9800 Wireless Controller에서 비인가 AP/클라이언트 식별 및 찾기

목차

소개

이 문서에서는 9800 무선 컨트롤러를 사용하여 비인가 액세스 포인트 또는 비인가 클라이언트를 탐지하고 찾는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 사항.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Wireless 9800-L Controller IOS® XE 17.12.1
- Cisco Catalyst 9130AXI Series Access Point.

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.

배경 정보

Cisco 비인가 액세스 포인트는 네트워크 관리자가 모르거나 승인하지 않고 네트워크에 설치된 무단

무선 액세스 포인트를 의미합니다. 이러한 비인가 액세스 포인트는 네트워크에 보안 위험을 초래할 수 있으며, 공격자는 이러한 액세스 포인트를 사용하여 무단 액세스를 얻거나, 민감한 정보를 가로채거나, 기타 악의적인 활동을 실행할 수 있습니다. Cisco WIPS(Wireless Intrusion Prevention System)는 비인가 액세스 포인트를 식별하고 관리하도록 설계된 솔루션입니다.

비인가 스테이션 또는 비인가 장치라고도 하는 Cisco 비인가 클라이언트는 비인가 액세스 포인트에 연결된 비인가 및 악성 가능성이 있는 무선 클라이언트 장치를 의미합니다. 비인가 액세스 포인트와 마찬가지로, 비인가 클라이언트는 공격자가 적절한 권한 부여 없이 네트워크에 연결할 수 있기 때문에 보안 위험이 있습니다. Cisco는 네트워크 보안을 유지하기 위해 비인가 클라이언트의 존재를 탐지하고 완화하는 데 도움이 되는 툴과 솔루션을 제공합니다.

시나리오

시나리오 1: 비인가 액세스 포인트 탐지 및 찾기

다음 단계에서는 9800 무선 컨트롤러를 사용하여 사용자 네트워크에서 관리되지 않는 비인가 클라이언트 또는 액세스 포인트를 탐지하는 방법을 보여줍니다.

1. 무선 컨트롤러를 사용하여 어떤 액세스 포인트가 비인가 디바이스를 감지했는지 확인합니다.

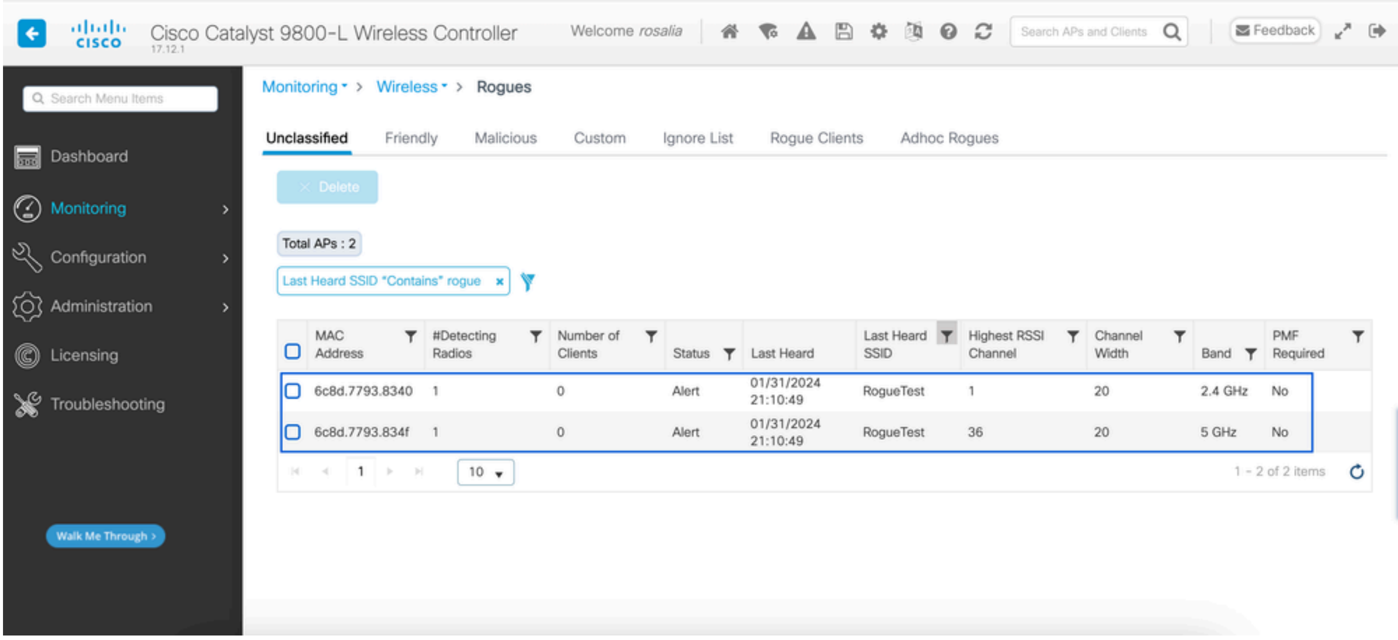
GUI 또는 CLI를 통해 비인가 액세스 포인트 또는 비인가 클라이언트를 볼 수 있습니다. GUI의 경우 Monitoring(모니터링) 탭, Wireless(무선)로 이동한 다음 Rogue(비인가)를 선택하면 필터를 사용하여 비인가 디바이스를 찾을 수 있습니다. CLI의 경우 show wireless wps rogue ap summary(무선 wps 비인가 ap 요약) 명령을 사용하여 탐지된 모든 비인가 디바이스를 볼 수 있습니다. 또는 show wireless wps rogue ap detailed <mac-addr> 명령을 사용하여 특정 비인가 디바이스에 대한 세부 정보를 볼 수 있습니다.

다음은 CLI에서 show wireless wps rogue ap summary 명령을 통해 비인가 디바이스 목록을 확인한 결과입니다.

```
9800L#show wireless wps rogue ap summary
Rogue Location Discovery Protocol : Disabled
Validate rogue APs against AAA : Disabled
Rogue Security Level : Custom
Rogue on wire Auto-Contain : Disabled
Rogue using our SSID Auto-Contain : Disabled
Valid client on rogue AP Auto-Contain : Disabled
Rogue AP timeout : 1200
Rogue init timer : 180

Total Number of Rogue APs : 137
MAC Address Classification State #APs #Clients Last Heard Highest-RSSI-Det-AP RSSI Channel Ch.Width GHz
------------------------------------------------------------------------------------------------------------------
0014.d1d6.a6b7 Unclassified Alert 1 0 01/31/2024 21:28:09 1416.9d7f.a220 -85 1 20 2.4
002a.10d3.4f0f Unclassified Alert 1 0 01/31/2024 21:17:39 1416.9d7f.a220 -54 36 80 5
002a.10d4.b2e0 Unclassified Alert 1 0 01/31/2024 21:17:39 1416.9d7f.a220 -60 36 40 5
0054.afca.4d3b Unclassified Alert 1 0 01/31/2024 21:26:29 1416.9d7f.a220 -86 1 20 2.4
00a6.ca8e.ba80 Unclassified Alert 1 2 01/31/2024 21:27:20 1416.9d7f.a220 -49 11 20 2.4
00a6.ca8e.ba8f Unclassified Alert 1 0 01/31/2024 21:27:50 1416.9d7f.a220 -62 140 80 5
00a6.ca8e.bacf Unclassified Alert 1 0 01/31/2024 21:27:50 1416.9d7f.a220 -53 140 40 5
00f6.630d.e5c0 Unclassified Alert 1 0 01/31/2024 21:28:09 1416.9d7f.a220 -48 1 20 2.4
```

```
00f6.630d.e5cf Unclassified Alert 1 0 01/31/2024 21:27:40 1416.9d7f.a220 -72 128 20 5
04f0.212d.20a8 Unclassified Alert 1 0 01/31/2024 21:27:19 1416.9d7f.a220 -81 1 20 2.4
04f0.2148.7bda Unclassified Alert 1 0 01/31/2024 21:24:19 1416.9d7f.a220 -82 1 20 2.4
0c85.259e.3f30 Unclassified Alert 1 0 01/31/2024 21:21:30 1416.9d7f.a220 -63 11 20 2.4
0c85.259e.3f32 Unclassified Alert 1 0 01/31/2024 21:21:30 1416.9d7f.a220 -63 11 20 2.4
0c85.259e.3f3c Unclassified Alert 1 0 01/31/2024 21:27:30 1416.9d7f.a220 -83 64 20 5
0c85.259e.3f3d Unclassified Alert 1 0 01/31/2024 21:27:30 1416.9d7f.a220 -82 64 20 5
0c85.259e.3f3f Unclassified Alert 1 0 01/31/2024 21:27:30 1416.9d7f.a220 -82 64 20 5
12b3.d617.aac1 Unclassified Alert 1 0 01/31/2024 21:28:09 1416.9d7f.a220 -72 1 20 2.4
204c.9e4b.00ef Unclassified Alert 1 0 01/31/2024 21:27:40 1416.9d7f.a220 -59 116 20 5
22ad.56a5.fa54 Unclassified Alert 1 0 01/31/2024 21:28:09 1416.9d7f.a220 -85 1 20 2.4
4136.5afc.f8d5 Unclassified Alert 1 0 01/31/2024 21:27:30 1416.9d7f.a220 -58 36 20 5
5009.59eb.7b93 Unclassified Alert 1 0 01/31/2024 21:28:09 1416.9d7f.a220 -86 1 20 2.4
683b.78fa.3400 Unclassified Alert 1 0 01/31/2024 21:28:00 1416.9d7f.a220 -69 6 20 2.4
683b.78fa.3401 Unclassified Alert 1 0 01/31/2024 21:28:00 1416.9d7f.a220 -69 6 20 2.4
683b.78fa.3402 Unclassified Alert 1 0 01/31/2024 21:28:00 1416.9d7f.a220 -72 6 20 2.4
683b.78fa.3403 Unclassified Alert 1 0 01/31/2024 21:28:00 1416.9d7f.a220 -72 6 20 2.4
...
```

2. 9800 컨트롤러에 구성된 WLAN 중 하나를 필터링하여 동일한 WLAN을 브로드캐스트하는 비인가 디바이스가 있는지 확인할 수 있습니다. 다음 그림은 C9130이 두 대역 모두에서 이 비인가를 탐지한 결과를 보여줍니다.



Total APs : 2

Last Heard SSID "Contains" rogue

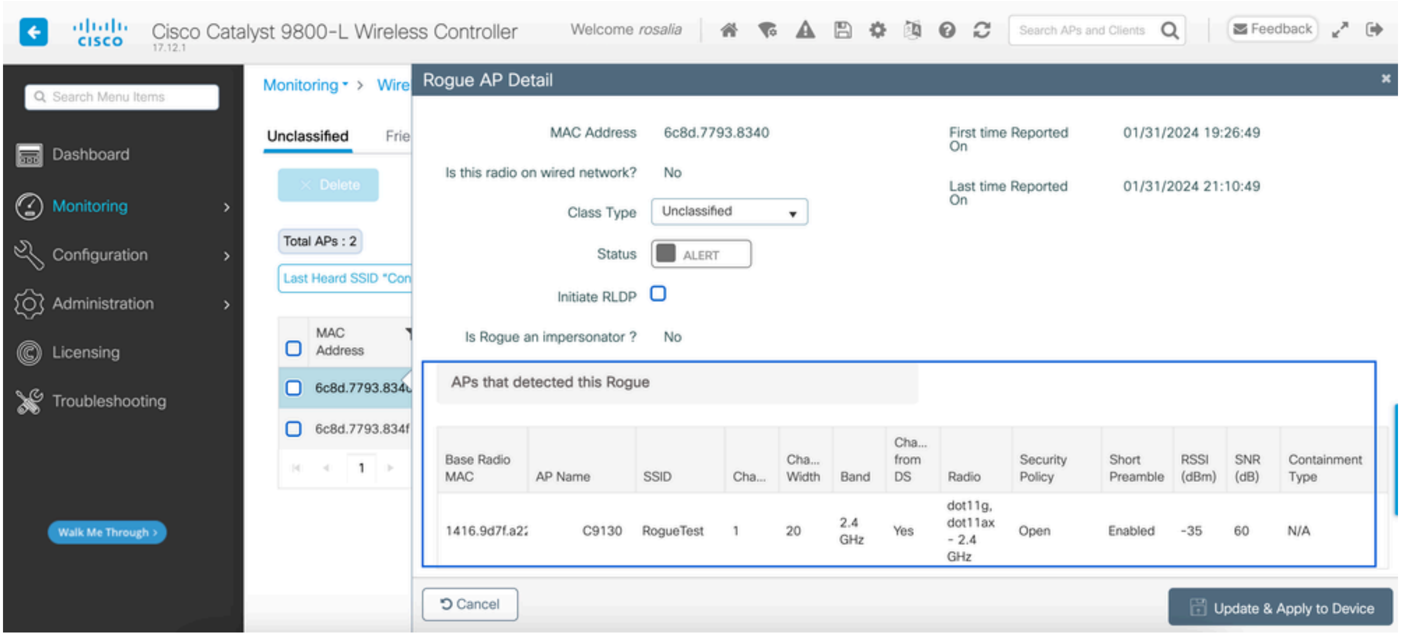
□	MAC Address	#Detecting Radios	Number of Clients	Status	Last Heard	Last Heard SSID	Highest RSSI Channel	Channel Width	Band	PMF Required
□	6c8d.7793.8340	1	0	Alert	01/31/2024 21:10:49	RogueTest	1	20	2.4 GHz	No
□	6c8d.7793.834f	1	0	Alert	01/31/2024 21:10:49	RogueTest	36	20	5 GHz	No

1 - 2 of 2 items

GUI 비인가 목록

3. 비인가 디바이스를 탐지한 액세스 포인트를 나열합니다.

비인가 디바이스를 탐지한 AP를 볼 수 있습니다. 다음 그림에는 이 비인가를 탐지한 AP, 채널, RSSI 값 및 추가 정보가 나와 있습니다.



Rogue AP Detail

MAC Address 6c8d.7793.8340

Is this radio on wired network? No

Class Type Unclassified

Status ALERT

Initiate RLDP □

Is Rogue an impersonator ? No

First time Reported On 01/31/2024 19:26:49

Last time Reported On 01/31/2024 21:10:49

APs that detected this Rogue

Base Radio MAC	AP Name	SSID	Cha...	Cha... Width	Band	Cha... from DS	Radio	Security Policy	Short Preamble	RSSI (dBm)	SNR (dB)	Containment Type
1416.9d7f.a2:	C9130	RogueTest	1	20	2.4 GHz	Yes	dot11g, dot11ax - 2.4 GHz	Open	Enabled	-35	60	N/A

GUI 비인가 AP 세부 정보

CLI에서 show wireless wps rogue ap detailed <mac-addr> 명령을 통해 이 정보를 볼 수 있습니다.

4. 가장 가까운 RSSI 값을 기준으로 비인가 디바이스에 가장 가까운 액세스 포인트를 찾습니다.

비인가 디바이스를 탐지한 액세스 포인트 수를 기준으로 무선 컨트롤러에 표시된 RSSI 값을 기준으로 가장 가까운 AP를 찾아야 합니다. 다음 예에서는 비인가를 탐지한 AP가 하나뿐이지만 RSSI 값이 높으므로 비인가 디바이스가 내 AP와 매우 가깝습니다.

다음 명령은 show wireless wps rogue ap detailed <mac-addr> 명령을 출력하여 AP/WLC에서 이 비인가 디바이스를 수신한 채널 및 RSSI 값을 확인합니다.

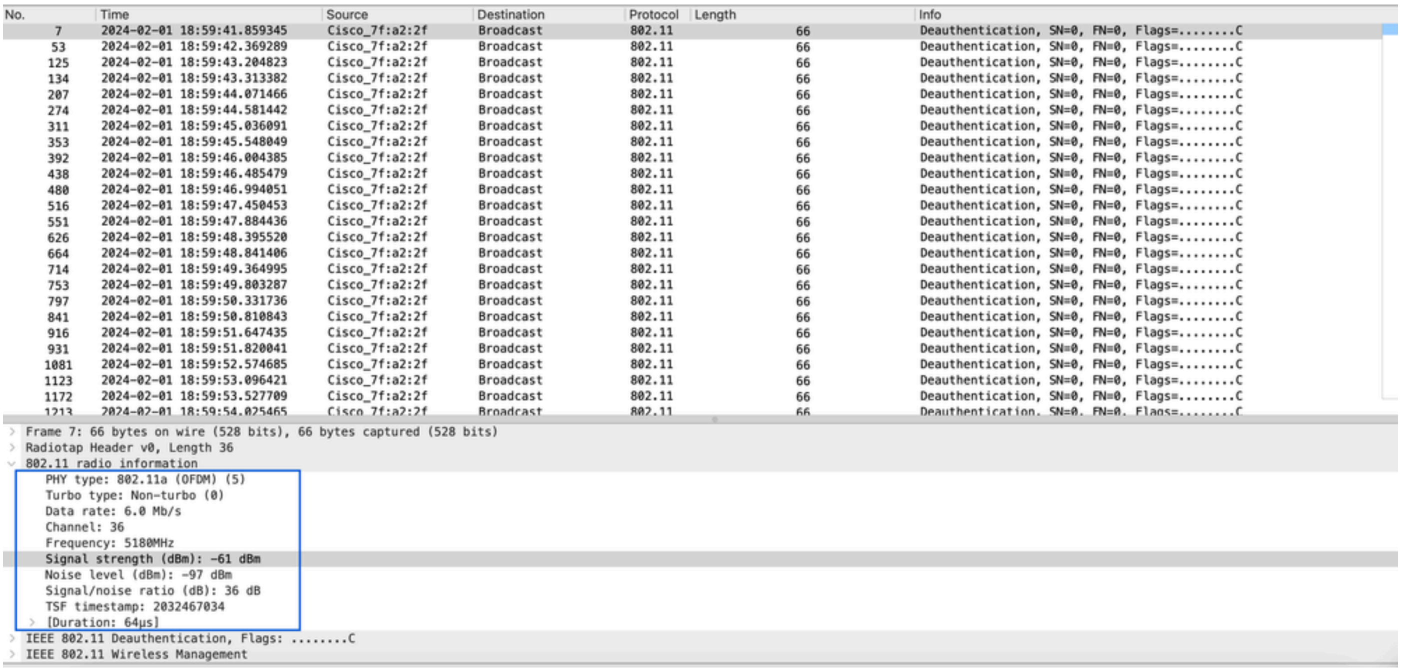
```
9800L#show wireless wps rogue ap detailed 6c8d.7793.834f
Rogue Event history

Timestamp #Times Class/State Event Ctx RC
-------------------------- -------- ----------- -------------------- ------------------------- ----
01/31/2024 22:45:39.814917 1154 Unc/Alert FSM_GOTO Alert 0x0
01/31/2024 22:45:39.814761 1451 Unc/Alert EXPIRE_TIMER_START 1200s 0x0
01/31/2024 22:45:39.814745 1451 Unc/Alert RECV_REPORT 1416.9d7f.a220/34 0x0
01/31/2024 22:45:29.810136 876 Unc/Alert NO_OP_UPDATE 0x0
01/31/2024 19:36:10.354621 1 Unc/Pend HONEYPOT_DETECTED 0x0
01/31/2024 19:29:49.700934 1 Unc/Alert INIT_TIMER_DONE 0xab98004342001907 0x0
01/31/2024 19:26:49.696820 1 Unk/Init INIT_TIMER_START 180s 0x0
01/31/2024 19:26:49.696808 1 Unk/Init CREATE 0x0


Rogue BSSID : 6c8d.7793.834f
Last heard Rogue SSID : RogueTest
802.11w PMF required : No
Is Rogue an impersonator : No
Is Rogue on Wired Network : No
Classification : Unclassified
Manually Contained : No
State : Alert
First Time Rogue was Reported : 01/31/2024 19:26:49
```

```
Last Time Rogue was Reported : 01/31/2024 22:45:39

Number of clients : 0

Reported By
AP Name : C9130
MAC Address : 1416.9d7f.a220
Detecting slot ID : 1
Radio Type : dot11ax - 5 GHz
SSID : RogueTest
Channel : 36 (From DS)
Channel Width : 20 MHz
RSSI : -43 dBm
SNR : 52 dB
ShortPreamble : Disabled
Security Policy : Open
Last reported by this AP : 01/31/2024 22:45:39
```

5. 비인가 위치를 파악하기 위해 같은 채널에서 무선 촬영을 수집합니다.

이제 이 비인가 AP가 브로드캐스트하는 채널이 발견되며, RSSI 값에 따라 9130 액세스 포인트가 -35dBm에서 이 비인가를 수신했습니다. 이는 매우 가까운 것으로 간주되며, 이 비인가가 어느 영역에 있는지 알려줍니다. 다음 단계는 무선 캡처를 수집하는 것입니다.

다음 그림에서는 채널 36의 무선 캡처를 보여줍니다. OTA에서 비인가 AP가 관리 액세스 포인트로 억제 인증 해제 공격을 수행하는 것을 볼 수 있습니다.



No.	Time	Source	Destination	Protocol	Length	Info
7	2024-02-01 18:59:41.859345	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
53	2024-02-01 18:59:42.369289	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
125	2024-02-01 18:59:43.204823	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
134	2024-02-01 18:59:43.313382	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
207	2024-02-01 18:59:44.071466	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
274	2024-02-01 18:59:44.581442	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
311	2024-02-01 18:59:45.036091	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
353	2024-02-01 18:59:45.548049	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
392	2024-02-01 18:59:46.004385	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
438	2024-02-01 18:59:46.485479	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
480	2024-02-01 18:59:46.994051	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
516	2024-02-01 18:59:47.450453	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
551	2024-02-01 18:59:47.884436	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
626	2024-02-01 18:59:48.395520	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
664	2024-02-01 18:59:48.841406	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
714	2024-02-01 18:59:49.364995	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
753	2024-02-01 18:59:49.803287	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
797	2024-02-01 18:59:50.331736	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
841	2024-02-01 18:59:50.810843	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
916	2024-02-01 18:59:51.647435	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
931	2024-02-01 18:59:51.820041	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
1081	2024-02-01 18:59:52.574685	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
1123	2024-02-01 18:59:53.096421	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
1172	2024-02-01 18:59:53.527709	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C
1213	2024-02-01 18:59:54.025465	Cisco_7f:a2:2f	Broadcast	802.11	66	Deauthentication, SN=0, FN=0, Flags=........C

```
> Frame 7: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Radiotap Header v0, Length 36
v 802.11 radio information
    PHY type: 802.11a (OFDM) (5)
    Turbo type: Non-turbo (0)
    Data rate: 6.0 Mb/s
    Channel: 36
    Frequency: 5180MHz
    Signal strength (dBm): -61 dBm
    Noise level (dBm): -97 dBm
    Signal/noise ratio (dB): 36 dB
    TSF timestamp: 2032467034
  > [Duration: 64µs]
> IEEE 802.11 Deauthentication, Flags: ........C
> IEEE 802.11 Wireless Management
```

비인가 AP OTA 캡처

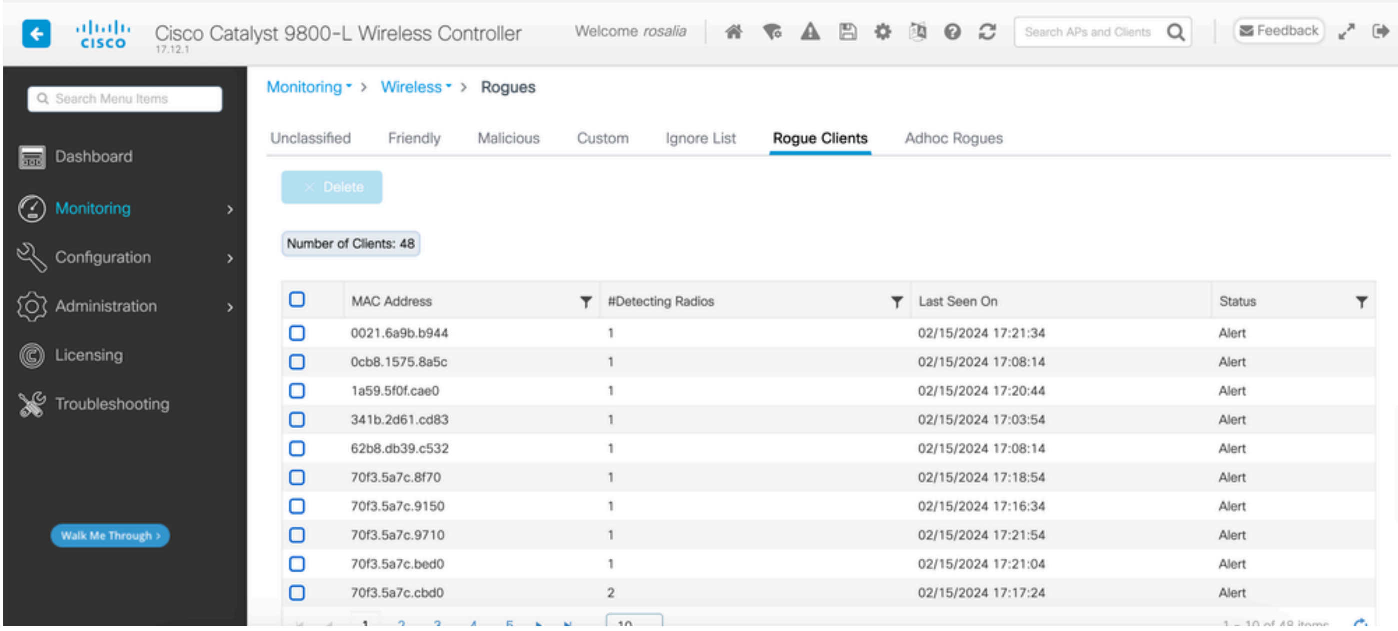
이전 그림의 정보를 사용하여 이 비인가 액세스 포인트가 얼마나 가까이 있는지 파악할 수 있습니다. 적어도 이 비인가 액세스 포인트가 물리적으로 어디에 있는지 파악할 수 있습니다. 비인가 AP 무선 mac 주소를 통해 필터링할 수 있습니다. 비인가 AP 무선 MAC 주소가 현재 활성 상태인지 여부를 확인할 수 있습니다. 비인가 패킷이 무선으로 전송되는지 확인할 수 있습니다.

시나리오 2: 인증 취소 플러드를 전송하는 비인가 클라이언트 탐지 및 찾기

다음 단계에서는 9800 무선 컨트롤러를 사용하여 사용자 네트워크에서 관리하지 않는 비인가 액세스 포인트에 연결된 비인가 클라이언트 또는 인증 취소 공격을 수행하는 비인가 클라이언트를 찾는 방법을 보여 줍니다.

1. 무선 컨트롤러를 사용하여 비인가 클라이언트를 찾습니다.

무선 컨트롤러 GUI에서 Monitoring(모니터링) 탭 Wireless(무선)로 이동한 다음 Rogue Clients(비인가 클라이언트)를 선택합니다. 또는 CLI에서 show wireless wps rogue client summary(무선 wps 비인가 클라이언트 요약 표시) 명령을 사용하여 컨트롤러에서 탐지된 비인가 클라이언트를 나열할 수 있습니다.



Number of Clients: 48

□	MAC Address	#Detecting Radios	Last Seen On	Status
□	0021.6a9b.b944	1	02/15/2024 17:21:34	Alert
□	0cb8.1575.8a5c	1	02/15/2024 17:08:14	Alert
□	1a59.5f0f.cae0	1	02/15/2024 17:20:44	Alert
□	341b.2d61.cd83	1	02/15/2024 17:03:54	Alert
□	62b8.db39.c532	1	02/15/2024 17:08:14	Alert
□	70f3.5a7c.8f70	1	02/15/2024 17:18:54	Alert
□	70f3.5a7c.9150	1	02/15/2024 17:16:34	Alert
□	70f3.5a7c.9710	1	02/15/2024 17:21:54	Alert
□	70f3.5a7c.bed0	1	02/15/2024 17:21:04	Alert
□	70f3.5a7c.cbd0	2	02/15/2024 17:17:24	Alert

비인가 클라이언트 목록 GUI

다음 출력에서는 CLI 결과를 보여줍니다.

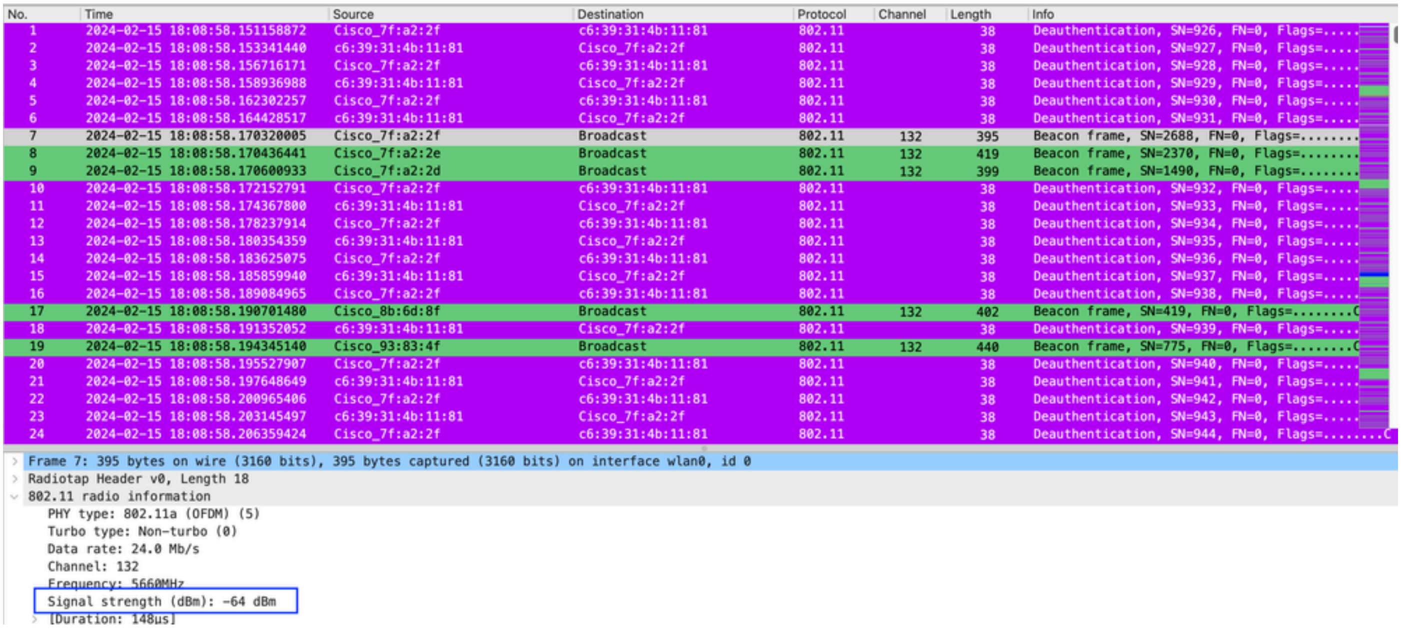
```
9800L#show wireless wps rogue client summary

Validate rogue clients against AAA : Disabled
Validate rogue clients against MSE : Disabled

Number of rogue clients detected : 49

MAC Address State # APs Last Heard
------------------------------------------------------------------------
0021.6a9b.b944 Alert 1 02/15/2024 17:22:44
0cb8.1575.8a5c Alert 1 02/15/2024 17:08:14
1a59.5f0f.cae0 Alert 1 02/15/2024 17:20:44
341b.2d61.cd83 Alert 1 02/15/2024 17:03:54
62b8.db39.c532 Alert 1 02/15/2024 17:08:14
70f3.5a7c.8f70 Alert 1 02/15/2024 17:18:54
70f3.5a7c.9150 Alert 1 02/15/2024 17:23:04
70f3.5a7c.9710 Alert 1 02/15/2024 17:22:34
70f3.5a7c.bed0 Alert 1 02/15/2024 17:22:54
```

```
70f3.5a7c.cbd0 Alert 2 02/15/2024 17:17:24
70f3.5a7c.d030 Alert 1 02/15/2024 17:20:44
70f3.5a7c.d050 Alert 1 02/15/2024 17:20:44
70f3.5a7c.d0b0 Alert 1 02/15/2024 17:16:54
70f3.5a7c.d110 Alert 2 02/15/2024 17:18:24
70f3.5a7c.d210 Alert 1 02/15/2024 17:20:24
70f3.5a7c.d2f0 Alert 2 02/15/2024 17:23:04
70f3.5a7c.f850 Alert 1 02/15/2024 17:19:04
70f3.5a7f.8971 Alert 1 02/15/2024 17:16:44
...
```

2. 다음 출력 예에서는 채널 132의 관리 AP 9130에 의해 탐지된 mac 주소 0021.6a9b.b944의 비인가 클라이언트에 대한 세부 정보를 보여 줍니다. 다음 출력에서는 자세한 정보를 보여 줍니다.

```
9800L#show wireless wps rogue client detailed 0021.6a9b.b944

Rogue Client Event history

Timestamp #Times State Event Ctx RC
-------------------------- -------- ----------- -------------------- ------------------------- ----
02/15/2024 17:22:44.551882 5 Alert FSM_GOTO Alert 0x0
02/15/2024 17:22:44.551864 5 Alert EXPIRE_TIMER_START 1200s 0x0
02/15/2024 17:22:44.551836 5 Alert RECV_REPORT 0x0
02/15/2024 17:15:14.543779 1 Init CREATE 0x0

Rogue BSSID : 6c8d.7793.834f
SSID : Testing-Rogue
Gateway : 6c8d.7793.834f
Rogue Radio Type : dot11ax - 5 GHz
State : Alert
First Time Rogue was Reported : 02/15/2024 17:15:14
Last Time Rogue was Reported : 02/15/2024 17:22:44

Reported by
AP : C9130
MAC Address : 1416.9d7f.a220
Detecting slot ID : 1
RSSI : -83 dBm
SNR : 12 dB
Channel : 132
Last reported by this AP : 02/15/2024 17:22:44
```

3. 동일한 채널에서 OTA(over-the-air) 캡처를 수집한 후 인증되지 않은 플러드가 있음을 확인할 수 있습니다. 여기서 비인가 클라이언트는 관리되는 액세스 포인트 BSSID 중 하나를 사용하여 클라이언트 연결을 끊습니다.



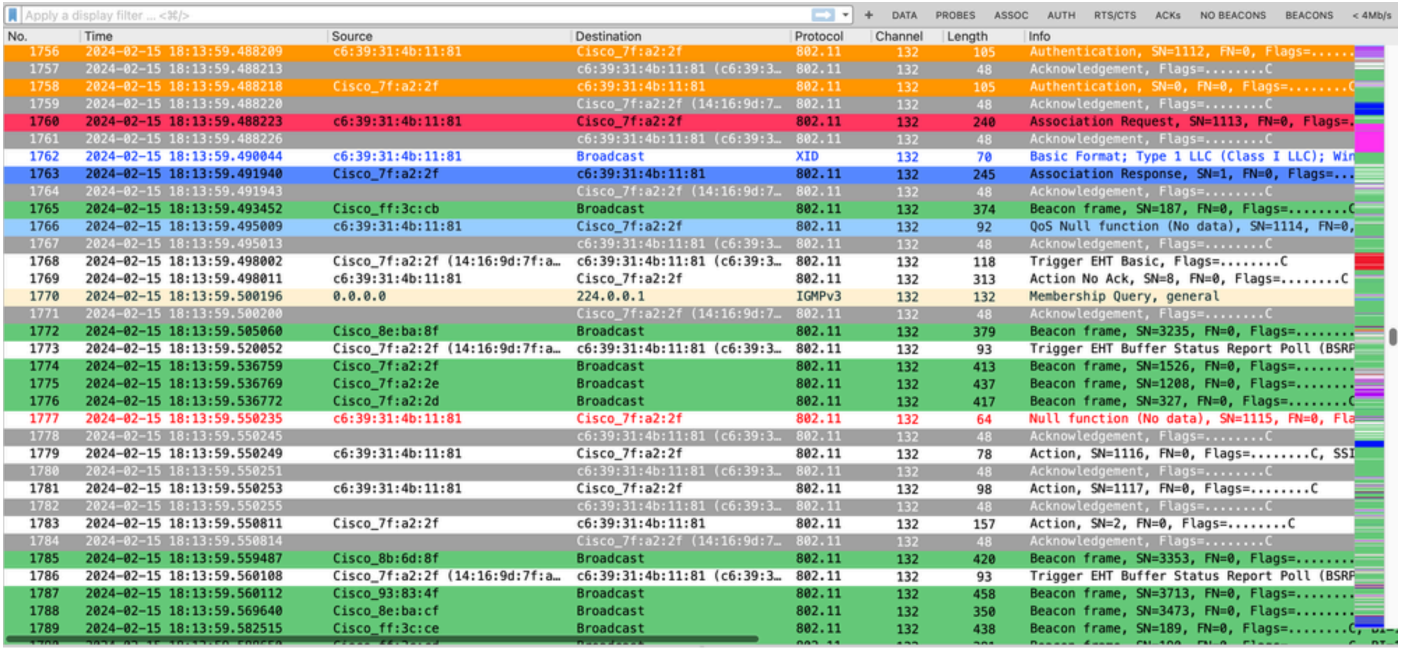
No.	Time	Source	Destination	Protocol	Channel	Length	Info
1	2024-02-15 18:08:58.151158872	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11		38	Deauthentication, SN=926, FN=0, Flags=.....
2	2024-02-15 18:08:58.153341440	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11		38	Deauthentication, SN=927, FN=0, Flags=.....
3	2024-02-15 18:08:58.156716171	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11		38	Deauthentication, SN=928, FN=0, Flags=.....
4	2024-02-15 18:08:58.158936988	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11		38	Deauthentication, SN=929, FN=0, Flags=.....
5	2024-02-15 18:08:58.162302257	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11		38	Deauthentication, SN=930, FN=0, Flags=.....
6	2024-02-15 18:08:58.164428517	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11		38	Deauthentication, SN=931, FN=0, Flags=.....
7	2024-02-15 18:08:58.170320005	Cisco_7f:a2:2f	Broadcast	802.11	132	395	Beacon frame, SN=2688, FN=0, Flags=........
8	2024-02-15 18:08:58.170436441	Cisco_7f:a2:2e	Broadcast	802.11	132	419	Beacon frame, SN=2370, FN=0, Flags=........
9	2024-02-15 18:08:58.170600933	Cisco_7f:a2:2d	Broadcast	802.11	132	399	Beacon frame, SN=1490, FN=0, Flags=........
10	2024-02-15 18:08:58.172152791	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11		38	Deauthentication, SN=932, FN=0, Flags=.....
11	2024-02-15 18:08:58.174367800	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11		38	Deauthentication, SN=933, FN=0, Flags=.....
12	2024-02-15 18:08:58.178237914	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11		38	Deauthentication, SN=934, FN=0, Flags=.....
13	2024-02-15 18:08:58.180354359	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11		38	Deauthentication, SN=935, FN=0, Flags=.....
14	2024-02-15 18:08:58.183625075	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11		38	Deauthentication, SN=936, FN=0, Flags=.....
15	2024-02-15 18:08:58.185859940	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11		38	Deauthentication, SN=937, FN=0, Flags=.....
16	2024-02-15 18:08:58.189084965	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11		38	Deauthentication, SN=938, FN=0, Flags=.....
17	2024-02-15 18:08:58.190701480	Cisco_8b:6d:8f	Broadcast	802.11	132	402	Beacon frame, SN=419, FN=0, Flags=........C
18	2024-02-15 18:08:58.191352052	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11		38	Deauthentication, SN=939, FN=0, Flags=.....
19	2024-02-15 18:08:58.194345140	Cisco_93:83:4f	Broadcast	802.11	132	440	Beacon frame, SN=775, FN=0, Flags=........C
20	2024-02-15 18:08:58.195527907	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11		38	Deauthentication, SN=940, FN=0, Flags=.....
21	2024-02-15 18:08:58.197648649	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11		38	Deauthentication, SN=941, FN=0, Flags=.....
22	2024-02-15 18:08:58.200965406	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11		38	Deauthentication, SN=942, FN=0, Flags=.....
23	2024-02-15 18:08:58.203145497	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11		38	Deauthentication, SN=943, FN=0, Flags=.....
24	2024-02-15 18:08:58.206359424	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11		38	Deauthentication, SN=944, FN=0, Flags=........C

```
> Frame 7: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface wlan0, id 0
> Radiotap Header v0, Length 18
v 802.11 radio information
    PHY type: 802.11a (OFDM) (5)
    Turbo type: Non-turbo (0)
    Data rate: 24.0 Mb/s
    Channel: 132
    Frequency: 5660MHz
    Signal strength (dBm): -64 dBm
  > [Duration: 148µs]
```

OTA 인증 취소

패킷의 RSSI 값이 높습니다. 즉, 비인가 클라이언트가 관리되는 액세스 포인트에 물리적으로 가까이 있습니다.

4. 네트워크에서 비인가 클라이언트를 제거한 후 다음 그림은 깨끗한 네트워크와 정상적인 환경을 무선으로 보여줍니다.



No.	Time	Source	Destination	Protocol	Channel	Length	Info
1756	2024-02-15 18:13:59.488209	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11	132	105	Authentication, SN=1112, FN=0, Flags=......
1757	2024-02-15 18:13:59.488213		c6:39:31:4b:11:81 (c6:39:3…	802.11	132	48	Acknowledgement, Flags=........C
1758	2024-02-15 18:13:59.488218	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11	132	105	Authentication, SN=0, FN=0, Flags=........C
1759	2024-02-15 18:13:59.488220		Cisco_7f:a2:2f (14:16:9d:7…	802.11	132	48	Acknowledgement, Flags=........C
1760	2024-02-15 18:13:59.488223	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11	132	240	Association Request, SN=1113, FN=0, Flags=.
1761	2024-02-15 18:13:59.488226		c6:39:31:4b:11:81 (c6:39:3…	802.11	132	48	Acknowledgement, Flags=........C
1762	2024-02-15 18:13:59.490044	c6:39:31:4b:11:81	Broadcast	XID	132	70	Basic Format; Type 1 LLC (Class I LLC); Win
1763	2024-02-15 18:13:59.491940	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11	132	245	Association Response, SN=1, FN=0, Flags=...
1764	2024-02-15 18:13:59.491943		Cisco_7f:a2:2f (14:16:9d:7…	802.11	132	48	Acknowledgement, Flags=........C
1765	2024-02-15 18:13:59.493452	Cisco_ff:3c:cb	Broadcast	802.11	132	374	Beacon frame, SN=187, FN=0, Flags=........C
1766	2024-02-15 18:13:59.495009	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11	132	92	QoS Null function (No data), SN=1114, FN=0,
1767	2024-02-15 18:13:59.495013		c6:39:31:4b:11:81 (c6:39:3…	802.11	132	48	Acknowledgement, Flags=........C
1768	2024-02-15 18:13:59.498002	Cisco_7f:a2:2f (14:16:9d:7f:a…	c6:39:31:4b:11:81 (c6:39:3…	802.11	132	118	Trigger EHT Basic, Flags=........C
1769	2024-02-15 18:13:59.498011	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11	132	313	Action No Ack, SN=8, FN=0, Flags=........C
1770	2024-02-15 18:13:59.500196	0.0.0.0	224.0.0.1	IGMPv3	132	132	Membership Query, general
1771	2024-02-15 18:13:59.500200		Cisco_7f:a2:2f (14:16:9d:7…	802.11	132	48	Acknowledgement, Flags=........C
1772	2024-02-15 18:13:59.505060	Cisco_8e:ba:8f	Broadcast	802.11	132	379	Beacon frame, SN=3235, FN=0, Flags=........
1773	2024-02-15 18:13:59.520052	Cisco_7f:a2:2f (14:16:9d:7f:a…	c6:39:31:4b:11:81 (c6:39:3…	802.11	132	93	Trigger EHT Buffer Status Report Poll (BSRP
1774	2024-02-15 18:13:59.536759	Cisco_7f:a2:2f	Broadcast	802.11	132	413	Beacon frame, SN=1526, FN=0, Flags=........
1775	2024-02-15 18:13:59.536769	Cisco_7f:a2:2e	Broadcast	802.11	132	437	Beacon frame, SN=1208, FN=0, Flags=........
1776	2024-02-15 18:13:59.536772	Cisco_7f:a2:2d	Broadcast	802.11	132	417	Beacon frame, SN=327, FN=0, Flags=........C
1777	2024-02-15 18:13:59.550235	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11	132	64	Null function (No data), SN=1115, FN=0, Fla
1778	2024-02-15 18:13:59.550245		c6:39:31:4b:11:81 (c6:39:3…	802.11	132	48	Acknowledgement, Flags=........C
1779	2024-02-15 18:13:59.550249	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11	132	78	Action, SN=1116, FN=0, Flags=........C, SSI
1780	2024-02-15 18:13:59.550251		c6:39:31:4b:11:81 (c6:39:3…	802.11	132	48	Acknowledgement, Flags=........C
1781	2024-02-15 18:13:59.550253	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11	132	98	Action, SN=1117, FN=0, Flags=........C
1782	2024-02-15 18:13:59.550255		c6:39:31:4b:11:81 (c6:39:3…	802.11	132	48	Acknowledgement, Flags=........C
1783	2024-02-15 18:13:59.550811	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11	132	157	Action, SN=2, FN=0, Flags=........C
1784	2024-02-15 18:13:59.550814		Cisco_7f:a2:2f (14:16:9d:7…	802.11	132	48	Acknowledgement, Flags=........C
1785	2024-02-15 18:13:59.559487	Cisco_8b:6d:8f	Broadcast	802.11	132	420	Beacon frame, SN=3353, FN=0, Flags=........
1786	2024-02-15 18:13:59.560108	Cisco_7f:a2:2f (14:16:9d:7f:a…	c6:39:31:4b:11:81 (c6:39:3…	802.11	132	93	Trigger EHT Buffer Status Report Poll (BSRP
1787	2024-02-15 18:13:59.560112	Cisco_93:83:4f	Broadcast	802.11	132	458	Beacon frame, SN=3713, FN=0, Flags=........
1788	2024-02-15 18:13:59.569640	Cisco_8e:ba:cf	Broadcast	802.11	132	350	Beacon frame, SN=3473, FN=0, Flags=........
1789	2024-02-15 18:13:59.582515	Cisco_ff:3c:ce	Broadcast	802.11	132	438	Beacon frame, SN=189, FN=0, Flags=........C, BI=

건강한 OTA

관련 정보

- 비인가 디바이스 관리
- 비인가 액세스 포인트 분류
- 802.11 무선 스니핑 분석 및 문제 해결
- Cisco 기술 지원 및 다운로드

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 번역 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.