

# Identificar e localizar um AP/cliente invasor em controladores sem fio 9800

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Cenários](#)

[Cenário 1: Detecção E Localização De Um Ponto De Acesso Invasor](#)

[Cenário 2: detectar e localizar um cliente invasor que envia uma inundação de desautenticação](#)

[Informações Relacionadas](#)

---

## Introdução

Este documento descreve como detectar e localizar um ponto de acesso não autorizado ou um cliente não autorizado com o uso do controlador sem fio 9800.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Fundamentos do IEEE 802.11.

### Componentes Utilizados

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

- Controlador Cisco Wireless 9800-L IOS® XE 17.12.1
- Ponto de acesso Cisco Catalyst 9130AXI Series.

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

## Informações de Apoio

Um ponto de acesso invasor da Cisco se refere a um ponto de acesso sem fio não autorizado que foi instalado em uma rede sem o conhecimento ou a aprovação do administrador da rede. Esses pontos de acesso invasores podem apresentar riscos de segurança para uma rede, e os invasores podem usá-los para obter acesso não autorizado, interceptar informações confidenciais ou iniciar outras atividades mal-intencionadas. [O Cisco Wireless Intrusion Prevention System \(WIPS\)](#) é uma solução projetada para identificar e gerenciar pontos de acesso não autorizados.

Um cliente invasor da Cisco, também conhecido como estação ou dispositivo invasor, refere-se a um dispositivo cliente sem fio não autorizado e potencialmente mal-intencionado conectado a um ponto de acesso invasor. Semelhante aos pontos de acesso invasores, os clientes invasores apresentam riscos de segurança porque um invasor pode se conectar a uma rede sem a autorização adequada. A Cisco fornece ferramentas e soluções para ajudar a detectar e mitigar a presença de clientes invasores para manter a segurança da rede.

## Cenários

### Cenário 1: Detecção E Localização De Um Ponto De Acesso Invasor

As próximas etapas mostram como usar os controladores sem fio 9800 para ajudar a detectar um cliente invasor ou um ponto de acesso que não é gerenciado pela rede do usuário:

1. Use o controlador sem fio para descobrir qual dos seus pontos de acesso detectou o dispositivo invasor:

Você pode exibir os pontos de acesso invasores ou os clientes invasores via GUI ou CLI; para a GUI, vá para a guia Monitoramento, Wireless e escolha Rogue; em seguida, você pode usar os filtros para localizar o dispositivo invasor e, para a CLI, você pode usar o comando `show wireless wps rogue ap summary` para exibir todos os dispositivos invasores detectados ou você pode usar o comando `show wireless wps rogue ap detailed <mac-addr>` para exibir os detalhes de um dispositivo invasor específico.

Este é o resultado do CLI para exibir a lista de dispositivos invasores por meio do 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. Você pode filtrar em uma das WLANs configuradas no seu controlador 9800 para ver se há dispositivos invasores que transmitam as mesmas WLANs. A próxima figura mostra o resultado em que o meu C9130 detectou esse invasor em ambas as bandas:

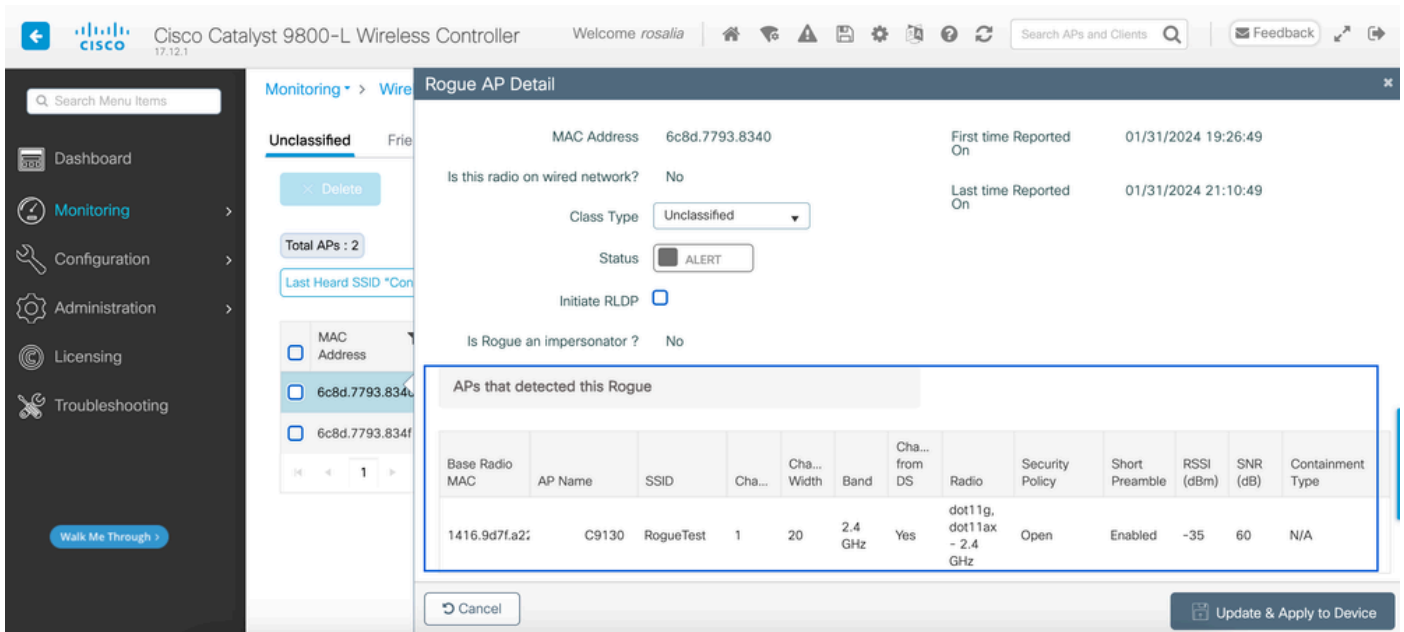
The screenshot shows the Cisco Catalyst 9800-L Wireless Controller GUI. The main content area is titled 'Monitoring > Wireless > Rogues'. There are tabs for 'Unclassified', 'Friendly', 'Malicious', 'Custom', 'Ignore List', 'Rogue Clients', and 'Adhoc Rogues'. The 'Unclassified' tab is selected. A search filter is applied: 'Last Heard SSID "Contains" rogue'. Below the filter, there is a table 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 rows of data are visible:

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 invasores da GUI

3. Liste os pontos de acesso que detectaram o dispositivo invasor.

Você pode visualizar os APs que detectaram o dispositivo invasor, a próxima figura mostra o AP que detectou esse invasor, canal, valor RSSI e mais informações:



Detalhes do AP invasor da GUI

Na CLI, você pode exibir essas informações por meio do comando `show wireless wps rogue ap detailed <mac-addr>`.

4. Localize o ponto de acesso mais próximo do dispositivo invasor com base no valor de RSSI mais próximo.

Com base nos resultados de quantos pontos de acesso detectaram o dispositivo invasor, você tem que procurar o AP mais próximo com base no valor de RSSI exibido no controlador sem fio. No próximo exemplo, apenas um AP detectou o invasor, no entanto, com um valor de RSSI alto, o que significa que o dispositivo invasor está muito próximo do meu AP.

O próximo é a saída do comando `show wireless wps rogue ap detailed <mac-addr>` para exibir o canal em que o AP/WLC ouviu esse dispositivo invasor, além do valor de 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. Reúna a captura pelo ar no mesmo canal para localizar o invasor.

Agora, o canal onde esse AP invasor transmite é encontrado, e com base no valor de RSSI, o ponto de acesso 9130 ouviu esse invasor em -35dBm, que é considerado muito próximo, isso dá uma ideia sobre qual área esse invasor está localizado, a próxima etapa é coletar uma captura pelo ar.

A próxima figura mostra uma captura pelo ar no canal 36, a partir do OTA, você pode ver que o AP invasor executa um ataque de desautenticação de contenção ao access point gerenciado:

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 18:59:54.075465	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 OTA de AP invasor

Você pode usar as informações da figura anterior para entender quão próximo esse invasor está

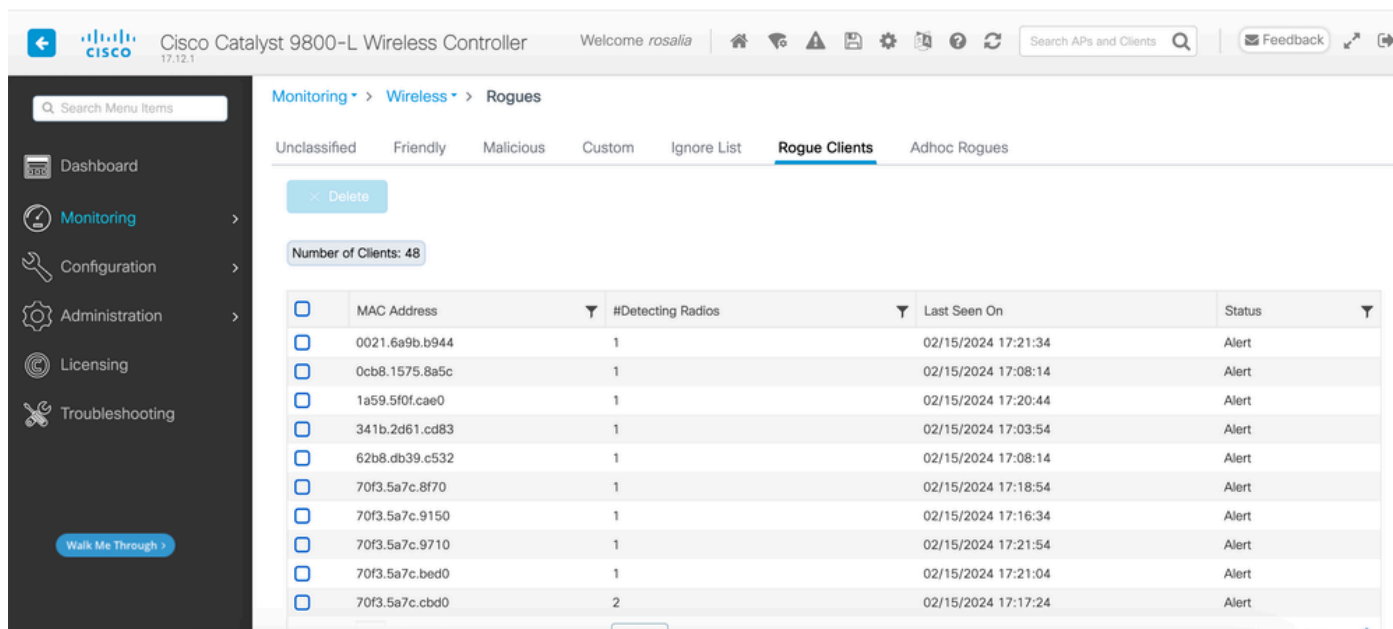
e, pelo menos, pode ter uma ideia de onde fisicamente esse ponto de acesso invasor está localizado. Você pode filtrar por meio do endereço MAC de rádio do AP invasor, você poderá ver se o invasor está ativo atualmente ou não se verificar se você tem pacotes de beacon no ar.

## Cenário 2: detectar e localizar um cliente invasor que envia uma inundação de desautenticação

As próximas etapas mostram como usar o controlador sem fio 9800 para localizar um cliente invasor conectado a um ponto de acesso não autorizado que não é gerenciado pela rede do usuário ou um cliente invasor que faz um ataque de desautenticação:

1. Use o controlador sem fio para localizar o cliente invasor.

Na GUI do controlador sem fio, navegue até a guia Monitoring (Monitoramento), Wireless (Sem fio), escolha Rogue Clients (Clientes invasores) ou use o comando `show wireless wps rogue client summary` da CLI para listar os clientes invasores detectados no controlador:



The screenshot shows the Cisco Catalyst 9800-L Wireless Controller GUI. The breadcrumb navigation is Monitoring > Wireless > Rogues. The 'Rogue Clients' tab is selected, showing a list of 48 clients. The table columns are MAC Address, #Detecting Radios, Last Seen On, and Status. The status for all listed clients is 'Alert'.

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

GUI da lista de clientes invasores

A próxima saída mostra o resultado da 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. O próximo exemplo de saída mostra os detalhes sobre o cliente invasor com o endereço mac 0021.6a9b.b944, que foi detectado por um AP 9130 gerenciado no canal 132. A próxima saída mostra mais detalhes:

```
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. Depois de coletar uma captura pelo ar no mesmo canal, você pode ver que há uma inundação não autenticada, na qual o cliente invasor usa um dos BSSID de ponto de acesso gerenciado para desconectar 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	132	38	Deauthentication, SN=926, FN=0, Flags=.....C
2	2024-02-15 18:08:58.153341440	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11	132	38	Deauthentication, SN=927, FN=0, Flags=.....C
3	2024-02-15 18:08:58.156716171	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11	132	38	Deauthentication, SN=928, FN=0, Flags=.....C
4	2024-02-15 18:08:58.158936988	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11	132	38	Deauthentication, SN=929, FN=0, Flags=.....C
5	2024-02-15 18:08:58.162302257	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11	132	38	Deauthentication, SN=930, FN=0, Flags=.....C
6	2024-02-15 18:08:58.164428517	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11	132	38	Deauthentication, SN=931, FN=0, Flags=.....C
7	2024-02-15 18:08:58.170320005	Cisco_7f:a2:2f	Broadcast	802.11	132	395	Beacon frame, SN=2688, FN=0, Flags=.....C
8	2024-02-15 18:08:58.170436441	Cisco_7f:a2:2e	Broadcast	802.11	132	419	Beacon frame, SN=2370, FN=0, Flags=.....C
9	2024-02-15 18:08:58.170600933	Cisco_7f:a2:2d	Broadcast	802.11	132	399	Beacon frame, SN=1490, FN=0, Flags=.....C
10	2024-02-15 18:08:58.172152791	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11	132	38	Deauthentication, SN=932, FN=0, Flags=.....C
11	2024-02-15 18:08:58.174367800	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11	132	38	Deauthentication, SN=933, FN=0, Flags=.....C
12	2024-02-15 18:08:58.178237914	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11	132	38	Deauthentication, SN=934, FN=0, Flags=.....C
13	2024-02-15 18:08:58.180354359	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11	132	38	Deauthentication, SN=935, FN=0, Flags=.....C
14	2024-02-15 18:08:58.183625075	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11	132	38	Deauthentication, SN=936, FN=0, Flags=.....C
15	2024-02-15 18:08:58.185859940	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11	132	38	Deauthentication, SN=937, FN=0, Flags=.....C
16	2024-02-15 18:08:58.189084965	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11	132	38	Deauthentication, SN=938, FN=0, Flags=.....C
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	132	38	Deauthentication, SN=939, FN=0, Flags=.....C
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	132	38	Deauthentication, SN=940, FN=0, Flags=.....C
21	2024-02-15 18:08:58.197648649	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11	132	38	Deauthentication, SN=941, FN=0, Flags=.....C
22	2024-02-15 18:08:58.200965406	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11	132	38	Deauthentication, SN=942, FN=0, Flags=.....C
23	2024-02-15 18:08:58.203145497	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11	132	38	Deauthentication, SN=943, FN=0, Flags=.....C
24	2024-02-15 18:08:58.206359424	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11	132	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

> 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 desautenticação

O valor de RSSI para os pacotes é alto, o que significa que o cliente invasor está fisicamente próximo ao ponto de acesso gerenciado.

4. Depois de remover o cliente invasor da rede, a próxima figura mostra uma rede limpa e um ambiente saudável pelo ar:

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=.....C
1757	2024-02-15 18:13:59.488213	Cisco_7f:a2:2f	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	105	Authentication, SN=0, FN=0, Flags=.....C
1759	2024-02-15 18:13:59.488220	Cisco_7f:a2:2f	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)	Cisco_7f:a2:2f	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	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)	Cisco_7f:a2:2f	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)	Cisco_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)	Cisco_7f:a2:2f	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)	Cisco_7f:a2:2f	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)	Cisco_7f:a2:2f	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)	Cisco_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 íntegro

## Informações Relacionadas

- [Gerenciamento de dispositivos invasores](#)
- [Classificando pontos de acesso não autorizados](#)
- [Analisar e solucionar problemas de sniffing da rede sem fio 802.11](#)
- [Suporte técnico e downloads da Cisco](#)



## Sobre esta tradução

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

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

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