9800ワイヤレスコントローラ上の不正なAP/ク ライアントの特定と特定

内容
はじめに
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>シナリオ</u>
<u>シナリオ1:不正なアクセスポイントの検出と特定</u>
<u>シナリオ2:認証解除フラッドを送信する不正クライアントの検出と特定</u>
関連情報

はじめに

このドキュメントでは、9800ワイヤレスコントローラを使用して不正なアクセスポイント(AP)または不正なクライアントを検出して見つける方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

・ IEEE 802.11の基本

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ・ Cisco Wireless 9800-LコントローラIOS® XE 17.12.1
- ・ Cisco Catalyst 9130AXIシリーズアクセスポイント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

シスコの不正なアクセスポイントとは、ネットワーク管理者の知らないうちに、またはネットワ ーク管理者の承認なしにネットワークにインストールされた不正なワイヤレスアクセスポイント のことです。これらの不正なアクセスポイントは、ネットワークにセキュリティリスクを与える 可能性があり、攻撃者はこれを利用して不正アクセスを取得し、機密情報を傍受し、その他の悪 意のある活動を開始することができます。<u>Cisco Wireless Intrusion Prevention System(WIPS)</u>は 、不正なアクセスポイントを特定して管理するように設計されたソリューションです。

シスコの不正クライアントは、不正なステーションまたは不正なデバイスとも呼ばれ、不正なア クセスポイントに接続された、不正で潜在的に悪意のあるワイヤレスクライアントデバイスを指 します。不正なアクセスポイントと同様に、攻撃者は適切な許可なしにネットワークに接続でき るため、不正なクライアントはセキュリティリスクをもたらします。シスコは、不正なクライア ントの検出と緩和を支援するツールとソリューションを提供して、ネットワークセキュリティを 維持します。

シナリオ

シナリオ1:不正なアクセスポイントの検出と特定

次の手順では、9800ワイヤレスコントローラを使用して、ユーザネットワークによって管理され ていない不正なクライアントやアクセスポイントを検出する方法を示します。

1. ワイヤレスコントローラを使用して、不正デバイスを検出したアクセスポイントを特定しま す。

GUIでは、Monitoringタブ、Wirelessの順に選択し、Rogueを選択します。次に、フィルタを使用 して不正デバイスを見つけ、CLIでは、show wireless wps rogue ap summaryコマンドを使用して すべての検出された不正デバイスを表示するか、またはshow wireless wps rogue ap detailed <mac-addr>コマンドを使用して特定の不正デバイスの詳細を表示できます。

show wireless wps rogue ap summaryコマンドを使用して不正デバイスのリストを表示したCLIの 結果を次に示します。

```
9800L#show wireless wps rogue ap summary
Roque 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
Roque AP timeout : 1200
Roque 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	1416.9d71	F.a220	-62	140	80	5
00a6.ca8e.bacf	Unclassified	Alert	1	0	01/31/2024	21:27:50	1416.9d71	F.a220	-53	140	40	5
00f6.630d.e5c0	Unclassified	Alert	1	0	01/31/2024	21:28:09	1416.9d7	F.a220	-48	1 2	02	.4
00f6.630d.e5cf	Unclassified	Alert	1	0	01/31/2024	21:27:40	1416.9d7	F.a220	-72	128	20	5
04f0.212d.20a8	Unclassified	Alert	1	0	01/31/2024	21:27:19	1416.9d7	F.a220	-81	1 2	02	.4
04f0.2148.7bda	Unclassified	Alert	1	0	01/31/2024	21:24:19	1416.9d7	F.a220	-82	1 2	02	.4
0c85.259e.3f30	Unclassified	Alert	1	0	01/31/2024	21:21:30	1416.9d7	F.a220	-63	11	20	2.4
0c85.259e.3f32	Unclassified	Alert	1	0	01/31/2024	21:21:30	1416.9d71	F.a220	-63	11	20	2.4
0c85.259e.3f3c	Unclassified	Alert	1	0	01/31/2024	21:27:30	1416.9d71	F.a220	-83	64	20	5
0c85.259e.3f3d	Unclassified	Alert	1	0	01/31/2024	21:27:30	1416.9d71	F.a220	-82	64	20	5
0c85.259e.3f3f	Unclassified	Alert	1	0	01/31/2024	21:27:30	1416.9d71	F.a220	-82	64	20	5
12b3.d617.aac1	Unclassified	Alert	1	0	01/31/2024	21:28:09	1416.9d71	F.a220	-72	1 2	02	.4
204c.9e4b.00ef	Unclassified	Alert	1	0	01/31/2024	21:27:40	1416.9d71	F.a220	-59	116	20	5
22ad.56a5.fa54	Unclassified	Alert	1	0	01/31/2024	21:28:09	1416.9d71	F.a220	-85	1 2	02	.4
4136.5afc.f8d5	Unclassified	Alert	1	0	01/31/2024	21:27:30	1416.9d71	F.a220	-58	36	20	5
5009.59eb.7b93	Unclassified	Alert	1	0	01/31/2024	21:28:09	1416.9d71	F.a220	-86	1 2	02	.4
683b.78fa.3400	Unclassified	Alert	1	0	01/31/2024	21:28:00	1416.9d71	F.a220	-69	6 2	02	.4
683b.78fa.3401	Unclassified	Alert	1	0	01/31/2024	21:28:00	1416.9d71	F.a220	-69	6 2	02	.4
683b.78fa.3402	Unclassified	Alert	1	0	01/31/2024	21:28:00	1416.9d71	F.a220	-72	6 2	02	.4
683b.78fa.3403	Unclassified	Alert	1	0	01/31/2024	21:28:00	1416.9d71	F.a220	-72	6 2	02	.4

2.9800コントローラ上で設定されたWLANの1つをフィルタリングして、同じWLANをブロード キャストする不正デバイスがないかどうかを確認できます。次の図は、C9130が両方の帯域でこ の不正を検出した結果を示しています。

¢	altalta cisco	Cisco Cata	lyst 980	00-L Wireless	s Controller	Welcome ros	alia 🖌 倄		* 10 0	Search AP	and Clients Q		eedback	2 🕩
0	Search Menu Ite	ems	Monito	oring • > Wirele	ss ▼ > Rogues									
	Dashboard		Unclas	ssified Friend	dly Malicious	Custom	Ignore List	Rogue Clien	ts Adhoc R	ogues				
3	Monitoring	>		C Delete										
Ľ	Configuration	ı >	Tota	I APs : 2	ins" roque									
Ś	Administratio	n >	Lost		ria logue 🖌 Y									
C	Licensing		0	MAC Y Address	#Detecting T Radios	Number of T Clients	Status Y	Last Heard	Last Heard Y SSID	Highest RSSI Y Channel	Channel T Width	Band T	PMF Required	Ŧ
×	Troubleshoot	ing	O	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	
			ų.	< 1 > →	10 🔻							1 - 3	2 of 2 items	Ċ
	Mole Ma Theory													
	waik me Inroug													

GUIの不正リスト

3.不正デバイスを検出したアクセスポイントをリストします。

不正デバイスを検出したAPを表示できます。次の図に、この不正デバイスを検出したAP、チャ ネル、RSSI値などを示します。

Cisco Cata	alyst 9800-L Wireless	s Controller Welcome	rosalia	a 10	A	B ¢	1	02	Search APs a	nd Clients	2	Fee	dback 🛃 🕞
Q Search Menu Items	Monitoring - > Wire	Rogue AP Detail											×
Bashboard	Unclassified Frie	MAC Address	6c8d.779	3.8340				First time On	Reported	01/31/2	2024 19:	26:49	
Monitoring >	× Delete	Is this radio on wired network? Class Type	No Unclassifie	No Unclassified				Last time Reported 01/3 On		01/31/2	1/2024 21:10:49		
Configuration >	Total APs : 2	Status	ALERT										
Administration	Last Heard SSID Con	Initiate RLDP	0										
© Licensing	Address	Is Rogue an impersonator ?	No										
X Troubleshooting	6c8d.7793.834L	APs that detected this Rog	ue										
	6c8d.7793.834f						Cha						
		Base Radio MAC AP Name	SSID	Cha	Cha Width	Band	from DS	Radio	Security Policy	Short Preamble	RSSI (dBm)	SNR (dB)	Containment Type
Walk Me Through >		1416.9d7f.a2; C9130	RogueTest	1	20	2.4 GHz	Yes	dot11g, dot11ax - 2.4 GHz	Open	Enabled	-35	60	N/A
		Cancel									🗒 U	pdate &	Apply to Device

GUIの不正APの詳細

CLIから、コマンドshow wireless wps rogue ap detailed <mac-addr>を使用してこの情報を表示できます。

4.最も近いRSSI値に基づいて、不正デバイスに最も近いアクセスポイントを見つけます。

不正デバイスが検出されたアクセスポイントの数の結果に基づいて、ワイヤレスコントローラに 表示されるRSSI値に基づいて最も近いAPを探す必要があります。次の例では、1つのAPのみが不 正を検出していますが、RSSI値が高いため、不正デバイスはAPのすぐ近くにあります。

次に、show wireless wps rogue ap detailed <mac-addr>コマンドの出力を示します。これは、 AP/WLCがこの不正デバイスを検出したチャネルと、RSSI値を表示します。

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.同じチャネルでOver-the-Air Capture(OTAP)を収集して、不正の場所を特定します。

この不正なAPがブロードキャストしているチャネルが検出され、RSSI値に基づいて、9130アク セスポイントはこの不正を–35 dBmで受信しました。これは非常に近いと見なされ、この不正が 存在するエリアを特定できます。次のステップは、地上波キャプチャを収集することです。

次の図は、チャネル36の地上波キャプチャを示しています。OTAから、不正APが管理対象アクセ スポイントに対して封じ込め認証解除攻撃を実行していることがわかります。

No.	Time	Source	Destination	Protocol Leng	th	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. Flaos=C
> Frame 7:	66 bytes on wire (528 bits).	66 bytes captured (528	bits)			
> Radiotap	Header v0. Length 36					
< 802.11 ra	dio information					
PHY ty	pe: 802.11a (OFDM) (5)					
Turbo	type: Non-turbo (0)					
Data r	ate: 6.0 Mb/s					
Channe	1: 36					
Freque	ncv: 5180MHz					
Signal	strength (dBm): -61 dBm					
Noise	level (dBm): -97 dBm					
Signal	/noise ratio (dB): 36 dB					
TSF ti	mestamp: 2032467034					
> [Durat	ion: 64usl					
IEEE 802.	11 Deauthentication, Flags: .	C				
TEEE 002	11 Wiseless Management					

不正AP OTAキャプチャ

前の図の情報を使用して、この不正の近さを把握し、少なくとも、この不正なアクセスポイント が物理的にどこにあるのかを把握できます。不正APの無線MACアドレスを使用してフィルタリン グできます。地上波のビーコンパケットがあるかどうかを確認すれば、不正が現在アクティブか どうかを確認できます。

シナリオ2:認証解除フラッドを送信する不正クライアントの検出と特定

次の手順では、9800ワイヤレスコントローラを使用して、ユーザネットワークによって管理され ていない不正アクセスポイントに接続されている不正クライアントや、認証解除攻撃を行う不正 クライアントを見つける方法を示します。

1.ワイヤレスコントローラを使用して不正クライアントを見つけます。

ワイヤレスコントローラのGUIで、MonitoringタブのWirelessに移動し、Rogue Clientsを選択する か、CLIからshow wireless wps rogue client summaryコマンドを使用して、コントローラで検出 された不正クライアントを一覧表示できます。

Cisco Cisco	co Catalys	st 9800	-L Wireless Controller	Weld	come rosalia 🛛 🐔		¢	Search APs and Clients	Q Feedback	×* 🕩
Q. Search Menu Items		Monitorin	g - > Wireless - > Rogues							
Dashboard		Unclassif	ed Friendly Malicious	Cus	tom Ignore List	Rogue Clients	,	Adhoc Rogues		
	>	×D	lelete							
Configuration	>	Number	r of Clients: 48							
C Administration	>		MAC Address	Ŧ	#Detecting Radios		Ŧ	Last Seen On	Status	Ŧ
~			0021.6a9b.b944		1			02/15/2024 17:21:34	Alert	
C Licensing			0cb8.1575.8a5c		1			02/15/2024 17:08:14	Alert	
			1a59.5f0f.cae0		1			02/15/2024 17:20:44	Alert	
Moubleshooting			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	
Walk Me Through >			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	
		- w - 2	1 2 2 4 5 1		10				1 - 10 of 49 itoms	c.

不正クライアントリストGUI

次の出力は、CLIの結果を示しています。

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 17:20:24
70f3.5a7c.f850 Alert 1 02/15/2024 17:19:04
70f3.5a7f.8971 Alert 1 02/15/2024 17:16:44
...
```

2.次の出力例は、MACアドレス0021.6a9b.b944を持つ不正クライアントに関する詳細を示してい ます。これは、チャネル132の管理対象AP 9130によって検出されたものです。次の出力は詳細を 示しています。

_____ ___

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.同じチャネルでOver-the-Airキャプチャを収集した後、認証解除フラッドが発生し、不正クライ アントが管理対象アクセスポイントの1つのBSSIDを使用してクライアントを切断していることが わかります。

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=
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=
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				
> Radio1	tap Header v0, Length 18						
~ 802.11	l radio information						
PHY	type: 802.11a (OFDM) (5)						
Tur	bo type: Non-turbo (0)						
Dat	a rate: 24.0 Mb/s						
Cha	nnel: 132						
Fre	quency: 5660MHz						
Sig	nal strength (dBm): -64 dBm						
> [Du	ration: 148µs]						

認証解除OTA

パケットのRSSI値が高いため、不正なクライアントが管理対象アクセスポイントの物理的な近く にあることを意味します。

4.ネットワークから不正クライアントを削除した後、次の図はクリーンなネットワークと健全な Over-the-Air環境を示しています。

Apply a	display filter <%/>				+ DATA	PROBES AS	SOC AUTH F	RTS/CTS	ACKs NO BEACONS	BEACONS	< 4Mb/s
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	Authentic	ation, S	SN=1112, FN=0, M	⁼lags=	
1757											
1758											.0
1759								igement,			
1760	2024-02-15 18:13:59.488223	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11	132	240	Associati	on Reque	est, SN=1113, FM	I=0, Flags	.=.
1761	2024-02-15 18:13:59.488226			802.11				igement,			
1762	2024-02-15 18:13:59.490044	c6:39:31:4b:11:81	Broadcast	XID	132	70	Basic For	mat; Typ	pe 1 LLC (Class	I LLC); W	/in
1763	2024-02-15 18:13:59.491940	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11	132	245	Associati	on Respo	onse, SN=1, FN=6), Flags=.	•••
1764											
1765	2024-02-15 18:13:59.493452	Cisco_ff:3c:cb	Broadcast	802.11	132	374	Beacon fr	ame, SN:	=187, FN=0, Flag	s=	.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	n (No data), SN⊧	=1114, FN=	-0,
1767	2024-02-15 18:13:59.495013		c6:39:31:4b:11:81 (c6:39:3				Acknowled	lgement,	Flags=		
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 E	HT Basic	c, 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, St	N=8, FN=0, Flags	;=	.c
1770	2024-02-15 18:13:59.500196	0.0.0	224.0.0.1	IGMPv3	132	132	Membershi	p Query,	, general		
1771	2024-02-15 18:13:59.500200		Cisco_7f:a2:2f (14:16:9d:7	802.11	132	48	Acknowled	gement,	Flags=		
1772	2024-02-15 18:13:59.505060	Cisco_8e:ba:8f	Broadcast	802.11	132	379	Beacon fr	ame, SN:	=3235, FN=0, Fla	ngs=	
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 E	HT Buffe	er Status Report	: Poll (BS	SRP
1774	2024-02-15 18:13:59.536759	Cisco_7f:a2:2f	Broadcast	802.11	132	413	Beacon fr	ame, SN:	=1526, FN=0, Fla	igs=	
1775	2024-02-15 18:13:59.536769	Cisco_7f:a2:2e	Broadcast	802.11	132	437	Beacon fr	ame, SN:	=1208, FN=0, Fla	ags=	
1776	2024-02-15 18:13:59.536772	Cisco_7f:a2:2d	Broadcast	802.11	132	417	Beacon fr	ame, SN:	=327, FN=0, Flag	s=	. c
1777	2024-02-15 18:13:59.550235	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11	132	64	Null func	tion (Nr	o data), SN=111	5, FN=0, F	la
1778	2024-02-15 18:13:59.550245		c6:39:31:4b:11:81 (c6:39:3	802.11	132	48	Acknowled	igement,	Flags=		
1779	2024-02-15 18:13:59.550249	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11	132	78	Action, S	N=1116,	FN=0, Flags=	C, S	SI
1780	2024-02-15 18:13:59.550251		c6:39:31:4b:11:81 (c6:39:3	802.11	132	48	Acknowled	igement,	Flags=		
1781	2024-02-15 18:13:59.550253	c6:39:31:4b:11:81	Cisco_7f:a2:2f	802.11	132	98	Action, S	N=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	Acknowled	igement,	Flags=		
1783	2024-02-15 18:13:59.550811	Cisco_7f:a2:2f	c6:39:31:4b:11:81	802.11	132	157	Action, S	N=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	Acknowled	igement,	Flags=		
1785	2024-02-15 18:13:59.559487	Cisco_8b:6d:8f	Broadcast	802.11	132	420	Beacon fr	ame, SN:	=3353, FN=0, Fla	ags=	
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 E	HT Buffe	er Status Report	Poll (BS	SRF
1787	2024-02-15 18:13:59.560112	Cisco_93:83:4f	Broadcast	802.11	132	458	Beacon fr	ame, SN:	=3713, FN=0, Fla	ags=	
1788	2024-02-15 18:13:59.569640	Cisco_8e:ba:cf	Broadcast	802.11	132	350	Beacon fr	ame, SN:	=3473, FN=0, Fla	gs=	
1789	2024-02-15 18:13:59.582515	Cisco_ff:3c:ce	Broadcast	802.11	132	438	Beacon fr	ame, SN:	=189, FN=0, Flag	s=	

健全なOTA

関連情報

- <u>不正デバイスの管理</u>
- 不正なアクセスポイントの分類
- <u>802.11 ワイヤレススニッフィングの分析とトラブルシュート</u>
- シスコのテクニカルサポートとダウンロード

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。