在Catalyst 9800無線控制器上以監聽器模式設定 存取點

目錄

 箇介

 必要條件

 需求

 採用元件

 設定

 網路圖表

 組態

 通過GUI在監聽器模式下配置AP

 在監聽器模式下通過CLI配置AP

 配置AP以通過GUI掃描通道

 配置AP以通過CLI掃描通道

 配置Wireshark以收集資料包捕獲

 驗證

 疑難排解

 相關資訊

簡介

本文說明如何透過圖形使用者介面(GUI)或指令行介面(CLI)在Catalyst 9800系列無線控制器(9800 WLC)上以監聽器模式設定存取點(AP),以及如何使用監聽器AP透過空氣收集封包擷取(PCAP),以 便進行無線行為疑難排解和分析。

必要條件

需求

思科建議您瞭解以下主題:

- 9800 WLC組態
- •802.11標準中的基本知識

採用元件

本文中的資訊係根據以下軟體和硬體版本:

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

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設

)的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

設定

需要考慮的事項:

- 建議讓監聽器AP靠近目標裝置以及此裝置所連線的AP。
- 確保您知道客戶端裝置和AP使用哪個802.11通道和寬度。

網路圖表



組態

通過GUI在監聽器模式下配置AP

步驟1。在9800 WLC GUI上,導覽至**Configuration > Wireless > Access Points** > All Access Points,如下圖所示。



Cisco Catalyst 9800-CL Wireless Controller

Q Search Menu Items		Interface	0	Services
📰 Dashboard		Logical Ethernet Wireless		AireOS Config Translator Application Visibility Cloud Services
	›	Layer2		Custom Application IOx
	>	Discovery Protocols VLAN VTP		mDNS Multicast
Administration	s tu <	Radio Configurations		Python Sandbox QoS RA Throttle Policy
		High Throughput Media Parameters Network	ER R≣	Tags & Profiles
		Parameters RRM		EoGRE Flex
		Routing Protocols Static Routing		Policy Remote LAN
	\$	Security AAA		Tags WLANs
		ACL Advanced EAP	Ş	Wireless
		PKI Management Guest User		Advanced Air Time Fairness
		Local Policy		Fabric

步驟2.選擇在監聽器模式下希望使用的AP。在General索引標籤上,更新AP的名稱,如下圖所示。

Cisco Cata	Cisco Catalyst 9800-CL Wireless Controller												
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	Admin ~ IP ots ~ Status Ad	v Ba dress M	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								

步驟3.確認Admin Status為Enabled,並將AP Mode變更為Sniffer,如下圖所示。

Cisco Catal	yst 9800-CL Wireless Controller		Welcome admin 🖌 🐔
Q Search Menu Items	Configuration * > Wireless * > Access Points	Edit AP	
 Dashboard Monitoring > 	Vumber of AP(s): 1	General Interfaces General	High Availability Inventory
Configuration >	AP ~ AP ~ Admin ~ IP ~ E Name Model Slots ~ Status Address M	AP Name* 3: M Location*	2802-carcerva-sniffer
() Administration >	2802- AIR- carcerva AP2802I- 2 ♥ 172.16.0.125 a	Base Radio MAC	a03d.6f92.9400
© Licensing	I I ► I0 ▼ 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

系統會顯示一個彈出視窗,其中包含下一個附註:

"警告:更改AP模式將導致AP重新啟動。點選更新並應用到裝置以繼續」

選擇OK,如下圖所示。



步驟4.按一下Update & Apply to Device,如下圖所示。

Edit AP								×
General	Interfaces	High Availability	Inventory	ICap	Advanced	Support Bund	dle	
General				Version				
AP Name*		2802-carcerva-sn	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	1AC	00a2.eedf.6114		Next Retry	Time	N/A		
Admin Sta	tus	ENABLED		Boot Versio	n	1.1.2.4		
AP Mode		Sniffer	•	IOS Version	1	17.3.2.32		-
Operation	Status	Registered		Mini IOS Ve	rsion	0.0.0.0		
Fabric Sta	tus	Disabled		IP Config				Jided As
LED State		ENABLED		CAPWAP P	referred Mode	IPv4		sistance
LED Bright	LED Brightness 8			DHCP IPv4	Address	172.16.0.125		
a				Static IP (IP	v4/IPv6)	0		
Cancel						Up 🗐 🗍	date & Apply to De	evice

系統將顯示一個彈出視窗,以確認更改和AP彈出,如下圖所示。



在監聽器模式下通過CLI配置AP

步驟1.確定需要用作監聽器模式的AP,並獲取AP名稱。

步驟2.修改AP名稱。

此命令將修改AP名稱。其中<AP-name>是AP的當前名稱。

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

配置AP以通過GUI掃描通道

步驟1。在9800 WLC GUI中,導覽至Configuration > Wireless > Access Points。

步驟2.在Access Points頁面上,顯示5 GHz Radio或2.4 GHz Radio選單清單。這取決於掃描所需的 通道,如圖所示。

¢	cisco	Cisco Ca 17.3.2a	talys	st 98	00-CL Wireless Control	ler	Welcome admin	*	V o	Ð	¢	1	0 0	Searc	h APs and Client	Q	(•
0	Q Search Menu It	lems	(Confi	guration * > Wireless * > A	ccess Points	5											
	Dashboard		I.	>	All Access Points													
C) Monitoring			>	5 GHz Radios													
Ľ	Configuratio			>	2.4 GHz Radios													
ŝ	Administratio	on >	Ľ	>	Dual-Band Radios													
© v) Licensing	the e		>	Country													
ð	roubleshoo	ung																

步驟2.搜尋AP。按一下**向下箭頭按鈕**以顯示搜尋工具,從下拉選單中選擇**Contains**,然後鍵入**AP名 稱**,如下圖所示。

¢	cisco	Cisco Catal 17.3.2a	yst 9800-CL Wi	reless Cont	1	Welcome a	dmin	*	V o		ф		0	C	
Q	Search Menu Ite	ems	Configuration > >	Wireless * >	Access Poin	nts									
III	Dashboard		> All Access	Points											
C	Monitoring	>	💙 5 GHz Rad	lios											
Ľ	Configuration	n >	Number of AP(s): 1												
503	Administratio	on >	AP Name	✓ Slot No ~	Base Radio MAC	~	Admin Status	~ 0 S	Operation Status	~	Policy Tag	~	Site	Tag	~
C	Licensing		2802-carcerva- sniffer	Show items with Contains sniffer	value that: 40 •	00	•		ø		webauth	n_test	defa tag	ault-si	te-
×	Troubleshoot	ting	> 2.4 GHz R	Filter	Clear										

步驟3.選擇AP,並勾選**Configure** > Sniffer Channel Assignment底下的**Enable Sniffer**覈取方塊,如 下圖所示。



步驟4.從**Sniff Channel**下拉選單中選擇Channel,然後鍵入**Sniffer IP address**(使用Wireshark的伺 服器IP地址),如下圖所示。

Cisco Catal	yst 9800-CL Wireless Controller	Welcome admin 🛛 🕋 🜾
Q Search Menu Items	Configuration - > W Edit Radios 5 G	iHz Band
📰 Dashboard	All Access P	onni
Monitoring >	 Antenna A 5 GHz Radio: Antenna B 	Ø
Configuration >	Number of AP(s): 1 AP Name " Contains" Antenna C	Ø
Administration	Antenna D	Ø
C Licensing	AP Name Antenna Gain	10
X Troubleshooting	Sniffer Channe	el Assignment
	Enable Sniffing	Ø
	Sniff Channel	36 🔻
	> Dual-Band R Sniffer IP*	172.16.0.190
	Sniffer IP Status	Valid
	LSC Provisio	Dump to bootflash
	Cancel	

步驟5.選擇目標裝置和AP在連線時使用的通道寬度。

導覽至Configure > RF Channel Assignment以設定此設定,如下圖所示。

		Edit Radios 5 GHz Band											
Dashboard	 All Access Period 	Configure Detail											
Monitoring >	Number of AP(s): 1	General		RF Channel Assignment									
Configuration >	AP ~ AP Name Model	AP Name	2802-carcerva-	Current Channel	36								
(〇) Administration >	2802- AIR- carcerva- AP2802 spiffer & B-K9	Admin Status		Channel Width	40 MHz •								
© Licensing		CleanAir Admin Status		Assignment Method	40 MHz								
X Troubleshooting	✓ 5 GHz Radio:	Antenna Parameters		Channel Number	80 MHz 160 MHz								
				Tx Power Level Assignme	ent								
	Number of AP(s): 1	Antenna Type	Internal v	Current Ty Power Lovel	6								
	AP Name 🗸	Antenna Mode	Omni	Current TX Fower Level	0								
	2802-carcerva-	Antenna A	Ø	Assignment Method	Custom								
	≪ ≪ 1 ►	Antenna B	Ø	Transmit Power	6 v								

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

範例:

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

配置Wireshark以收集資料包捕獲

步驟1.啟動Wireshark。

步驟2.從Wireshark中選擇Capture options選單圖示,如下圖所示。



步驟3.此操作將顯示一個彈出視窗。從清單中選擇有線介面作為捕獲源,如下圖所示。

		Wireshark ·	Capture Options				
		Input O	utput Options				
Interface	Traffic		Link-layer Header	Prom	isci Snaplen (B)	Buffer (MB)	Monitor
▶ utun4			BSD loopback		default	2	
▶ utun5			BSD loopback		default	2	
atur 0			DOD loopback		d-f-ult	2	
USB 10/100/1000 LAN: en10			Ethernet		default	2	_
Loopbook: Io0	1		BCD loopbook		defeult	2	
Wi-Fi: en0			Ethernet	Solution	default	2	
Thunderbolt Bridge: bridge0			Ethernet	Image: A start and a start a st start a start a sta	default	2	
Thunderbolt 1: en1			Ethernet	Image: A start and a start a st start a start a sta	default	2	
Thunderbolt 2: en2			Ethernet	Solution	default	2	
Thunderbolt 3: en3			Ethernet	Solution	default	2	
Enable promiscuous mode on all interface Capture filter for selected interfaces:	s ter a capture	filter			Man	age Interfac Compile B	es PFs
Help						Close	Start

步驟4.在Capture filter for selected interfaces下: 欄位框中, 鍵入udp port 5555, 如下圖所示。

terface	Traffic	Link-layer Header	Promiscu	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
utuna		вър юорраск	M	detault	2		
utun4		BSD loopback	S	default	2		
utun5		BSD loopback	S	default	2		
utun6		BSD loopback	S	default	2		
USB 10/100/1000 LAN: en10		Ethernet	S	default	2		udp port 5555
Loopback: Io0	month more	BSD loopback	S	default	2		
Wi-Fi: en0		Ethernet	S	default	2		
Thunderbolt Bridge: bridge0		Ethernet	S	default	2		
Thunderbolt 1: en1		Ethernet	S	default	2		
Thunderbolt 2: en2		Ethernet	S	default	2		
Thunderbolt 3: en3		Ethernet	S	default	2		
						_	
Enable promiscuous mode on all in	terfaces						Manage Interfaces
pture filter for selected interfaces:	udp port 5555					•	Compile BPFs

步驟5.按一下Start,如下圖所示。

	W	ireshark · C	apture Options					
	In	put Out	out Options					
Interface	Traffic	Link-layer H	ader	Promiscu	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
▶ utun4		BSD loopt	ack		default	2		
▶ utun5		BSD loopt	ack		default	2		
utun6		BSD loopt	ack		default	2		
USB 10/100/1000 LAN: en10		Ethernet			default	2		udp port 5555
Loopback: lo0		BSD loopt	ack	V	default	2		
Wi-Fi: en0		Ethernet		V	default	2		
Thunderbolt Bridge: bridge0		Ethernet		V	default	2		
Thunderbolt 1: en1		Ethernet		N	default	2		
Thunderbolt 2: en2		Ethernet		V	default	2		
Thunderbolt 3: en3		Ethernet			default	2		
Enable promiscuous mode on all interfaces Capture filter for selected interfaces:	port 5555						•	Manage Interfaces Compile BPFs
Help								Close

步驟6.等待Wireshark收集所需資訊,然後從Wireshark中選擇停止按鈕,如下圖所示。

4	(💿			্		⇒		豪	ځ	_		€	Q	Q	8	
	 lay filter	<೫/>														
No.	Time				P	rotoco	d	Si	ignal s	trength	n SSID			Time	e delta fr	rom

提示:如果WLAN使用加密(例如預共用金鑰(PSK)),請確保擷取會擷取AP和所需使用者端之間的四次握手。如果OTA PCAP在裝置與WLAN關聯之前啟動,或者如果客戶端在捕獲運行時 被取消身份驗證並重新身份驗證,則可以完成此操作。

步驟7. Wireshark不會自動解碼資料包。要對資料包進行解碼,請從捕獲中選擇一行,使用按一下 右鍵以顯示選項,然後選擇**解碼為……**(如圖所示)。

۷	4 🗖	æ	0			×	6	٩	(⇒		ᢙ	<u> </u>	-		Ð,	Q
L	Apply a	displ	ay filter	<೫/>													
Ν	lo.		Time		Dest	Proto	col	Sou	urce Po	ort	Info					Signal	strer
ſ	_	1	2021	-03	1	UDP		55	55		5555	; →	5000	Len=	-400		
		2	2021	-03	1	UDP		55	55		5555	; →	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		-	Mark	/Unma	ark Pac	:ket		.en=	-385		
		10	2021	-03	1	UDP		-	Ignore/Unignore Packet					.en=	=400		
		11	2021	-03	1	UDP		Set/Unset Time Reference Time Shift Packet Comment Edit Resolved Name					.en=	-387			
		12	2021	-03	1	UDP							.en=	-385			
		13	2021	-03	1	UDP								.en=	=400		
		14	2021	-03	1	UDP							.en=	-387			
		15	2021	-03	1	UDP		-	Annly	v as Fi	ilter			.en=	-385		
		16	2021	-03	1	UDP		5	Prepa	are as	Filter			.en=	=400		
		17	2021	-03	1	UDP		-	Conv	ersati	on Filte	er	•	.en=	=387		
		18	2021	-03	1	UDP		-	Color	rize Co	onversa	atior	1 Þ	.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		-	55p)					.en=	=400		
		23	2021	-03	1	UDP			Droto	icol Pr	referen	200		en=	-387		
		24	2021	-03	1	UDP			Deco	de As				en=	-385		
		25	2021	-03	1	UDP		1	Snow	/ Раск		ew \	vindow	len=	=379		

步驟8.出現一個彈出視窗。選擇新增按鈕並新增新條目,選擇以下選項:UDP連線埠從欄位、5555 from Value、SIGCOMP from Default和PEEKREMOTE from Current,如下圖所示。



步驟9.按一下OK。封包已解碼並準備開始分析。

驗證

使用本節內容,確認您的組態是否正常運作。

若要確認存取點是否在9800 GUI上處於監聽器模式:

步驟1。在9800 WLC GUI上導覽至Configuration > Wireless > Access Points > All Access Points。

步驟2.搜尋AP。按一下向下箭頭按鈕以顯示搜尋工具,從下拉選單中選擇**Contains**,然後鍵入AP名 稱,如圖所示。 Cisco Catalyst 9800-CL Wireless Controller



步驟3.驗證Admin Status是否具有緣色複選標籤,以及AP Mode是否為Sniffer,如下圖所示。

¢	cisco	Cisco Cata 17.3.2a	lyst 9800-C	L Wireles	ss Contro	oller	Welcom	e admin 🖌 😭	\$	¢ 🕸 0	Search A	Ps and Clients	λ	۲
Q	, Search Menu Ite	ems	Configuration	n≛> Wire	eless*>	Access Po	ints							
Dashboard All Access Points														
C	Monitoring	>	Number of AP(s	s): T					¢°					
Ľ	Configuration	n >	AP ~ Name	AP ~ Model	Slots ~	Admin ~ Status	IP ~ Address	Base Radio v MAC	AP ↓ Mode	Operation ~ Status	Configuration v 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 I = 1 I I items per page 1 - 1 of 1 access points 🖒											5		
×	Troubleshoot	ting	E CH	Dadiaa										

以便從9800 CLI確認AP是否處於監聽器模式。運行以下命令:

111111

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 為了確認封包已在Wireshark上解碼。通訊協定從UDP變更為802.11,且已看到Beacon frames,如 下圖所示。

•														
		ø	© 🖿		×	6	Q	(•	🔮	· 🕹 🛛		Ð,	Q
Ар	ply a d	ispla	y filter <郑/>											
No.		<u> </u>	Time	Dest	Protoc	col	Sou	irce Po	ort	Info			Signa	l stren
		1	2021–03–…	В	802.	11	55	55		Beacon	frame,	SN=23	-39	dBm
		2	2021–03–…	B	802.	11	55	55		Beacon	frame,	SN=23	-39	dBm
		3	2021–03–…	B	802.	11	55	55		Beacon	frame,	SN=23	-39	dBm
		4	2021–03–…	B	802.	11	55	55		Beacon	frame,	SN=23	-39	dBm
		5	2021–03–…	В	802.	11	55	55		Beacon	frame,	SN=23	-39	dBm
		6	2021–03–…	В	802.	11	55	55		Beacon	frame,	SN=23	-39	dBm
		7	2021–03–…	В	802.	11	55	55		Beacon	frame,	SN=23	-39	dBm
		8	2021–03–…	B	802.	11	55	55		Beacon	frame,	SN=23	-39	dBm
		9	2021–03–…	B	802.	11	55	55		Beacon	frame,	SN=23	-39	dBm
		10	2021–03–…	B	802.	11	55	55		Beacon	frame,	SN=23	-39	dBm
		11	2021–03–…	В	802.	11	55	55		Beacon	frame,	SN=23	-39	dBm
		12	2021–03–…	B	802.	11	55	55		Beacon	frame,	SN=23	-39	dBm
		13	2021–03–…	B	802.	11	55	55		Beacon	frame,	SN=23	-39	dBm

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

問題:Wireshark不會從AP接收任何資料。

解決方案:無線管理介面(WMI)必須能夠訪問Wireshark伺服器。 請確認Wireshark伺服器與WLC中的WMI之間的連通性。

相關資訊

- Cisco Catalyst 9800系列無線控制器軟體配置指南, Cisco IOS XE Amsterdam 17.3.x 章節
 : 監聽器模式
- 802.11 無線監聽的基礎知識
- <u>技術支援與文件 Cisco Systems</u>