# 在Catalyst 9800无线控制器上以嗅探器模式配置 接入点

## 目录

<u>简介</u> <u>先决条件</u> 要求 使用的组件 配置 网络图 配置 通过GUI在嗅探器模式下配置AP 通过CLI在嗅探器模式下配置AP 通过CLI在嗅探器模式下配置AP 配置AP以通过GUI扫描通道 配置AP以通过CLI扫描通道 配置Wireshark以收集数据包捕获 验证 故障排除 相关信息

## 简介

本文档介绍如何通过图形用户界面(GUI)或命令行界面(CLI)在Catalyst 9800系列无线控制器(9800 WLC)的嗅探器模式下配置接入点(AP),以及如何通过空中(OTA)收集数据包捕获(PCAP)),以便对 无线行为进行故障排除和分析。

## 先决条件

### 要求

Cisco 建议您了解以下主题:

- 9800 WLC配置
- •802.11标准中的基本知识

### 使用的组件

本文档中的信息基于以下软件和硬件版本:

- AP 2802
- 9800 WLC Cisco IOS®-XE版本17.3.2a
- Wireshark 3.X

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

### 配置

注意事项:

- 建议使嗅探器AP靠近目标设备和此设备所连接的AP。
- 确保您知道客户端设备和AP使用哪个802.11通道和宽度。

网络图



配置

#### 通过GUI在嗅探器模式下配置AP

步骤1.在9800 WLC GUI上,导航至**Configuration > Wireless > Acces Points > All Acces** Points,如图所示。



Q	Search Menu Items			Interface	0	Services	
				Logical		AireOS Config Translat	tor
==	Dashboard			Ethernet		Application Visibility	
			_	wireless		Cioud Services	
$\bigcirc$	Monitoring	>	₽ <u></u>	Layer2			
		_		Discovery Protocols		mDNS	
R	Configuration	>		VLAN		Multicast	
V				VTP		NetFlow	
503	Administration	>	പിയ	Radio Configurations		Python Sandbox	
$\sim$						QoS	
Ô	Licensing			CleanAir High Throughout		RA Throttle Policy	
				Media Parameters		Tags & Profiles	
X	Troubleshooting			Network			
6-6				Parameters		AP JOIN	
				RRM		Elex	
				Pouting Protocols		Policy	
			U			Remote LAN	
				Static Routing		RF	
			$\oplus$	Security		Tags	
				AAA		WLANs	
				ACL	0	Wireless	
				Advanced EAP	V	Assess Deinte	
				PKI Management		Access Points	
				Guest User		Air Time Fairness	
				Local EAP		Fabric	
				Local Policy			

步骤2.选择希望在嗅探器模式下使用的AP。在General选项卡上,更新AP的名称,如图所示。

Cisco Cata	lyst 9800-CL Wireless C	Controller			Welcome admin 🛛 🏠 🕵
Q Search Menu Items	Configuration - > Wireless	Access Points		Edit AP	
Dashboard	All Access Points Number of AP(s): 1	General Interfaces	High Availability Inventory		
Monitoring >		AP Name*	2802-carcerva-sniffer		
Configuration >	AP ~ AP ~ Name Model Sig	Location*	default location		
() Administration >	2802- AIR- carcerva AP2802I- & B-K9	• 17:	2.16.0.125 aC	Base Radio MAC	a03d.6f92.9400
C Licensing	⊲ ⊲ 1 ▶ 10	▼ items per page		Ethernet MAC	00a2.eedf.6114
X Troubleshooting	5 GHz Padios		Admin Status	ENABLED	
				AP Mode	Flex v
	> 2.4 GHz Radios		Operation Status	Registered	

步骤3.验证Admin Status是否已启用,并将AP Mode更改为Sniffer,如图所示。

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 × AP × Admin × IP × Admin × Address	AP Name* B: M Location*	2802-carcerva-sniffer
() Administration >	2802- AIR- carcerva AP2802I- 2 ♥ 172.16.0.125 a	a Base Radio MAC	a03d.6f92.9400
C Licensing	I I ► I I ▼ items per page	Ethernet MAC	00a2.eedf.6114
X Troubleshooting		Admin Status	
	5 GHz Radios	AP Mode	Sniffer 🔻
	> 2.4 GHz Radios	Operation Status	Registered

系统将显示一个弹出窗口,其中包含下一个注释:

"警告:更改AP模式将导致AP重新启动。点击更新并应用到设备以继续"

选择OK,如图所示。



#### 步骤4.单击"更**新并应用到设**备",如图所示。

Edit AP								×
General	Interfaces	High Availability	Inventory	lCap	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		
Base Radi	o MAC	a03d.6f92.9400		Predownloa	aded Version	N/A		
Ethernet N	/AC	00a2.eedf.6114		Next Retry	Time	N/A		
Admin Sta	itus	ENABLED		Boot Versio	n	1.1.2.4		
AP Mode		Sniffer	•	IOS Version	1	17.3.2.32		-
Operation	Status	Registered		Mini IOS Ve	ersion	0.0.0.0		
Fabric Sta	tus	Disabled		IP Config				iided As
LED State		ENABLED		CAPWAP P	referred Mode	IPv4		sistance
LED Brigh Level	tness	8	•	DHCP IPv4	Address	172.16.0.125		
<b>_</b>				Static IP (IP	v4/IPv6)	0		
Cancel						📑 Update	e & Apply to Dev	ice

#### 系统将显示一个弹出窗口,确认更改和AP退回,如图所示。



#### 通过CLI在嗅探器模式下配置AP

步骤1.确定希望用作嗅探器模式的AP并获取AP名称。

步骤2.修改AP名称。

此命令修改AP名称。其中,<AP-name>是AP的当前名称。

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

#### 配置AP以通过GUI扫描通道

步骤1.在9800 WLC GUI中,导航至Configuration > Wireless > Acces Points。

步骤2.在"接**入点"**页面上,显**示5 GHz**无线电**或2.4 GHz无线电菜**单列表。这取决于要扫描的通道 ,如图所示。

¢	cisco	Cisco Cat 17.3.2a	talys	st 98	800-CL Wireless (	Controller	Welcome admin	*	<b>V</b> o	E	¢	1	9 2	Se	arch APs and Clients	Q	•
0	), Search Menu It	lems	C	Confi	guration > Wireles	S* > Access Points											
li	Dashboard		I,	>	All Access Points												
C	Monitoring			>	5 GHz Radios												
Ľ	Configuratio			>	2.4 GHz Radios												
ŝ	Administratio	on >	Ľ	>	Dual-Band Radios	;											
© ve		tipo		>	Country												
<i>~</i>	110001031100	ung															

步骤2.搜索AP。单击向下**箭头**按钮以显示搜索工具,从下拉列表中选**择**"包含",然后键入**AP名**称 ,如图所示。

¢	cisco	Cisco Cataly	yst 9800–CL Wi	reless Cont	roller		Welcome	admi	n 🖌 🎢	To		¢	1	0	C
Q	Search Menu Ite	ems	Configuration * >	Wireless * >	Access Poi	ints									
III	Dashboard		> All Access	Points											
	Monitoring	>	✓ 5 GHz Rad	lios											
Ľ	Configuratior	n >	Number of AP(s): 1												
<i>i</i> ði	Administratio	on >	AP Name	✓ Slot No ~	Base Radio MAC	~	Admin Status	~	Operation Status	~	Policy Tag	~	Site	Tag	~
©	Licensing		2802-carcerva- sniffer	Show items with Contains sniffer	value that:	100 9	٢		Θ		webautł	h_test	defa tag	ault-si	te-
X	Troubleshoot	ting	> 2.4 GHz R	Filter	Clear										

步骤3.选择AP并勾选Configure > Sniffer Channel Assignment**下的Enable Sniffer**复选框,如图所示。



步骤4.从Sniff Channel下拉列表中**选择Channel**,然后键入**Sniffer IP address**(Server IP address with Wireshark),如图所示。



步骤5.选择目标设备和AP在连接时使用的通道宽度。

#### 导航至Configure > RF Channel Assignment以配置此配置,如图所示。

		Edit Radios 5 GHz Banc	i		
ashboard	<ul> <li>All Access Period</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
(Ŏ) Administration >	2802- AIR- carcerva- AP28021 sniffer & B-K9	Admin Status		Channel Width	40 MHz v
© Licensing		CleanAir Admin Status		Assignment Method	40 MHz
K Troubleshooting	✓ 5 GHz Radios	Antenna Parameters		Channel Number	160 MHz
	Number of AD(c), 1			Tx Power Level Assignme	ent
	Number of AP(s): 1	Antenna Type	Internal v	Current Tx Power Level	6
	AP Name v	Antenna Mode	Omni		
	2802-carcerva-	Antenna A	Ø	Assignment Method	Custom
	4 4 1 ⊨	Antenna B	Ø	Transmit Power	6 🗸

配置AP以通过CLI扫描通道

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

#### 示例:

carcerva-9k-upg#ap name 2802-carcerva-sniffer sniff dot11a 36 172.16.0.190
配置Wireshark以收集数据包捕获

步骤1.启动Wireshark。

步骤2.从Wireshark中选择"捕获选项"菜单图标,如图所示。



步骤3.此操作将显示弹出窗口。从列表中选择有线接口作为捕获的源,如图所示。

•		Wireshark	<ul> <li>Capture Options</li> </ul>				
Г		Input C	Output Options				
	Interface	Traffic	Link-layer Header	Promiscu	Snaplen (B)	Buffer (MB)	Monitor
	► utun4		BSD loopback		default	2	
	▶ utun5		BSD loopback		default	2	
	utun0		DOD loopback	-	default	2	_
	<ul> <li>USB 10/100/1000 LAN: en10</li> </ul>		Ethernet	<b>V</b>	default	2	-
	Ecophonic IcO	A A	PSD loopbook		dofoult	2	
	Wi-Fi: en0		Ethernet	<b>V</b>	default	2	
	Thunderbolt Bridge: bridge0		Ethernet	<b>N</b>	default	2	
	Thunderbolt 1: en1		Ethernet	<b>S</b>	default	2	
	Thunderbolt 2: en2		Ethernet	<b>S</b>	default	2	
	Thunderbolt 3: en3		Ethernet	<b>S</b>	default	2	
	Enable promiscuous mode on all interface Capture filter for selected interfaces: <a href="https://www.selected.com">mttps://www.selected.com</a>	<b>s</b> ter a capture filter		•	Mana	ige Interfaci Compile B	es PFs
	Help				l	Close	Start

步骤4.在Capture(捕获)**过滤器下,选择的接口:**字段框,键入udp端口5555,如图所示。

utun3	terface	Traffic	Link-layer Header	Promiscu	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
utun4	utuna		взр юорраск	<u> </u>	detault	2		
utun5       BSD loopback       Image Interfaces         utun6       BSD loopback       Image Interfaces         USB 10/100/1000 LAN: en10       Ethernet       Image Interfaces	▶ utun4		BSD loopback		default	2		
utun6       BSD loopback       Image Interfaces         USB 10/100/1000 LAN: en10       Ethernet       Image Interfaces         Wi-Fi: en0       Ethernet       Image Interfaces	▶ utun5		BSD loopback		default	2		
USB 10/100/1000 LAN: en10       Ethernet       Image Interfaces         Loopback: Io0       Image Interfaces         Wi-Fi: en0       Ethernet       Image Interfaces         Thunderbolt Bridge: bridge0       Ethernet       Image Interfaces	utun6		BSD loopback		default	2		
Loopback: Io0	USB 10/100/1000 LAN: en10		Ethernet	<b>S</b>	default	2		udp port 5555
Wi-Fi: en0       Ethernet       Image Interfaces         Thunderbolt Bridge: bridge0       Ethernet       Image Interfaces         Thunderbolt 1: en1       Ethernet       Image Interfaces         Thunderbolt 2: en2       Ethernet       Image Interfaces	Loopback: Io0	huhan Marin	BSD loopback	<b>S</b>	default	2		
Thunderbolt Bridge: bridge0       Ethernet       Image: bridge0       Image: bridge0         Thunderbolt 1: en1       Ethernet       Image: bridge0       Image: bridge0         Thunderbolt 2: en2       Ethernet       Image: bridge0       Image: bridge0         Thunderbolt 3: en3       Ethernet       Image: bridge0       Image: bridge0         Image: bridge0       Image: bridge0       Image: bridge0	Wi-Fi: en0		Ethernet	<b>S</b>	default	2		
Thunderbolt 1: en1      Ethernet       Image: default 2 in the second	Thunderbolt Bridge: bridge0		Ethernet	<b>S</b>	default	2		
Thunderbolt 2: en2      Ethernet       Image: default       2	Thunderbolt 1: en1		Ethernet	<b>S</b>	default	2		
Thunderbolt 3: en3      Ethernet       Image: default 2	Thunderbolt 2: en2		Ethernet	<b>S</b>	default	2		
Enable promiscuous mode on all interfaces     Manage Interfaces	Thunderbolt 3: en3		Ethernet	<b>S</b>	default	2		
	Enable promiscuous mode on all i	nterfaces					N	Manage Interfaces
apture filter for selected interfaces: 📕 udp port 5555 Compile BPF	apture filter for selected interfaces:	udp port 5555				×	•	Compile BPFs

步骤5.单击"**开始**",如图所示。

		W	′ireshark ∙ Cap	ture Options					
			out Outour	Ontions					
			put Outpu	Options					
Inte	erface	Traffic	Link-layer Hea	ler	Promiscı	Snaplen (B)	Buffer (MB	)   Monito	r    Capture Filter
	utun3 utun4		BSD loopbac	r. k	2	default	2		
	utun5		BSD loopbac	k	2	default	2		
	utun6		BSD loopbac	k		default	2		
►	USB 10/100/1000 LAN: en10		Ethernet		<b>V</b>	default	2		udp port 5555
►	Loopback: Io0		BSD loopbac	k	<b>V</b>	default	2		
	Wi-Fi: en0		Ethernet			default	2		
	Thunderbolt Bridge: bridge0		Ethernet		<b>V</b>	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 interface	s							Manage Interfaces
Сар	oture filter for selected interfaces: 🔲 ud	p port 5555					×	•	Compile BPFs
Help									Close

步骤6.等待Wireshark收集所需信息,然后从Wireshark中选择"停止"按钮,如图所示。

4	. 🗆	[ (0)			6	ৎ	¢	<b> </b>		豪	♣			€	Q	Q	9 6	
No.		lay filter .   <b>Time</b>	<೫/>	 			P	rotoco	bl	Si	ignal s	trength	n   SSID			Time	e delta fr	rom

**提示:**如果WLAN使用加密(如预共享密钥(PSK)),请确保捕获捕获AP与所需客户端之间的四 次握手。如果OTA PCAP在设备与WLAN关联之前启动,或者如果客户端在捕获运行期间取消 身份验证并重新进行身份验证,则可以执行此操作。

步骤7. Wireshark不会自动解码数据包。要对数据包进行解码,请从捕获中选择一行,使用右键单 击显示选项,然后选择**解码为……**,如图所示。

۷	₫ 🗖	Ø	0		00000	×		্	<b>(</b>	⇒		ᢙ	<u></u>			Ð	Q
L	Apply a	displ	ay filter	<೫/>													
N	lo.		Time		Dest	Proto	col	Sou	urce Po	ort	Info					Signal	strer
ſ	_	1	2021	-03	1	UDP		55	55		5555	i →	5000	Len=	400		
		2	2021	-03	1	UDP		55	55		5555	i →	5000	Len=	387		
		3	2021	-03	1	UDP		55	55		5555	i →	5000	Len=	385		
		4	2021	-03	1	UDP		55	55		5555	i →	5000	Len=	400		
		5	2021	-03	1	UDP		55	55		5555	i →	5000	Len=	387		
		6	2021	-03	1	UDP		55	55		5555	i →	5000	Len=	385		
		7	2021	-03	1	UDP		55	55		5555	i →	5000	Len=	400		
		8	2021	-03	1	UDP		55	55		5555	i →	5000	Len=	:387		
		9	2021	-03	1	UDP		5	Mark	/Unma	ark Pac	ket		.en=	385		
		10	2021	-03	1	UDP		-	Ignor	e/Uniç	gnore F	Pack	et	.en=	400		
		11	2021	-03	1	UDP		1	Set/L	Jnset	Time R	efer	ence	.en=	387		
		12	2021	-03	1	UDP		-	Dack	Shift.	 nment			.en=	385		
		13	2021	-03	1	UDP		-	Fack			••		.en=	400		
		14	2021	-03	1	UDP		-	Edit F	Resolv	ed Nar	ne		.en=	387		
		15	2021	-03	1	UDP		-	Annh	/ as Fi	lter			.en=	385		
		16	2021	-03	1	UDP		1	Prepa	are as	Filter			.en=	400		
		17	2021	-03	1	UDP		1	Conv	ersati	on Filte	er	•	.en=	387		
		18	2021	-03	1	UDP		-	Color	rize Co	onversa	ation	•	.en=	385		
		19	2021	-03	1	UDP		1	SCTF	•			►	.en=	400		
		20	2021	-03	1	UDP		1	Follo	w			►	.en=	387		
		21	2021	-03	1	UDP		-	Copy					.en=	385		
		22	2021	-03	1	UDP		-	COPY					.en=	400		
		23	2021	-03	1	UDP			Droto	icol Dr	oforon			en=	387		
		24	2021	-03	1	UDP		1	Deco	de As				en=	385		
		25	2021	-03	1	UDP		1	Snow	/ Раск	et in N	ew v	vinaow	len=	:379		

步骤8.系统将显示弹出窗口。选择添加按钮并添加新条目,选择以下选项:**来自字段的UDP端口、 来自值的5555、来自默认的SIGCOMP和来自当前的PEEKREMOTE,如图所示。** 



步骤9.单击OK。数据包已解码并准备开始分析。

### 验证

使用本部分可确认配置能否正常运行。

要从9800 GUI确认AP处于嗅探器模式:

步骤1.在9800 WLC GUI上,导航至Configuration > Wireless > Acces Points > All Acces Points。

步骤2.搜索AP。单击向下箭头按钮显示搜索工具,从下拉列表中选择**Contains**,然后键入AP名称 ,如图所示。

11111 Cisco Catalyst 9800-CL Wireless Controller **CISCO** 17.3.2a Configuration >> Wireless >> Access Points Q Search Menu Items All Access Points Dashboard == Number of AP(s): 1 Monitoring > AP AP Admin IP Configuration > Name tatus Ac Show items with value that: 2802-Contains Ŧ Administration >  $\odot$ 17 carcerva sniffer sniffer Licensing 1 -4 s per page Troubleshooting 5 GHz Radios

步骤3.如图所示,验证Admin Status为绿色,AP Mode 为Sniffer。

¢	cisco	Cisco Cata 17.3.2a	alyst 9800-C	L Wireles	ss Contro	oller	Welcom	e admin 🖌 😭	<b>\$</b>	¢ 🕸 0	Search	APs and Clients 🤇	ג	۲
0	Search Menu Iti	ems	Configuration	n≛> Wire	eless* > /	Access Poi	ints							
	Dashboard V All Access Points													
C	Monitoring	Number of AP(s): 1 Monitoring >											¢°	
Ľ	Configuration		AP ~ Name	AP ~ Model	Slots ~	Admin ~ Status	IP Address	<ul> <li>Base Radio ~</li> <li>MAC</li> </ul>	AP ↓ Mode	Operation ~ Status	Configuration Status	<ul> <li>Policy</li> <li>Tag</li> </ul>	Site v Tag	r F
Ś	Administratio	on >	2802- carcerva- sniffer 👍	AIR- AP2802I- B-K9	2	۰	172.16.0.125	5 a03d.6f92.9400	Sniffer	Registered	Healthy	webauth_test	default- site-tag	c r
C	Licensing		H 4	1 ⊩	10 🔻 ite	ems per page	9					1 - 1 of 1 access	points	c
×	Troubleshoo	ting	5.014	Dedies										

为了从9800 CLI确认AP处于嗅探器模式。运行以下命令:

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

为了确认数据包在Wireshark上已解码。协议从UDP更改为802.11,并且出现Beacon帧,如图所示。

•													
		۲	© 🖿		🔀 🎑		۹ 🔇	• 🔿	警 쥼	🕹 🛽		Ð,	Q
Apply a display filter <೫/>													
No.		Ľ	Time	Dest	Protocol		Source	Port	Info			Signa	l stren
		1	2021–03–…	B	802.11		5555		Beacon	frame,	SN=23	-39	dBm
		2	2021–03–…	В	802.11		5555		Beacon	frame,	SN=23	-39	dBm
		3	2021–03–…	B	802.11		5555		Beacon	frame,	SN=23	-39	dBm
		4	2021–03–…	B	802.11		5555		Beacon	frame,	SN=23	-39	dBm
		5	2021–03–…	В	802.11		5555		Beacon	frame,	SN=23	-39	dBm
		6	2021–03–…	В	802.11		5555		Beacon	frame,	SN=23	-39	dBm
		7	2021–03–…	В	802.11		5555		Beacon	frame,	SN=23	-39	dBm
		8	2021–03–…	B	802.11		5555		Beacon	frame,	SN=23	-39	dBm
		9	2021–03–…	B	802.11		5555		Beacon	frame,	SN=23	-39	dBm
		10	2021-03	B	802.11		5555		Beacon	frame,	SN=23	-39	dBm
		11	2021-03	B	802.11		5555		Beacon	frame,	SN=23	-39	dBm
		12	2021-03	B	802.11		5555		Beacon	frame,	SN=23	-39	dBm
		13	2021-03	B	802.11		5555		Beacon	frame,	SN=23	-39	dBm

### 故障排除

本部分提供了可用于对配置进行故障排除的信息。

问题:Wireshark不从AP接收任何数据。

解决方案:Wireshark服务器必须可通过无线管理接口(WMI)访问。 请确认Wireshark服务器与 WLC中的WMI之间的可达性。

## 相关信息

- <u>Cisco Catalyst 9800系列无线控制器软件配置指南,Cisco IOS XE Amsterdam 17.3.x 第章</u> <u>: 嗅探器模式</u>
- 802.11无线嗅探的基础
- <u>技术支持和文档 Cisco Systems</u>