識別並找到9800無線控制器上的惡意AP/客戶端

目錄

簡介

本文說明如何使用9800無線控制器檢測和定位欺詐接入點或欺詐客戶端。

必要條件

需求

思科建議您瞭解以下主題：

- IEEE 802.11基礎知識。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco無線9800-L控制器IOS® XE 17.12.1
- Cisco Catalyst 9130AXI系列存取點。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

思科欺詐接入點是指在網路管理員不知情或未經網路管理員批准的情況下安裝在網路上的未經授權的無線接入點。這些惡意接入點可能會給網路帶來安全風險，攻擊者可以利用它們獲取未經授權的訪問、攔截敏感資訊或發起其他惡意活動。Cisco Wireless Intrusion Prevention System(WIPS)是一種旨在識別和管理欺詐接入點的解決方案。

思科欺詐客戶端（也稱為欺詐工作站或欺詐裝置）是指連線到欺詐接入點的未經授權且可能惡意的

無線客戶端裝置。與惡意接入點類似，惡意客戶端也會帶來安全風險，因為攻擊者無需正確授權即可連線到網路。思科提供工具和解決方案，幫助檢測並緩解欺詐客戶端的存在，以維護網路安全。

案例

場景1：檢測並定位欺詐接入點

接下來的步驟顯示如何使用9800無線控制器幫助檢測非法客戶端或非由使用者網路管理的接入點：

1. 使用無線控制器查詢哪個接入點檢測到欺詐裝置：

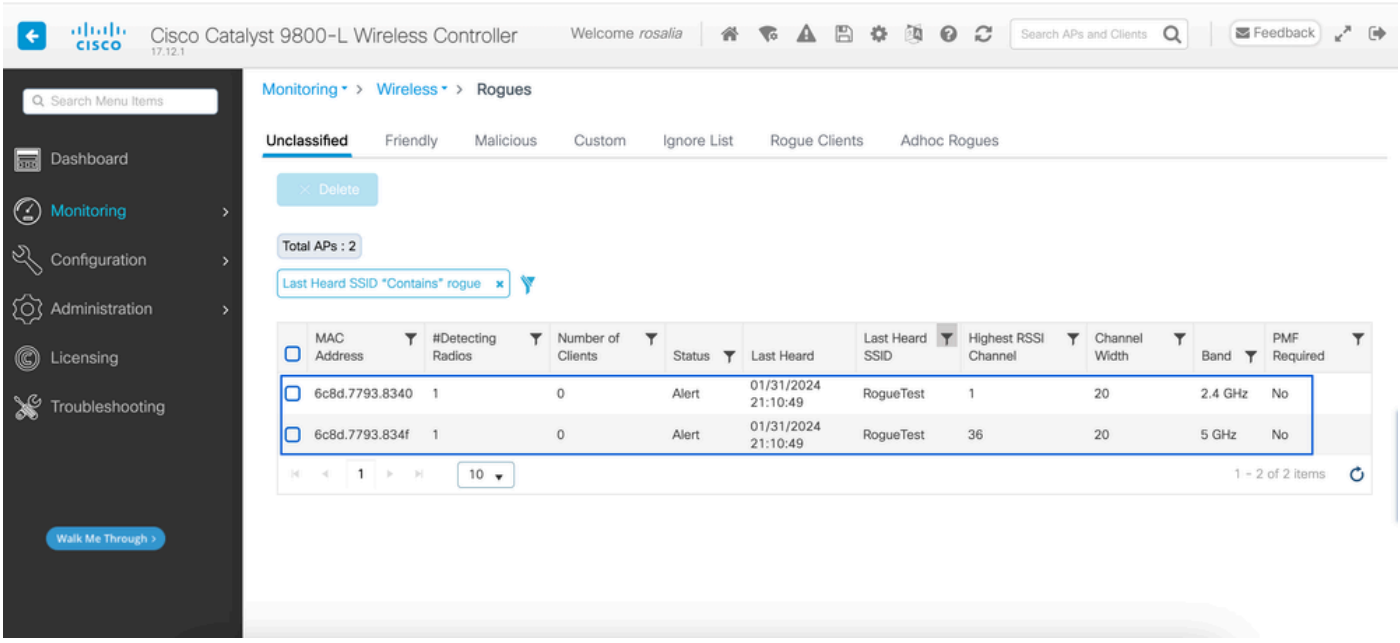
您可以通過GUI或CLI檢視欺詐接入點或欺詐客戶端；對於GUI，請依次轉到「監控」頁籤、「無線」並選擇「欺詐」，然後可以使用過濾器來查詢欺詐裝置，對於CLI，可以使用命令show wireless wps rogue ap summary來檢視所有檢測到的欺詐裝置，也可以使用命令show wireless wps rogue ap detailed <mac-addr>來檢視特定欺詐裝置的詳細資訊。

以下是通過show wireless wps rogue ap summary命令從CLI檢視無管理系統裝置清單的結果：

```
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
...
```

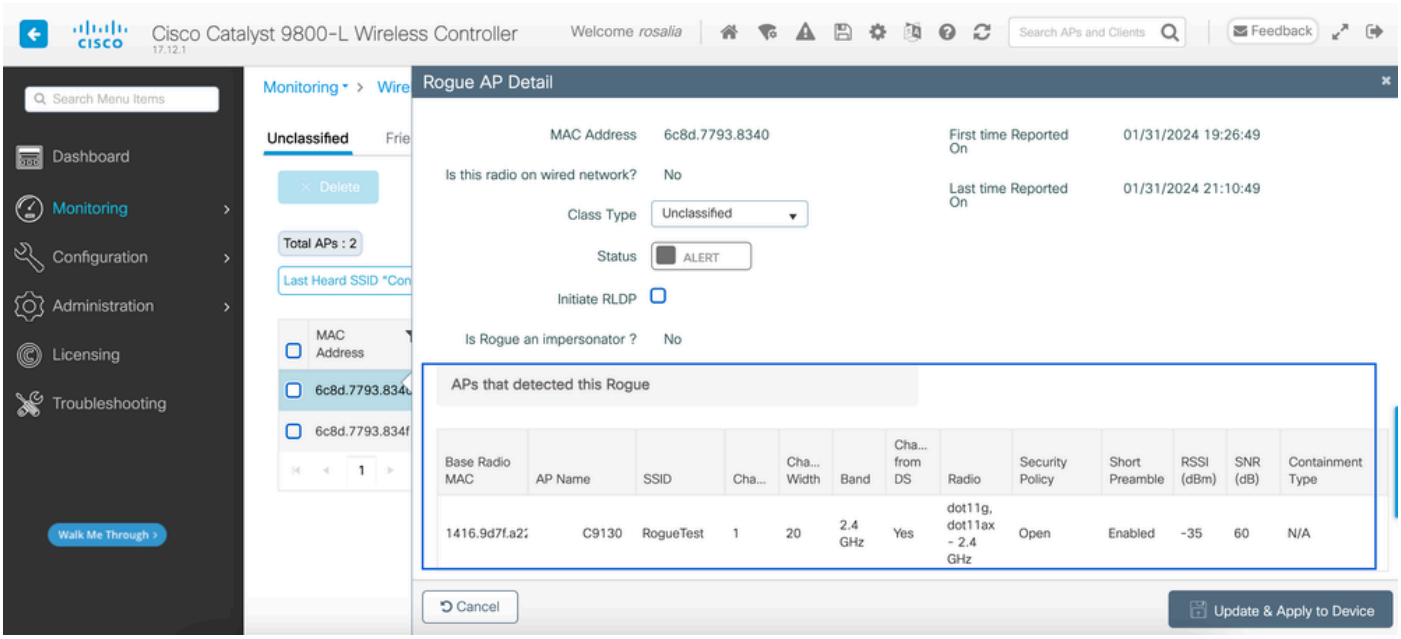
2.您可以對9800控制器上配置的其中一個WLAN進行過濾，檢視是否有任何非法裝置廣播相同的WLAN，下圖顯示我的C9130在兩個頻段上檢測到此惡意裝置的結果：



GUI欺詐清單

3.列出檢測到欺詐裝置的接入點。

您可以檢視檢測到欺詐裝置的AP，下圖顯示檢測到此欺詐裝置的AP、通道、RSSI值和其他資訊：



GUI惡意AP詳細資訊

您可以在CLI中通過show wireless wps rogue ap detailed <mac-addr>命令檢視此資訊。

4.根據最近的RSSI值找到離欺詐裝置最近的接入點。

根據檢測到欺詐裝置的接入點數結果，您必須根據無線控制器上顯示的RSSI值查詢最近的AP，在下一個示例中，只有一個AP檢測到欺詐裝置，但RSSI值很高，這意味著欺詐裝置離我的AP非常近。

下一個是命令show wireless wps rogue ap detailed <mac-addr>的輸出，用於檢視AP/WLC聽到此欺詐裝置的通道，加上RSSI值：

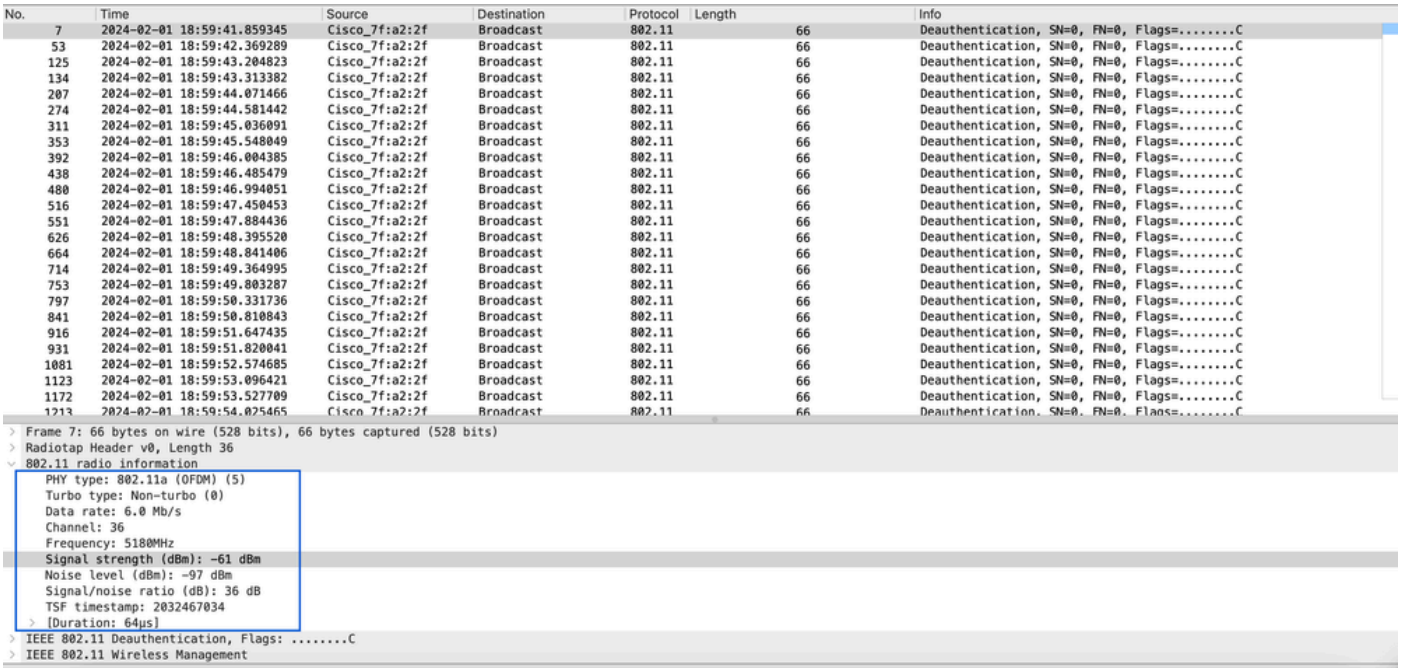
```
9800L#show wireless wps rogue ap detailed 6c8d.7793.834f
Rogue Event history

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.在同一通道收集空中捕捉以定位惡意。

現在找到此惡意AP廣播的通道，根據RSSI值，9130接入點在–35dBm（被認為是非常接近的）處聽

到此惡意AP廣播，這使您知道此惡意接入點位於哪個區域，下一步是收集無線捕獲。

下圖顯示通道36上的空中捕獲，從OTA可以看到欺詐AP對託管接入點執行遏製取消身份驗證攻擊：



欺詐AP OTA捕獲

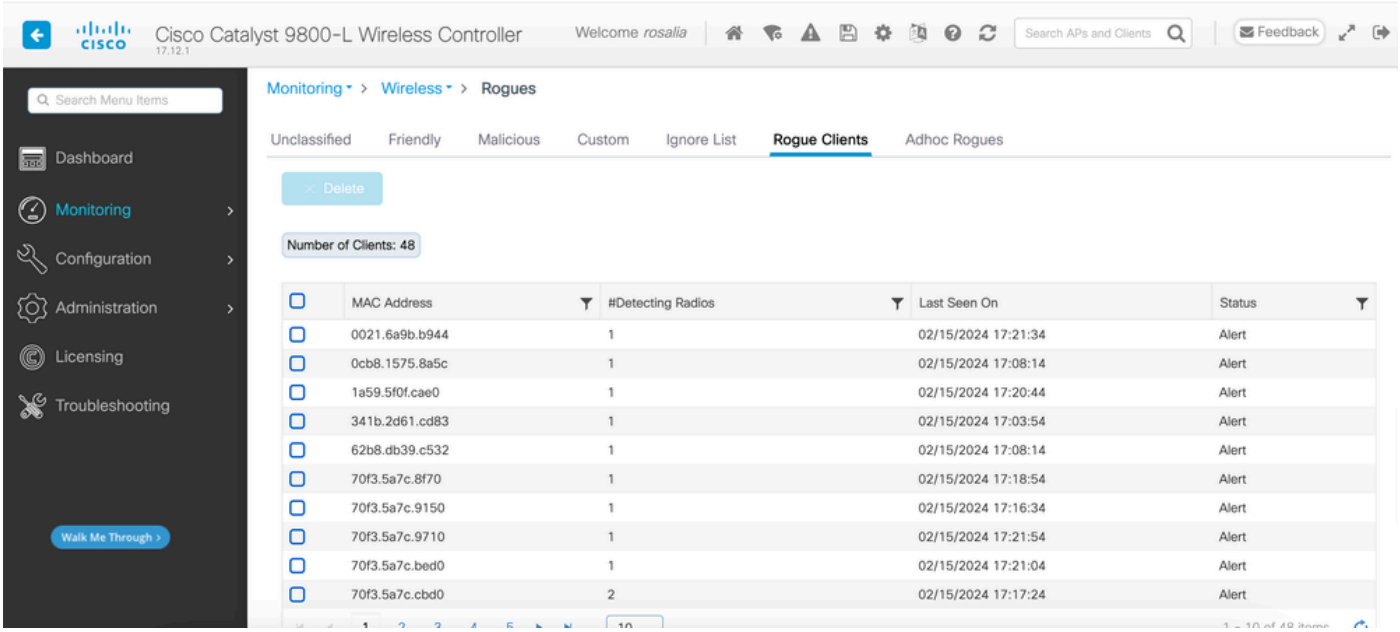
您可以使用上圖中的資訊瞭解此欺詐接入點的距離有多近，至少您可以瞭解此欺詐接入點實際位於何處。您可以通過欺詐無線接入點的mac地址進行過濾，如果檢查空中是否有信標資料包，您將能夠看到欺詐當前是否處於活動狀態。

場景2：檢測並定位傳送取消身份驗證泛洪的惡意客戶端

接下來的步驟顯示如何使用9800無線控制器查詢連線到非由使用者網路管理的欺詐接入點的欺詐客戶端或執行去身份驗證攻擊的欺詐客戶端：

1.使用無線控制器查詢欺詐客戶端。

在無線控制器GUI中，導航到Monitoring（監控）頁籤Wireless（無線），然後選擇Rogue Clients（無管理系統客戶端），或者可以使用CLI中的命令show wireless wps rogue client summary來列出控制器上檢測到的無管理系統客戶端：



惡意客戶端清單GUI

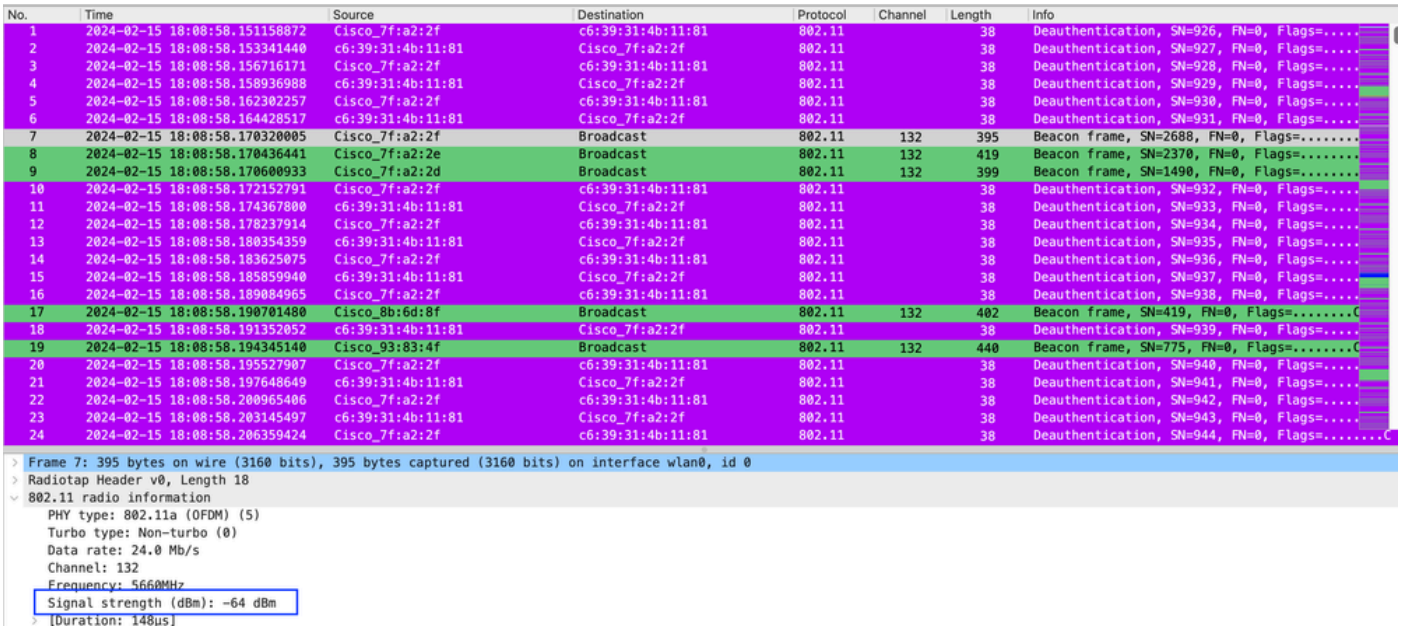
下一個輸出顯示CLI結果：

```
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.下一個輸出示例顯示了有關mac地址為0021.6a9b.b944的惡意客戶端的詳細資訊（由通道132上的託管AP 9130檢測到），下一個輸出顯示了更多詳細資訊：

```
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
```

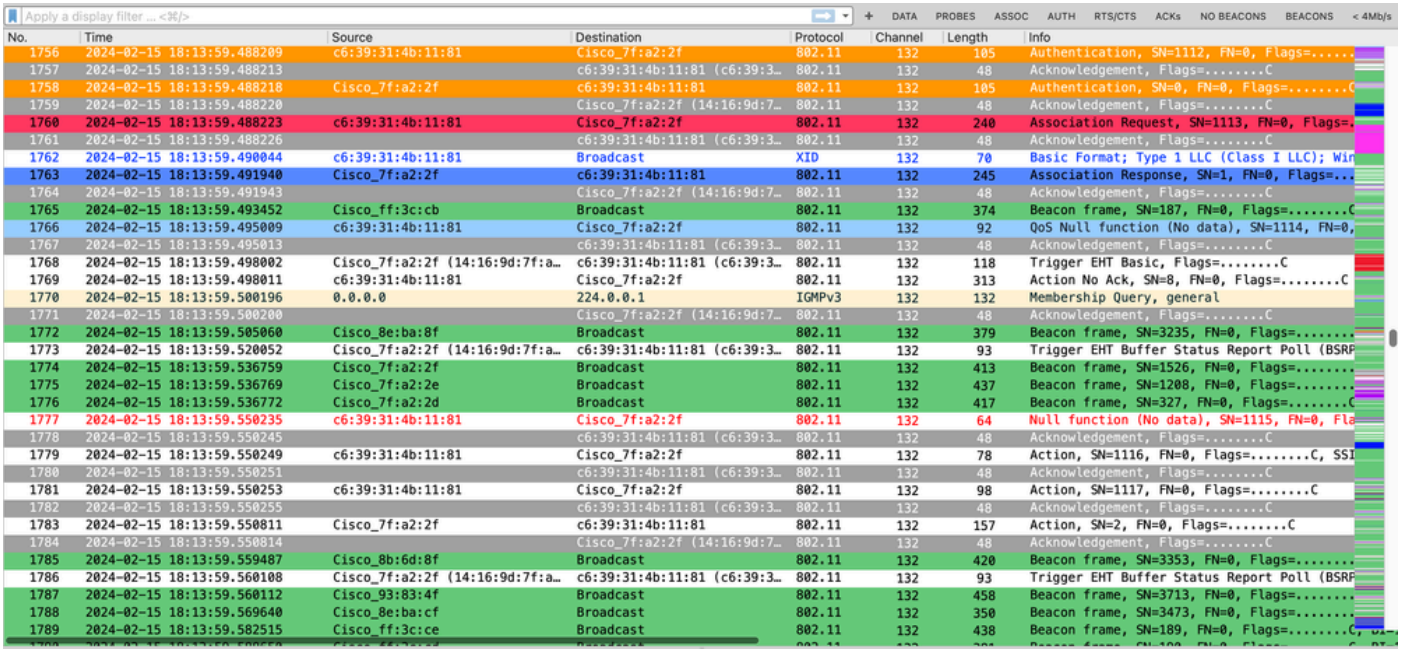
3.在同一通道上收集無線捕獲後，您會發現存在未經身份驗證的泛洪，其中惡意客戶端使用其中一個託管接入點BSSID斷開客戶端：



取消驗證OTA

封包的RSSI值很高，這表示惡意使用者端實際位於受管存取點附近。

4.將欺詐客戶端從網路中移除後，下圖顯示了乾淨的網路和健康的無線環境：



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

正常的OTA

相關資訊

- 管理欺詐裝置
- 對惡意接入點分類
- 分析及疑難排解 802.11 無線監聽相關問題
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。