

Identificación y localización de un cliente/punto de acceso no autorizado en los controladores inalámbricos 9800

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Escenarios](#)

[Situación 1: Detección Y Localización De Un Punto De Acceso No Autorizado](#)

[Situación 2: detección y localización de un cliente no autorizado que envía una inundación de desautenticación](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo detectar y localizar un punto de acceso no autorizado o un cliente no autorizado mediante el uso del controlador inalámbrico 9800.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Fundamentos de IEEE 802.11.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Controlador Cisco Wireless 9800-L IOS® XE 17.12.1
- Punto de acceso Cisco Catalyst serie 9130AXI.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Un punto de acceso no autorizado de Cisco hace referencia a un punto de acceso inalámbrico no autorizado que se ha instalado en una red sin el conocimiento o la aprobación del administrador de la red. Estos puntos de acceso desconocidos pueden suponer riesgos de seguridad para una red, y los atacantes pueden utilizarlos para obtener acceso no autorizado, interceptar información confidencial o iniciar otras actividades malintencionadas. [Cisco Wireless Intrusion Prevention System \(WIPS\)](#) es una solución diseñada para identificar y gestionar puntos de acceso desconocidos.

Un cliente no autorizado de Cisco, también conocido como estación o dispositivo no autorizado, hace referencia a un dispositivo cliente inalámbrico no autorizado y potencialmente malintencionado conectado a un punto de acceso no autorizado. Al igual que los puntos de acceso desconocidos, los clientes desconocidos plantean riesgos de seguridad, ya que un atacante puede conectarse a una red sin la autorización adecuada. Cisco proporciona herramientas y soluciones que ayudan a detectar y mitigar la presencia de clientes desconocidos para mantener la seguridad de la red.

Escenarios

Situación 1: Detección Y Localización De Un Punto De Acceso No Autorizado

Los siguientes pasos le muestran cómo utilizar los controladores inalámbricos 9800 para ayudar a detectar un cliente no autorizado o un punto de acceso que no está administrado por la red del usuario:

1. Utilice el controlador inalámbrico para buscar cuál de los puntos de acceso ha detectado el dispositivo no fiable:

Puede ver los puntos de acceso desconocidos o los clientes desconocidos a través de la GUI o la CLI; para la GUI, vaya a la ficha Supervisión, luego a Inalámbrico y elija Desconocido, luego puede utilizar los filtros para encontrar su dispositivo desprotegido y para la CLI, puede utilizar el comando `show wireless wps rogue ap summary` para ver todos los dispositivos desconocidos detectados, o puede utilizar el comando `show wireless wps rogue ap detailed <mac-addr>` para ver los detalles de un dispositivo desprotegido específico.

Este es el resultado de la CLI para ver la lista de dispositivos no autorizados mediante el 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. Puede filtrar una de las WLAN configuradas en su controlador 9800 para ver si tiene algún dispositivo no autorizado que difunda las mismas WLAN. La siguiente figura muestra el resultado donde mi C9130 detectó este dispositivo no autorizado en ambas bandas:

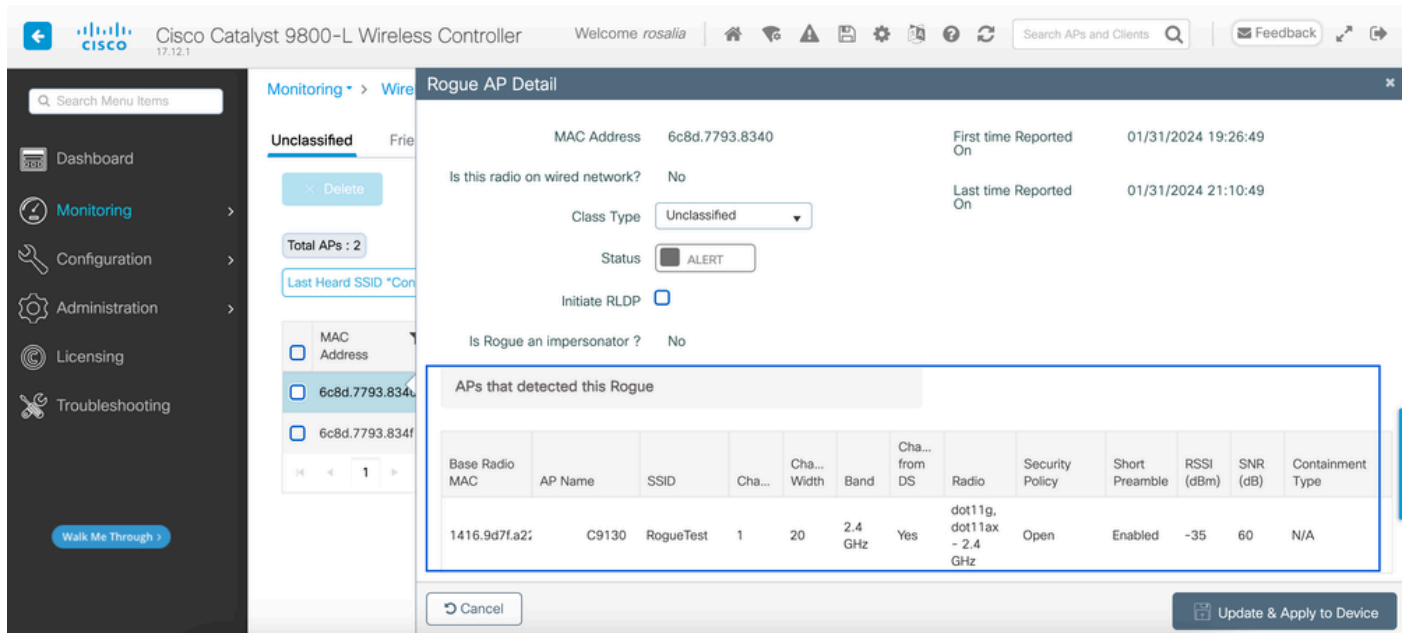
The screenshot shows the Cisco Catalyst 9800-L Wireless Controller interface. The main content area is titled "Monitoring > Wireless > Rogues". Below this, there are tabs for "Unclassified", "Friendly", "Malicious", "Custom", "Ignore List", "Rogue Clients", and "Adhoc Rogues". The "Unclassified" tab is selected. A "Delete" button is visible. Below the button, it says "Total APs : 2". A search filter is applied: "Last Heard SSID 'Contains' rogue". A table displays the results:

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

Lista de acceso no deseado GUI

3. Enumere los puntos de acceso que detectaron el dispositivo no autorizado.

Puede ver los AP que detectaron el dispositivo no autorizado; la siguiente figura muestra el AP que detectó este no fiable, canal, valor RSSI y más información:



Detalles del punto de acceso desconocido GUI

Desde la CLI, puede ver esta información mediante el comando `show wireless wps rogue ap detailed <mac-addr>`.

4. Busque el punto de acceso más cercano al dispositivo no autorizado en función del valor RSSI más cercano.

En función de los resultados de la cantidad de puntos de acceso detectados por el dispositivo no autorizado, debe buscar el AP más cercano en función del valor RSSI que se muestra en el controlador inalámbrico; en el siguiente ejemplo, solo un AP detectó al no autorizado, aunque con un valor RSSI alto, lo que significa que el dispositivo no autorizado está muy cerca de mi AP.

La siguiente es la salida del comando `show wireless wps rogue ap detailed <mac-addr>` para ver el canal en el que el AP/WLC escuchó este dispositivo no autorizado, más el valor 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. Recopile la captura por el aire en el mismo canal para localizar al delincuente.

Ahora el canal donde se encuentra este punto de acceso no autorizado transmite, y en función del valor RSSI, el punto de acceso 9130 escuchó este punto no autorizado a -35dBm, que se considera muy cercano, esto le da una idea de en qué área se encuentra este punto no autorizado, el siguiente paso es recopilar una captura por aire.

En la siguiente figura se muestra una captura por aire en el canal 36, desde la OTA, puede ver que el AP no autorizado realiza un ataque de desautenticación de contención al punto de acceso administrado:

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

```

Captura de OTA de AP dudosa

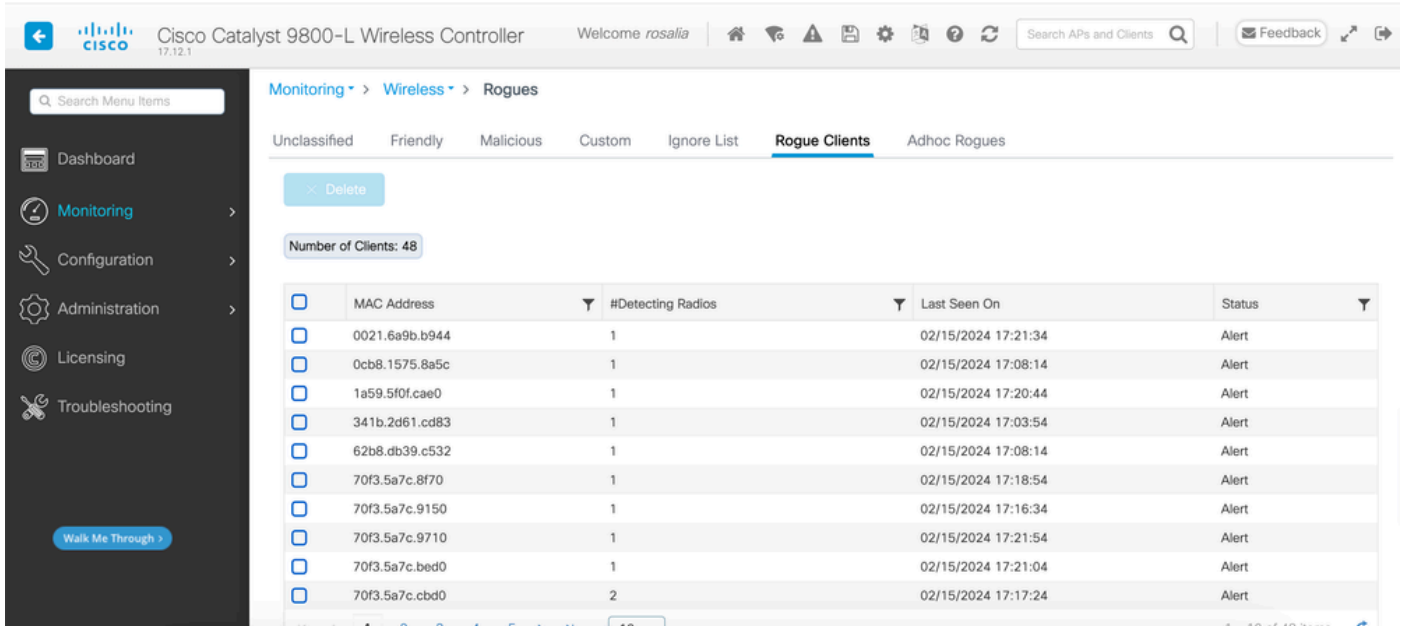
Puede utilizar la información de la figura anterior para comprender lo cerca que está este punto de acceso no autorizado y, al menos, puede hacerse una idea de dónde se encuentra físicamente. Puede filtrar a través de la dirección MAC de radio del punto de acceso no autorizado; podrá ver si el punto de acceso no autorizado está actualmente activo o no si comprueba si tiene paquetes de baliza por el aire.

Situación 2: detección y localización de un cliente no autorizado que envía una inundación de desautenticación

Los siguientes pasos le muestran cómo utilizar el controlador inalámbrico 9800 para encontrar un cliente no autorizado conectado a un punto de acceso no autorizado que no está gestionado por la red de usuarios o un cliente no autorizado que realiza un ataque de desautenticación:

1. Utilice el controlador inalámbrico para encontrar el cliente no autorizado.

Desde el controlador inalámbrico GUI, navegue hasta la ficha Monitoring, Wireless, y luego elija Rogue Clients, o puede utilizar el comando show wireless wps rogue client summary de la CLI para enumerar los clientes desconocidos detectados en el controlador:



GUI de lista de clientes desconocidos

El siguiente resultado muestra el resultado de 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. El siguiente ejemplo de salida muestra los detalles sobre el cliente no autorizado con dirección mac 0021.6a9b.b944, que fue detectado por un AP 9130 administrado en el canal 132, el

siguiente resultado muestra más detalles:

```
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. Después de recopilar una captura por el aire en el mismo canal, puede ver que tiene una inundación no autenticada, donde el cliente no autorizado utiliza uno de los BSSID del punto de acceso administrado para desconectar a los clientes:

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	446	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]

OTA de desautenticación

El valor RSSI para los paquetes es alto, lo que significa que el cliente no autorizado está físicamente cerca del punto de acceso administrado.

4. Después de eliminar el cliente no autorizado de la red, la siguiente figura muestra una red limpia y un entorno saludable en el aire:

The screenshot displays a network protocol analyzer interface with a table of captured packets. The table has columns for No., Time, Source, Destination, Protocol, Channel, Length, and Info. The packets are color-coded by protocol type. The 'Info' column provides details for each packet, such as 'Authentication, SN=1112, FN=0, Flags=.....C', 'Association Request, SN=1113, FN=0, Flags=.....C', 'Basic Format; Type 1 LLC (Class I LLC); Win...', 'Association Response, SN=1, FN=0, Flags=.....C', 'Beacon frame, SN=187, FN=0, Flags=.....C', 'QoS Null function (No data), SN=1114, FN=0, Flags=.....C', 'Trigger EHT Basic, Flags=.....C', 'Action No Ack, SN=8, FN=0, Flags=.....C', 'Membership Query, general', 'Beacon frame, SN=3235, FN=0, Flags=.....C', 'Trigger EHT Buffer Status Report Poll (BSRP)', 'Beacon frame, SN=1526, FN=0, Flags=.....C', 'Beacon frame, SN=1208, FN=0, Flags=.....C', 'Beacon frame, SN=327, FN=0, Flags=.....C', 'Null function (No data), SN=1115, FN=0, Flags=.....C', 'Action, SN=1116, FN=0, Flags=.....C, SSI', 'Action, SN=2, FN=0, Flags=.....C', 'Beacon frame, SN=3353, FN=0, Flags=.....C', 'Trigger EHT Buffer Status Report Poll (BSRP)', 'Beacon frame, SN=3713, FN=0, Flags=.....C', 'Beacon frame, SN=3473, FN=0, Flags=.....C', and 'Beacon frame, SN=189, FN=0, Flags=.....C'. The interface also shows a search filter at the top and various tabs like DATA, PROBES, ASSOC, AUTH, RTS/CTS, ACKS, NO BEACONS, and BEACONS.

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); 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=.....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	Cisco_7f:a2:2f	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

OTA saludable

Información Relacionada

- [Administración de dispositivos no fiables](#)
- [Clasificación de puntos de acceso no fiables](#)
- [Análisis y solución de problemas del analizador de protocolos inalámbrico 802.11](#)
- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).