Identification et localisation d'un point d'accès/client non autorisé sur les contrôleurs sans fil 9800

Table des matières

Introduction

Ce document décrit comment détecter et localiser un point d'accès non autorisé ou un client non autorisé à l'aide du contrôleur sans fil 9800.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Principes fondamentaux de la norme IEEE 802.11

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur Cisco Wireless 9800-L IOS® XE 17.12.1
- Point d'accès Cisco Catalyst 9130AXI.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Un point d'accès non autorisé Cisco fait référence à un point d'accès sans fil non autorisé qui a été installé sur un réseau à l'insu ou sans l'approbation de l'administrateur réseau. Ces points d'accès indésirables peuvent représenter un risque pour la sécurité d'un réseau et les pirates peuvent les utiliser pour obtenir un accès non autorisé, intercepter des informations sensibles ou lancer d'autres activités malveillantes. Cisco Wireless Intrusion Prevention System (WIPS) est une solution conçue pour identifier et gérer les points d'accès non autorisés.

Un client non autorisé Cisco, également appelé station non autorisée ou périphérique non autorisé, fait référence à un périphérique client sans fil non autorisé et potentiellement malveillant connecté à un point d'accès non autorisé. Tout comme les points d'accès non autorisés, les clients non autorisés présentent des risques pour la sécurité, car un pirate peut se connecter à un réseau sans autorisation appropriée. Cisco fournit des outils et des solutions pour aider à détecter et à réduire la présence de clients indésirables afin de maintenir la sécurité du réseau.

Scénarios

Scénario 1 : Détection Et Localisation D'Un Point D'Accès Non Autorisé

Les étapes suivantes vous montrent comment utiliser les contrôleurs sans fil 9800 pour détecter un client non autorisé ou un point d'accès qui n'est pas géré par le réseau de l'utilisateur :

1. Utilisez le contrôleur sans fil pour identifier les points d'accès qui ont détecté le périphérique non autorisé :

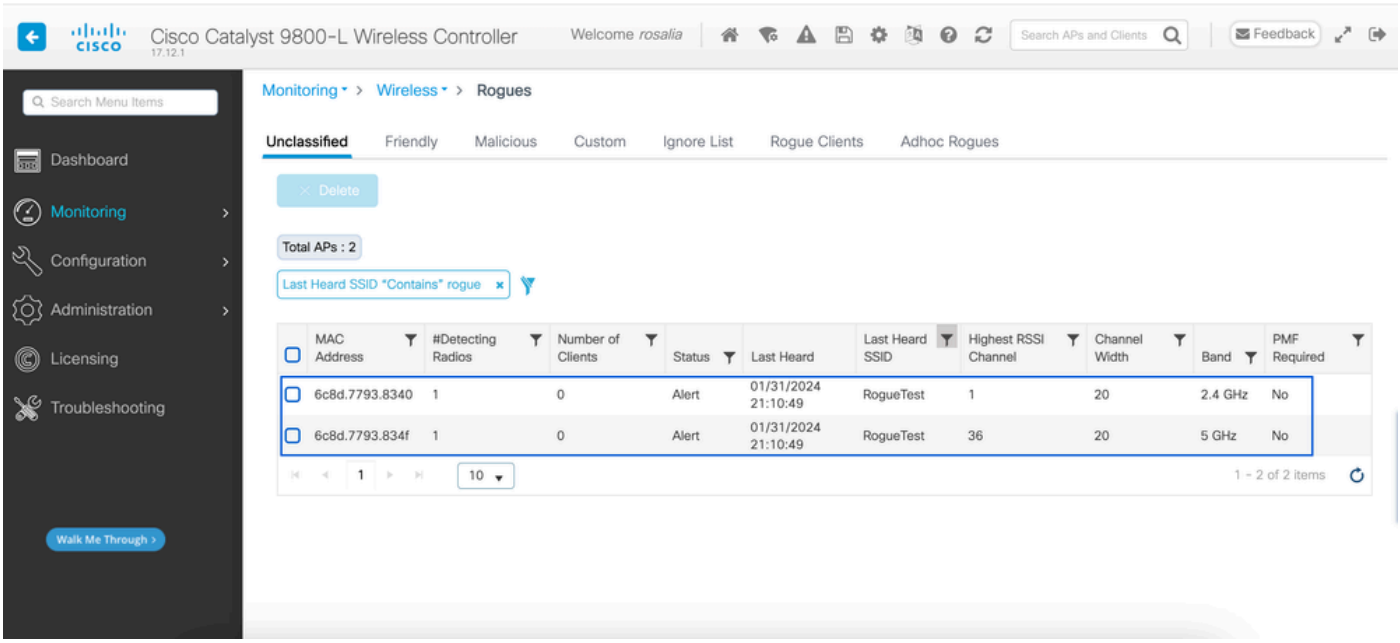
Vous pouvez afficher les points d'accès indésirables ou les clients indésirables via l'interface GUI ou CLI ; pour l'interface GUI, accédez à l'onglet Surveillance, puis à Wireless, et choisissez Rogue, puis vous pouvez utiliser les filtres pour trouver votre périphérique indésirable, et pour l'interface CLI, vous pouvez utiliser la commande show wireless wps rogue ap summary pour afficher tous les périphériques indésirables détectés, ou vous pouvez utiliser la commande show wireless wps rogue ap detailed <mac-addr> pour afficher les détails sur un périphérique indésirable spécifique.

Voici le résultat de l'interface de ligne de commande pour afficher la liste des périphériques indésirables via la commande 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
...
```

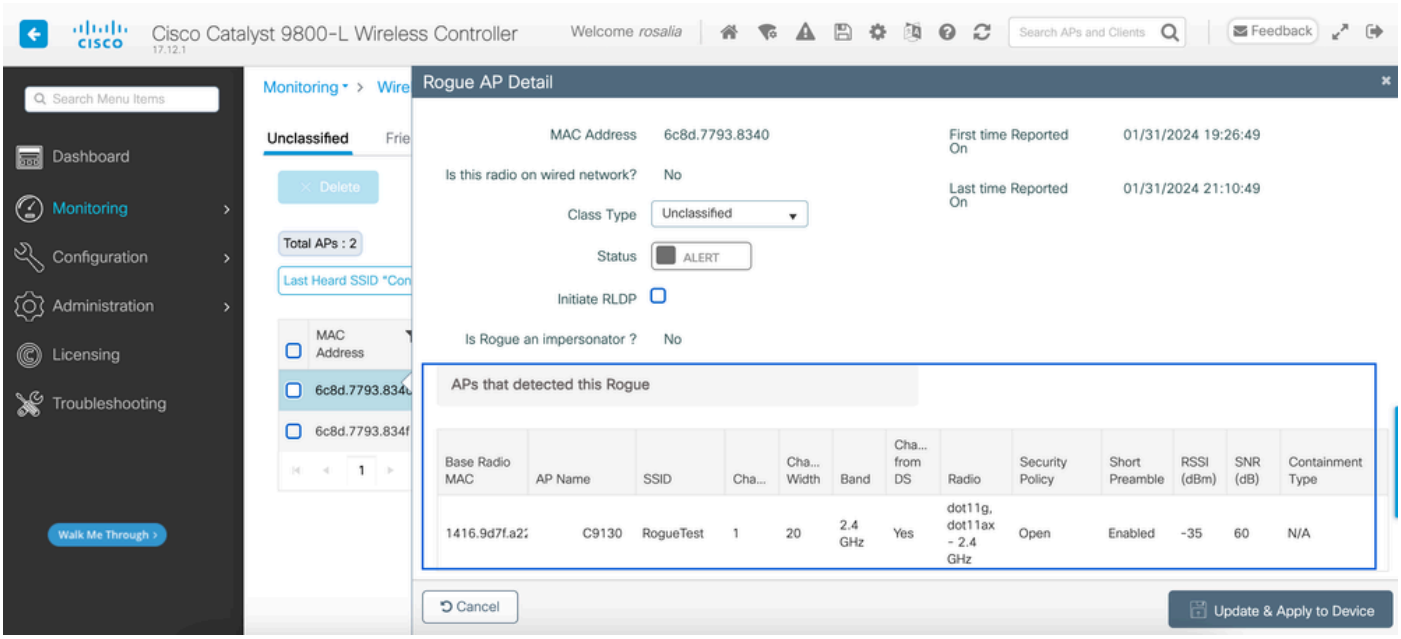
2. Vous pouvez filtrer sur l'un des WLAN configurés sur votre contrôleur 9800 pour voir si vous avez des périphériques non autorisés qui diffusent les mêmes WLAN. La figure suivante montre le résultat où mon C9130 a détecté ce périphérique non autorisé sur les deux bandes :



Liste non fiable GUI

3. Répertoriez les points d'accès qui ont détecté le périphérique non autorisé.

Vous pouvez afficher les points d'accès qui ont détecté le périphérique non autorisé, la figure suivante montre le point d'accès qui a détecté ce périphérique non autorisé, le canal, la valeur RSSI et plus d'informations :



Détails des points d'accès indésirables

À partir de l'interface de ligne de commande, vous pouvez afficher ces informations via la commande show wireless wps rogue ap detailed <mac-addr>.

4. Recherchez le point d'accès le plus proche du périphérique indésirable en fonction de la valeur RSSI la plus proche.

En fonction des résultats du nombre de points d'accès détectés par le périphérique indésirable, vous devez rechercher le point d'accès le plus proche en fonction de la valeur RSSI affichée sur le contrôleur sans fil. Dans l'exemple suivant, un seul point d'accès a détecté le périphérique indésirable, mais avec une valeur RSSI élevée, ce qui signifie que le périphérique indésirable est très proche de mon point d'accès.

La suivante est le résultat de la commande show wireless wps rogue ap detailed <mac-addr> pour afficher le canal sur lequel le point d'accès/WLC a entendu ce périphérique indésirable, plus la valeur RSSI :

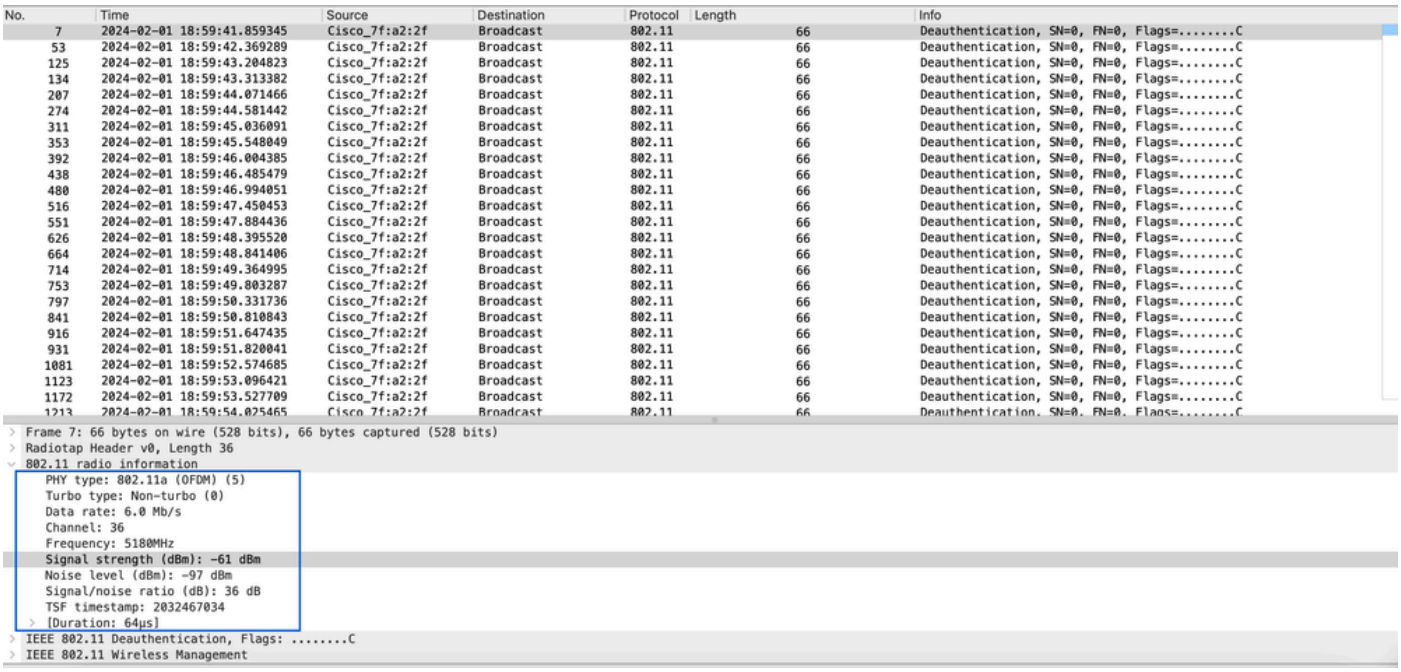
```
9800L#show wireless wps rogue ap detailed 6c8d.7793.834f
Rogue Event history

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. Collectez la capture en direct sur le même canal pour localiser le pirate.

Maintenant, le canal où ce point d'accès indésirable diffuse est trouvé, et sur la base de la valeur RSSI, le point d'accès 9130 a entendu ce point d'accès indésirable à -35 dBm, qui est considéré comme très proche, cela vous donne une idée sur quelle zone ce point d'accès indésirable est situé, l'étape suivante est de recueillir une capture en direct.

La figure suivante montre une capture sans fil sur le canal 36, à partir de l'OTA. Vous pouvez voir que le point d'accès non autorisé exécute une attaque de désauthentification de confinement vers le point d'accès géré :



Capture OTA des points d'accès indésirables

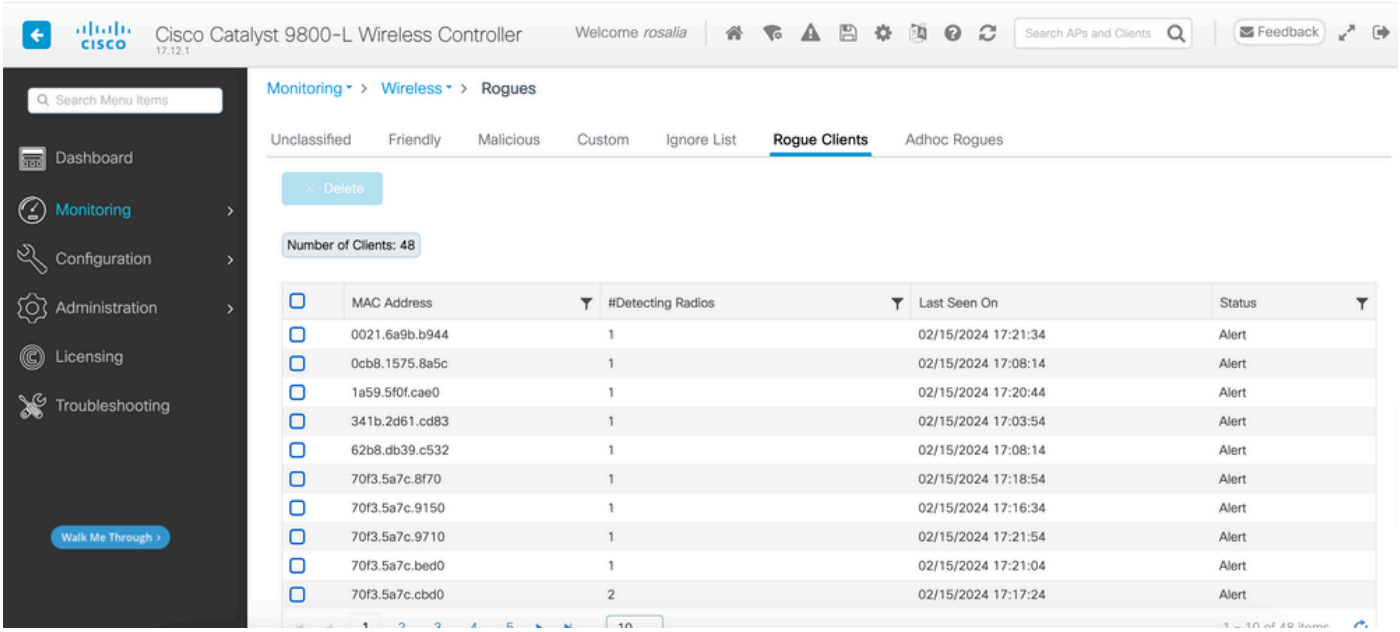
Vous pouvez utiliser les informations de la figure précédente pour comprendre la proximité de ce point d'accès non autorisé et au moins vous pouvez avoir une idée de l'emplacement physique de ce point d'accès non autorisé. Vous pouvez filtrer via l'adresse MAC radio du point d'accès non autorisé, vous serez en mesure de voir si le point d'accès non autorisé est actuellement actif ou non si vous vérifiez si vous avez des paquets de balise sur l'air.

Scénario 2 : détection et localisation d'un client non autorisé qui envoie un déluge de désauthentification

Les étapes suivantes vous montrent comment utiliser le contrôleur sans fil 9800 pour trouver un client non autorisé connecté à un point d'accès non autorisé qui n'est pas géré par le réseau de l'utilisateur ou un client non autorisé qui effectue une attaque de désauthentification :

1. Utilisez le contrôleur sans fil pour trouver le client non autorisé.

Dans l'interface utilisateur graphique du contrôleur sans fil, accédez à l'onglet Surveillance, Wireless, puis choisissez Rogue Clients. Vous pouvez également utiliser la commande show wireless wps rogue client summary de l'interface de ligne de commande pour répertorier les clients indésirables détectés sur le contrôleur :



Interface utilisateur graphique Liste des clients indésirables

Le résultat suivant montre le résultat CLI :

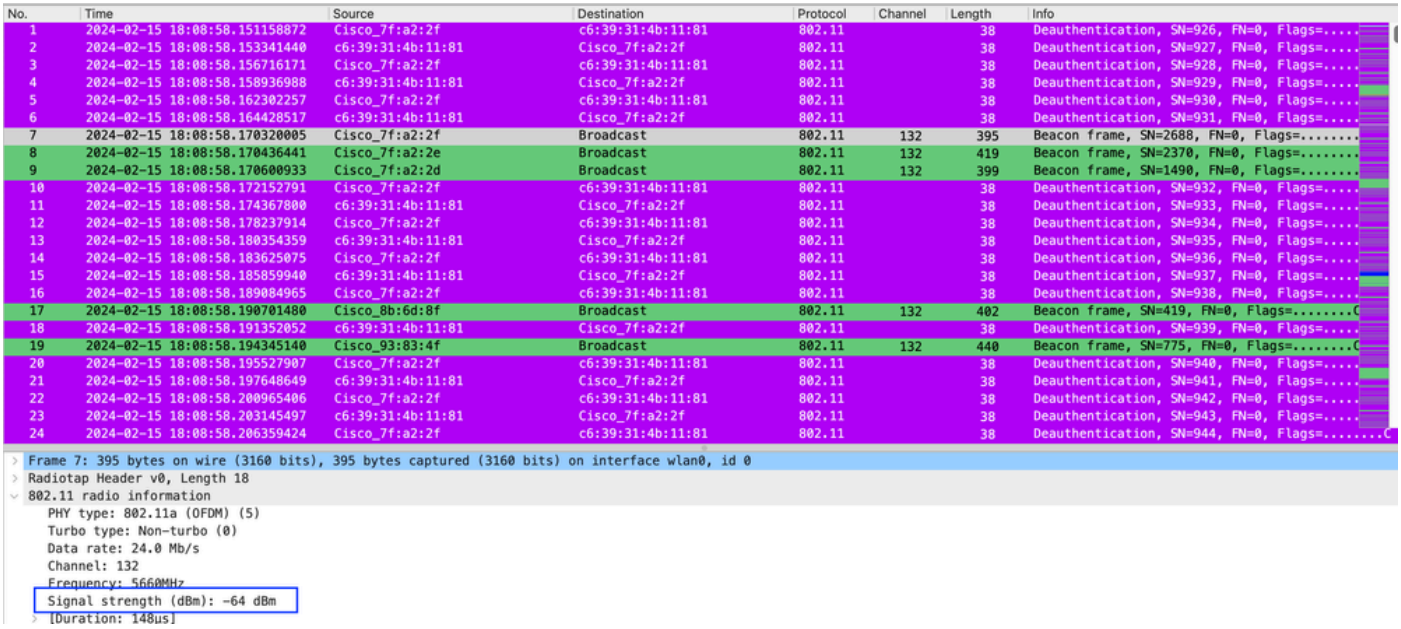
```
9800L#show wireless wps rogue client summary

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. L'exemple de sortie suivant montre les détails sur le client indésirable avec l'adresse MAC 0021.6a9b.b944, qui a été détecté par un AP géré 9130 sur le canal 132, la sortie suivante montre

plus de détails :

```
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
```

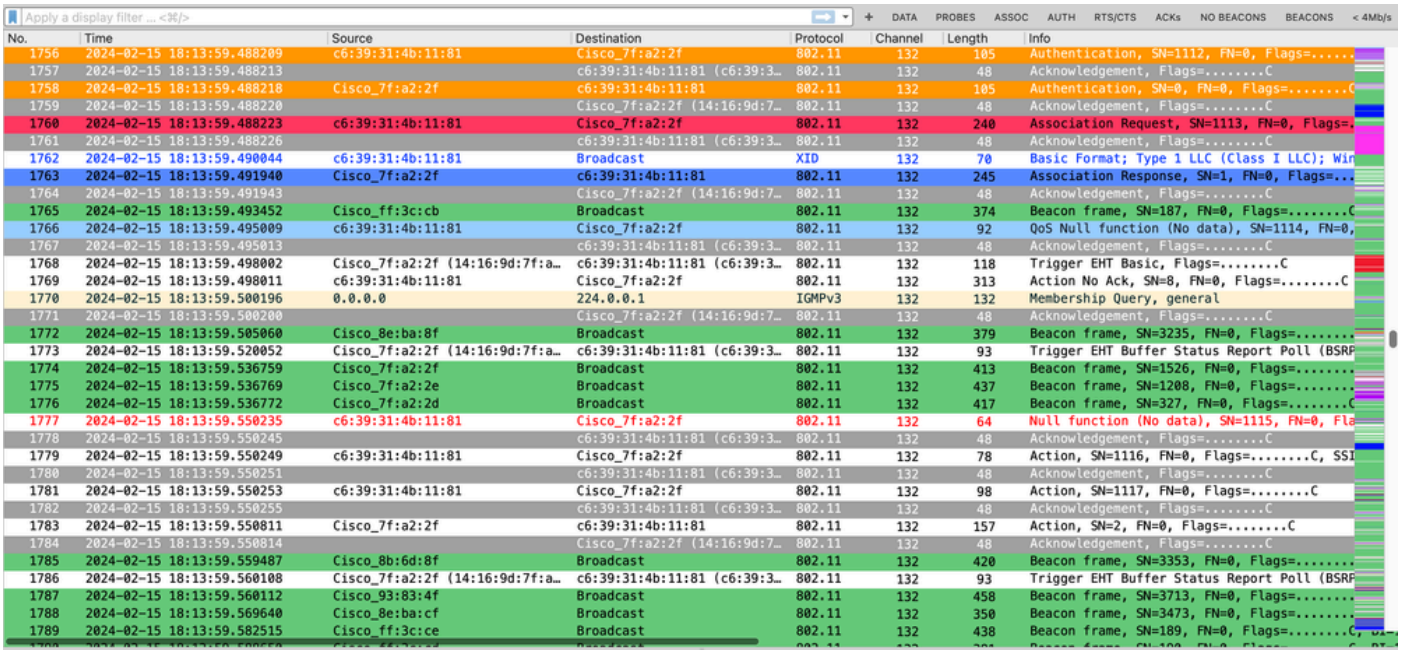
3. Après avoir collecté une capture en direct sur le même canal, vous pouvez voir que vous avez une inondation désauthentifiée, où le client non autorisé utilise l'un des BSSID de point d'accès géré pour déconnecter les clients :



OTA de désauthentification

La valeur RSSI des paquets est élevée, ce qui signifie que le client non autorisé se trouve physiquement à proximité du point d'accès géré.

4. Après avoir retiré le client indésirable du réseau, la figure suivante illustre un réseau propre et un environnement sain par liaison radio :



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); Wir
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=.....

Sain OTA

Informations connexes

- Gestion des périphériques indésirables
- Classification des points d'accès indésirables
- Analyse et dépannage de l'analyseur de réseau sans fil 802.11
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.