Configurar o ponto de acesso no modo de farejador nos Catalyst 9800 Wireless Controllers

Contents

Introduction Prerequisites Requirements Componentes Utilizados Configurar Diagrama de Rede Configurações Configurar o AP no modo Sniffer via GUI Configurar o AP no modo Sniffer via CLI Configurar o AP para digitalizar um canal por meio da GUI Configurar o AP para digitalizar um canal via CLI Configurar o AP para digitalizar um canal via CLI Configurar o Wireshark para coletar a captura de pacote Verificar Troubleshoot Informações Relacionadas

Introduction

Este documento descreve como configurar um ponto de acesso (AP) no modo de farejador em um Catalyst 9800 Series Wireless Controller (9800 WLC) por meio da Interface Gráfica de Usuário (GUI) ou da Interface de Linha de Comando (CLI) e como coletar uma Captura de Pacote (PCAP - Packet Capture) Sobre o Ar (OTA - Packet Capture) com o AP de ffer para identificar e identificar problemas e analisar comportamentos sem fio.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de WLC 9800
- Conhecimento básico no padrão 802.11

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- AP 2802
- 9800 WLC Cisco IOS®-XE versão 17.3.2a

• Wireshark 3.X

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Pontos a serem considerados:

- Recomenda-se que o AP do farejador esteja próximo do dispositivo de destino e do AP ao qual esse dispositivo está conectado.
- Certifique-se de saber qual canal e largura 802.11, o dispositivo cliente e o AP usam.

Diagrama de Rede



Configurações

Configurar o AP no modo Sniffer via GUI

Etapa 1. Na GUI do 9800 WLC, navegue para **Configuration > Wireless > Access Points > All Access Points**, como mostrado na imagem.



Q Search Menu Items			Interface	6	Services	
E Dashboard			Logical Ethernet Wireless		AireOS Config Translato Application Visibility Cloud Services	r
	> d	560	Layer2		Custom Application IOx	
	>		Discovery Protocols VLAN VTP		mDNS Multicast	
Administration	> ,	11®	Radio Configurations CleanAir		Python Sandbox QoS RA Throttle Policy	
Troubleshooting			High Throughput Media Parameters Network Parameters	<u>₩8</u> 8≋	Tags & Profiles AP Join	
	(Ĵ.	RRM Routing Protocols		Flex Policy Remote LAN	
	l	⊕	Static Routing Security AAA		RF Tags WLANs	
			ACL Advanced EAP	Ŷ	Wireless Access Points	
			Guest User Local EAP Local Policy		Advanced Air Time Fairness Fabric	

Etapa 2. Selecione o AP desejado para ser usado no modo sniffer. Na guia **Geral**, atualize o nome do AP, como mostrado na imagem.

Cisco Catal	Cisco Catalyst 9800-CL Wireless Controller Welcome admin													
Q. Search Menu Items	Configuration > Wir	E	Edit AP											
Dashboard	 All Access Point Number of AP(s): 1 		General Interfaces General	High Availability Inventory										
(Monitoring >		AP Name*	2802-carcerva-sniffer											
Configuration	AP V AP Name Model	Slots ~	Admin ~ Status	IP ~ Address	B; M	Location*	default location							
(Ò) Administration	2802- AIR- carcerva AP2802I- & B-K9	2	۲	172.16.0.125	a	Base Radio MAC	a03d.6f92.9400							
C Licensing	< < 1 ⊳	10 🔻 it	ems per page			Ethernet MAC	00a2.eedf.6114							
X Troubleshooting	> 5 GHz Radios	Admin Status												
					_	AP Mode	Flex v							
	> 2.4 GHz Radio	Operation Status	Registered											

Etapa 3. Verifique se Admin Status está Habilitado e altere o AP Mode para Sniffer, como mostrado na imagem.

Cisco Cisco Cataly	yst 9800-CL V	Wireless Con	troller				Welcome admin 🛛 🏠 😵		
Q Search Menu Items	Configuration *	E	Edit AP						
Dashboard Monitoring	V All Acce Number of AP(s): 1	General Interfaces General	High Availability Inventory						
Configuration	AP v Al Name M	P v lodel Slots	Admin ~ ~ Status	B; M	AP Name*	2802-carcerva-sniffer			
() Administration	2802- Al carcerva Al da B-	IR- P2802I- 2 -K9	۰	172.16.0.125	a	Base Radio MAC	a03d.6f92.9400		
C Licensing	≪ ≪ 1	► 10 •	items per page			Ethernet MAC	00a2.eedf.6114		
K Troubleshooting		_	Admin Status						
	> 5 GHz R		AP Mode	Sniffer 🗸					
	> 2.4 GHz	Radios				Operation Status	Registered		

Uma janela pop-up é exibida com a próxima nota:

"aviso: Alterar o modo AP fará com que o AP seja reinicializado. Clique em Atualizar e aplicar ao dispositivo para continuar"

Selecione OK, como mostrado na imagem.



Etapa 4. Clique em Atualizar e aplicar ao dispositivo, conforme mostrado na imagem.

Edit AP								×		
General	Interfaces	High Availability	Inventory	ICap	Advanced	Support Bundle				
General				Version						
AP Name	*	2802-carcerva-sni	ffer	Primary Sof	tware Version	17.3.2.32	17.3.2.32			
Location*		default location		Predownloa	aded Status	N/A				
Base Rad	io MAC	a03d.6f92.9400		Predownloa	aded Version	N/A				
Ethernet MAC		00a2.eedf.6114		Next Retry	Time	N/A				
Admin St	atus	ENABLED	ENABLED		n	1.1.2.4				
AP Mode		Sniffer	•	IOS Version		17.3.2.32		C.		
Operatior	Status	Registered		Mini IOS Ve	rsion	0.0.0.0				
Fabric Sta	atus	Disabled		IP Config				ded Ass		
LED State	9	ENABLED		CAPWAP P	referred Mode	IPv4		istance		
LED Brigh Level	ntness	8	•	DHCP IPv4	Address	172.16.0.125				
				Static IP (IP	v4/IPv6)	0				
Cance						🛛 🗄 Update	e & Apply to Dev	vice		

Um pop-up aparece para confirmar as alterações e o AP reflete, como mostrado na imagem.



Configurar o AP no modo Sniffer via CLI

Etapa 1. Determine o AP desejado para ser usado como modo de farejador e pegue o nome do AP.

Etapa 2. Modifique o nome do AP.

Esse comando modifica o nome do AP. Onde <AP-name> é o nome atual do AP.

carcerva-9k-upg#**ap name** <AP-name> **name 2802-carcerva-sniffer** Etapa 3. Configure o AP no modo Sniffer.

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

Configurar o AP para digitalizar um canal por meio da GUI

Etapa 1. Na GUI do 9800 WLC, navegue para Configuration > Wireless > Access Points.

Etapa 2. Na página **Pontos de acesso**, exiba a lista de menus **Rádios de 5 GHz** ou **Rádios de 2,4 GHz**. Isso depende do canal desejado para digitalização, como mostrado na imagem.



Etapa 2. Procure o AP. Clique no botão **seta para baixo** para exibir a ferramenta de pesquisa, selecione **Contém** na lista suspensa e digite o **nome do AP**, como mostrado na imagem.

Cisco Catal	yst 9800-CL Wireless Controller Welcome admin 🛛 💣 🔞 🚱 😂
Q. Search Menu Items	Configuration > Wireless > Access Points
n Dashboard	> All Access Points
Monitoring >	✓ 5 GHz Radios
Configuration	Number of AP(s): 1
∫ Administration >	AP Name Slot No v MAC Status Status Tag Site Tag v
© Licensing	2802-carcerva- Show items with value that: sniffer Contains V 400 O webauth_test default-site- tag
X Troubleshooting	> 2.4 GHz R

Etapa 3. Marque o AP e marque a caixa de seleção **Enable Sniffer** em **Configure > Sniffer Channel Assignment**, como mostrado na imagem.

Cisco Cata	alyst 9800–CL Wirele	ess Controller	Welcome admin 🛛 👫 🕵
Q, Search Menu Items	Configuration ▼ > W	Edit Radios 5 GHz Ban	d
ashboard	All Access Pr	Antenna Moue	UIIIII
G Monitoring >	✓ 5 GHz Radios	Antenna A	Ø
Configuration >	Number of AP(s): 1	Antenna B	
	AP Name "Contains"	Antenna C	
203 Administration >	AP Name 🗸	Antenna D	
© Licensing	2802-carcerva-	Antenna Gain	10
K Troubleshooting	4 4 1 ⊨	Sniffer Channel Assignr	nent
		Enable Sniffing	Ø
	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	ootflash
	LSC Provisio	Cancel	

Etapa 4. Selecione o canal na lista suspensa **Sniff Channel** e digite o **Sniffer IP address** (Server IP address with Wireshark, endereço IP do servidor com Wireshark), como mostrado na imagem.

Cisco Catal	yst 9800-CL Wireless	Controller	Welcome admin 🛛 🏠 🕵
Q Search Menu Items	Configuration ▼ > W Edit	Radios 5 GHz Band	
📻 Dashboard	> All Access P		Umm
Monitoring >	 A 5 GHz Radios 	ntenna A	
	A Number of AP(s): 1	ntenna B	
	AP Name " Contains"	ntenna C	
¿Of Administration >	AP Name	ntenna D	
C Licensing	A 2802-carcerva-	ntenna Gain	10
X Troubleshooting	shifter S	Sniffer Channel Assignme	ent
	EI	nable Sniffing	Ø
	> 2.4 GHz Radi	niff Channel	36 🗸
	> Dual-Band R	niffer IP*	172.16.0.190
	> Country	niffer IP Status	Valid
	Do	ownload Core Dump to boo	otflash
) Cancel	

Etapa 5. Selecione a **largura do canal** que o dispositivo de destino e o AP usam quando conectados.

Navegue até **Configurar > Atribuição de canal RF** para configurar isso, como mostrado na imagem.

		Edit Radios 5 GHz Ban	d		
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
(○) Administration →	2802- AIR- carcerva- AP2802	Admin Status		Channel Width	40 MHz 🔻
© Licensing		CleanAir Admin Status		Assignment Method	20 MHz 40 MHz
X Troubleshooting		Antenna Parameters		Channel Number	80 MHz 160 MHz
	Number of AP(s): 1	Antonna Turco	Internal	Tx Power Level Assignm	ent
	AP Name	Antenna Mode	Omni	Current Tx Power Level	6
	2802-carcerva-	Antenna A	Ø	Assignment Method	Custom
		Antenna B	Ø	Transmit Power	6 🔹

Configurar o AP para digitalizar um canal via CLI

Etapa 1. Ative o farejador de canal no AP. Execute este comando:

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

Exemplo:

carcerva-9k-upg#ap name 2802-carcerva-sniffer sniff dot11a 36 172.16.0.190 Configurar o Wireshark para coletar a captura de pacote

Etapa 1. Inicie o Wireshark.

Etapa 2. Selecione o ícone do menu Capture options no Wireshark, como mostrado na imagem.



Etapa 3. Esta ação exibe uma janela pop-up. Selecione a Interface com fio na lista como a origem da captura, como mostrado na imagem.

•				Wiresha	rk · Cap	ture Options					
				Input	Output	t Options					
	In	terface ▶ urup:s	Traffic		L	ink-layer Header	Pro	omisci	Snaplen (B)	Buffer (MB)	Monitor
		utun4			E	SD loopback			default	2	
		rutun5			E	SD loopback		i	default	2	
		- ctur.C	-			OD loopback			default	2	_
	Þ	• USB 10/100/1000 LAN: en10			E	thernet)	default	2	-
	-	Leopheski leO				PD loophools		-	defeult	2	
		Wi-Fi: en0			E	thernet			default	2	
		Thunderbolt Bridge: bridge0			E	thernet			default	2	
		Thunderbolt 1: en1			E	thernet			default	2	
		Thunderbolt 2: en2			E	thernet			default	2	
		Thunderbolt 3: en3			E	thernet			default	2	
	∨ Ca	Enable promiscuous mode on all interface	i s ter a captur	re filter				•	Mana)	ge Interfaco Compile B	es PFs
	lel	P							(Close	Start

Etapa 4. No **filtro Capturar para interfaces selecionadas:** caixa de campo, digite **udp port 5555**, como mostrado na imagem.

Interface ▶ utun3	Traffic	Link-layer Header	Promisci	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
▶ utun4		BSD loopback		default	2		
▶ utun5		BSD loopback		default	2		
utun6		BSD loopback	S	default	2		
USB 10/100/1000 LAN: en1	0	Ethernet	S	default	2		udp port 5555
Loopback: lo0	marhana	BSD loopback	S	default	2		
Wi-Fi: en0		Ethernet	S	default	2		
Thunderbolt Bridge: bridge	0	Ethernet	S	default	2		
Thunderbolt 1: en1		Ethernet	S	default	2		
Thunderbolt 2: en2		Ethernet	S	default	2		
Thunderbolt 3: en3		Ethernet		default	2		
🗹 Enable promiscuous mode o	n all interfaces					N	lanage Interfaces
Capture filter for selected interf	aces: 📕 udp port 5555					•	Compile BPFs

Etapa 5. Clique em Iniciar, conforme mostrado na imagem.

nte ⊳	rface utun≾	Traffic	Link-lay	er Header	Promisci	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
•	utun4		BSD lo	opback		default	2		
Þ	utun5		BSD lo	opback	N	default	2		
	utun6		BSD lo	opback		default	2		
-	USB 10/100/1000 LAN: en10		Ethern	et	V	default	2		udp port 5555
Þ	Loopback: IoO	mar Marka Maria	BSD lo	opback		default	2		
	Wi-Fi: en0		Ethern	et	V	default	2		
	Thunderbolt Bridge: bridge0		Ethern	et	V	default	2		
	Thunderbolt 1: en1		Ethern	et	V	default	2		
	Thunderbolt 2: en2		Ethern	et	V	default	2		
	Thunderbolt 3: en3		Ethern	et		default	2		
) E	nable promiscuous mode on all interface	s						N	lanage Interfaces
ар	ture filter for selected interfaces: 📜 🛄	p port 5555						•	Compile BPFs

Etapa 6. Aguarde o Wireshark coletar as informações necessárias e selecione o botão **Parar** no Wireshark, como mostrado na imagem.



Tip: Se a WLAN usar criptografia como chave pré-compartilhada (PSK), assegure-se de que a captura capture o handshake de quatro vias entre o AP e o cliente desejado. Isso pode ser feito se o PCAP OTA for iniciado antes do dispositivo ser associado à WLAN ou se o cliente for desautenticado e reautenticado enquanto a captura é executada.

Passo 7. O Wireshark não decodifica os pacotes automaticamente. Para decodificar os pacotes, selecione uma linha da captura, clique com o botão direito do mouse para exibir as opções e selecione **Decodificar como...**, como mostrado na imagem.

		-																	
۷	1		U	0		4303 0310 0310	×		٩		⇒		ᢙ	<u></u>	-			Ð	Q
	Appl	y a dis	pla	y filter	<೫/>														
Ν	o.		Ι.	Time		Dest	Proto	col	Sou	urce Po	ort	Info						Signal	strer
ſ	_	:	1	2021-	-03	1	UDP		55	55		5555	→	5000	Len	1=4	00		
		2	2	2021-	-03	1	UDP		55	55		5555	→	5000	Len	1=3	87		
		3	3	2021-	-03	1	UDP		55	55		5555	→	5000	Len	1=3	85		
		4	1	2021-	-03	1	UDP		55	55		5555	→	5000	Len	1=4	00		
		5	5	2021-	-03	1	UDP		55	55		5555	→	5000	Len	1=3	87		
		(5	2021-	-03	1	UDP		55	55		5555	→	5000	Len	1=3	85		
		7	7	2021-	-03	1	UDP		55	55		5555	→	5000	Len	1=4	00		
		1	3	2021-	-03	1	UDP		_55	55		5555	-	5000	Len	1=3	87		
		9	9	2021-	-03	1	UDP		5	Mark	/Unma	ark Pac	ket		.en	1=3	85		
		10	0	2021-	-03	1	UDP		5	Ignor	e/Uni	gnore F	ack	et	.en	1=4	00		
		1:	1	2021-	-03	1	UDP		5	Set/L	Shift	I Ime R	eter	ence	.en	1=3	87		
		12	2	2021-	-03	1	UDP		-	Pack	et Cor	 nment			.en	1=3	85		
		13	3	2021-	-03	1	UDP		-	Fack		innent.	•		.en	1=4	00		
		14	1	2021-	-03	1	UDP		-	Edit I	Resolv	ed Nar	ne		.en	1=3	87		
		15	5	2021-	-03	1	UDP		-	Apply	v as Fi	lter			.en	1=3	85		
		10	õ	2021-	-03	1	UDP		-	Prepa	are as	Filter		•	.en	1=4	00		
		17	7	2021-	-03	1	UDP		-	Conv	ersati	on Filte	er	►	.en	1=3	87		
		18	3	2021-	-03	1	UDP		-	Color	rize Co	onversa	atior	▶	.en	1=3	85		
		19		2021-	-03	1	UDP		-	SCTF	>			►	.en	1=4	100		
		20	0	2021-	-03	1	UDP			Follo	w			•	.en	1=3	87		
		2:	L	2021-	-03	1	UDP			Сору	,			•	.en	1=3	85		
		22	2	2021-	-03	1	UDP		-						en	1=4	00		
		2.	5	2021-	-03	1	UDP			Drote	ide As	atoron			en	1=3	188		
		24	+	2021-	-03	1	UDP			Deco			D14/ -1	VIDGOW	en	5=1	85		
		- 25	>	2021-	-03	1	UDP		4	SHOW	Pack		ew v	window	len	1=3	5/9		

Etapa 8. Uma janela pop-up é exibida. Selecione o botão adicionar e adicione uma nova entrada, selecione estas opções: **Porta UDP do Field, 5555 from Value, SIGCOMP from Default** e **PEEKREMOTE** from **Current**, como mostrado na imagem.



Etapa 9. Click **OK**. Os pacotes são decodificados e estão prontos para iniciar a análise.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Para confirmar se o AP está no modo Sniffer na GUI do 9800:

Etapa 1. Na GUI do 9800 WLC, navegue para **Configuration > Wireless > Access Points > All Access Points**.

Etapa 2. Procure o AP. Clique no botão de seta para baixo para exibir a ferramenta de pesquisa, selecione **Contém** na lista suspensa e digite o nome do AP, como mostrado na imagem.

.1 1.1 1. 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 > carcerva 17 sniffer sniffer Licensing 4 -4 s per page Troubleshooting 5 GHz Radios

Etapa 3. Verifique se o **status Admin** está com a **marca de seleção em verde** e se o **modo AP** é **Sniffer**, como mostrado na imagem.

¢	cisco	Cisco Cata 17.3.2a	lyst 9800-C	L Wireles	ss Contro	oller	Welcome	admin 🖌 😭	F	¢ 🕸 G	Search /	Ps and Clients 🕻	λ	۲
Q	Q Search Menu Items Configuration > Wireless > Access Points													
I	Dashboard V All Access Points													
C	Monitoring	itoring >												\$°
Ľ	Configuration		AP ~ Name	AP ~ Model	Slots ~	Admin ~ Status	IP ~ Address	Base Radio v	AP ↓ Mode	Operation ~ Status	Configuration Status	Policy ~ Tag	Site ~ Tag	F
Ś	Administratic	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	censing Image: Image 1 - 1 of 1 access points C												c
X	Troubleshoot	iting	E CH	Dadiaa										

Para confirmar se o AP está no modo Sniffer da CLI 9800. Execute estes comandos:

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

Para confirmar se os pacotes estão decodificados no Wireshark. O protocolo muda de **UDP** para **802.11** e há **quadros Beacon**, como mostrado na imagem.

		ال	© 🖿		×	6	Q	(⇒	2 🖄	ē 🕹 🛛		Ð	Q
Apply a display filter <\%/>														
No.		Ľ	Time	Dest	Proto	col	Sοι	urce Po	ort	Info			Signa	l stren
		1	2021–03–…	B	802	.11	55	55		Beacor	frame,	SN=23	-39	dBm
		2	2021–03–…	B	802	.11	55	55		Beacor	frame,	SN=23	-39	dBm
		3	2021–03–…	B	802	.11	55	55		Beacor	frame,	SN=23	-39	dBm
		4	2021–03–…	В	802	.11	55	55		Beacor	frame,	SN=23	-39	dBm
		5	2021–03–…	В	802	. 11	55	55		Beacor	frame,	SN=23	-39	dBm
		6	2021–03–…	В	802	. 11	55	55		Beacor	frame,	SN=23	-39	dBm
		7	2021–03–…	В	802	. 11	55	55		Beacor	frame,	SN=23	-39	dBm
		8	2021–03–…	B	802	.11	55	55		Beacor	frame,	SN=23	-39	dBm
		9	2021–03–…	В	802	.11	55	55		Beacor	frame,	SN=23	-39	dBm
		10	2021–03–…	В	802	. 11	55	55		Beacor	frame,	SN=23	-39	dBm
		11	2021–03–…	B	802	. 11	55	55		Beacor	frame,	SN=23	-39	dBm
		12	2021-03	B	802	. 11	55	55		Beacon	frame,	SN=23	-39	dBm
		13	2021-03	В	802	. 11	55	55		Beacon	frame,	SN=23	-39	dBm

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Problema: O Wireshark não recebe nenhum dado do AP.

Solução: O servidor do Wireshark deve estar acessível pela Interface de Gerenciamento Sem Fio (WMI - Wireless Management Interface). Confirme a acessibilidade entre o servidor Wireshark e a WMI da WLC.

Informações Relacionadas

- <u>Guia de configuração do software Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS</u> XE Amsterdam 17.3.x - Capítulo: Modo de farejador
- Fundamentos do 802.11 Wireless Sniffing
- Suporte Técnico e Documentação Cisco Systems