Konfigurieren des Access Points im Sniffer-Modus auf den Catalyst Wireless Controllern der Serie 9800

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfiguration Netzwerkdiagramm Konfigurationen Konfigurieren des Access Points im Sniffer-Modus über die GUI Konfigurieren des Access Points im Sniffer-Modus über die CLI Konfigurieren des AP zum Scannen eines Kanals über die Benutzeroberfläche Konfigurieren des AP zum Scannen eines Kanals über die CLI Konfigurieren des AP zum Scannen eines Kanals über die CLI Konfigurieren von Wireshark zum Erfassen der Paketerfassung Überprüfung Fehlerbehebung Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie Sie einen Access Point (AP) im Sniffer-Modus auf einem Catalyst Wireless Controller der Serie 9800 (9800 WLC) über die grafische Benutzeroberfläche (GUI) oder die Befehlszeilenschnittstelle (CLI) konfigurieren und eine Packet Capture (PCAP) Over the Air (OTA) mit dem Sniffer AP erfassen, um Fehler zu beheben und das Verhalten von Wireless-Geräten zu analysieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfiguration des 9800 WLC
- Grundkenntnisse des 802.11-Standards

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- AP 2802
- 9800 WLC Cisco IOS®-XE Version 17.3.2a
- Wireshark 3.x

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfiguration

Wichtige Punkte:

- Es wird empfohlen, den Sniffer-Access Point in der Nähe des Zielgeräts und des AP zu haben, mit dem das Gerät verbunden ist.
- Stellen Sie sicher, dass Sie wissen, welche 802.11-Kanäle und welche Breite, welches Client-Gerät und welcher AP verwendet werden.

Netzwerkdiagramm



Konfigurationen

Konfigurieren des Access Points im Sniffer-Modus über die GUI

Schritt 1: Navigieren Sie auf der Benutzeroberfläche des 9800 WLC zu **Configuration > Wireless > Access Points** > All Access Points (**Konfiguration > Wireless > Access Points** > Alle Access Points), wie im Bild gezeigt.



Q Search Menu Items			Interface	0	Services	
			Logical		AireOS Config Translato	r
📻 Dashboard			Ethernet		Application Visibility	
		_	Wireless		Cloud Services	
	>	<u>.</u>	Layer2		Custom Application	
	_		Discovery Protocols			
	>		VLAN		Multicast	
			VTP		NetFlow	
	``		Dadia Configurations		Python Sandbox	
	ĺ.	111 1753	Radio Configurations		OoS	
			CleanAir		RA Throttle Policy	
Censing			High Throughput	≣र्झ		
M Troubloohaating			Media Parameters	10 H	Tags & Profiles	
Troubleshooting			Network		AP Join	
			Parameters		EoGRE	
		~	RRM		Flex	
		(1	Routing Protocols		Policy	
			Static Routing		Remote LAN	
			a <i>i</i>		RF	
		Ð	Security		Tags	
			AAA		WLANs	
			ACL	Ş	Wireless	
			Advanced EAP	Ť	Access Points	
			PKI Management		Advanced	
			Guest User		Air Time Fairness	
			Local EAP		Fabric	
			Local Policy			

Schritt 2: Wählen Sie den AP aus, der im Sniffer-Modus verwendet werden soll. Aktualisieren Sie auf der Registerkarte **Allgemein** den Namen des Access Points, wie im Bild gezeigt.

Cisco Catal	yst 9800-CL Wireless (Controller			Welcome admin 🛛 🗌 🍖
Q Search Menu Items	Configuration > Wireless	s > Access Point	ts	Edit AP	
Dashboard	All Access Points Number of AP(s): 1			General Interfaces General	High Availability Inventory
(Monitoring >			-	AP Name*	2802-carcerva-sniffer
Configuration	AP V AP V Name Model Sig	Admin ~ lots ~ Status	IP V Ba Address M	Location*	default location
() Administration	2802- AIR- carcerva AP2802I- 2 4 B-K9	٢	172.16.0.125 a0	Base Radio MAC	a03d.6f92.9400
C Licensing	⊲ ⊲ 1 ⊳ 10) 🔻 items per page		Ethernet MAC	00a2.eedf.6114
X Troubleshooting	> 5 GHz Radios			Admin Status	
				AP Mode	Flex v
	> 2.4 GHz Radios			Operation Status	Registered

Schritt 3: Überprüfen Sie, ob der Admin-Status aktiviert ist und ändern Sie den AP-Modus in Sniffer, wie im Bild gezeigt.

Cisco Catal	yst 9800–CL Wire	less Conti	roller				Welcome admin 🛛 🏠 📢
Q Search Menu Items	Configuration * > V	Vireless * >	Access Poi	nts	E	Edit AP	
n Dashboard	All Access F Number of AP(s): 1	Points				General Interfaces General	High Availability Inventory
Monitoring >						AP Name*	2802-carcerva-sniffer
Configuration	AP ~ AP Name Model	Slots 、	Admin ~ Status	IP ~ Address	Bi M	Location*	default location
(〇) Administration >	2802- AIR- carcerva AP280 & B-K9	21- 2	۲	172.16.0.125	a	Base Radio MAC	a03d.6f92.9400
C Licensing	∈	10 🔻	items per page			Ethernet MAC	00a2.eedf.6114
X Troubleshooting					_	Admin Status	
	5 GHz Radio	S			_	AP Mode	Sniffer 🗸
	> 2.4 GHz Rad	lios				Operation Status	Registered

Ein Popup-Fenster wird mit dem nächsten Hinweis angezeigt:

"Warnung: Wenn Sie den AP-Modus ändern, wird der Access Point neu gestartet. Klicken Sie auf Aktualisieren und auf Gerät anwenden, um fortzufahren."

Wählen Sie OK, wie im Bild gezeigt.



Schritt 4: Klicken Sie auf Aktualisieren und auf Gerät anwenden, wie im Bild gezeigt.

Edit AP									×
General	Interfaces	High Availability	Inventory	ICap	Advanced	Supp	oort Bundle		
General				Version					
AP Name	÷	2802-carcerva-sn	iffer	Primary Sof	ftware Version	1	17.3.2.32		
Location*		default location		Predownloa	aded Status	٦	N/A		
Base Radi	o MAC	a03d.6f92.9400		Predownloa	aded Version	٢	N/A		
Ethernet N	/AC	00a2.eedf.6114		Next Retry	Time	٦	N/A		
Admin Sta	itus	ENABLED		Boot Versio	n	1	1.1.2.4		
AP Mode		Sniffer	•	IOS Version	n	1	17.3.2.32		-
Operation	Status	Registered		Mini IOS Ve	ersion	C	0.0.0.0		
Fabric Sta	tus	Disabled		IP Config					lided As
LED State		ENABLED		CAPWAP P	referred Mode	IPv4			sistance
LED Brigh Level	tness	8	•	DHCP IPv4	Address	172.16	0.0.125		
<u> </u>				Static IP (IP	v4/IPv6)	0			
Cancel							🕆 Update 8	& Apply to De	vice

Ein Popup-Fenster wird angezeigt, um die Änderungen zu bestätigen und der Access Point springt, wie im Bild gezeigt.



Konfigurieren des Access Points im Sniffer-Modus über die CLI

Schritt 1: Bestimmen Sie den AP, der als Sniffer-Modus verwendet werden soll, und greifen Sie den AP-Namen zu.

Schritt 2: Ändern Sie den Namen des Access Points.

Mit diesem Befehl wird der AP-Name geändert. wobei <AP-Name> der aktuelle Name des Access Points ist.

carcerva-9k-upg#ap name <AP-name> name 2802-carcerva-sniffer Schritt 3: Konfigurieren Sie den Access Point im Sniffer-Modus.

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

Konfigurieren des AP zum Scannen eines Kanals über die Benutzeroberfläche

Schritt 1: Navigieren Sie in der Benutzeroberfläche des 9800 WLC zu **Configuration > Wireless >** Access Points (Konfiguration > Wireless > Access Points).

Schritt 2: Zeigen Sie auf der Seite Access Points die Menüliste 5-GHz-Funkmodule oder 2,4-GHz-Funkmodule an. Dies hängt vom Kanal ab, der gescannt werden soll, wie im Bild gezeigt.

Cisco Cata	Ilyst 9800-CL Wireless Controller Welcome admin 💣 🕏 🖺 🏟 🖗 🧭 🎜 Search APs and Clients Q
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	> Country

Schritt 2: Durchsuchen Sie den Access Point. Klicken Sie auf den **Pfeil nach unten**, um das Suchwerkzeug anzuzeigen, wählen Sie **Container** aus der Dropdown-Liste aus, und geben Sie den **AP-Namen ein**, wie im Bild gezeigt.

Cisco Catal	yst 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
∫ Administration →	AP Name Slot No v MAC Status Status Tag Site Tag v
© Licensing	2802-carcerva- sniffer Show items with value that: Contains 400 Image: Webauth_test tag default-site- tag Image: Im
X Troubleshooting	> 2.4 GHz R

Schritt 3: Wählen Sie den Access Point aus, und aktivieren Sie das Kontrollkästchen **Enable Sniffer** unter **Configure**> Sniffer Channel Assignment (**Sniffer-Zuweisung aktivieren**), wie im Bild gezeigt.

Cisco Catal	yst 9800–CL Wirele	ess Controller	Welcome admin 🛛 😭 🜾
Q Search Menu Items	Configuration ▼ > W	Edit Radios 5 GHz Ban	d
Dashboard	> All Access P	Antenna Moue	Umm
(2) Monitoring >	✓ 5 GHz Radios	Antenna A	$\ensuremath{\oslash}$
	Number of AP(s): 1	Antenna B	Ø
	AP Name " Contains"	Antenna C	\oslash
(O) Administration		Antenna D	$\ensuremath{\oslash}$
© Licensing	2802-carcerva-	Antenna Gain	10
K Troubleshooting	sniffer	Sniffer Channel Assign	ment
		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	pootflash
	LSC Provisio	Cancel	

Schritt 4: Wählen Sie den Kanal aus der Dropdown-Liste "**Sniff Channel**" aus, und geben Sie die **Sniffer-IP-Adresse** (Server-IP-Adresse mit Wireshark) ein, wie im Bild gezeigt.

Cisco Cisco Cata	lyst 9800-CL Wireless Controller	Welcome admin 🛛 🏠 🕵
Q Search Menu Items	Configuration -> W Edit Radios 5 GH	Hz Band
Dashboard	> All Access P	Unni
Monitoring >	Antenna A S GHz Radio:	
	Antenna B Number of AP(s): 1	\oslash
Configuration >	AP Name " Contains" Antenna C	$\tilde{$
(文) Administration >	Antenna D	Ø
© Licensing	AP Name Antenna Gain	10
÷ -	2802-carcerva-	
X Troubleshooting	Sniffer Channel	Assignment
	Enable Sniffing	Ø
	2.4 GHz Radi Sniff Channel	36 🔹
	Dual-Band R	172.16.0.190
	Sniffer IP Status	Valid
	Download Core Du	ump to bootflash
	> LSC Provisio	

Schritt 5: Wählen Sie die Kanalbreite aus, die das Zielgerät und der Access Point beim Anschluss verwenden.

Navigieren Sie zu **Configure> RF Channel Assignment**, um dies zu konfigurieren, wie im Bild gezeigt.

		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- AP28021	Admin Status	sniffer	Channel Width	40 MHz 🗸
	sniffer 🚠 B-K9	Admin Status		Assignment Method	20 MHz
6 Electioning		CleanAir Admin Status	ENABLED	Channel Number	40 MHz 80 MHz
K Troubleshooting	S GHz Radio	Antenna Parameters		Channel Number	160 MHz
				Tx Power Level Assignment	ent
	Number of AP(s): 1	Antenna Type	Internal 🔻		
	AP Name 🗸	Antenna Mode	Omni	Current Tx Power Level	6
	2802-carcerva-	Antenna A	Ø	Assignment Method	Custom v
		Antenna B	Ø	Transmit Power	6 🔹

Konfigurieren des AP zum Scannen eines Kanals über die CLI

Schritt 1: Aktivieren Sie den Kanalschniff auf dem Access Point. Führen Sie diesen Befehl aus:

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

Beispiel:

carcerva-9k-upg#ap name 2802-carcerva-sniffer sniff dot11a 36 172.16.0.190 Konfigurieren von Wireshark zum Erfassen der Paketerfassung

Schritt 1: Starten Sie Wireshark.

Schritt 2: Wählen Sie das Menüsymbol Capture options aus Wireshark, wie im Bild gezeigt.



Schritt 3: Bei dieser Aktion wird ein Popup-Fenster angezeigt. Wählen Sie die Kabelschnittstelle aus der Liste als Quelle der Erfassung aus, wie im Bild gezeigt.

••	•	1	Wireshark · Ca	pture Options				
			Input Outp	ut Options				
	Interface	Traffic		Link-layer Header	Promiscı	Snaplen (B)	Buffer (MB)	Monitor
	▶ utun4			BSD loopback		default	2	
	▶ utun5			BSD loopback		default	2	
	eter.9			DOD loopback		default	2	_
	USB 10/100/1000 LAN: en10			Ethernet	 ✓ 	default	2	-
	Loopbook: Io0	A. 40 A		PCD loophool:		dofoult	2	
	Wi-Fi: en0			Ethernet	S	default	2	
	Thunderbolt Bridge: bridge0			Ethernet		default	2	
	Thunderbolt 1: en1			Ethernet		default	2	
	Thunderbolt 2: en2			Ethernet	S	default	2	
	Thunderbolt 3: en3			Ethernet	S	default	2	
	 Enable promiscuous mode on all interfa Capture filter for selected interfaces: 	ces Inter a capture t	filter		•	Mana	ge Interface Compile Bl	PFs
E	lelp					(Close	Start

Schritt 4: Unter dem **Erfassungsfilter für ausgewählte Schnittstellen:** Geben Sie **udp port 5555 ein**, wie im Bild gezeigt.

late de se	17-040-	Litela leves the des	l Brownia and	0 (0)	0.41 (140)		l Ocentrar Ellera
Interface ▶ utun3	Traffic	LINK-layer Header	Promisci	detault	Z	Monitor	Capture Filter
▶ utun4		BSD loopback	S	default	2		
▶ utun5		BSD loopback	S	default	2		
utun6		BSD loopback	S	default	2		
USB 10/100/1000 LAN: e	n10	Ethernet	S	default	2		udp port 5555
Loopback: Io0		BSD loopback	S	default	2		
Wi-Fi: en0		Ethernet		default	2		
Thunderbolt Bridge: brid	ge0	Ethernet	S	default	2		
Thunderbolt 1: en1		Ethernet		default	2		
Thunderbolt 2: en2		Ethernet		default	2		
Thunderbolt 3: en3		Ethernet		default	2		
🗹 Enable promiscuous mode	e on all interfaces						Manage Interfaces
Capture filter for selected int	erfaces: 📕 udp port 5555					•	Compile BPFs

Schritt 5: Klicken Sie auf Start, wie im Bild gezeigt.

terfac	ce JD-3	Traffic	Link-layer Head	ler K	Promisci	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
utu	un4		BSD loopbac	k		default	2		
utu	Jn5		BSD loopbac	k	S	default	2		
utu	n6		BSD loopbac	k	S	default	2		
US	B 10/100/1000 LAN: en10		Ethernet			default	2		udp port 5555
Loc	opback: Io0		BSD loopbac	k	S	default	2		
Wi	-Fi: en0		Ethernet		S	default	2		
Th	underbolt Bridge: bridge0		Ethernet		S	default	2		
Th	underbolt 1: en1		Ethernet		S	default	2		
Th	underbolt 2: en2		Ethernet		S	default	2		
Th	underbolt 3: en3		Ethernet			default	2		
Enal	ble promiscuous mode on all interface:	5							Manage Interfaces
pture	e filter for selected interfaces: 📙 udg	o port 5555					×	-	Compile BPFs

Schritt 6: Warten Sie, bis Wireshark die erforderlichen Informationen erfasst hat, und wählen Sie die **Stopp-**Schaltfläche aus Wireshark aus, wie im Bild gezeigt.



Tipp: Wenn das WLAN Verschlüsselung wie Pre-shared Key (PSK) verwendet, stellen Sie sicher, dass die Erfassung den 4-Wege-Handshake zwischen dem Access Point und dem gewünschten Client abfängt. Dies kann erfolgen, wenn der OTA-PCAP startet, bevor das Gerät dem WLAN zugeordnet wird, oder wenn der Client deauthentifiziert und erneut authentifiziert wird, während die Erfassung ausgeführt wird.

Schritt 7: Wireshark decodiert die Pakete nicht automatisch. Um die Pakete zu dekodieren, wählen Sie eine Zeile aus der Erfassung aus, klicken Sie mit der rechten Maustaste, um die Optionen anzuzeigen, und wählen Sie **Decode As...**, wie im Bild gezeigt.

۷	1		0) 🖿	0000	×	6	٩	(⇒		$\overline{\mathbf{e}}$	<u> </u>			Ð	Q
	Apply	a disp	lay filte	r <೫/>	,												
Ν	o.		Time		Dest	Proto	col	So	urce P	ort	Info					Signa	strer
ſ	_	1	202	1–03–	. 1	UDP		55	555		5555	i →	5000	Len:	=400		
		2	202	1–03–	. 1	UDP		55	55		5555	i →	5000	Len:	=387		
		3	202	1–03–	. 1	UDP		55	55		5555	i →	5000	Len:	=385		
		4	202	1–03–	. 1	UDP		55	55		5555	i →	5000	Len=	=400		
		5	202	1–03–	. 1	UDP		55	55		5555	i →	5000	Len:	=387		
		6	202	1–03–	. 1	UDP		55	55		5555	i →	5000	Len:	=385		
		7	202	1–03–	. 1	UDP		55	555		5555	i →	5000	Len:	=400		
		8	202	1–03–	. 1	UDP		55	55		5555	i →	5000	Len	=387		
		9	202	1–03–	. 1	UDP		1	Mark/Unmark Packet Ignore/Unignore Packet Set/Unset Time Reference Time Shift Packet Comment					.en=	=385		
		10	202	1–03–	. 1	UDP		1						.en=	=400		
		11	202	1–03–	. 1	UDP		1						.en=	=387		
		12	202	1–03–	. 1	UDP		-						.en=	=385		
		13	202	1–03–.	. 1	UDP		-	Tuek			••		.en=	=400		
		14	202	1-03	. 1	UDP		-	Edit I	Resolv	ed Nar	ne		.en=	=387		
		15	202	1-03	. 1	UDP			Appl	v as Fi	ilter			.en=	=385		
		16	202	1-03	. 1	UDP		-	Prep	are as	Filter		•	.en=	=400		
		17	202	1-03	. 1	UDP			Conv	ersati	on Filte	er	•	.en=	=387		
		18	202	1-03	. 1	UDP			Colo	rize Co	onversa	ation	1 Þ	.en=	=385		
		19	202	1-03	. 1	UDP			SCT	>			•	.en=	=400		
		20	202	1-03	. 1	UDP			Follo	w			<u> </u>	.en=	=387		
		21	202	1-03	. 1	UDP			Сору	,			•	.en=	=385		
		22	202	1-03	1	UDP		-						.en=	=400		
		23	202	1 03	. I	UDP			Deer		otoron	000		en	-38/		
		24	202	1-03	. 1	UDP		1	Deco		et in N	914/ 1	NIDGON	en-	-385		
		25	202	1-03	. I	UDP		4	31100	Frack		ew i	Thuow	en=	=3/9		

Schritt 8: Ein Popup-Fenster wird angezeigt. Wählen Sie die Schaltfläche Hinzufügen aus, und fügen Sie einen neuen Eintrag hinzu. Wählen Sie die folgenden Optionen aus: **UDP-Port** von **Field, 555** von **Value**, **SIGCOMP** von **Default** und PEEKREMOTE von Current, wie im Bild gezeigt.



Schritt 9: Klicken Sie auf OK. Die Pakete werden dekodiert und sind bereit, die Analyse zu starten.

Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

So überprüfen Sie, ob sich der Access Point über die Benutzeroberfläche des 9800 im Sniffer-Modus befindet:

Schritt 1: Navigieren Sie auf der Benutzeroberfläche des 9800 WLC zu **Configuration > Wireless >** Access Points> All Access Points (Konfiguration > Wireless > Access Points > Zugangspunkte).

Schritt 2: Durchsuchen Sie den Access Point. Klicken Sie auf den Pfeil nach unten, um das Suchtool anzuzeigen, wählen Sie aus der Dropdown-Liste **Contains** aus, und geben Sie den AP-Namen ein, wie im Bild gezeigt.

.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

Schritt 3: Stellen Sie sicher, dass der Admin-Status mit dem Häkchen in grün und der AP-Modus Sniffer lautet, wie im Bild gezeigt.

¢	cisco	Cisco Cata 17.3.2a	alyst 9800-C	L Wirele	ss Contro	oller	Welcom	e admin 🖌 😭	\$	¢ 🕸 6	Search /	APs and Clients (ג	۲
Q	Search Menu It	ems	Configuratio	n*> Wire	eless≛>	Access Poi	ints							
R	Dashboard		💙 All Ac	cess Poi	nts									
3	Monitoring >										\$°			
Ľ	Configuration		AP ~ Name	AP ~ Model	Slots ~	Admin v Status	IP v Address	Base Radio v MAC	AP ↓ Mode	Operation ~ Status	Configuration Status	Policy V Tag	Site v Tag	r 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		H	1 ⊫	10 🔻 ite	ems per page	•					1 - 1 of 1 access	points	c
×	Troubleshoo	ting	E CU	Dedice										

Um zu überprüfen, ob sich der Access Point in der CLI 9800 im Sniffer-Modus befindet. Führen Sie folgende Befehle aus:

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

Um zu bestätigen, dass die Pakete auf Wireshark dekodiert werden. Das Protokoll wechselt von **UDP** zu **802.11** und es werden **Beacon-Frames** angezeigt, wie im Bild gezeigt.

•														
		ø	© 🖿		×	6	Q	(⇒	警 쥼	· 🕹 🛛		Ð	Q
📕 Ap	oply a d	ispla	y filter <೫/>											
No.		<u> </u>	Time	Dest	Protoc	:ol	Sou	ırce 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–…	В	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–…	В	802.	11	55	55		Beacon	frame,	SN=23	-39	dBm
		11	2021–03–…	B	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

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Problem: Wireshark empfängt keine Daten vom Access Point.

Lösung: Der Wireshark-Server muss über die Wireless Management Interface (WMI) erreichbar sein. Bestätigen Sie die Erreichbarkeit zwischen dem Wireshark-Server und der WMI vom WLC.

Zugehörige Informationen

- Cisco Catalyst Wireless Controller Software Configuration Guide 9800, Cisco IOS XE Amsterdam 17.3.x - Kapitel: Sniffer-Modus
- Grundlagen von 802.11 Wireless Sniffing
- <u>Technischer Support und Dokumentation für Cisco Systeme</u>