

Identificazione e individuazione di un access point/client non autorizzato sui controller wireless 9800

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Scenari](#)

[Scenario 1: Rilevamento E Individuazione Di Un Access Point Non Autorizzato](#)

[Scenario 2: Rilevamento e individuazione di un client non autorizzato che invia un flusso di dati di deautenticazione](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come rilevare e individuare un punto di accesso non autorizzato o un client non autorizzato con l'uso del controller wireless 9800.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Nozioni fondamentali di IEEE 802.11.

Componenti usati

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

- Cisco Wireless 9800-L Controller IOS® XE 17.12.1
- Access point Cisco Catalyst serie 9130AXI.

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.

Premesse

Un punto di accesso non autorizzato Cisco fa riferimento a un punto di accesso wireless non autorizzato installato in una rete senza che l'amministratore di rete ne sia a conoscenza o abbia ricevuto l'approvazione. Questi punti di accesso non autorizzati possono rappresentare un rischio per la sicurezza della rete e gli utenti malintenzionati possono utilizzarli per ottenere accessi non autorizzati, intercettare informazioni riservate o avviare altre attività dannose. [Cisco Wireless Intrusion Prevention System \(WIPS\)](#) è una soluzione progettata per identificare e gestire i punti di accesso non autorizzati.

Un client non autorizzato Cisco, noto anche come stazione non autorizzata o dispositivo non autorizzato, si riferisce a un dispositivo client wireless non autorizzato e potenzialmente dannoso connesso a un punto di accesso non autorizzato. Analogamente ai punti di accesso non autorizzati, i client non autorizzati pongono rischi di sicurezza in quanto un utente non autorizzato può connettersi a una rete. Cisco fornisce strumenti e soluzioni per rilevare e mitigare la presenza di client non autorizzati e mantenere la sicurezza della rete.

Scenari

Scenario 1: Rilevamento E Individuazione Di Un Access Point Non Autorizzato

I passaggi successivi mostrano come utilizzare i controller wireless 9800 per rilevare un client non autorizzato o un punto di accesso non gestito dalla rete dell'utente:

1. Utilizzare il controller wireless per individuare il punto di accesso che ha rilevato il dispositivo non autorizzato:

È possibile visualizzare i punti di accesso non autorizzati o i client non autorizzati tramite GUI o CLI; per la GUI, andare alla scheda Monitoraggio, quindi fare clic su Wireless e scegliere Non autorizzato, quindi usare i filtri per trovare il dispositivo non autorizzato e per la CLI, usare il comando `show wireless wps rogue ap summary` per visualizzare tutti i dispositivi non autorizzati rilevati oppure usare il comando `show wireless wps rogue ap detail <mac-addr>` per visualizzare i dettagli di un dispositivo non autorizzato specifico.

Di seguito viene riportato il risultato restituito dalla CLI per visualizzare l'elenco dei dispositivi non autorizzati con il comando `show wireless wps rogue ap summary`:

```
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. È possibile filtrare in base a una delle WLAN configurate sul controller 9800 per verificare se sono presenti dispositivi non autorizzati che trasmettono le stesse WLAN. La figura seguente mostra il risultato del rilevamento del problema da parte del C9130 su entrambe le bande:

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller interface. The main content area is titled "Monitoring > Wireless > Rogues". Below this, there are tabs for "Unclassified", "Friendly", "Malicious", "Custom", "Ignore List", "Rogue Clients", and "Adhoc Rogues". The "Unclassified" tab is selected. A "Delete" button is visible. Below the tabs, there is a "Total APs : 2" indicator and a search filter: "Last Heard SSID 'Contains' rogue". A table of detected rogue clients is displayed with the following columns: MAC Address, #Detecting Radios, Number of Clients, Status, Last Heard, Last Heard SSID, Highest RSSI Channel, Channel Width, Band, and PMF Required. Two entries are shown:

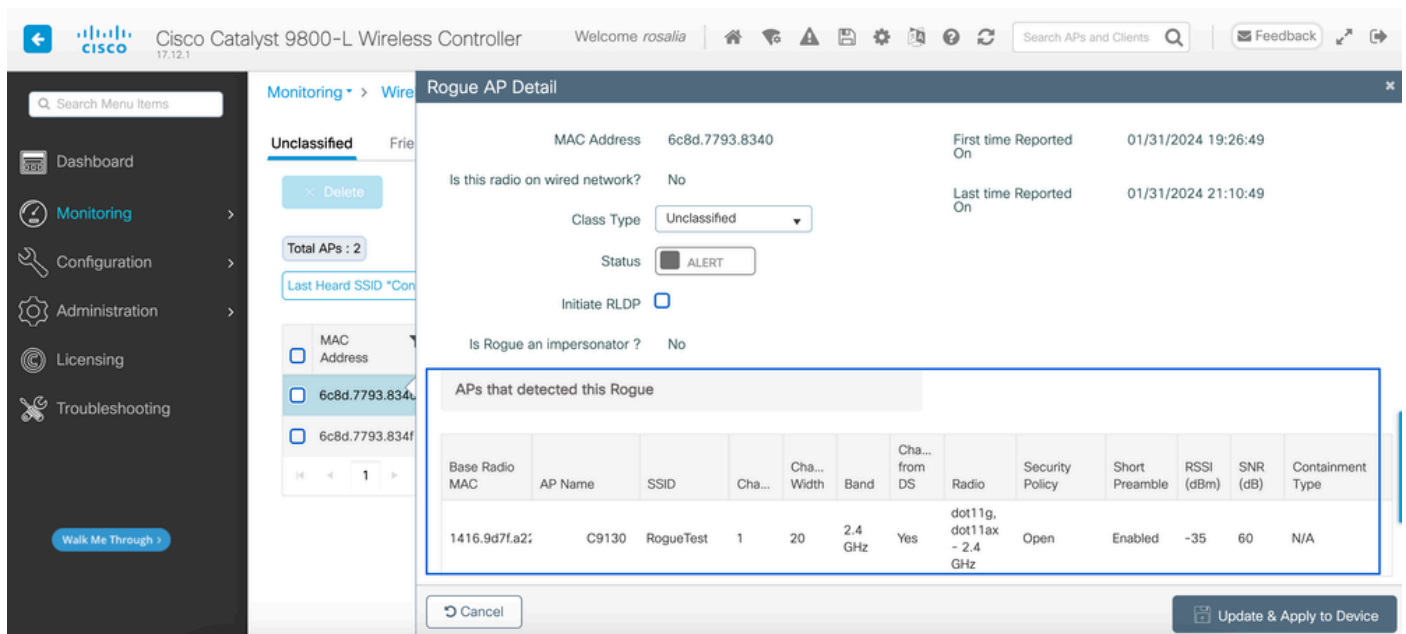
| MAC Address | #Detecting Radios | Number of Clients | Status | Last Heard | Last Heard SSID | Highest RSSI Channel | Channel Width | Band | PMF Required |
|----------------|-------------------|-------------------|--------|---------------------|-----------------|----------------------|---------------|---------|--------------|
| 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 |

At the bottom of the table, there is a pagination control showing "1" of "10" items and "1 - 2 of 2 items".

Elenco interfacce non supportate

3. Elencare i punti di accesso che hanno rilevato il dispositivo non autorizzato.

È possibile visualizzare gli access point che hanno rilevato il dispositivo anomalo; nella figura seguente viene mostrato l'access point che ha rilevato il dispositivo anomalo, il canale, il valore RSSI e ulteriori informazioni:



Dettagli GUI Rogue AP

Dalla CLI è possibile visualizzare queste informazioni con il comando `show wireless wps rogue ap detail <mac-addr>`.

4. Individuare il punto di accesso più vicino al dispositivo non autorizzato in base al valore RSSI più vicino.

In base ai risultati del numero di punti di accesso rilevati dal dispositivo non autorizzato, è necessario cercare l'access point più vicino in base al valore RSSI visualizzato sul controller wireless. Nell'esempio seguente, solo un access point ha rilevato il dispositivo non autorizzato, tuttavia con un valore RSSI elevato, il che significa che il dispositivo non autorizzato è molto vicino all'access point.

Di seguito viene riportato l'output del comando `show wireless wps rogue ap dettagliato <mac-addr>` per visualizzare il canale su cui l'AP/WLC ha sentito questo dispositivo anomalo, più il valore RSSI:

```
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. Raccogliere l'acquisizione over-the-air sullo stesso canale per individuare il rogue.

Ora, il canale dove viene trovato questo access point canaglia, e basandosi sul valore RSSI, il punto di accesso 9130 ha sentito questo canaglia a -35 dBm, che è considerato molto vicino, questo vi dà un'idea su quale area si trova questo canaglia, il passo successivo è raccogliere una cattura over-the-air.

La figura seguente mostra un'acquisizione over-the-air sul canale 36, da OTA, che mostra come l'access point anomalo esegua un attacco di deautenticazione di contenimento al punto di accesso gestito:

| 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
  > 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

```

Acquisizione OTA per punti di accesso non autorizzati

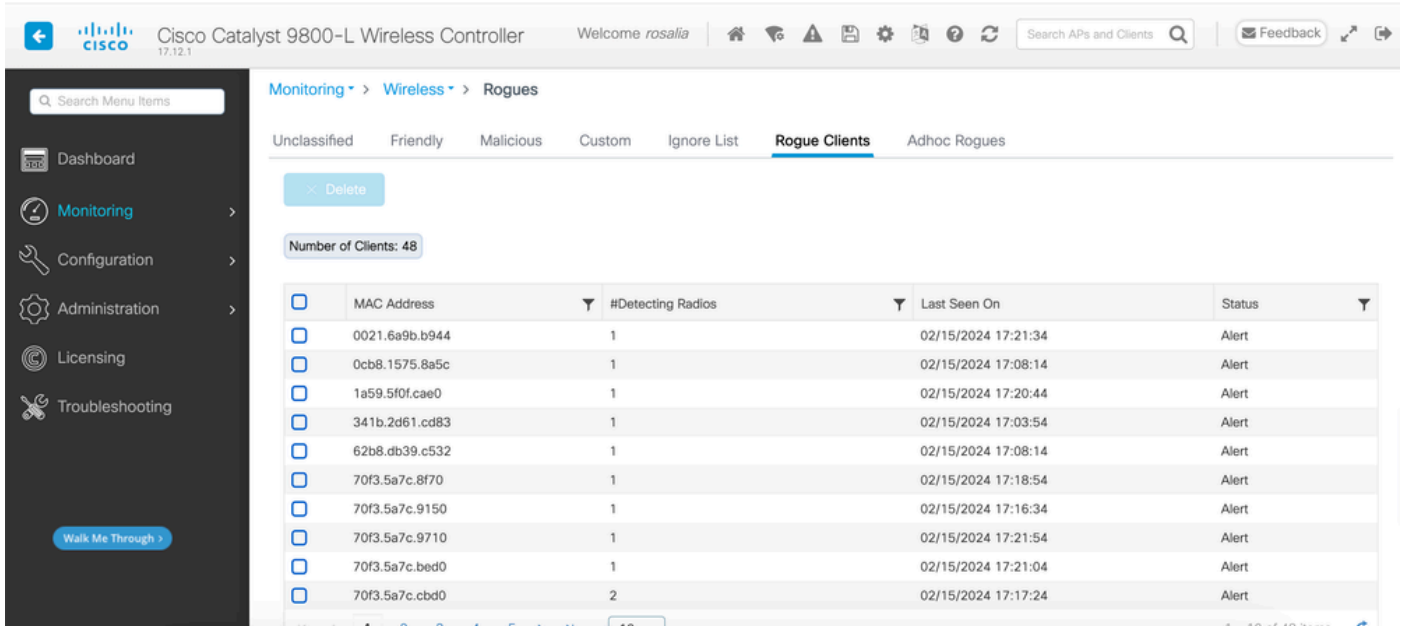
È possibile utilizzare le informazioni riportate nella figura precedente per comprendere quanto sia vicino questo punto di accesso non autorizzato e per lo meno avere un'idea della posizione fisica del punto di accesso non autorizzato. È possibile filtrare i dati tramite l'indirizzo MAC del punto di accesso non autorizzato. Per verificare se il punto di accesso non autorizzato è attivo o meno, controllare se i pacchetti del beacon sono trasmessi via etere.

Scenario 2: Rilevamento e individuazione di un client non autorizzato che invia un flusso di dati di deautenticazione

I passaggi successivi mostrano come utilizzare il controller wireless 9800 per trovare un client non autorizzato connesso a un punto di accesso non autorizzato non gestito dalla rete utente o un client non autorizzato che esegue un attacco di deautenticazione:

1. Utilizzare il controller wireless per trovare il client non autorizzato.

Dall'interfaccia utente del controller wireless, passare alla scheda Monitoraggio, Wireless, quindi scegliere Rogue Client. In alternativa, è possibile usare il comando `show wireless wps rogue client summary` dalla CLI per elencare i client rogue rilevati sul controller:



GUI elenco client non autorizzati

L'output successivo mostra il risultato della CLI:

```
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. Nell'esempio di output successivo vengono mostrati i dettagli relativi al client non autorizzato con indirizzo mac 0021.6a9b.b944, rilevato da un access point gestito 9130 sul canale 132.

Nell'output successivo vengono mostrati ulteriori dettagli:

```
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. Dopo aver raccolto un'acquisizione over-the-air sullo stesso canale, si nota che si è verificato un flood non autenticato, in cui il client non autorizzato utilizza uno dei BSSID del punto di accesso gestito per disconnettere i client:

| 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=..... |
| 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=..... |
| 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=..... |

> Frame 7: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface wlan0, id 0
> Radiotap Header v0, Length 18
 > 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: 148us]

Disautenticazione OTA

Il valore RSSI dei pacchetti è alto, il che significa che il client non autorizzato è fisicamente vicino al punto di accesso gestito.

4. Dopo aver rimosso il client non autorizzato dalla rete, la figura seguente mostra una rete pulita e un ambiente sano via etere:

| 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 | 185 | Authentication, SN=1112, FN=0, Flags=.....C |
| 1757 | 2024-02-15 18:13:59.488213 | | c6:39:31:4b:11:81 (c6:39:31:4b:11:81) | 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 | 185 | Authentication, SN=0, FN=0, Flags=.....C |
| 1759 | 2024-02-15 18:13:59.488220 | | Cisco_7f:a2:2f (14:16:9d:7f:a2:2f) | 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=.....C |
| 1761 | 2024-02-15 18:13:59.488226 | | c6:39:31:4b:11:81 (c6:39:31:4b:11:81) | 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); Wire |
| 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=.....C |
| 1764 | 2024-02-15 18:13:59.491943 | | Cisco_7f:a2:2f (14:16:9d:7f:a2:2f) | 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, Flags=.....C |
| 1767 | 2024-02-15 18:13:59.495013 | | c6:39:31:4b:11:81 (c6:39:31:4b:11:81) | 802.11 | 132 | 48 | Acknowledgement, Flags=.....C |
| 1768 | 2024-02-15 18:13:59.498002 | Cisco_7f:a2:2f (14:16:9d:7f:a2:2f) | c6:39:31:4b:11:81 (c6:39:31:4b:11:81) | 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:7f:a2:2f) | 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=.....C |
| 1773 | 2024-02-15 18:13:59.520052 | Cisco_7f:a2:2f (14:16:9d:7f:a2:2f) | c6:39:31:4b:11:81 (c6:39:31:4b:11:81) | 802.11 | 132 | 93 | Trigger EHT Buffer Status Report Poll (BSRP) |
| 1774 | 2024-02-15 18:13:59.536759 | | Broadcast | 802.11 | 132 | 413 | Beacon frame, SN=1526, FN=0, Flags=.....C |
| 1775 | 2024-02-15 18:13:59.536769 | Cisco_7f:a2:2e | Broadcast | 802.11 | 132 | 437 | Beacon frame, SN=1208, FN=0, Flags=.....C |
| 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, Flags=.....C |
| 1778 | 2024-02-15 18:13:59.550245 | | c6:39:31:4b:11:81 (c6:39:31:4b:11:81) | 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 (c6:39:31:4b:11:81) | 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 (c6:39:31:4b:11:81) | 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:7f:a2:2f) | 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=.....C |
| 1786 | 2024-02-15 18:13:59.560108 | Cisco_7f:a2:2f (14:16:9d:7f:a2:2f) | c6:39:31:4b:11:81 (c6:39:31:4b:11:81) | 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=.....C |
| 1788 | 2024-02-15 18:13:59.569640 | Cisco_8e:ba:cf | Broadcast | 802.11 | 132 | 350 | Beacon frame, SN=3473, FN=0, Flags=.....C |
| 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, P |

OTA integra

Informazioni correlate

- [Gestione di dispositivi non autorizzati](#)
- [Classificazione dei punti di accesso non autorizzati](#)
- [Analisi e risoluzione dei problemi relativi allo sniffing wireless 802.11](#)
- [Supporto tecnico Cisco e download](#)

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).