
- 7. AP에서 연결 응답을 보낼 수 있습니다.
- 8. AP와 클라이언트 장치 간에 4방향 핸드셰이크가 발생할 수 있습니다.
- 9. 성공적인 키 관리 후에는 L2 PSK가 성공할 수 있습니다.
- 10. 클라이언트는 DHCP. ARP 등에서 IP를 가져올 수 있습니다.
- 11. 클라이언트는 RUN 상태로 전환할 수 있습니다.
- 12. WISE를 지원하지 않는 클라이언트 디바이스인 경우 OPEN SSID 자체에 프로브 요청을 보낼수 있으며 RUN 상태로 갈 수 있는 것보다 직접 IP를 가져올 수 있습니다.

원래 비컨 프레임

• 여기서 AIR PCAP는 SSID "OPEN-WISE" 브로드캐스트(비콘 프레임)를 보여줍니다. 전환 SSID 세부사항이 포함되어 있으며 "OWE-Transition"이라고 합니다.



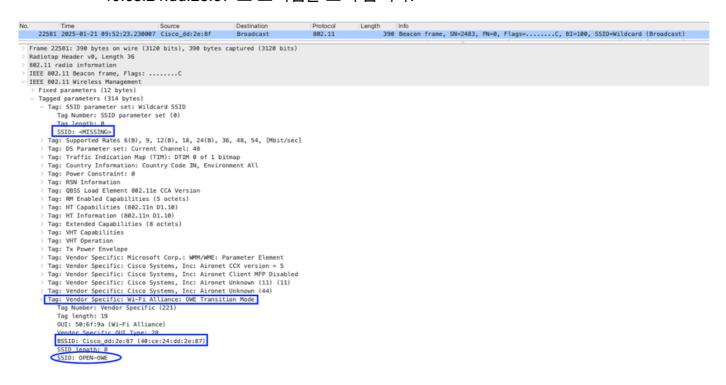
이미지-1: 개방형 SSID의 비콘 프레임

숨겨진 SSID 비콘

- WLAN 컨피그레이션에 따라 이 "OWE-Transition" SSID에 대해 "broadcasting"이 비활 성화되지만 AIR PCAP에서 SSID 이름 "Wildcard"가 포함된 숨겨진 SSID 신호를 볼 수 있습니다. 그러나 해당 패킷을 선택하면 WISE-Transition 세부 정보가 포함됩니다.
- 이 패킷을 사용하여 숨겨진 SSID의 BSSID를 가져옵니다(예: "40:ce:24:dd:2e:8f"). 패킷

캡처에서 검색합니다.

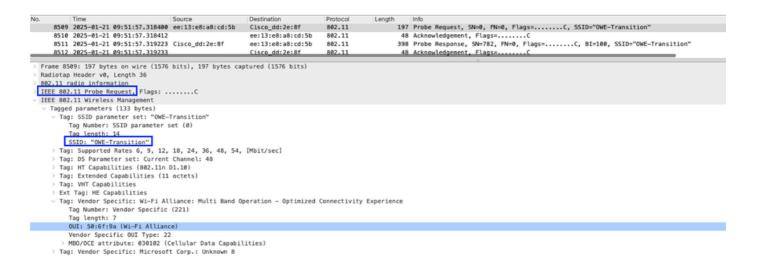
• 이 패킷에서는 SSID가 "Missing"이고 전환 SSID가 "OPEN-WISE"로, BSSID가 "40:ce:24:dd:2e:87"로 표시됨을 보여 줍니다.



이미지-2: 숨겨진 SSID - OWE 전환

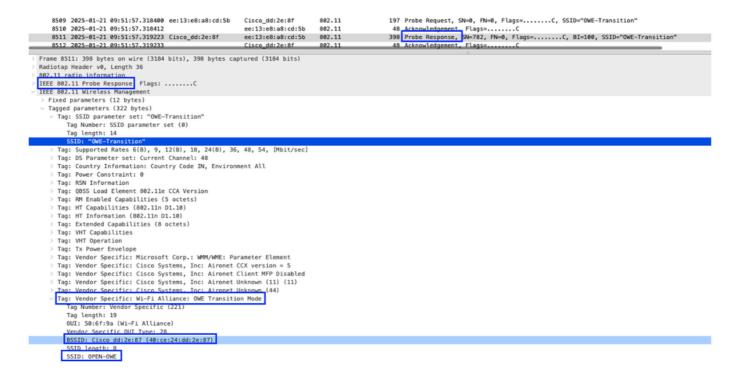
클라이언트에서 WISE 전환 SSID로 전송된 프로브 요청

- 비콘 프레임 "OPEN-WISE" SSID를 기반으로 클라이언트는 연결해야 하는 다른 SSID 세부사항을 알게 됩니다. 이 시나리오에서 "WISE-Transition"입니다. 클라이언트가 WISE 암호화를 지원할 수 있는 경우 프로브 요청을 "WISE-Transition" SSID로 전송하고 응답을 받을 수 있습니다.
- 프로브 요청이 WISE-Transition BSSID "40:ce:24:dd:2e:8f"로 전송되었으며 응답을 받 았습니다. 이 프로브 응답 패킷 내에서도 OPEN-WISE SSID 세부사항을 볼 수 있습니다



AP에서 클라이언트로 전송된 프로브 응답

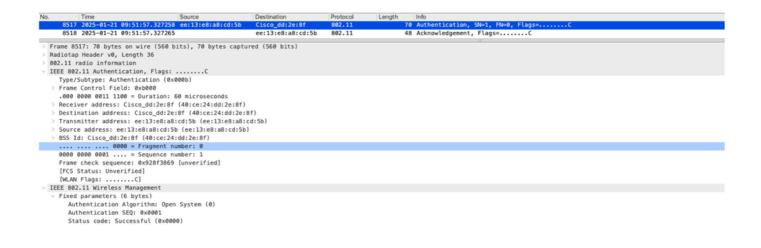
• 클라이언트는 SSID "OWE-Transition"에 대한 프로브 응답을 받았지만 WiFi Alliance에 원래 SSID 세부사항 "OPEN-OWE"가 있습니다.



이미지-4: 프로브 응답

OPEN 인증

• 프로브 응답을 받은 후 연결 전에 클라이언트와 AP 간에 OPEN 인증을 수행하여 클라이언트 wifi 세부사항/기능을 확인할 수 있습니다.

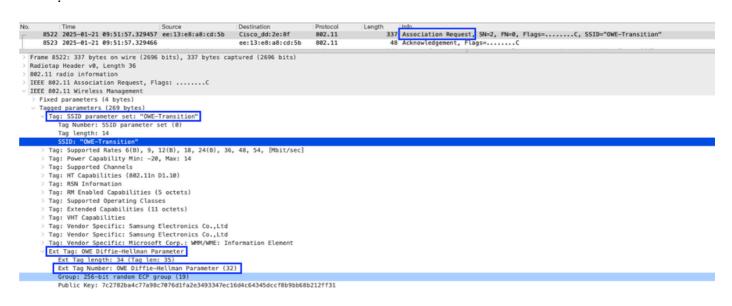


	Time	Source	Destination	Protocol	Length	Info				
	2025-01-21 09:51:57.327278		ee:13:e8:a8:cd:5b	802.11		Authentication, SN=783, FN=0, Flags=C				
8521	2025-01-21 09:51:57.327349		Cisco_dd:2e:8f	802.11		Acknowledgement, Flags=C				
8522	2025-01-21 09:51:57.329457	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	802.11	337	Association Request, SN=2, FN=0, Flags=C, SSID="OWE-Transition"				
8523	2025-01-21 09:51:57.329466		ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=C				
	20: 70 bytes on wire (560 b	its), 70 bytes captur	red (560 bits)			*				
	Header v0, Length 36									
> 802.11 radio information										
✓ IEEE 802.11 Authentication, Flags:C										
	ubtype: Authentication (0x0	100b)								
Frame Control Field: 0xb000										
.000 0000 0011 1100 = Duration: 60 microseconds										
Receive	er address: ee:13:e8:a8:cd:	:5b (ee:13:e8:a8:cd:5	b)							
> Destination address: ee:13:e8:a8:cd:5b (ee:13:e8:a8:cd:5b)										
> Transm:	itter address: Cisco_dd:2e:	8f (40:ce:24:dd:2e:8	f)							
Source	address: Cisco_dd:2e:8f (4	10:ce:24:dd:2e:8f)								
> BSS Id:	: Cisco_dd:2e:8f (40:ce:24:	dd:2e:8f)								
0011 00	000 1111 = Sequence nu	ımber: 783								
Frame of	check sequence: 0xc3c21908	[unverified]								
[FCS St	tatus: Unverified]									
[WLAN F	Flags:C]									
IEEE 802.	11 Wireless Management									
∨ Fixed p	parameters (6 bytes)									
Auth	hentication Algorithm: Open	System (0)								
Auth	hentication SEQ: 0x0002									
	tus code: Successful (0x000)									

이미지-5: Probe 성공 후 OPEN 인증

클라이언트에서 AP로의 연결 요청

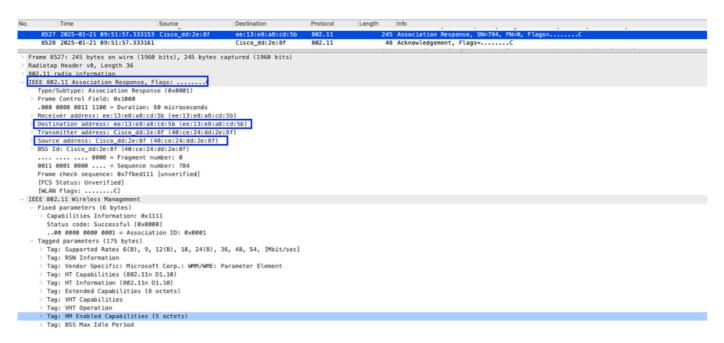
• 이 패킷에서는 클라이언트가 암호화를 위해 Diffie-Hellman 매개변수 값을 연결할 수 있습니다



• RA 추적에서는 Association(연결) 단계에서 클라이언트 로그를 볼 수 있습니다.

```
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
```

AP에서 클라이언트로 보낸 연결 응답



이미지-7: 연결 응답

```
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
```

키 교환

AP와 클라이언트 장치 간에 4-way 핸드셰이크가 발생할 수 있습니다.

Key-1 send by AP(AP에 의한 키-1 전송)

Key-2 클라이언트에서 전송

Key-3 send by AP(AP에 의한 키-3 전송)

Key-4 클라이언트에서 전송

No.	Time	Source	Destination	Protocol	Length	Info /
854	0 2025-01-21 09:51:57.360919	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAP0L	193	Key (Message 1 of 4)
854	1 2025-01-21 09:51:57.360930		Cisco_dd:2e:8f	802.11	48	Acknowledgement, Flags=C
854	2 2025-01-21 09:51:57.363375	Cisco_dd:2e:87	Broadcast	802.11	376	Beacon frame, SN=3335, FN=0, Flags=C, BI=100, SSID="OPEN-OWE"
854	3 2025-01-21 09:51:57.365594	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	215	6 Key (Message 2 of 4) ✓
854	4 2025-01-21 09:51:57.365603		ee:13:e8:a8:cd:5b	802.11		Acknowledgement, Flags=C
854	5 2025-01-21 09:51:57.366921	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	267	7 Key (Message 3 of 4) 🗸
854	6 2025-01-21 09:51:57.366929		Cisco_dd:2e:8f	802.11	48	Acknowledgement, Flags=C
854	7 2025-01-21 09:51:57.368482	Cisco_dd:2e:86	Broadcast	802.11		Beacon frame, SN=3336, FN=0, Flags=C, BI=100, SSID="newssidd"
854	8 2025-01-21 09:51:57.373313	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL		L Key (Message 4 of 4)✓
854	9 2025-01-21 09:51:57.373334		ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=C
> Logical > 802.1X Vers Type Leng Key [Mes > Key Key Repl	02.11 QoS Data, Flags: I-Link Control Authentication ion: 802.1X-2004 (2): Key (3) th: 117 Descriptor Type: EAPOL RSN Ke sage number: 1] Information: 0x0088 Length: 16 ay Counter: 0	ey (2)				
WPA WPA WPA WPA	Key Nonce: 1728f47ac24274217; IV: 000000000000000000000000000000000000	999999999		e05ded		

이미지-8: 4-Way 핸드셰이크

```
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.cd5b 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 Cli 2025/01/21 15:21:57.426748998 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b Cli 2025/01/21 15:21:57.426725965 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b Cli 2025/01/21 15:21:57.426725965 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b Cli 2025/01/21 15:21:57.426725965 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b Cli 2025/01/21 15:21:57.426727805 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b Cli 2025/01/21 15:21:57.426727805 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b Cli 2025/01/21 15:21:57.434078994 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b Cli 2025/01/21 15:21:57.434099154 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b Cli 2025/01/21 15:21:57.434099154 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b Cli 2025/01/21 15:21:57.434099154 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b Cli 2025/01/21 15:21:57.434099154 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b Cli 2025/01/21 15:21:57.434099154 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b Cli 2025/01/21 15:21:57.434099154 {wncd_x_R0-0}{1}: [
```

L2 인증 성공

```
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
```

IP 학습 상태

```
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]: (info): 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]: (info): TX: DHCPv4 from interfac 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
```

클라이언트 실행 상태

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

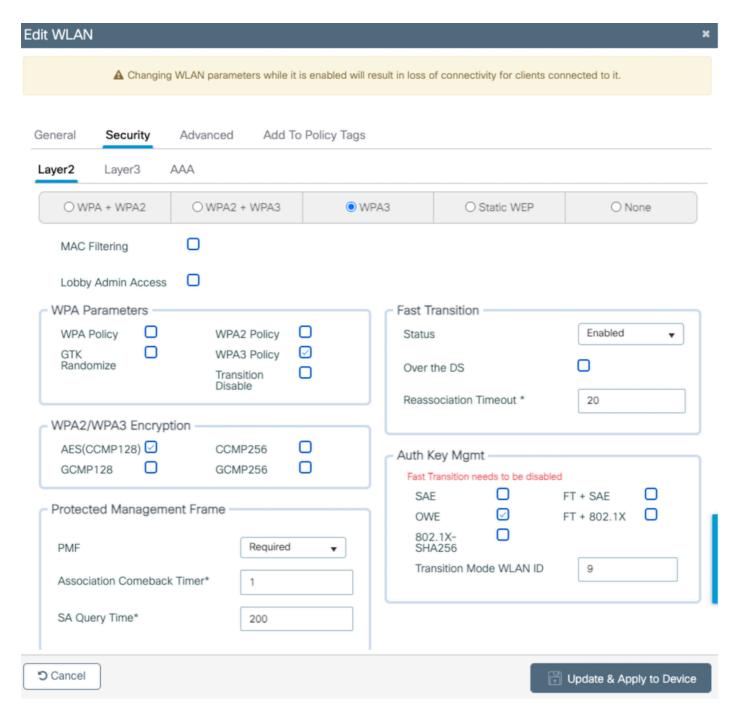
WISE 암호화가 지원되지 않는 클라이언트

• 비콘 프레임 자체를 검토하면 클라이언트는 이 암호화 방법을 지원할 수 있는지 여부를 알게 됩니다. 지원되지 않는 경우, SSID "OPEN-WISE"를 열기 위해 프로브 요청을 보내고 일반적 인 개방형 인증을 수행하여 IP 주소를 가져온 다음 RUN 상태로 전환할 수 있습니다.

```
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: d037.4587.8f3 2025/01/16 15:36:10.305777492 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
```

빠른 전환 정보

- OPEN 인증 또는 Webauth(CWA/LWA/EWA)에서만 OWE를 구성할 수 있습니다.
- FT는 OWE 변환에서 지원되지 않습니다.
- FT를 활성화하면 다음과 같은 오류 메시지가 표시됩니다.



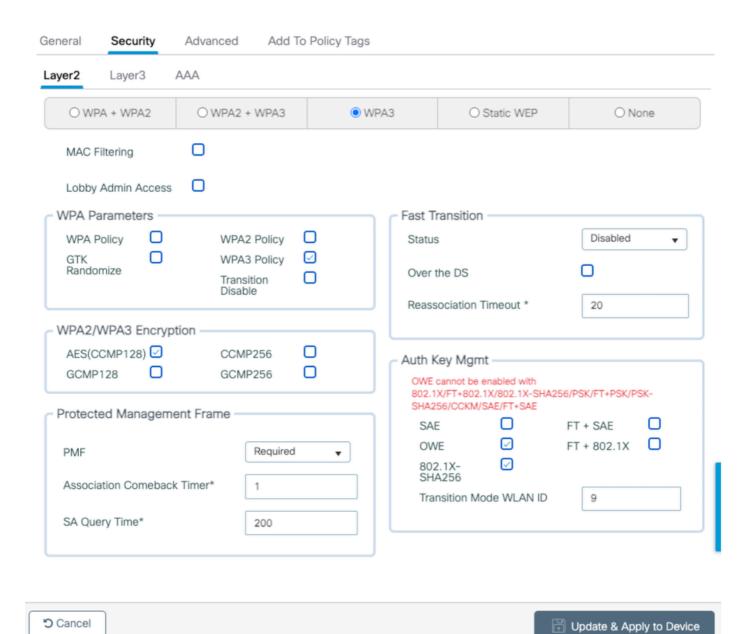
이미지-9: Owne Transition SSID에서 FT를 활성화하는 경우 오류 메시지

WISE는 PSK/dot1x에서 지원되지 않습니다.

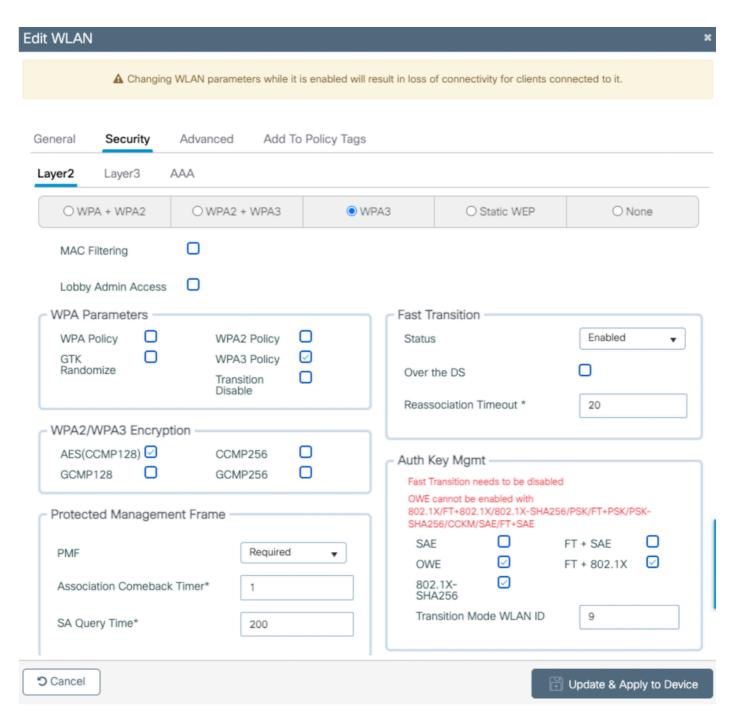
이러한 조합에서는 OWE를 활성화할 수 없습니다.

- 1. 802.1x 또는 FT+802.1x
- 2. PSK 또는 FT+PSK 또는 PSK-SHA256
- 3. SAE 또는 FT+SAE
- 4. 802.1x-SHA256 또는 FT+802.1x-SHA256
- 이러한 방법 중 하나를 활성화하려고 하면

Edit WLAN *

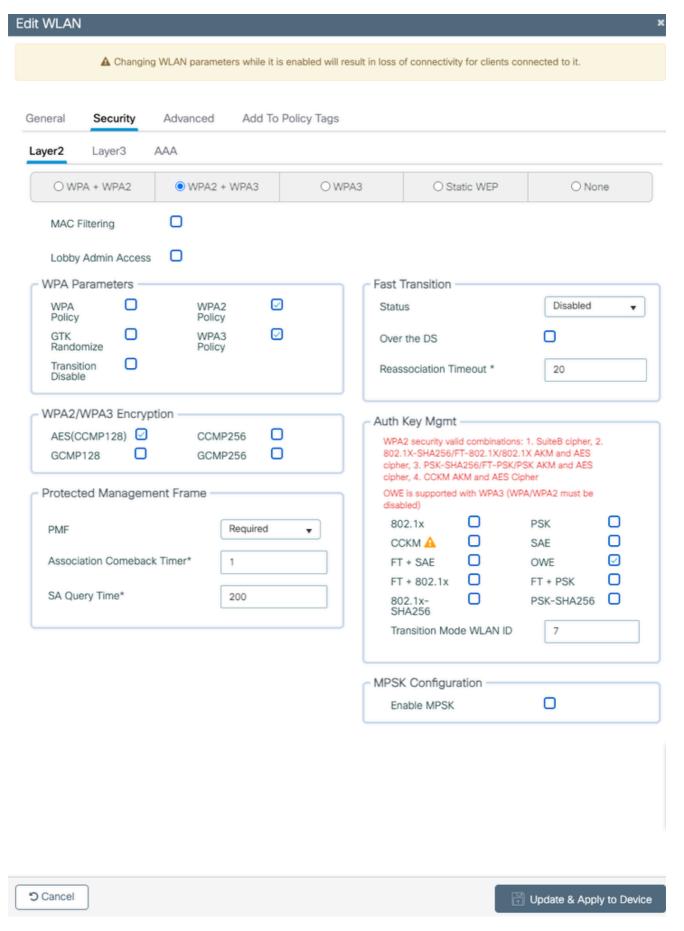


이미지-10: WISE SSID에서 다른 인증 방법을 활성화하는 동안 오류 메시지를 받습니다.



이미지-11: AKM을 활성화하는 동안 오류 메시지 표시

 Cisco IOS® XE 17.9.6 IOS 버전에서는 "WPA2+WPA3"을 선택하면 AKM에서 "OWE" 옵션을 볼 수 있지만 이 조합에서는 OWE를 사용할 수 없다는 오류 메시지가 표시됩니다.



이미지-12: WPA2+WPA3을 선택할 때 오류 메시지 표시

• Cisco IOS® XE 17.12.4 버전에서는 "WPA2+WPA3"을 선택하면 AKM에서 "OWE" 옵션을 사

용할 수 없습니다.

Edit WLAN		×										
▲ Changing WLAN parameters while it is enabled will	result in loss of connectivity for clients cor	nnected to it.										
General Security Advanced Add To Policy Tags												
Layer2 Layer3 AAA												
○ WPA + WPA2 ● WPA2 + WPA3 ○ V	VPA3 O Static WEP	O None										
MAC Filtering												
Lobby Admin Access												
WPA Parameters	Fast Transition											
WPA Policy ☐ WPA2 Policy ☑	Status	Enabled 🔻										
GTK WPA3 Policy												
Randomize Transition Disable	Over the DS											
Disable	Reassociation Timeout *	20										
WPA2/WPA3 Encryption —	ր և											
AES(CCMP128) ☑ CCMP256 ☐	Auth Key Mgmt											
GCMP128 GCMP256 C	WPA2 security valid combinations: 1. SuiteB cipher, 2.											
Protected Management Frame	802.1X-SHA256/FT-802.1X/802.1X AKM and AES cipher, 3. PSK-SHA256/FT-PSK/PSK AKM and AES											
Protected Management Frame	cipher, 4. CCKM AKM and AES Cipher WPA3 security valid combinations: 1. SuiteB cipher, 2.											
PMF Required ▼	802.1X-SHA256/FT-802.1X AKM and AES cipher, 3. SAE/FT-SAE/OWE AKM and AES cipher.											
Association Comeback Timer* 1		PSK 🗆										
Association comedack filler	ССКМ 🛕 🔲	SAE 🗆										
SA Query Time* 200	FT + SAE	FT + 802.1X										
		802.1X- SHA256										
	PSK-SHA256											
	MPSK Configuration											
	Enable MPSK	0										
Cancel Update & Apply to Device												

문제 해결

- 1. WLAN, OPEN SSID 및 OWE Transition SSID 모두에서 컨피그레이션을 확인하려면 전환 WLAN ID가 매핑되어야 합니다.
- 2. Broadcasting 옵션은 WISE 전환 SSID에서 비활성화해야 하며 OPEN SSID에서만 활성화해야 합니다.
- 3. 이 문서에 설명된 지원되는 인증/암호화/FT 방법을 확인하십시오.
- 4. WLC 쪽에서 컨피그레이션이 괜찮은 경우, 에서는 필요한 로그와 출력을 수집하여 문제를 좁혀 주십시오.

RA 추적 및 EPC(임베디드 패킷 캡처)

WLC GUI에 로그인 -> 문제 해결 -> Radioactive Trace(방사능 추적) -> Add client wifi MAC address(클라이언트 wifi MAC 주소 추가) -> Click that clients(해당 클라이언트) 확인란 -> Start(시작)

WLC GUI에 로그인 -> 문제 해결 -> 패킷 캡처 -> 새 파일 이름 추가 -> 업링크 인터페이스 및 WMI VLAN/Interface -> Start(시작)를 선택합니다.

클라이언트 컴퓨터에서: 가능하면 wireshark 애플리케이션을 설치하고 WiFi 인터페이스를 선택하여 패킷 캡처를 수집할 수 있습니다.

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

항공 모함

MAC 랩톱을 사용하거나 AP 중 하나를 스니퍼 모드로 구성하여 수집할 수 있습니다. 이 링크를 참조하십시오.

MAC 노트북 컴퓨터에서:

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

스니퍼 AP에서:

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

한 랩톱(wireshark 서버)을 스위치 포트에 연결하고 wireshark 애플리케이션이 설치되어 있어야 하며 이 wireshark 서버는 WLC WMI 인터페이스에 연결할 수 있어야 합니다. WLC와 wireshark 서버사이에 프로토콜이 있는 경우 방화벽에서 "5555 또는 5000 또는 5556"을 허용해야 합니다.

wireshark가 설치된 PC에 "gscaler"가 설치되어 있는지 확인하고, "꺼주십시오", Windows Defender와 같은 방화벽이나 그 안에 있는 것이 있으면 비활성화하고 PCAP를 수집해 보십시오.

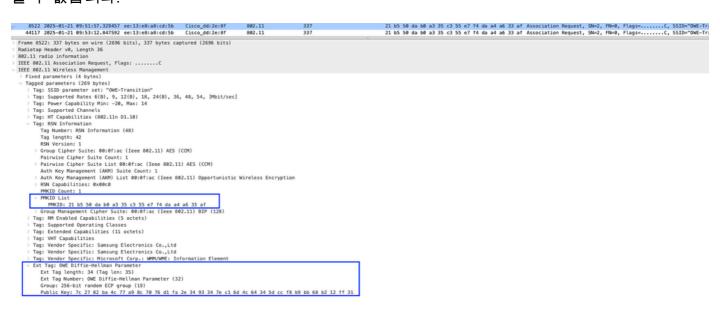
로밍

클라이언트가 한 AP에서 다른 AP로 로밍할 때 다음 단계를 수행해야 합니다.

- 다시 연결/연결을 전송해야 함 클라이언트 요청에 따라 다릅니다.
- 연결 요청에서 DH(Diffie-Helman) 세부 정보를 전송해야 합니다.
- 클라이언트는 이 PMK가 클라이언트와 AP 모두에서 생성됨을 기반으로 AP로부터 연결 응답에서 DH 세부사항을 가져올 수 있습니다.
- AP와 클라이언트 간에 4-Way 핸드셰이크가 발생할 수 있습니다.
- OWE에서는 FT를 활성화할 수 없으므로 802.11r을 사용할 수 없습니다.
- 클라이언트가 로밍할 때마다 DH 교환 후 4방향 핸드셰이크를 해야 합니다.
- 자체 PMKID를 사용하는 클라이언트와 AP는 각 AP 및 클라이언트마다 고유합니다.
- 클라이언트가 동일한 AP에 연결하는 경우 동일한 PMKID를 사용할 수 없습니다. 어떤 시나리 오에서는 클라이언트가 AP보다 삭제되어 새 PMKID를 생성할 수 있지만 클라이언트는 4방향 핸드셰이크에 동일한 PMKID를 사용합니다.

예:

클라이언트가 동일한 AP에 연결된 경우 Association-Request 및 Association-Response 모두에서 동일한 PMKID를 볼 수 있습니다. 연결 응답에서 동일한 PMKID를 사용하는 경우 DH 세부사항을 볼 수 없습니다.

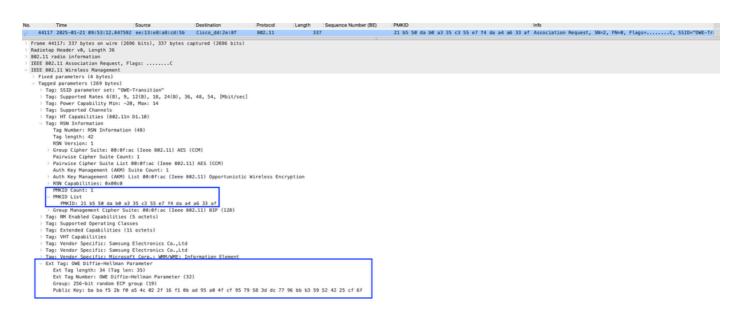


이미지-14: 동일한 PMKID 사용



이미지-15: 동일한 PMKID와의 연결 응답

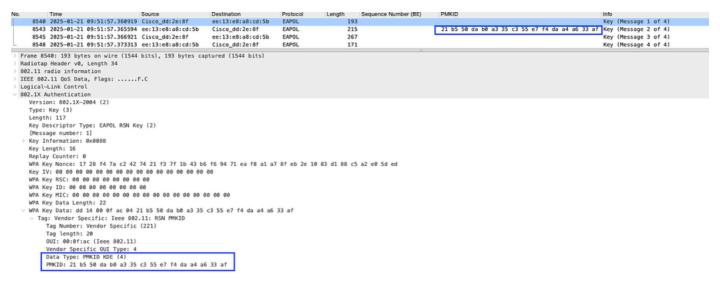
테스트를 위해 WLC에서 이 클라이언트를 수동으로 삭제하고 동일한 AP에 다시 연결했습니다. 이때 클라이언트는 동일한 PMKID를 전송하지만 AP는 연결 응답으로 DH 세부 정보를 전송합니다.



이미지-16: 삭제 후 클라이언트가 DH 세부사항이 포함된 동일한 PMKID를 전송했습니다.

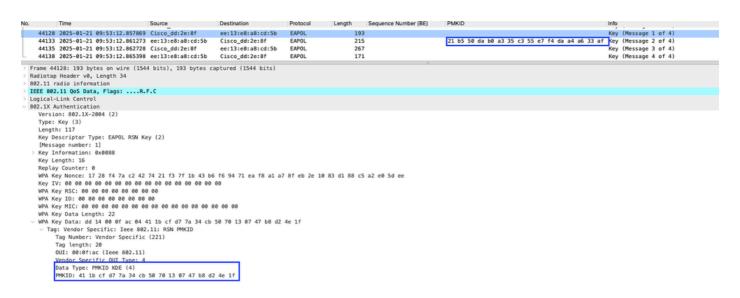
이미지-17: AP는 DH 값을 사용하여 새 PMKID를 생성합니다.

이 예에서는 다음을 수행합니다. AP와 클라이언트 모두 4-Way 핸드셰이크를 수행하는 동안 동일한 PMKID를 사용하며 "M1 및 M2" 메시지를 체크인합니다.



이미지- 18: 동일한 PMKID를 사용하는 AP 및 클라이언트

이 예에서는 다음을 수행합니다. 동일한 PMKID를 사용하지만 클라이언트가 삭제된 후 생성된 다른 PMKID를 사용하는 AP를 사용하는 클라이언트는 "M1 및 M2" 메시지를 확인합니다.



이미지-19: 다른 PMKID를 사용하는 AP 및 클라이언트

내부 RA 추적에서:

이 예에서는 다음을 수행합니다. 클라이언트가 연결 요청에서 DH 매개변수를 보냈고 AP가 PMK를 생성한 것보다 처리했습니다.

```
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 \\ 2025/01/21 \ 15:18:50.157841380 \ \{wncd_x_R0-0\}\{1\}: \ [dot11-frame] \ [21675]: \ (debug): \ MAC: \ ee13.e8a8.cd5b \ OW \\ 2025/01/21 \ 15:18:50.157841380 \ \{wncd_x_R0-0\}\{1\}: \ [dot11-frame] \ [21675]: \ (debug): \ MAC: \ ee13.e8a8.cd5b \ OW \\ 2025/01/21 \ 15:18:50.157841380 \ \{wncd_x_R0-0\}\{1\}: \ [dot11-frame] \ [21675]: \ (debug): \ MAC: \ ee13.e8a8.cd5b \ OW \\ 2025/01/21 \ 15:18:50.157841380 \ \{wncd_x_R0-0\}\{1\}: \ [dot11-frame] \ [21675]: \ (debug): \ MAC: \ ee13.e8a8.cd5b \ OW \\ 2025/01/21 \ 15:18:50.157841380 \ \{wncd_x_R0-0\}\{1\}: \ [dot11-frame] \ [21675]: \ (debug): \ MAC: \ ee13.e8a8.cd5b \ OW \\ 2025/01/21 \ 15:18:50.157841380 \ \{wncd_x_R0-0\}\{1\}: \ [dot11-frame] \ [21675]: \ (debug): \ MAC: \ ee13.e8a8.cd5b \ OW \\ 2025/01/21 \ 15:18:50.157841380 \ \{wncd_x_R0-0\}\{1\}: \ [dot11-frame] \ [
```

그 후 동일한 클라이언트가 동일한 AP에 연결되었지만 AP에서 새 PMKID를 생성하지 않았습니다.

```
 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 \\ 2025/01/21 \ 15:21:57.391906329 \ \{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 \\ 2025/01/21 \ 15:21:57.391906329 \ \{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 \\ 2025/01/21 \ 15:21:57.391906329 \ \{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 \\ 2025/01/21 \ 15:21:57.391906329 \ \{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 \\ 2025/01/21 \ 15:21:57.391906329 \ \{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] \ [dot1
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.