# Catalyst 9800ワイヤレスコントローラのスニフ ァモードでのアクセスポイントの設定

### 内容

概要
前提条件
要件
使用するコンポーネント
設定
ネットワーク図
設定
GUIによるスニファモードでのAPの設定
CLIによるスニファモードでのAPの設定
GUIを使用してチャネルをスキャンするようにAPを設定する
CLIを使用してチャネルをスキャンするためのAPの設定
パケットキャプチャを収集するためのWiresharkの設定
確認
トラブルシュート
関連情報

### 概要

このドキュメントでは、Graphic User Interface(GUI)またはCommand Line Interface (CLI;コマ ンドラインインターフェイス)を使用して、Catalyst 9800シリーズワイヤレスコントローラ (9800 WLC)のスニファモードでアクセスポイント(AP)を設定する方法と、Air(PCAP)を収集する 方法について説明しますワイヤレスビヘイビアーのトラブルシューティングと分析を行うために 、スニファAPを使用します。

# 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。

- ・9800 WLCの設定
- ・802.11規格の基礎知識

### 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。

- AP 2802
- 9800 WLC Cisco IOS®-XEバージョン17.3.2a

Wireshark 3.X

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、初期(デフォルト)設定の状態から起動しています 。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。

### 設定

考慮するべき事柄:

- スニファAPをターゲットデバイスと、このデバイスが接続されているAPの近くにすることを 推奨します。
- ・使用する802.11チャネルと幅、クライアントデバイスとAPを確認します。

ネットワーク図



#### 設定

GUIによるスニファモードでのAPの設定

ステップ1:図に示すように、9800 WLC GUIで、[**Configuration] > [Wireless] > [Access Points] >** [All Access Points]に移動します。



Q	Search Menu Items		Interface	Ø	Services	
			Logical		AireOS Config Translate	or
	Dashboard		Ethernet		Application Visibility	
رددی			Wireless		Cloud Services	
$\bigcirc$	Monitoring	、 よ	Laver2		Custom Application	
I	wonitoning	/ 000	Discover Protocolo		IOx	
N	Orafanatian		Discovery Protocols		mDNS	
S	Configuration	>			Multicast	
~~			VIP		NetFlow	
र्छ	Administration	»اله <	Radio Configurations		Python Sandbox	
			CleanAir		QoS	
C	Licensing		High Throughput		RA Throttle Policy	
_			Media Parameters	<u>≣8</u> 8≣	Tags & Profiles	
X	Troubleshooting		Network		AP Join	
			Parameters		EoGRE	
			RRM		Flex	
		(Ir	Routing Protocols		Policy	
			Statia Douting		Remote LAN	
		~	Static Routing		RF	
		$\oplus$	Security		Tags	
			ААА		WLANs	
			ACL	0	Wireless	
			Advanced EAP			
			PKI Management		Access Points	
			Guest User		Advanced	
			Local EAP		Air Time Fairness	
			Local Policy		Fabric	

ステップ2:スニファモードで使用するAPを選択します。図に示すように**[General]**タブで、APの 名前を更新します。

Cisco Catal	Cisco Catalyst 9800-CL Wireless Controller											
Q Search Menu Items	Configuration > Wir	eless * >	Access Poir	nts	ł	Edit AP						
Dashboard	<ul> <li>All Access Point</li> <li>Number of AP(s): 1</li> </ul>	,	General Interfaces General	High Availability Inventory								
Monitoring >						AP Name*	2802-carcerva-sniffer					
Configuration	AP V AP V Name Model	Slots ~	Admin v Status	IP ~ Address	B; M	Location*	default location					
(O) Administration >	2802- AIR- carcerva AP2802I- & B-K9	2	٥	• 172.16.0.125		Base Radio MAC	a03d.6f92.9400					
C Licensing		10 🔻 it	ems per page			Ethernet MAC	00a2.eedf.6114					
💥 Troubleshooting	5 GHz Radios		Admin Status	ENABLED								
						AP Mode	Flex v					
	> 2.4 GHz Radio	Operation Status	Registered									

ステップ3 : 図に示すように、[Admin Status] が[Enabled] であることを確認し、[**AP Mode**]を [**Sniffer**]に変更します。

¢	cisco		Welcome admin 🛛 🌴 📢							
Q	Search Menu Ite	ems	Configurat	ion • > Wir	eless * >	Access Poi	nts	I	Edit AP	
	Dashboard Monitoring	,	Vumber of A	Access Poi P(s): 1	nts		General Interfaces General	High Availability Inventory		
n N	Configuration	n >	AP Name	~ AP ~ Model	Slots	Admin ~ ~ Status	IP v Address	B; M	AP Name* Location*	2802-carcerva-sniffer default location
ঠ্যে	Administratic	on >	2802- carcerva	AIR- AP2802I- B-K9	2	۲	172.16.0.125	a	Base Radio MAC	a03d.6f92.9400
C	Licensing		H 4	1 ⊨	10 🔻	items per page			Ethernet MAC	00a2.eedf.6114
X	Troubleshoo	ting		U- Dedies					Admin Status	
	> 5 GHz Radios								AP Mode	Sniffer 🔻
			> 2.4	Operation Status	Registered					

次の注記がポップアップに表示されます。

"警告:APモードを変更すると、APがリブートします。[Update & Apply to Device to Proceed]を クリックします。

図に示すように[OK]を選択します。



ステップ4:図に示すように、[Update & Apply to Device]をクリックします。

Edit AP								×	
General	Interfaces	High Availability	Inventory	ICap	Advanced	Support Bundle			
General				Version					
AP Name	*	2802-carcerva-sn	iffer	Primary Sof	ftware Version	17.3.2.32			
Location*		default location	Predownloa	aded Status	N/A	N/A			
Base Rad	io MAC	a03d.6f92.9400	Predownloa	aded Version	N/A	N/A			
Ethernet 1	VAC	00a2.eedf.6114		Next Retry	Time	N/A	N/A		
Admin Sta	atus	ENABLED		Boot Versio	n	1.1.2.4			
AP Mode		Sniffer	Sniffer 🔻		ı	17.3.2.32		-	
Operation	Status	Registered	Registered		ersion	0.0.0.0			
Fabric Sta	atus	Disabled		IP Config		lided As:			
LED State		ENABLED	ENABLED		referred Mode	IPv4		sistance	
LED Brigh Level	tness	8	•	DHCP IPv4	Address	172.16.0.125			
<u> </u>				Static IP (IP	v4/IPv6)	0			
Cancel						📑 Update	e & Apply to Dev	vice	

図に示すように、変更とAPのバウンスを確認するポップアップが表示されます。



#### CLIによるスニファモードでのAPの設定

ステップ1:スニファモードとして使用するAPを特定し、AP名を取得します。

ステップ2:AP名を変更します。

このコマンドは、AP名を変更します。ここで、<AP-name>はAPの現在の名前です。

carcerva-9k-upg#**ap name** <AP-name> **name 2802-carcerva-sniffer** ステップ3:スニファモードでAPを設定します。

carcerva-9k-upg#ap name 2802-carcerva-sniffer mode sniffer

#### GUIを使用してチャネルをスキャンするようにAPを設定する

ステップ1:9800 WLC GUIで、[Configuration] > [Wireless] > [Access Points]に移動します。

ステップ2:[アク**セスポイ**ント]ページで、[**5 GHz Radios**]または[**2.4 GHz Radios]メニュ**ーリスト を表示します。これは、図に示すように、スキャンするチャネルによって異なります。



ステップ2:APを検索します。矢印をクリックし**て検索ツー**ルを表示し、ドロップダウンリストから[Contains]を選択し、図に示すようにAP名を入力します。

Cisco Cataly	rst 9800-CL Wireless Controller Welcome admin 🛛 🎓 🖺 🌣 🖄 🥝 😂
Q. Search Menu Items	Configuration > Wireless > Access Points
📰 Dashboard	> All Access Points
Monitoring >	✓ 5 GHz Radios
Configuration >	Number of AP(s): 1
O Administration	AP Name Slot No v MAC Status S
© Licensing	2802-carcerva- sniffer       Show items with value that: Contains       400       Image: Contains the state of the s
X Troubleshooting	> 2.4 GHz R

ステップ3:APを選択し、図に示すように、[Configure] **> [Sniffer Channel Assignment]の下の [Enable Sniffer]チェックボックスをオン**にします。

Cisco Catal	yst 9800–CL Wirele	ess Controller	Welcome admin 🕋 🜾			
Q Search Menu Items	Configuration - W	Edit Radios 5 GHz Band	ł			
Dashboard	> All Access P	Configure Detail	UIIIII			
Monitoring >	✓ 5 GHz Radios	Antenna A Antenna B	Ø			
Configuration >	Number of AP(s): 1	Antenna C	Ø			
Administration →	AD Name	Antenna D	Ø			
C Licensing	2802-carcerva-	Antenna Gain	10			
X Troubleshooting		Sniffer Channel Assignment				
	2 4 GHz Padi	Enable Sniffing	Ø			
		Sniff Channel	36 🔻			
	Dual-Band R	Sniffer IP*	172.16.0.190			
	Country	Sniffer IP Status	Valid			
	LSC Provisio	Download Core Dump to be	ootflash			
		Cancel				

ステップ4:図に示すように、[Sniff Channel]ドロップダウン**リストから[Channel]**を選択し、 [Sniffer IP address (Server IP address with Wireshark)]を入力します。

Cisco Cisco Cata	lyst 9800-CL Wireless Controller	Welcome admin 🛛 👫 🛭 🕵
Q. Search Menu Items	Configuration - > W Edit Radios 5 GHz	Band
Dashboard	> All Access P	Unnii
Monitoring >	Antenna A S GHz Radio:	Ø
	Antenna B Number of AP(s): 1	Ø
Configuration >	AP Name " Contains"	Ø
() Administration >	Antenna D	$\oslash$
© Licensing	AP Name Antenna Gain	10
K Troubleshooting	Sniffer Channel As	signment
	Enable Sniffing	Ø
	Sniff Channel	36 🔹
	> Dual-Band R Sniffer IP*	172.16.0.190
	Sniffer IP Status Country	Valid
	Download Core Dum	p to bootflash
	"Cancel	

ステップ5:接続先デバイスとAPで使用するチャネル幅を選択します。

図に示すように、[Configure] > [RF Channel Assignment]に移動してこれを設定します。

		Edit Radios 5 GHz Band									
Dashboard	<ul> <li>All Access Po</li> </ul>	Configure Detail									
Monitoring >	Number of AP(s): 1	General		RF Channel Assignment							
Configuration	AP ~ AP Name Model	AP Name	2802-carcerva-	Current Channel	36						
() Administration	2802- AIR- carcerva- AP2802	Admin Status		Channel Width	40 MHz 🔻						
C Licensing	sniffer → B-K9	CleanAir Admin Status		Assignment Method	20 MHz 40 MHz						
X Troubleshooting		Antenna Parameters		Channel Number	80 MHz 160 MHz						
	5 GHz Radios			Tx Power Level Assignment							
	Number of AP(s): 1	Antenna Type	Internal v	Current Tx Power Level	6						
	AP Name v	Antenna Mode	Omni	Assignment Method	Quetom						
	2802-carcerva-	Antenna A	Ø	Assignment Method	Custom Y						
	∈ ⊲ 1 ⊳	Antenna B	Ø	i ransmit Power	• •						

#### CLIを使用してチャネルをスキャンするためのAPの設定

ステップ1:APでチャネルスニフを有効にします。次のコマンドを実行します。

carcerva-9k-upg#ap name <ap-name> sniff {dot11a for 5GHz | dot11bfor 2.4GHz | dual-band}

例:

carcerva-9k-upg#ap name 2802-carcerva-sniffer sniff dot11a 36 172.16.0.190 パケットキャプチャを収集するためのWiresharkの設定

ステップ1:Wiresharkを起動します。

ステップ2:図に示すように、Wireshark**から[Capture options]**メニューアイコンを選択します。



ステップ3:ポップアップウィンドウが表示されます。図に示すように、キャプチャのソースとして[Wired Interface]をリストから選択します。

un4 BSD loopback un5 BSD loopback un5 BSD loopback	✓ default 2 ✓ default 2 ✓ default 2
un5 BSD loopback	default 2
un0 200 loopbaak	
SB 10/100/1000 LAN: en10 Ethernet	🗸 default 2 -
ephaski la0	elefeult 2
i-Fi: en0 Ethernet	🗹 default 2
nunderbolt Bridge: bridge0 Ethernet	🗹 default 2 -
nunderbolt 1: en1 Ethernet	🗹 default 2 -
nunderbolt 2: en2 Ethernet	🗹 default 2 -
nunderbolt 3: en3 Ethernet	🗹 default 2 -
nunderbolt 1: en1      Ethernet       nunderbolt 2: en2      Ethernet       nunderbolt 3: en3      Ethernet	<ul> <li>✓ default 2</li> <li>✓ default 2</li> <li>✓ default 2</li> <li>✓ default 2</li> </ul>

ステップ4:[**Capture filter for selected interfaces:** 図に示すように、フィールド**ボックスにudpポー** ト555と入力します。

Interface	7	Link laure blooder	Desertes	0	Duffer (MD)	a and a start	Contract Filter
		Link-layer Header	Promisc	detault	Z	Monitor	Capture Filter
▶ utun4		BSD loopback	<b>S</b>	default	2		
▶ utun5		BSD loopback	<b>S</b>	default	2		
utun6		BSD loopback	<b>S</b>	default	2		
USB 10/100/1000 LAN: en10	0	Ethernet		default	2		udp port 5555
Loopback: lo0	And And American	Mark BSD loopback		default	2		
Wi-Fi: en0		Ethernet		default	2		
Thunderbolt Bridge: bridge	0	Ethernet		default	2		
Thunderbolt 1: en1		Ethernet		default	2		
Thunderbolt 2: en2		Ethernet		default	2		
Thunderbolt 3: en3		Ethernet		default	2		
Enable promiscuous mode or     Capture filter for selected interfi	n all interfaces aces: 🔲 udp port 5555					•	lanage Interfaces Compile BPFs

ステップ5:図に示すように、[Start]をクリックします。

terface	Traffic	Link-layer Header	Promisci	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
▶ utun3		_ вор юорраск	<u> </u>	detault	2		
▶ utun4		BSD loopback		default	2		
⊳ utun5		BSD loopback		default	2		
utun6		_ BSD loopback	Sec.	default	2	_	
<ul> <li>USB 10/100/1000 LAN: en10</li> </ul>		_ Ethernet	Sec.	default	2		udp port 5555
Loopback: lo0		BSD loopback	<b>S</b>	default	2		
Wi-Fi: en0		_ Ethernet		default	2		
Thunderbolt Bridge: bridge0		_ Ethernet		default	2		
Thunderbolt 1: en1		_ Ethernet	<b>S</b>	default	2		
Thunderbolt 2: en2		_ Ethernet	<b>S</b>	default	2		
Thunderbolt 3: en3		_ Ethernet		default	2		
Enable promiscuous mode on all ir	nterfaces						Nanage Interfaces
apture filter for selected interfaces:	udp port 5555				⊠	•	Compile BPFs

ステップ6:図に示すように、Wiresharkが必要な情報を収集するのを待ち、Wiresharkから [Stop]ボタンを選択します。



**ヒント**:WLANで事前共有キー(PSK)などの暗号化が使用されている場合は、APと目的のク ライアント間の4ウェイハンドシェイクがキャプチャされることを確認します。これは、デ バイスがWLANに関連付けられる前にOTA PCAPが起動する場合、またはキャプチャの実行 中にクライアントの認証と再認証が解除された場合に実行できます。

ステップ7:Wiresharkはパケットを自動的にデコードしません。パケットをデコードするには、キャプチャから行を選択し、右クリックしてオプションを表示し、図に示すようにDecode As...を 選択します。

4		] 🙍	0		0101 0110 0110	×	6	٩	<b>(</b>	⇒		ᢙ	<u> </u>	-		Ð	Q
	Apply	a displ	ay filter	· <೫/>													
Ν	o.		Time		Dest	Proto	col	So	urce Po	ort	Info					Signal	strer
٢	_	1	2021	-03	1	UDP		55	55		5555	<b>→</b>	5000	Len=	=400		
		2	2021	-03	1	UDP		55	55		5555	<b>→</b>	5000	Len=	-387		
		3	2021	-03	1	UDP		55	55		5555	<b>→</b>	5000	Len=	-385		
		4	2021	-03	1	UDP		55	55		5555	<b>→</b>	5000	Len=	=400		
		5	2021	-03	1	UDP		55	55		5555	<b>→</b>	5000	Len=	-387		
		6	2021	-03	1	UDP		55	55		5555	<b>→</b>	5000	Len=	-385		
		7	2021	-03	1	UDP		55	55		5555	<b>→</b>	5000	Len=	=400		
		8	2021	-03	1	UDP		55	55		5555		5000	Len=	=387		
		9	2021	-03	1	UDP		-	Mark	/Unma	ark Pac	ket		.en=	=385		
		10	2021	-03	1	UDP		-	Ignor	e/Uniç	gnore F	ack	et	.en=	=400		
		11	2021	-03	1	UDP		-	Set/L	Shift	I Ime R	eter	ence	.en=	=387		
		12	2021	-03	1	UDP		-	Pack	et Cor	 nment			.en=	=385		
		13	2021	-03	1	UDP		-	Tuen					.en=	=400		
		14	2021	-03	1	UDP		-	Edit I	Resolv	ed Nar	ne		.en=	=387		
		15	2021	-03	1	UDP			Apply	v as Fi	ilter		•	.en=	=385		
		16	2021	-03	1	UDP		-	Prepa	are as	Filter		•	.en=	=400		
		17	2021	-03	1	UDP		-	Conv	ersati	on Filte	er	►	.en=	=387		
		18	2021	-03	1	UDP		-	Colo	rize Co	onversa	atior	i 🕨	.en=	=385		
		19	2021	-03	1	UDP			SCTF	>			►	.en=	=400		
		20	2021	-03	1	UDP			Follo	w			•	.en=	=387		
		21	2021	-03	1	UDP			Copy	,			•	.en=	=385		
		22	2021	-03	1	UDP		1						.en=	=400		
		23	2021	-03	1	UDP			Droto	icel Dr	referen			en=	-387		
		24	2021	-03	1	UDP		1	Deco	de As		0144.0	wingow	en=	-385		
		25	2021	-03	1	UDP		1	SHOW	Раск		ew \	window	len=	-379		

ステップ8 : ポップアップウィンドウが表示されます。[add]ボタンを選択して新しいエントリを 追加し、次のオプションを選択します。**図に示すように、フィールドからのUDPポート、値から** 5555、デフォルトからSIGCOMP、および現在からPEEKREMOTE。



手順9:[OK]をクリックします。パケットがデコードされ、分析を開始する準備が整います。

### 確認

ここでは、設定が正常に機能しているかどうかを確認します。

9800 GUIからAPがスニファモードであることを確認するには、次の手順を実行します。

ステップ1:9800 WLC GUIで、[**Configuration**] > [**Wireless**] > [Access Points] > [All Access Points]に移動します。

ステップ2:APを検索します。矢印をクリックして検索ツールを表示し、ドロップダウンリストから[含**む]を選択**し、図に示すようにAP名を入力します。

Cisco Catalyst 9800-CL Wireless Controller

.1 1.1 1.



ステップ3:図に示すように、[Admin Status]に緑色のチェックマークが付いて、[AP Mode]に [Sniffer] が表示されていることを確認します。

¢	cisco Cisco	o Catalyst	t 9800-C	L Wireles	ss Contro	oller	Welcom	e admin 🛛 倄	<b>F</b>	¢ 🕸 0	Search /	APs and Clients C	λ	•
Q	Search Menu Items		Configuration	n≛> Wire	eless* > /	Access Poi	ints							
19	Dashboard   All Access Points													
C	Monitoring	Number of AP(s): 1												\$°
Ľ	Configuration	>	AP ~ Name	AP ~ Model	Slots ~	Admin v Status	IP ~ Address	Base Radio ~ ~ MAC	AP ~ Mode	Operation ~ Status	Configuration Status	Policy v Tag	Site v Tag	F
Ś	Administration	>	2802- carcerva- sniffer 🚠	AIR- AP2802I- B-K9	2	۰	172.16.0.125	a03d.6f92.9400	Sniffer	Registered	Healthy	webauth_test	default- site-tag	c r
C	Licensing		H 4	1 ⊩	10 🔻 ite	ems per page	•				1	- 1 of 1 access	points	c
×	Troubleshooting		E CU-	Dedies										

APが9800 CLIからスニファモードであることを確認するために。次のコマンドを実行します。

carcerva-9k-upg#show ap name 2802-carcerva-sniffer config general | i Administrative
Administrative State : Enabled
carcerva-9k-upg#show ap name 2802-carcerva-sniffer config general | i AP Mode
AP Mode : Sniffer
carcerva-9k-upg#show ap name 2802-carcerva-sniffer config dot11 5Ghz | i Sniff
AP Mode : Sniffer
Sniffing : Enabled
Sniff Channel : 36

Sniffer IP : 172.16.0.190 Sniffer IP Status : Valid Radio Mode : Sniffer

パケットがWiresharkでデコードされたことを確認します。図に示すように、プロト**コル**が UDPから802.11に変更さ**れ、ビーコンフ**レームが表示されます。

		ø	© 🖿		$\times$		٩	<b>(</b>	⇒	2	<u></u> €			Ð,	Q
Apply a display filter <\%/>															
No.		– I.	Time	Dest	Proto	col	Sou	urce Po	ort	Info				Signa	l stren
		1	2021–03–…	B	802	. 11	55	55		Beaco	n fi	rame,	SN=23	-39	dBm
		2	2021–03–…	В	802	. 11	55	55		Beaco	n fi	rame,	SN=23	-39	dBm
		3	2021–03–…	В	802	. 11	55	55		Beaco	n fi	rame,	SN=23	-39	dBm
		4	2021–03–…	В	802	. 11	55	55		Beaco	n fi	rame,	SN=23	-39	dBm
		5	2021–03–…	B	802	. 11	55	55		Beaco	n fi	rame,	SN=23	-39	dBm
		6	2021–03–…	В	802	. 11	55	55		Beaco	n fi	rame,	SN=23	-39	dBm
		7	2021–03–…	В	802	. 11	55	55		Beaco	n fi	rame,	SN=23	-39	dBm
		8	2021–03–…	B	802	. 11	55	55		Beaco	n fi	rame,	SN=23	-39	dBm
		9	2021–03–…	В	802	. 11	55	55		Beaco	n fi	rame,	SN=23	-39	dBm
		10	2021–03–…	В	802	. 11	55	55		Beaco	n fi	rame,	SN=23	-39	dBm
		11	2021–03–…	B	802	. 11	55	55		Beaco	n fi	rame,	SN=23	-39	dBm
		12	2021-03	B	802	.11	55	55		Beaco	n fi	rame,	SN=23	-39	dBm
		13	2021-03	B	802	. 11	55	55		Beaco	n fi	rame,	SN=23	-39	dBm

# トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

問題:WiresharkはAPからデータを受信しません。

ソリューション:Wiresharkサーバは、ワイヤレス管理インターフェイス(WMI)によって到達可能 である必要があります。 WiresharkサーバとWLCからのWMI間の到達可能性を確認してください 。

# 関連情報

- <u>Cisco Catalyst 9800シリーズワイヤレスコントローラソフトウェアコンフィギュレーション</u> ガイド、Cisco IOS XE Amsterdam 17.3.x - 章:スニファモード
- <u>802.11 ワイヤレス スニフィングの基礎</u>
- <u>テクニカル サポートとドキュメント Cisco Systems</u>