

Identificeer en lokaliseer een bedrieglijke AP/client op de 9800 draadloze controllers

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Scenario's](#)

[Scenario 1: Een bedrieglijk access point detecteren en lokaliseren](#)

[Scenario 2: Detecteer en lokaliseer een schurkenclient die een de-authenticatie vloed verstuurt](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u een bedrieglijk access point of een schurkenclient kunt detecteren en lokaliseren met behulp van de 9800 draadloze controller.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- basiskennis van IEEE 802.11.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco draadloze 9800-L controller IOS® XE 17.12.1
- Cisco Catalyst 9130AXI Series access point.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Een Cisco-schurkentoegangspunt verwijst naar een onbevoegd draadloos access point dat op een netwerk is geïnstalleerd zonder kennis of goedkeuring van de netwerkbeheerder. Deze bedrieglijke toegangspunten kunnen veiligheidsrisico's voor een netwerk vormen, en de aanvallers kunnen hen gebruiken om onbevoegde toegang te verkrijgen, gevoelige informatie te onderscheppen, of andere kwaadaardige activiteiten te lanceren. [Cisco Wireless Inbraakpreventiesysteem \(WIPS\)](#) is een oplossing die is ontworpen om bedrieglijke access points te identificeren en te beheren.

Een Cisco-schurkenclient, ook bekend als een schurkenstation of schurkenapparaat, verwijst naar een onbevoegd en potentieel kwaadaardig draadloos clientapparaat dat is aangesloten op een schurkentoegangspunt. Net als schurkentoegangspunten vormen schurkencliënten beveiligingsrisico's omdat een aanvaller zonder de juiste autorisatie verbinding kan maken met een netwerk. Cisco biedt tools en oplossingen om de aanwezigheid van frauduleuze clients te helpen detecteren en beperken om de netwerkbeveiliging te handhaven.

Scenario's

Scenario 1: Een bedrieglijk access point detecteren en lokaliseren

De volgende stappen tonen hoe u de 9800 draadloze controllers kunt gebruiken om een schurkenclient of een toegangspunt te detecteren dat niet wordt beheerd door het gebruikersnetwerk:

1. Gebruik de draadloze controller om te weten te komen welke van uw toegangspunten het bedrieglijke apparaat heeft gedetecteerd:

U kunt de bedrieglijke toegangspunten of de schurkencliënten via GUI of CLI bekijken; voor GUI, ga naar het tabblad Monitoring, dan Draadloos, en kies Rogue, dan kunt u de filters gebruiken om uw bedrieglijk apparaat te vinden, en voor de CLI, kunt u de opdracht tonen draadloze wps schurkenap samenvatting om alle gedetecteerde bedrieglijke apparaten te bekijken, of u kunt de opdracht gebruiken toont draadloze wps schurkenap gedetailleerde <mac-addr> om de details op een specifiek schurkenapparaat te bekijken.

Hier is het resultaat van de CLI om de lijst van de schurkenapparaten via het bevel te bekijken toont draadloze wps schurkenap samenvatting:

```
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
...

```

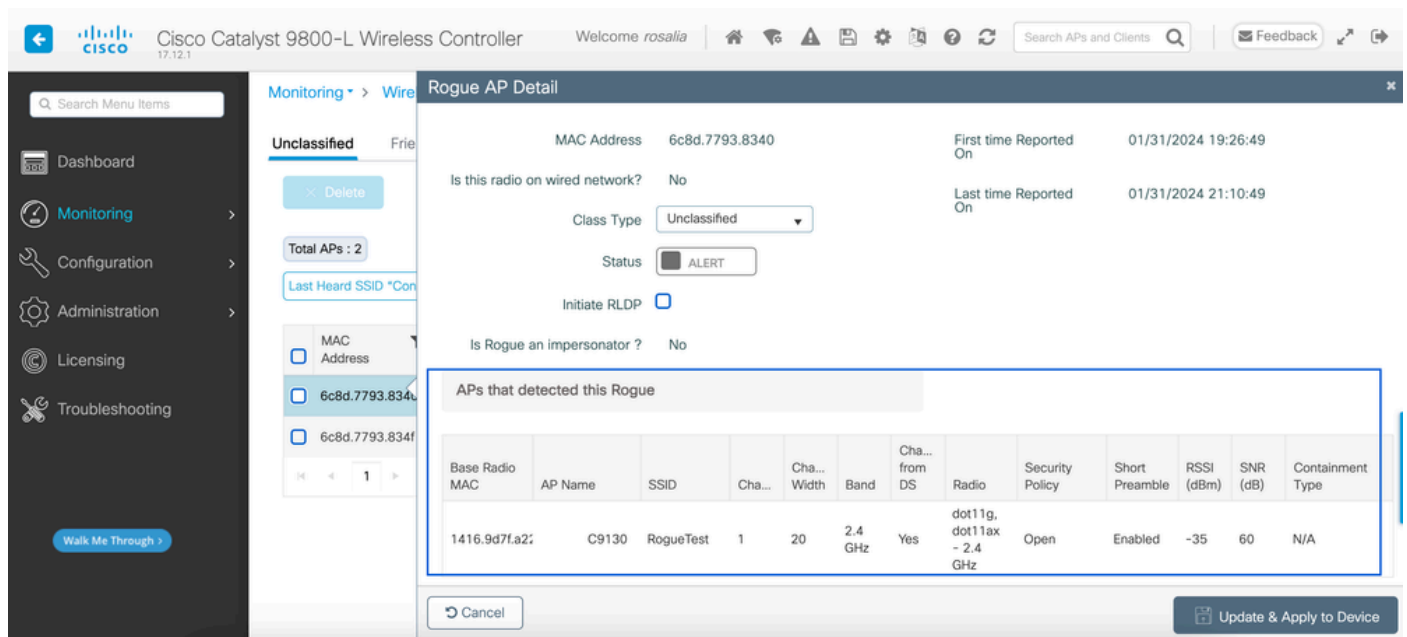
2. U kunt filteren op een van de WLAN's die op uw 9800-controller zijn geconfigureerd om te zien of u bedrieglijke apparaten hebt die dezelfde WLAN's uitzenden, het volgende cijfer toont het resultaat waar mijn C9130 deze bedrieglijke op beide banden heeft gedetecteerd:

GUI Rogue List

3. Maak een lijst van de toegangspunten die het fraudeapparaat hebben gedetecteerd.

U kunt de toegangspunten bekijken die het fraudeapparaat hebben gedetecteerd. Het volgende cijfer toont het toegangspunt dat deze frauduleuze handeling, dit kanaal, de RSSI-waarde en meer

informatie heeft gedetecteerd:



GUI Rogue AP Details

Vanuit de CLI kunt u deze informatie bekijken via de opdracht `show wireless wps rogue ap detailed <mac-addr>`.

4. Vind het dichtstbijzijnde toegangspunt tot het schurkenapparaat op basis van de dichtstbijzijnde RSSI-waarde.

Op basis van de resultaten van hoeveel toegangspunten gedetecteerd het bedrieglijke apparaat, moet u op zoek naar het dichtstbijzijnde AP op basis van de RSSI-waarde weergegeven op de draadloze controller, in het volgende voorbeeld slechts één AP gedetecteerd de bedrieger, echter met een hoge RSSI-waarde, wat betekent dat het bedrieglijke apparaat is zeer dichtbij mijn AP.

Het volgende is de output van bevel `show wireless wps schurkenkaart detailed <mac-addr>` om het kanaal te bekijken AP/WLC dit schurkenapparaat, plus de waarde van RSSI hoorde:

```
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. Verzamel over-de-lucht opname op hetzelfde kanaal om de schurk te lokaliseren.

Het kanaal waar deze schurkenAP uitzendt, en op basis van de RSSI-waarde, hoorde het 9130 access point deze schurk op -35dBm, die als heel dichtbij wordt beschouwd, dit geeft je een idee over welk gebied deze schurk zich bevindt, de volgende stap is het verzamelen van een over-de-lucht opname.

Volgende figuur toont een over-the-air opname op kanaal 36, van de OTA, kunt u zien bedrieglijke AP voert een insluiting de-authenticatie aanval aan het beheerde access point uit:

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 18:59:46.994851	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 18:59:53.527789	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

U kunt de informatie uit de vorige figuur gebruiken om te begrijpen hoe dicht deze schurk is, en u kunt ten minste een idee hebben waar fysiek dit schurkentoegangspunt zich bevindt. U kunt filteren via het frauduleuze AP-radiomailadres, zou u in staat zijn om te zien of de schurk momenteel actief is of niet als u controleert of u baken pakketten over de lucht.

Scenario 2: Detecteer en lokaliseer een schurkenclient die een de-authenticatie vloed verstuurt

De volgende stappen tonen u hoe u de 9800 draadloze controller kunt gebruiken om een schurkenclient te vinden die is aangesloten op een schurkentoegangspunt dat niet wordt beheerd door het gebruikersnetwerk of een schurkenclient die een de-authenticatie aanval uitvoert:

1. Gebruik de draadloze controller om de schurkenclient te vinden.

Van de draadloze controller GUI, navigeer naar het tabblad Monitoring, Wireless, kies vervolgens Rogue Clients, of u kunt de opdracht tonen draadloze wps schurkenclient samenvatting van de CLI gebruiken om de schurkenclients die op de controller gedetecteerd zijn te vermelden:

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller GUI. The main content area is titled 'Monitoring > Wireless > Rogues'. Underneath, there are tabs for 'Unclassified', 'Friendly', 'Malicious', 'Custom', 'Ignore List', 'Rogue Clients', and 'Adhoc Rogues'. The 'Rogue Clients' tab is selected. A 'Delete' button is visible at the top left of the table area. Below the button, it says 'Number of Clients: 48'. The table below has the following columns: 'MAC Address', '#Detecting Radios', 'Last Seen On', and 'Status'. The table contains 10 rows of data, all with a status of '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 van clientlijst voor fraudeurs

De volgende output toont het CLI resultaat:

```
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. Het volgende uitvoervoorbeeld toont de details over schurkenclient met mac-adres 0021.6a9b.b944, die werd gedetecteerd door een beheerde AP 9130 op kanaal 132, de volgende uitvoer toont meer details:

```
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. Nadat u een over-the-air opname via hetzelfde kanaal hebt verzameld, kunt u zien dat u een niet-geverifieerde overstroming hebt, waarbij de schurkenclient een van de beheerde access point

BSSID gebruikt om clients los te koppelen:

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-authenticatie ongedaan maken

De RSSI-waarde voor de pakketten is hoog, wat betekent dat de schurkenclient zich fysiek in de buurt van het beheerde access point bevindt.

4. Nadat u de schurkenclient van het netwerk verwijdert, toont het volgende cijfer een schoon netwerk en een gezonde omgeving over-the-air:

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	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	c6:39:31:4b:11:81	Cisco_7f:a2:2f (14:16:9d:7f:a...	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	c6:39:31:4b:11:81	Cisco_7f:a2:2f (14:16:9d:7f:a...	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:a...	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	c6:39:31:4b:11:81	Cisco_7f:a2:2f (14:16:9d:7f:a...	802.11	132	48	Acknowledgement, Flags=.....C
1772	2024-02-15 18:13:59.505060	Cisco_8e:ba:cf	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:a...	c6:39:31:4b:11:81	802.11	132	93	Trigger EHT Buffer Status Report Poll (BSRF)
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:a...	c6:39:31:4b:11:81	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:a...	c6:39:31:4b:11:81	802.11	132	93	Trigger EHT Buffer Status Report Poll (BSRF)
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, v...

Gezonde OTA

Gerelateerde informatie

- [Schuifapparaten beheren](#)
- [Rogue access points classificeren](#)

- [Analyze and Troubleshoot 802.11 Wireless Sniffing \(802.11 Wireless sniffing analyseren en troubleshooten\)](#)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.