# **Configure Access Point in Sniffer Mode on Catalyst 9800 Wireless Controllers**

### Contents

Introduction
<u>Prerequisites</u>
Requirements
Components Used
Caveats
<u>Configure</u>
Network Diagram
Configurations
Configure AP in Sniffer Mode via GUI
Configure AP in Sniffer Mode via CLI
Configure AP to Scan a Channel via GUI
Configure AP to Scan a Channel via CLI
Configure Wireshark to Collect the Packet Capture
<u>Verify</u>
Troubleshoot
Related Information

## Introduction

This document describes how to configure an Access Point (AP) in Sniffer Mode on a Catalyst 9800 Series Wireless Controller (9800 WLC) through the Graphic User Interface (GUI) or Command Line Interface (CLI) and how to collect a Packet Capture (PCAP) Over the Air (OTA) with the sniffer AP in order to troubleshoot and analyze wireless behaviors.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- 9800 WLC configuration
- Basic knowledge in the 802.11 standard

#### **Components Used**

The information in this document is based on these software and hardware versions:

- AP 2802
- 9800 WLC Cisco IOS®-XE version 17.3.2a
- Wireshark 3.4.4 or higher

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. If your network is live, ensure that you understand the potential impact of any command.

### Caveats

Do not use the Sniffer Mode AP feature if the 9800 is connected to Cisco Application Centric Infrastructure (ACI) with default endpoint learning. The 9800 will transmit its UDP-encapsulated 802.11 captured packets sourced from the 9800's egress IP address, but with the source MAC address being the sniffer AP's radio's MAC, with low-order nibble set to 0x0F. This will cause problems as ACI will see the same IP address



sourced from multiple MAC addresses. See Cisco bug ID CSCwa45713

### Configure

Things to consider:

- It is recommended to have the sniffer AP close to the target device and the AP to which this device is connected.
- Ensure you know which 802.11 Channel and Width, the client device and the AP use.



**Note**: Sniffer mode is not supported when the controller L3 interface is the Wireless Mangement Interface (WMI).



Note: The AP in sniffer mode is not supported on 9800-CL deployed on a Public Cloud.

**Network Diagram** 



### Configurations

#### Configure AP in Sniffer Mode via GUI

Step 1. On the 9800 WLC GUI, navigate to **Configuration > Wireless > Acces Points > All Acces Points**, as shown in the image.

Cisco Cisco C	ata	alyst 98	300-CL Wireless Control	ler	
17.3.2a					
Q Search Menu Items			Interface	0	Services
			Logical		AireOS Config Translator
ashboard			Ethernet		Application Visibility
		_	Wireless		Cloud Services
	>	品	Layer2		Custom Application
	_		Discovery Protocols		
	>		VLAN		Multicast
			VTP		NetFlow
(O) Administration	>	<b>.1</b> ®	Radio Configurations		Python Sandbox
			CleanAir		QoS
© Licensing			High Throughout		RA Throttle Policy
Ŭ			Media Parameters	<u>≣ 8</u> 18 ≣	Tags & Profiles
💥 Troubleshooting			Network		AP Join
			Parameters		EoGRE
			RRM		Flex
		$(\hat{I}_{\mathbf{i}})$	Routing Protocols		Policy
			- Static Pouting		Remote LAN
		Â			RF
		$\forall$	Security		Tags
			ААА		WLANs
			ACL	Ş	Wireless
			Advanced EAP		Access Points
			PKI Management		Advanced
					Air Time Fairness
			Local Policy		Fabric

Step 2. Select the AP that is desired to be used in sniffer mode. On the **General** tab, update the name of the AP, as shown in the image.

Cisco Catal	lyst 9800-CL Wirele	ss Contro	oller				Welcome admin 🔗 🕏
Q. Search Menu Items	Configuration > Wir	eless* >	Access Poi	nts		Edit AP	
Dashboard	<ul> <li>All Access Po</li> <li>Number of AP(s): 1</li> </ul>	nts			0	General Interfaces General	High Availability Inventory
Configuration	AP v AP v	Clata	Admin ~	IP v	Bi	AP Name*	2802-carcerva-sniffer
Administration	2802- AIR- carcerva AP2802I-	2		172.16.0.125	a	Location* Base Radio MAC	default location a03d.6f92.9400
C Licensing		10 🔻 iti	ems per page			Ethernet MAC	00a2.eedf.6114
X Troubleshooting	> 5 GHz Radios					Admin Status	ENABLED
	> 2.4 GHz Radio	s				Operation Status	Registered

Step 3. Verify the Admin Status is Enabled and change the AP Mode to Sniffer, as shown in the image.

Cisco Cata	yst 9800-CL Wireless Controller			Welcome admin 🔗 😵
Q Search Menu Items	Configuration * > Wireless * > Access Points		Edit AP	
☐ Dashboard	All Access Points Number of AP(s): 1		General Interfaces General	High Availability Inventory
Configuration	AP v AP v Admin v IF Name Model Slots v Status A	v Ba ddress M	AP Name*	2802-carcerva-sniffer
Administration         >	2802- AIR- carcerva AP2802I- 2 🔮 11 B-K9	2.16.0.125 aC	Base Radio MAC	a03d.6f92.9400
C Licensing	I I ► 10 ▼ items per page		Ethernet MAC	00a2.eedf.6114
K Troubleshooting			Admin Status	
	5 GHz Radios		AP Mode	Sniffer 🔹
	> 2.4 GHz Radios		Operation Status	Registered

A pop-up window appears with the next alert:

"Warning: Changing the AP mode will cause the AP to reboot. Click Update & Apply to Device to Proceed" Select **OK**, as shown in the image.



Step 4. Click on Update & Apply to Device, as shown in the image.

Edit AP								×
General	Interfaces	High Availability	Inventory	ICap	Advanced	Support Bundle		
General				Version				
AP Name	k	2802-carcerva-sni	iffer	Primary Sof	tware Version	17.3.2.32		
Location*		default location		Predownloa	ded Status	N/A		
Base Radi	o MAC	a03d.6f92.9400		Predownloa	ded Version	N/A		
Ethernet N	AC	00a2.eedf.6114		Next Retry	Time	N/A		
Admin Sta	atus			Boot Versio	n	1.1.2.4		
AP Mode		Sniffer	•	IOS Version	I	17.3.2.32		-
Operation	Status	Registered		Mini IOS Ve	rsion	0.0.0.0		و و
Fabric Sta	itus	Disabled		IP Config				Jided As
LED State		ENABLED		CAPWAP P	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	& Apply to De	evice

A pop-up appears to confirm the changes and the AP bounces, as shown in the image.



#### **Configure AP in Sniffer Mode via CLI**

Step 1. Determine the AP that is desired to be used as Sniffer Mode and grab the AP Name.

Step 2. Modify the AP name.

This command modifies the AP name. Where <AP-name> is the current name of the AP.

<#root> carcerva-9k-upg# ap name <AP-name> name 2802-carcerva-sniffer

Step 3. Configure the AP in Sniffer mode.

<#root>

```
carcerva-9k-upg#
```

ap name 2802-carcerva-sniffer mode sniffer

#### Configure AP to Scan a Channel via GUI

Step 1. In the 9800 WLC GUI, navigate to Configuration > Wireless > Acces Points.

Step 2. On the Access Points page, display the **5 GHz Radios** or **2.4 GHz Radios** menu list. This depends on the channel that is desired to scan, as shown in the image.

Cisco Ca	st 9800-CL Wireless Controller Welcome admin 🖀 🕏 🖹 🏟 🖗 🕄 Search APs and Clients (	۵ 🕩
Q Search Menu Items	Configuration * > Wireless * > Access Points	
👼 Dashboard	> All Access Points	
Monitoring >	> 5 GHz Radios	
Configuration	> 2.4 GHz Radios	
Administration	> Dual-Band Radios	
C Licensing	<b>N</b> 2007	
X Troubleshooting	Country	

Step 2. Search the AP. Click on the **arrow down** button to display the search tool, select **Contains** from the dropdown list, and type the **AP name**, as shown in the image.

Cisco Catal	lyst 9800-CL Wireless Controller Welcome admin 💣 📽 🖺 🌞 👰	02
Q Search Menu Items	Configuration > Wireless > Access Points	
📰 Dashboard	> All Access Points	
Monitoring >	✓ 5 GHz Radios	
Configuration	Number of AP(s): 1	
র্বি Administration	AP Name Slot No v MAC Admin v Operation v Policy v AP Name Admin v Operation v Policy v Tag Site	a Tag ∼
© Licensing	2802-carcerva- sniffer Contains v 400 vebauth_test defined	ault-site-
X Troubleshooting	> 2.4 GHz R	

Step 3. Select the AP and tick the **Enable Sniffer** checkbox under the **Configure** > **Sniffer Channel Assignment**, as shown in the image.

Cisco Cá	atalyst 9800-CL Wirele	ess Controller	Welcome admin 🕋 🕏
Q Search Menu Items	Configuration ▼ > W	Edit Radios 5 GHz Ban	d
Dashboard	> All Access P	Configure Detail	Omm
	► 5 GHz Radios	Antenna A	Ø
Configuration	Number of AP(s): 1	Antenna B Antenna C	Ø
(O) Administration	AP Name " Contains"	Antenna D	Ø
C Licensing	AP Name 2802-carcerva-	Antenna Gain	10
X Troubleshooting	sniffer	Sniffer Channel Assign	ment
		Enable Sniffing	
	2.4 GHZ Rad	Sniff Channel	36 🔻
	> Dual-Band R	Sniffer IP*	172.16.0.190
	> Country	Sniffer IP Status	Valid
	> ISC Provisio	Download Core Dump to b	pootflash
		Cancel	

Step 4. Select the Channel from the **Sniff Channel** dropdown list and type the **Sniffer IP address** (Server IP address with Wireshark), as shown in the image.

Cisco Cata	alyst 9800–CL Wirele	ess Controller	Welcome admin 🕋 🕏
Q Search Menu Items	Configuration - > W	Edit Radios 5 GHz Ban	d
Dashboard	> All Access P		Omm
Monitoring >	💙 5 GHz Radios	Antenna A	Ø
	Number of AP(s): 1	Antenna B	
2 comgutation 2	AP Name " Contains"	Antenna C	Ø
{O} Administration >	AD Name	Antenna D	Ø
© Licensing	2802-carcerva-	Antenna Gain	10
X Troubleshooting	sniffer	Sniffer Channel Assign	ment
		Enable Sniffing	$\oslash$
	2.4 GHz Radi	Sniff Channel	36 🗸
	Dual-Band R	Sniffer IP*	172.16.0.190
	> Country	Sniffer IP Status	Valid
		Download Core Dump to b	pootflash
	LSC Provisio-	Cancel	

Step 5. Select the **Channel width** that the target device and the AP use when connected.

Navigate to **Configure > RF Channel Assignment** in order to configure this, as shown in the image.

			Edit Radios 5 GHz Bai	nd							
📰 Da	ashboard	<ul> <li>All Access</li> </ul>	Configure Detail	Configure Detail							
C Ma	onitoring >	Number of AP(s): 1	General		RF Channel Assignment						
Z Co	onfiguration >	AP ~ AP Name Mod	AP Name	2802-carcerva-	Current Channel	36					
bA (نَ)	dministration >	2802- AIR- carcerva- AP28	Admin Status		Channel Width	40 MHz 🔹					
© Lic	censing	shifter da B-KS	CleanAir Admin Status		Assignment Method	20 MHz 40 MHz					
💥 Tro	oubleshooting		Antenna Parameters		Channel Number	80 MHz 160 MHz					
		V 5 GHZ Rac	110		Tx Power Level Assignment	ent					
		Number of AP(s): I	Antenna Type	Internal v	Current Tx Power Level	6					
		AP Name	<ul> <li>Antenna Mode</li> </ul>	Omni		Quature					
		2802-carcerva- sniffer	Antenna A	Ø	Assignment Method	Custom V					
			Antenna B	Ø	Transmit Power	6					

#### Configure AP to Scan a Channel via CLI

Step 1. Enable the channel sniff on the AP. Run this command:

carcerva-9k-upg#
ap name 2802-carcerva-sniffer sniff dot11a 36 172.16.0.190

#### **Configure Wireshark to Collect the Packet Capture**

Step 1. Launch Wireshark.

Step 2. Select the Capture options menu icon from Wireshark, as shown in the image.



Step 3. This action displays a pop-up window. Select the Wired Interface from the list as the source of the capture, as shown in the image.

			Wire	eshark · Ca	pture Options				
ſ			Inpu	ıt Outp	ut Options				
	l	nterface   ▶ utup≾	Traffic		Link-layer Header	Promiscı	Snaplen (B)	Buffer (MB)	Monitor
		▶ utun4			BSD loopback		default	2	
		▶ utun5			BSD loopback		default	2	
	-	eteno			DOD loopback		d-flt	2	
	IF	USB 10/100/1000 LAN: en10			Ethernet	Image: A start and a start	default	2	_
	L				PSD loopbook		defeult	2	
		Wi-Fi: en0			Ethernet	<b>_</b>	default	2	
		Thunderbolt Bridge: bridge0			Ethernet		default	2	
		Thunderbolt 1: en1			Ethernet		default	2	
		Thunderbolt 2: en2			Ethernet		default	2	
		Thunderbolt 3: en3			Ethernet		default	2	
	C	Enable promiscuous mode on all interface: apture filter for selected interfaces:	s er a capture filte	r		•	Mana	ge Interface Compile Bl	s PFs
	He	lp					(	Close	Start

Step 4. Under the **Capture filter for selected interfaces:** field box, type **udp port 5555**, as shown in the image.

Interface ▶ utuni3	Traffic	Link-layer Header	Promisc	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
▶ utun4		BSD loopback		default	2		
▶ utun5		BSD loopback		default	2		
utun6		BSD loopback		default	2		
<ul> <li>USB 10/100/1000 LAN: en10</li> </ul>		Ethernet	<b></b>	default	2		udp port 5555
Loopback: lo0	hard have norm	Manada BSD loopback		default	2		
Wi-Fi: en0		Ethernet		default	2		
Thunderbolt Bridge: bridge0		Ethernet		default	2		
Thunderbolt 1: en1		Ethernet		default	2		
Thunderbolt 2: en2		Ethernet		default	2		
Thunderbolt 3: en3		Ethernet		default	2		
Enable promiscuous mode on all i	nterfaces						Manage Interfaces
	ude part EEEE						Compile BDEs

Step 5. Click Start, as shown in the image.

nterfa	ce	Traffic	Link-layer He	eader	Promisci	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
⊳ uti	un3		BSD 100pp	аск		detault	2		
⊧ uti	un4		BSD loopb	ack	<u> </u>	default	2		
⊧ uti	unb		BSD loopb	ack	<u> </u>	default	2		
uti			BSD loopb	ack		default	2	_	
> US	SB 10/100/1000 LAN: en10		Ethernet			default	2		udp port 5555
⊳ Lo	oopback: lo0	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	BSD loopb	ack	<u> </u>	default	2		
Wi	i-Fi: en0		Ethernet			default	2		
Th	nunderbolt Bridge: bridge0		Ethernet			default	2		
Th	nunderbolt 1: en1		Ethernet			default	2		
Th	nunderbolt 2: en2		Ethernet		<b>S</b>	default	2		
Th	nunderbolt 3: en3		Ethernet		<b>V</b>	default	2		
C Ena	able promiscuous mode on all interface	s						N	lanage Interfaces
aptur	re filter for selected interfaces: 📘 ud	port 5555					×	•	Compile BPFs

Step 6. Wait for Wireshark to collect the information required and select the **Stop** button from Wireshark, as shown in the image.

4	🗖 , 🕻 🐵 🖿 🗎	🖹 🙆 🤇 🗢 🔿	🙋 🕢 生 🔳 🔳 🔍	
	lay filter <쁐/>			
No.	Time	Protocol	Signal strength  SSID	Time delta from

**Tip**: If the WLAN uses encryption such as Pre-shared Key (PSK), ensure the capture catches the fourway handshake between the AP and the desired client. This can be done if the OTA PCAP starts before the device is associated with the WLAN or if the client is deauthenticated and reauthenticated while the capture runs.

Step 7. Wireshark does not decode the packets automatically. In order to decode the packets select a line from the capture, use the right-click to display the options, and select **Decode As...**, as shown in the image.

4			Ø	0	)	0101	×	6	٩	<b>(</b>	⇒		$\overline{\mathbf{e}}$	<u> </u>	-		Ð	Q
	Ар	ply a di	spla	ay filter	r <%/>													
Ν	lo.			Time		Dest	Proto	col	So	ource P	ort	Info					Signa	al strer
٢	_		1	2021	.–03–…	1	UDP		55	555		5555	; →	5000	Len	=400		
			2	2021	.–03–…	1	UDP		55	555		5555	; →	5000	Len	=387		
			3	2021	.–03–…	1	UDP		55	555		5555	; →	5000	Len	=385		
			4	2021	.–03–…	1	UDP		55	555		5555	; →	5000	Len	=400		
			5	2021	03	1	UDP		55	555		5555	; →	5000	Len	=387		
			6	2021	03	1	UDP		55	555		5555	; →	5000	Len	=385		
			7	2021	.–03–	1	UDP		55	555		5555	; →	5000	Len	=400		
			8	2021	.–03–	1	UDP		5!	555		5555	j →	5000	Len	=387		
			9	2021	.–03–	1	UDP		5	Mark	/Unma	ark Pac	:ket		.en	=385		
		:	10	2021	03	1	UDP		1	Ignor	re/Uni	gnore I	Pack	et	.en	=400		
		:	11	2021	03	1	UDP		1	Set/l	Jnset	Time R	efer	ence	.en	=387		
		:	12	2021	03	1	UDP		1	Time	Shift.				.en	=385		
		:	13	2021	.–03–…	1	UDP		1	Раск	etCor	nment	•••		.en	=400		
		:	14	2021	03	1	UDP		1	Edit I	Resolv	ed Nar	me		.en	=387		
		:	15	2021	03	1	UDP		-	Appl	u an Ei	iltor			.en	=385		
		:	16	2021	.–03–	1	UDP		5	Dren	y as ri are as	Filter			.en	=400		
		:	17	2021	.–03–	1	UDP		1	Conv	ersati	on Filte	er		.en	=387		
		:	18	2021	03	1	UDP		5	Colo	rize Co	onversa	atior		.en	=385		
		:	19	2021	.–03–	1	UDP		1	SCT	>			•	.en	=400		
			20	2021	.–03–	1	UDP			Follo	w			►	.en	=387		
		2	21	2021	03	1	UDP		-	Con	,				.en	=385		
		2	22	2021	03	1	UDP		5	Copy					.en	=400		
		2	23	2021	03	1	UDP		-	Drote	neel D	referen	222		en	=387		
		2	24	2021	03	1	UDP		- 1	Deco	de As				en	=385		
		2	25	2021	03	1	UDP		1	Snov	и Раск	et in N	ew v	vinaow	Len	=379		

Step 8. A pop-up window appears. Select the add button and add a new entry, select these options: **UDP port** from **Field**, **5555** from **Value**, **SIGCOMP** from **Default**, and **PEEKREMOTE** from **Current**, as shown in the image.



Step 9. Click **OK**. The packets are decoded and ready to start the analysis.

# Verify

Use this section in order to confirm that your configuration works properly.

In order to confirm the AP is in Sniffer mode from the 9800 GUI:

Step 1. On the 9800 WLC GUI Navigate to Configuration > Wireless > Acces Points > All Acces Points.

Step 2. Search the AP. Click on the arrow down button to display the search tool, select **Contains** from the dropdown list, and type the AP name, as shown in the image.



Step 3. Verify the Admin Status is with the checkmark in green and the AP Mode is Sniffer, as shown in the image.

¢	cisco	Cisco Cata 17.3.2a	alyst 9800-C	L Wireles	ss Contr	oller	Welcome	admin 🖌 🎢	<b>F</b>	* 19 0	Search A	<sup>&gt;</sup> s and Clients C	2	۲
Q	, Search Menu It	ems	Configuratio	n≛> Wire	eless*>	Access Poi	ints							
	Dashboard V All Access Points													
C	Monitoring >												¢°	
Ľ	Configuratio		AP ~ Name	AP ~ Model	Slots	Admin ~ Status	IP v Address	Base Radio v MAC	AP ~ Mode	Operation ~ Status	Configuration ~ Status	Policy ~ Tag	Site ~ Tag	F
Ś	Administratio	on >	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		н. н.	1	10 🔻	tems per page	•				1	- 1 of 1 access p	points	c
×	Troubleshoo	ting	E CH	Dadiaa										

In order to confirm the AP is in Sniffer mode from the 9800 CLI. Run these commands:

```
<#root>
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

In order to confirm the packets are decoded on Wireshark. The Protocol changes from **UDP** to **802.11** and there are seen **Beacon frames**, as shown in the image.

•														
		ø	© 🖿	0101	×	6	Q	<b>4</b>	⇒	🔮 🗿	- 🕹 🛛		Ð,	Q
Apply a display filter <೫/>														
No.		<u> </u>	Time	Dest	Protoco	bl	Sou	irce Po	ort	Info			Signa	l stren
		1	2021–03–…	В	802.1	11	55	55		Beacon	frame,	SN=23	-39	dBm
		2	2021–03–…	В	802.1	11	55	55		Beacon	frame,	SN=23	-39	dBm
		3	2021–03–…	B	802.1	11	55	55		Beacon	frame,	SN=23	-39	dBm
		4	2021–03–…	B	802.1	11	55	55		Beacon	frame,	SN=23	-39	dBm
		5	2021–03–…	B	802.1	11	55	55		Beacon	frame,	SN=23	-39	dBm
		6	2021–03–…	B	802.1	11	55	55		Beacon	frame,	SN=23	-39	dBm
		7	2021–03–	В	802.1	11	55	55		Beacon	frame,	SN=23	-39	dBm
		8	2021–03–…	B	802.1	11	55	55		Beacon	frame,	SN=23	-39	dBm
		9	2021–03–…	B	802.1	11	55	55		Beacon	frame,	SN=23	-39	dBm
		10	2021–03–…	B	802.1	11	55	55		Beacon	frame,	SN=23	-39	dBm
		11	2021–03–…	B	802.1	11	55	55		Beacon	frame,	SN=23	-39	dBm
		12	2021–03–…	B	802.1	11	55	55		Beacon	frame,	SN=23	-39	dBm
		13	2021–03–…	B	802.3	11	55	55		Beacon	frame,	SN=23	-39	dBm

### Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Problem: Wireshark does not receive any data from the AP.

Solution: The Wireshark server must be reachable by the Wireless Management Interface (WMI). Confirm the reachability between the Wireshark server and the WMI from the WLC.

# **Related Information**

- <u>Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE</u> <u>Amsterdam 17.3.x - Chapter: Sniffer Mode</u>
- Fundamentals of 802.11 Wireless Sniffing
- <u>Technical Support & Documentation Cisco Systems</u>