识别并定位9800无线控制器上的非法AP/客户端

目录

简介

先决条件

要求

使用的组件

背景信息

场景

场景1：检测并定位欺诈接入点

场景2：检测并定位发送取消身份验证泛洪的恶意客户端

相关信息

简介

本文档介绍如何使用9800无线控制器检测和定位欺诈接入点或欺诈客户端。

先决条件

要求

Cisco 建议您了解以下主题：

- IEEE 802.11基础知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科无线9800-L控制器IOS® XE 17.12.1
- Cisco Catalyst 9130AXI系列接入点。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

Cisco非法接入点是指在网络管理员不知情或未经网络管理员批准的情况下安装的未经授权的无线接入点。这些恶意接入点可能会给网络带来安全风险，攻击者可以利用它们获得未经授权的访问、拦截敏感信息或发起其他恶意活动。Cisco Wireless Intrusion Prevention System(WIPS)是专为识别和管理欺诈接入点而设计的解决方案。

思科欺诈客户端（也称为欺诈工作站或欺诈设备）是指连接到欺诈接入点的未经授权且可能恶意的

无线客户端设备。与恶意接入点类似，恶意客户端也会带来安全风险，因为攻击者无需适当授权即可连接到网络。思科提供工具和解决方案，帮助检测并缓解欺诈客户端的存在，以维护网络安全。

场景

场景1：检测并定位欺诈接入点

接下来的步骤显示如何使用9800无线控制器帮助检测非法客户端或非用户网络管理的接入点：

1. 使用无线控制器查找哪个接入点检测到欺诈设备：

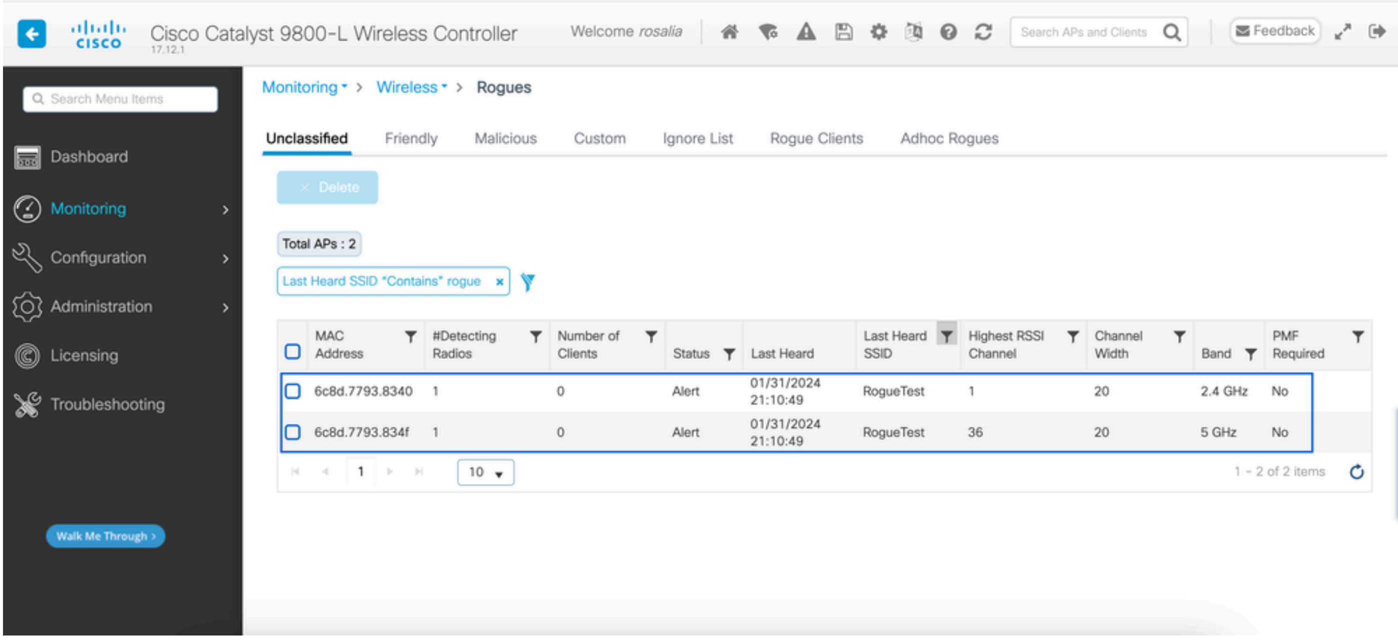
您可以通过GUI或CLI查看欺诈接入点或欺诈客户端；对于GUI，请依次转到Monitoring选项卡、Wireless并选择Rogue，然后可以使用过滤器查找欺诈设备，对于CLI，可以使用命令show wireless wps rogue ap summary查看所有检测到的欺诈设备，也可以使用命令show wireless wps rogue ap detailed <mac-addr>查看特定欺诈设备的详细信息。

以下是通过show wireless wps rogue ap summary命令从CLI查看非法设备列表的结果：

```
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.您可以过滤在9800控制器上配置的某个WLAN，以查看是否有任何非法设备广播相同的WLAN，下图显示我的C9130在两个频段上检测到此恶意设备的结果：



Total APs : 2

Last Heard SSID "Contains" rogue

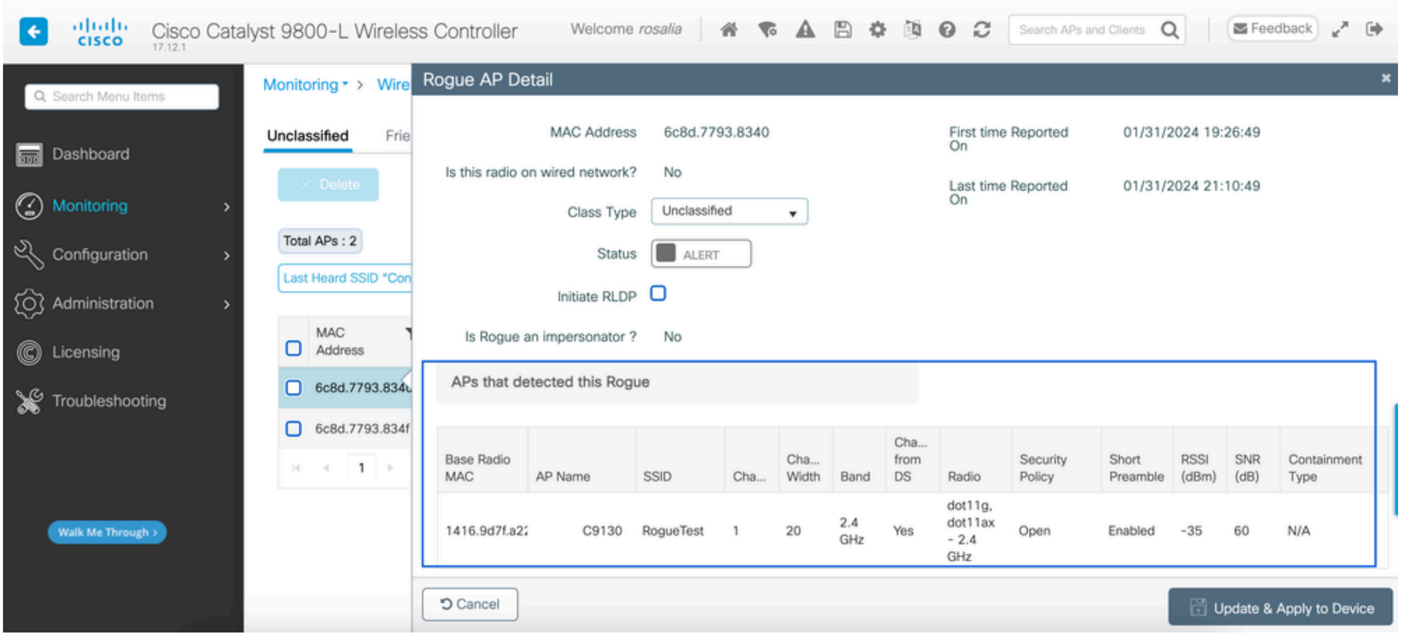
	MAC Address	#Detecting Radios	Number of Clients	Status	Last Heard	Last Heard SSID	Highest RSSI Channel	Channel Width	Band	PMF Required
□	6c8d.7793.8340	1	0	Alert	01/31/2024 21:10:49	RogueTest	1	20	2.4 GHz	No
□	6c8d.7793.834f	1	0	Alert	01/31/2024 21:10:49	RogueTest	36	20	5 GHz	No

1 - 2 of 2 items

GUI欺诈列表

3.列出检测到欺诈设备的接入点。

您可以查看检测到欺诈设备的AP，下图显示检测到此欺诈设备的AP、信道、RSSI值和其他信息：



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欺诈AP详细信息

在CLI中，您可以通过命令show wireless wps rogue ap detailed <mac-addr>查看此信息。

4.根据最近的RSSI值查找离欺诈设备最近的接入点。

根据检测到欺诈设备的接入点数量，您必须根据无线控制器上显示的RSSI值查找最近的AP，在下一个示例中，只有一个AP检测到欺诈设备，但是其RSSI值很高，这意味着欺诈设备离我的AP非常近。

接下来是show wireless wps rogue ap detailed <mac-addr>命令的输出，用于查看AP/WLC听到此欺诈设备的信道，以及RSSI值：

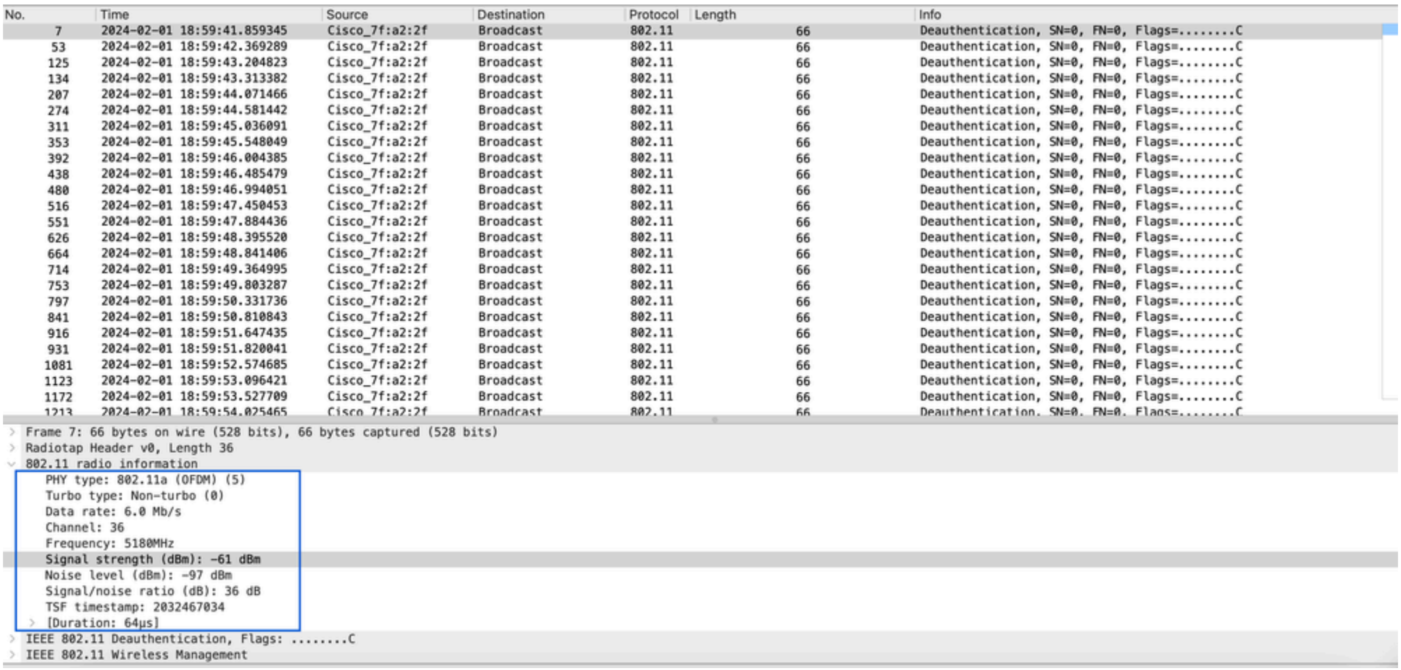
```
9800L#show wireless wps rogue ap detailed 6c8d.7793.834f
Rogue Event history

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.收集同一信道上的空中捕获以定位欺诈设备。

现在找到了此欺诈AP广播的通道，根据RSSI值，9130接入点在–35dBm处听到此欺诈，这被认为是

非常接近的，这样您就可以知道此欺诈位于哪个区域，下一步是收集无线捕获。

下图显示信道36上的空中捕获，从OTA您可以看到欺诈AP对受管接入点执行遏制取消身份验证攻击：



```
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
```

欺诈AP OTA捕获

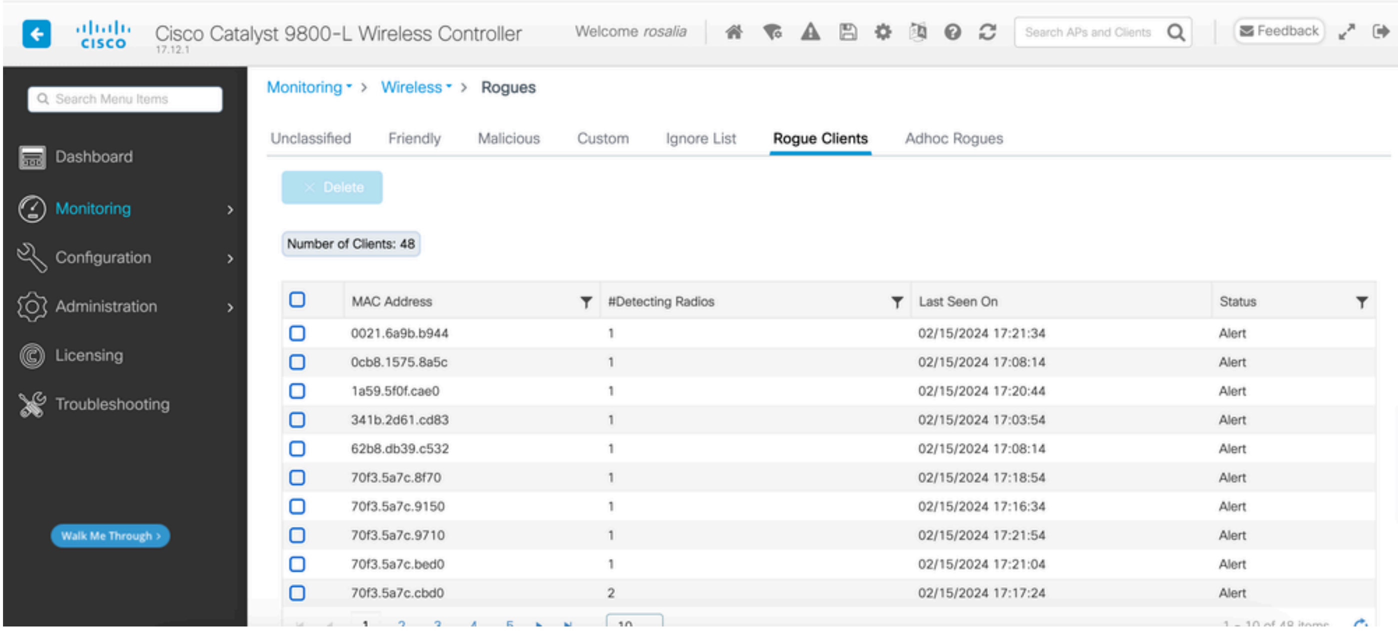
您可以使用上图中的信息了解此欺诈无线接入点的距离有多近，至少您可以了解此欺诈无线接入点实际位于何处。您可以通过欺诈AP无线电MAC地址进行过滤，如果检查空中是否有信标数据包，您将能够看到欺诈当前是否处于活动状态。

场景2：检测并定位发送取消身份验证泛洪的恶意客户端

接下来的步骤显示如何使用9800无线控制器查找连接到非由用户网络管理的欺诈接入点的欺诈客户端或执行取消身份验证攻击的欺诈客户端：

1.使用无线控制器查找欺诈客户端。

在无线控制器GUI中，导航到Monitoring选项卡Wireless，然后选择Rogue Clients，或者您可以从CLI使用命令show wireless wps rogue client summary列出在控制器上检测到的恶意客户端：



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

欺诈客户端列表GUI

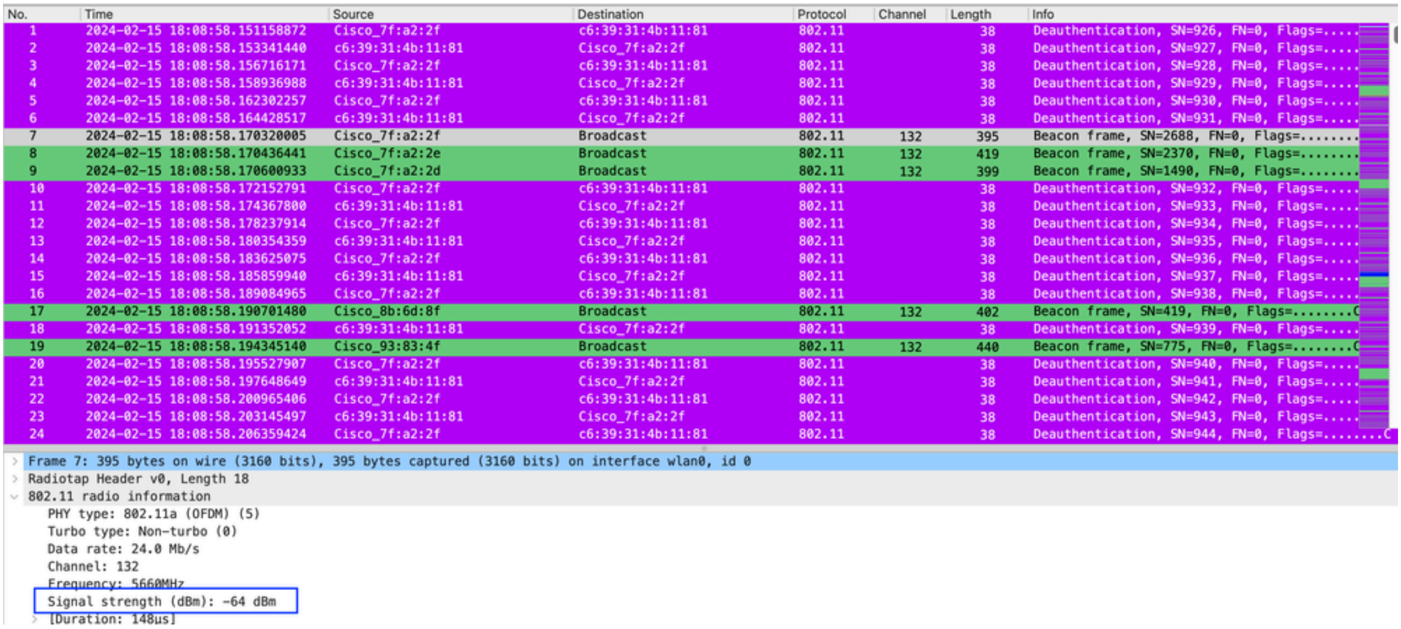
下一个输出显示CLI结果：

```
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.下一个输出示例显示有关托管的AP 9130在通道132上检测到的mac地址为0021.6a9b.b944的恶意客户端的详细信息，下一个输出显示更多详细信息：

```
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.收集同一信道上的空中捕获后，您可以看到您有未经身份验证的泛洪，其中恶意客户端使用其中一个托管接入点BSSID断开客户端：



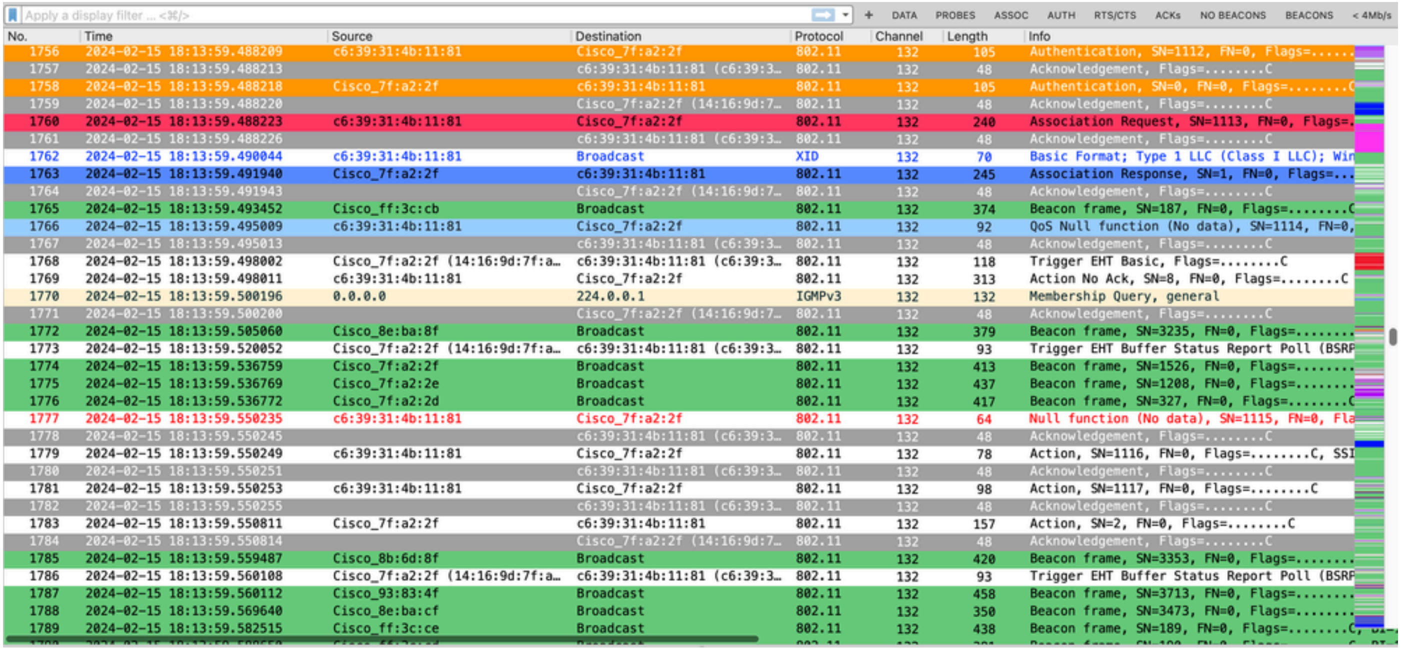
No.	Time	Source	Destination	Protocol	Channel	Length	Info
1	2024-02-15 18:08:58.151158872	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11		38	Deauthentication, SN=926, FN=0, Flags=....
2	2024-02-15 18:08:58.153341440	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11		38	Deauthentication, SN=927, FN=0, Flags=....
3	2024-02-15 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]
```

取消身份验证OTA

数据包的RSSI值很高，这意味着恶意客户端在物理上接近托管接入点。

4.将恶意客户端从网络中移除后，下图显示了一个干净的网络和一个健康的无线环境：



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=

正常的OTA

相关信息

- 管理欺诈设备
- 非法接入点分类
- 802.11 无线嗅探分析和故障排除
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。