

يجمع sniffer عضو في لوصول اة طقن نيوكت Catalyst 9800 اة كلس الال مكحت ال اادحو

اايوت حمل ال

[ةمدقم ال](#)

[ةيساس ال اابلطت ال](#)

[اابلطت ال](#)

[ةمدختس ال اانوكم ال](#)

[نيوكت ال](#)

[ةكبش ال ليطي طخت ال مسر ال](#)

[اانوكت ال](#)

[GUI قيرط نع بولس ا sniffer في AP تل كش](#)

[CLI قيرط نع بولس ا sniffer في ap تل كش](#)

[ةيموسر ال امدختس ال اة اوج اوج ريع اانق حسم لوصول اة طقن نيوكت](#)

[\(رم اوالا رطس اة اوج\) CLI ريع اانق حسم لوصول اة طقن نيوكت](#)

[ةمزحل ا طاقت ال اعمجل Wireshark نيوكت](#)

[ةحصل ال نم ققحت ال](#)

[اهحال ص او ااطخ ال افاشكت سا](#)

[ةلص ا اذ اامول عم](#)

ةمدقم ال

9800 اة زافح اة اام يجمع بولس ا sniffer في (ap) اة طقن اذف نم لكشي نا فيك اة قيثو اذف فص ي (CLI) نراق طخ رم ا و (gui) نراق لمعتسم مسر ال لال خ نم (9800 WLC) مكحت زا هج كلس ال sery تل لحو تيرحت sniffer ap in order to عم (OTA) اوه ال يلع (PCAP) ضبق طبر عم جي نا فيكو افرصت ي كلس ال .

ةيساس ال اابلطت ال

اابلطت ال

ةيلال ال اعيضاوم ل ابل اة فرعم كي دل نوكت نا ب Cisco ي صوت:

- 9800 WLC نيوكت
- 802.11 راي عم ب اة ساس اة فرعم

ةمدختس ال اانوكم ال

ةيلال ال اة اام ال اانوكم ل اوج ارب ال ااراص ال اذف دن تسم ال اذف اة اراول اامول عم ال دن تس:

- 2802 لوصول اة طقن
- 9800 WLC Cisco IOS®-XE، رادص ال 17.3.2a
- Wireshark 3.x

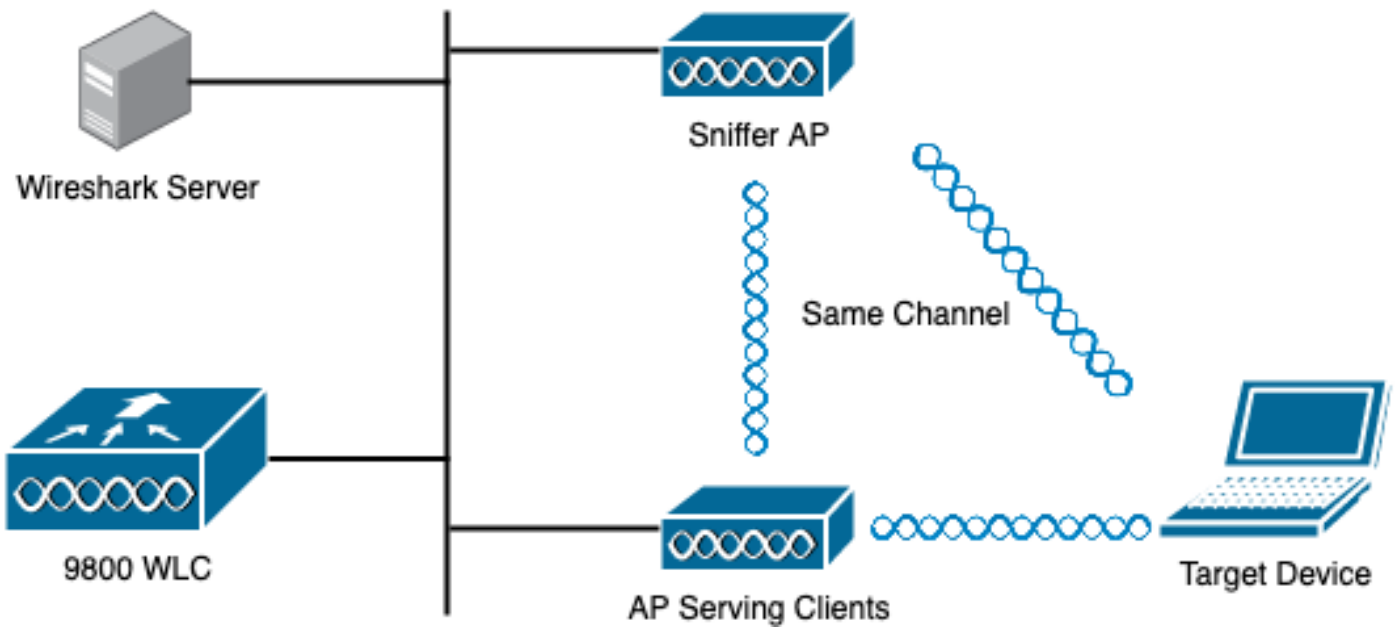
ةصاخ ةي لمعم ةئي ب ي ف ةدوجوملا ةزهجالا نم دنتسملا اذه ي ف ةدراولما تامولعملما ءاشنإ م ت ت ناك اذا . (يضا رتفا) حوسمم نيوكتب دنتسملا اذه ي ف ةمدختسملا ةزهجالا عيمج ت ادب رما يال لمحتحمل ريثاتلل كمهف نم دكات ف ، ليغشتلا دي ق كتكبش

نيوكتلا

اهي ف لماتلا بجي روما

- لوصولا ةطقنو فدهتسملا زاهجالا نم ةبيري ق sniffer لوصولا ةطقن نوكتي ناب ي صوي .
اهب الصتم زاهجالا اذه نوكتي يتلا
- لوصولا ةطقن مادختساو لي م عل زاهجو ضرعلاو 802.11 ةانقلا ةفرعم نم دكات

ةكبش ل ل ي طي تختلا مسرلا



تانيوكتلا

GUI قيرط نع بولسا sniffer ف AP تلاكش

(WLC) تاموسرلا مدختسم ةهجاوب ةصاخلا (GUI) ةيموسرلا مدختسملا ةهجاو ي ف 1. ةوطخلا وه امك ، لوصولا طاقن عيمج > لوصولا طاقن > يكلسال > نيوكتلا ل ل لقتنا ، 9800 زارط ةروصولا ي ف حضورم .



Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Licensing

Troubleshooting

Interface

Logical

Ethernet

Wireless

Layer2

Discovery Protocols

VLAN

VTP

Radio Configurations

CleanAir

High Throughput

Media Parameters

Network

Parameters

RRM

Routing Protocols

Static Routing

Security

AAA

ACL

Advanced EAP

PKI Management

Guest User

Local EAP

Local Policy

Services

AireOS Config Translator

Application Visibility

Cloud Services

Custom Application

IOx

mDNS

Multicast

NetFlow

Python Sandbox

QoS

RA Throttle Policy

Tags & Profiles

AP Join

EoGRE

Flex

Policy

Remote LAN

RF

Tags

WLANs

Wireless

Access Points

Advanced

Air Time Fairness

Fabric

بيوت الة مال ع لى ع sniffer. ع ض و ي ف ا م ا د خ ت س ا ي ف ب غ ر ت ي ت ل ا ل و ص و ل ا ة ط ق ن د د ح . 2 ة و ط خ ل ا ة ر و ص ل ا ي ف ح ض و م و ه ا م ك ، ل و ص و ل ا ة ط ق ن م س ا ث ي د ح ت ب م ق ، م ا ع .

Cisco Catalyst 9800-CL Wireless Controller 17.3.2a

Welcome admin

Configuration > Wireless > Access Points

All Access Points

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address	Bl
2802-carcerva	AIR-AP2802I-B-K9	2	✓	172.16.0.125	ac

1 10 items per page

5 GHz Radios

2.4 GHz Radios

Edit AP

General Interfaces High Availability Inventory

General

AP Name* 2802-carcerva-sniffer

Location* default location

Base Radio MAC a03d.6f92.9400

Ethernet MAC 00a2.eedf.6114

Admin Status **ENABLED**

AP Mode Flex

Operation Status Registered

ةروصل ال ي حضورم وه امك ، sniffer الى بولسأ ap ل تريغ نكمي عضو Admin تقود .3 ةوطخلا

Cisco Catalyst 9800-CL Wireless Controller 17.3.2a

Welcome admin

Configuration > Wireless > Access Points

All Access Points

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address	Bl
2802-carcerva	AIR-AP2802I-B-K9	2	✓	172.16.0.125	ac

1 10 items per page

5 GHz Radios

2.4 GHz Radios

Edit AP

General Interfaces High Availability Inventory

General

AP Name* 2802-carcerva-sniffer

Location* default location

Base Radio MAC a03d.6f92.9400

Ethernet MAC 00a2.eedf.6114

Admin Status **ENABLED**

AP Mode Sniffer

Operation Status Registered

ةيلات ال ةطخالمل ام قثب نم راطا رهظي:

قوف رقنا .لوصول ةطقن ديهمت ةداعا الى لوصول ةطقن عضو ريغت يدؤيس :ريذحت" ةعباتمل ل زاهجال الى ع قيبطتو شيذحت

ةروصل ال ي حضورم وه امك ، قفاوم دح

AP Configuration

Warning: Changing the AP mode will cause the AP to reboot . Click Update & Apply to Device to Proceed

OK

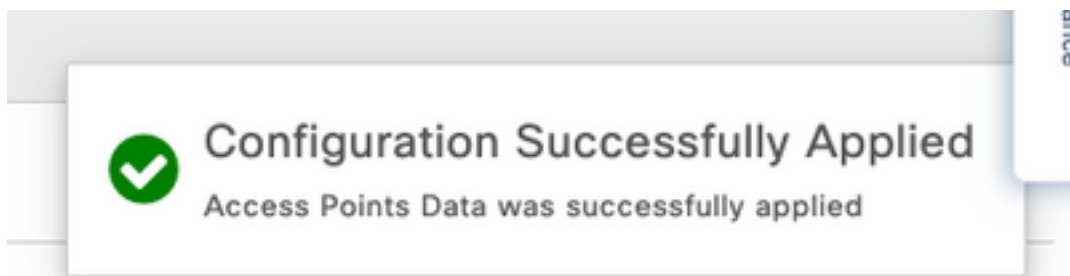
ة. لوصول ال ف حضم وه امك ، زاهال ال ل ق ب ط و ث د ح ت ال ع ر ق ن ا . 4 ة و ط خ ال

Edit AP

- General
- Interfaces
- High Availability
- Inventory
- ICap
- Advanced
- Support Bundle

General		Version	
AP Name*	2802-carcerva-sniffer	Primary Software Version	17.3.2.32
Location*	default location	Predownloaded Status	N/A
Base Radio MAC	a03d.6f92.9400	Predownloaded Version	N/A
Ethernet MAC	00a2.eedf.6114	Next Retry Time	N/A
Admin Status	ENABLED <input checked="" type="checkbox"/>	Boot Version	1.1.2.4
AP Mode	Sniffer	IOS Version	17.3.2.32
Operation Status	Registered	Mini IOS Version	0.0.0.0
Fabric Status	Disabled	IP Config	
LED State	ENABLED <input checked="" type="checkbox"/>	CAPWAP Preferred Mode	IPv4
LED Brightness Level	8	DHCP IPv4 Address	172.16.0.125
		Static IP (IPv4/IPv6)	<input type="checkbox"/>

ة. لوصول ال ف حضم وه امك ، لوصول ال ة ط ق ن ت ا ب و ت ا ر ي غ ت ال ال د ي ك ا ت ل ق ث ب ن م ر ا ط ا ره ظ ي



CLI ق ب ر ط ن ع ب و ل س ا س niffer ف ال ت ل ك ش

ة ط ق ن م س ا ذ خ ا ت و sniffer ع ض و ك ا م ا د خ ت س ا ف ب غ ر ت ي ت ال ل و ص و ل ال ة ط ق ن د ح . 1 ة و ط خ ال ل و ص و ل

ل و ص و ل ال ة ط ق ن م س ا ل ي د ع ت ب م ق . 2 ة و ط خ ال

ة ط ق ن ل ي ل ا ح ال م س ال ال وه <AP-name> ش ي ح . ل و ص و ل ال ة ط ق ن م س ا ل ي د ع ت ب ر م ال ال ا ذ ه م و ق ي ل و ص و ل

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

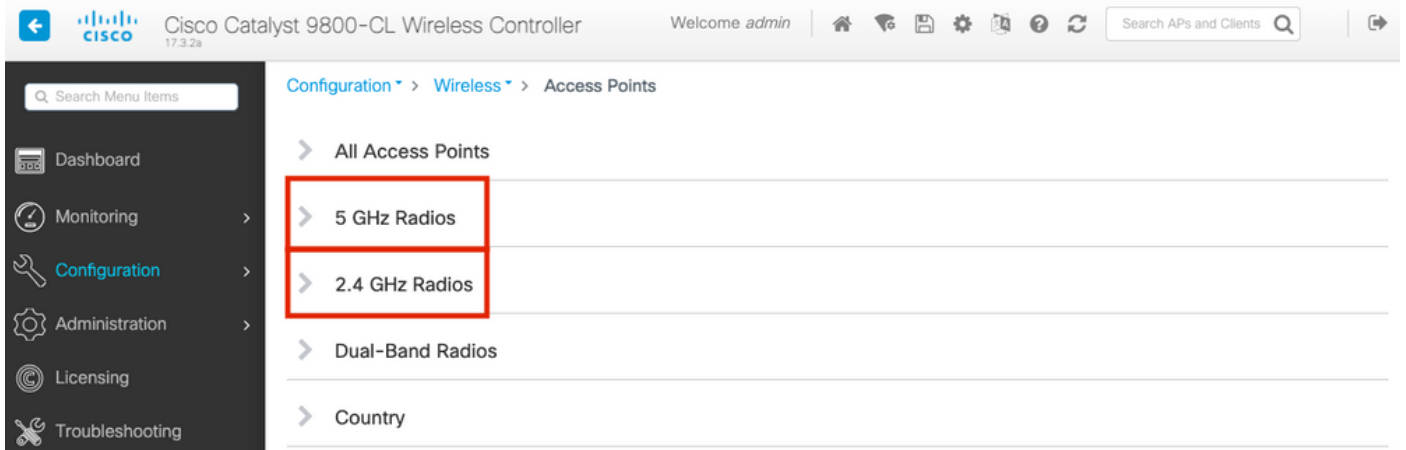
ب. بولسأ sniffer في ال ap ل تل كش 3. ةوطخل

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

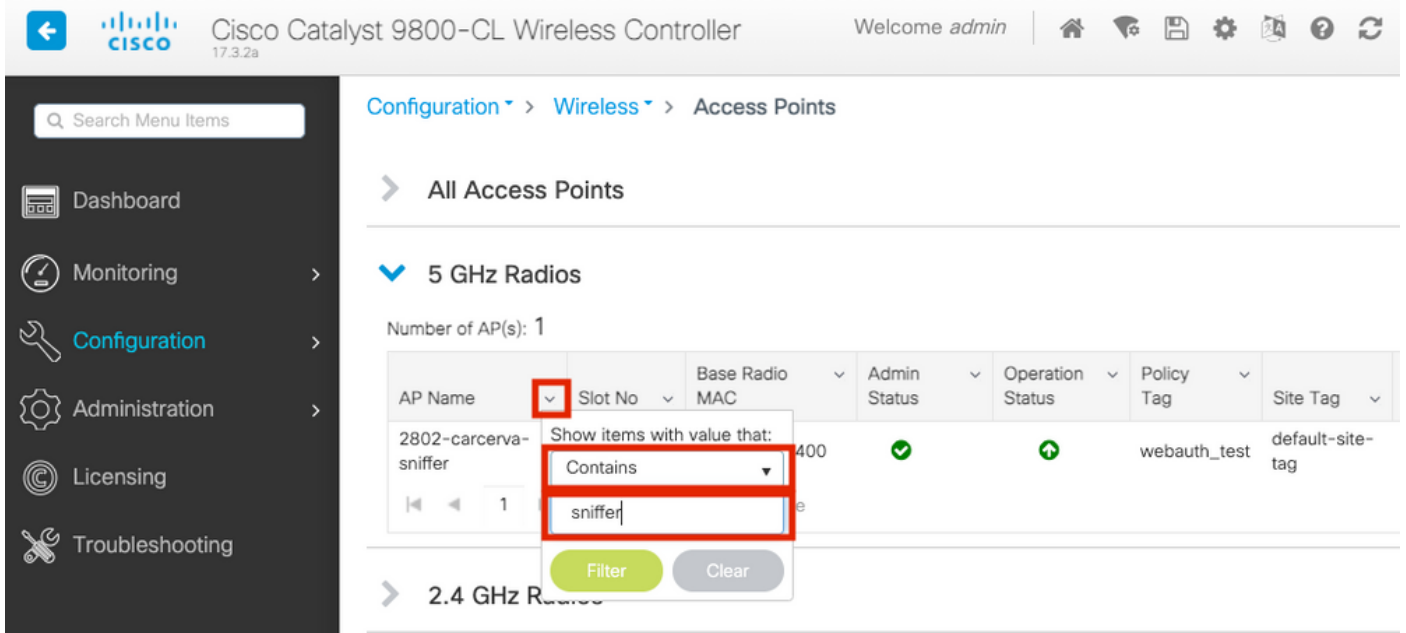
ةيموسرللا مدختسمللا ةهجاو ربع ةانق ح سمل لوصو ةطقن نيوكت

> يكلسال > نيوكتال ال ل لقتنا ، 9800 زارط WLC ةيموسرللا مدختسمللا ةهجاو في 1. ةوطخل
لوصولا طاقن .

ويدارلا ةزهجأ وأ زتره ايج 5 وي دارلا ةزهجأ ةمئاق ضرعب مق ، لوصولا طاقن ةح ف ص في 2. ةوطخل
في حضورم وه امك ، يئوضلا ح سمللا في ب غرت يتلا ةانق ال ال ل لذ دم تعي . زتره ايج 2. 4
ةروصللا .



ددحو ، شحبلا ةادأ ضرعل لفسأل مهسلا رز ال ل ع رقنا . لوصولا ةطقن في شحبا 2. ةوطخل
ةروصللا في حضورم وه امك ، لوصولا ةطقن مسا بتكاو ، ةلدسنملا ةمئاق ال نم Contains



ةانق <configure>sniffer تحت enable sniffer راي تخال ال ةناخ ددحو لوصولا ةطقن ددح 3. ةوطخل
ةروصللا في حضورم وه امك ، نييعت

Cisco Catalyst 9800-CL Wireless Controller 17.3.2a Welcome admin

Configuration > W Edit Radios 5 GHz Band

Configure Detail

All Access P

5 GHz Radios

Number of AP(s): 1

AP Name * Contains*

AP Name

2802-carcerva-sniffer

1

2.4 GHz Radi

Dual-Band R

Country

LSC Provisio

Antenna Mode	Omni
Antenna A	<input checked="" type="checkbox"/>
Antenna B	<input checked="" type="checkbox"/>
Antenna C	<input checked="" type="checkbox"/>
Antenna D	<input checked="" type="checkbox"/>
Antenna Gain	10

Sniffer Channel Assignment

Enable Sniffing

Sniff Channel 36

Sniffer IP* 172.16.0.190

Sniffer IP Status Valid

Download [Core Dump](#) to bootflash

Cancel

IP ناونع (IP Sniffer ناونع) بتك او Sniff ةانق ةلدسنملا ةمئاقلا نم ةانقلا ددح. 4 ةوطخلا ةروصلال يف حضوم وه امك، (Wireshark عم مداخلل

Cisco Catalyst 9800-CL Wireless Controller 17.3.2a

Welcome admin

Configuration > Edit Radios 5 GHz Band

Configure Detail

All Access Points

5 GHz Radios

Number of AP(s): 1

AP Name "Contains"

AP Name: 2802-carcerva-sniffer

2.4 GHz Radios

Dual-Band Radios

Country

LSC Provisioning

Antenna Mode: Omni

Antenna A:

Antenna B:

Antenna C:

Antenna D:

Antenna Gain: 10

Sniffer Channel Assignment

Enable Sniffing:

Sniff Channel: 36

Sniffer IP*: 172.16.0.190

Sniffer IP Status: Valid

Download Core Dump to bootflash

Cancel

ليوصول دنع لوصولو ةطقنو فدهت سمل زاوجل هم دختسي يذلا ةانقلا ضرع ددح 5 ةوطخل.
 ةروصلال ي فحزوم وه امك ، اذه نيوكتل يكلساللا ددرتلا ةانق نييعت > نيوكت لىل لقتنا

Dashboard

Monitoring

Configuration

Administration

Licensing

Troubleshooting

All Access Points

Number of AP(s): 1

AP Name	AP Model
2802-carcerva-sniffer	AIR-CT5502-K9

5 GHz Radios

Number of AP(s): 1

AP Name: 2802-carcerva-sniffer

General

AP Name: 2802-carcerva-sniffer

Admin Status: ENABLED

CleanAir Admin Status: ENABLED

Antenna Parameters

Antenna Type: Internal

Antenna Mode: Omni

Antenna A:

Antenna B:

RF Channel Assignment

Current Channel: 36

Channel Width: 40 MHz

Assignment Method: 40 MHz

Channel Number: 20 MHz, 40 MHz, 80 MHz, 160 MHz

Tx Power Level Assignment

Current Tx Power Level: 6

Assignment Method: Custom

Transmit Power: 6

(رماوالا رطس ةهجاو) CLI رب ةانق ح سمل لوصولو ةطقن نيوكت

رماً اذه لغش ap. لى ع sniff ةانقلا تنك 1. ةوطخلا

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

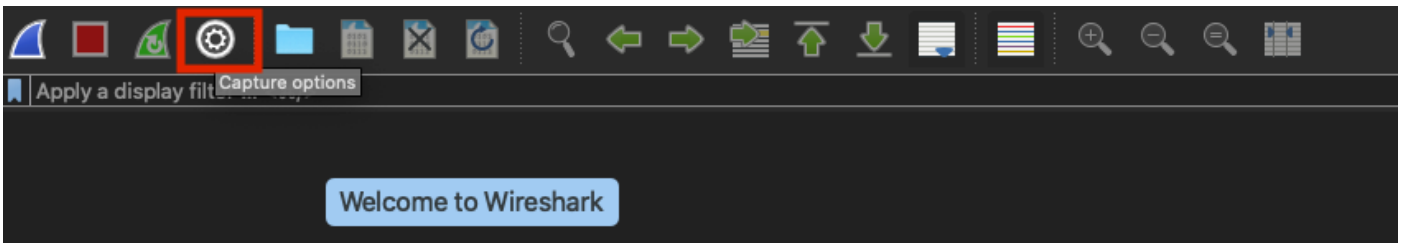
الاثم:

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

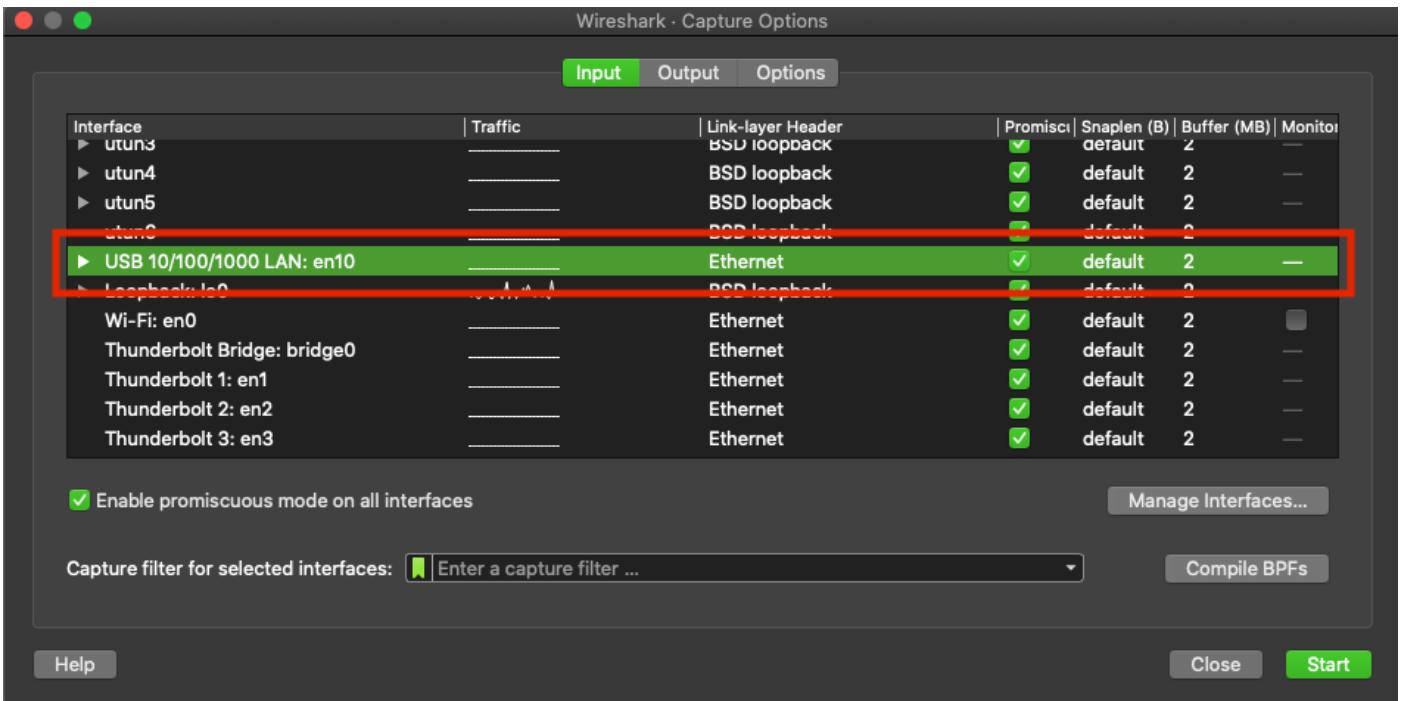
ةمزل طاقلا عمجل Wireshark نيوكت

Wireshark قالا ط 1. ةوطخلا

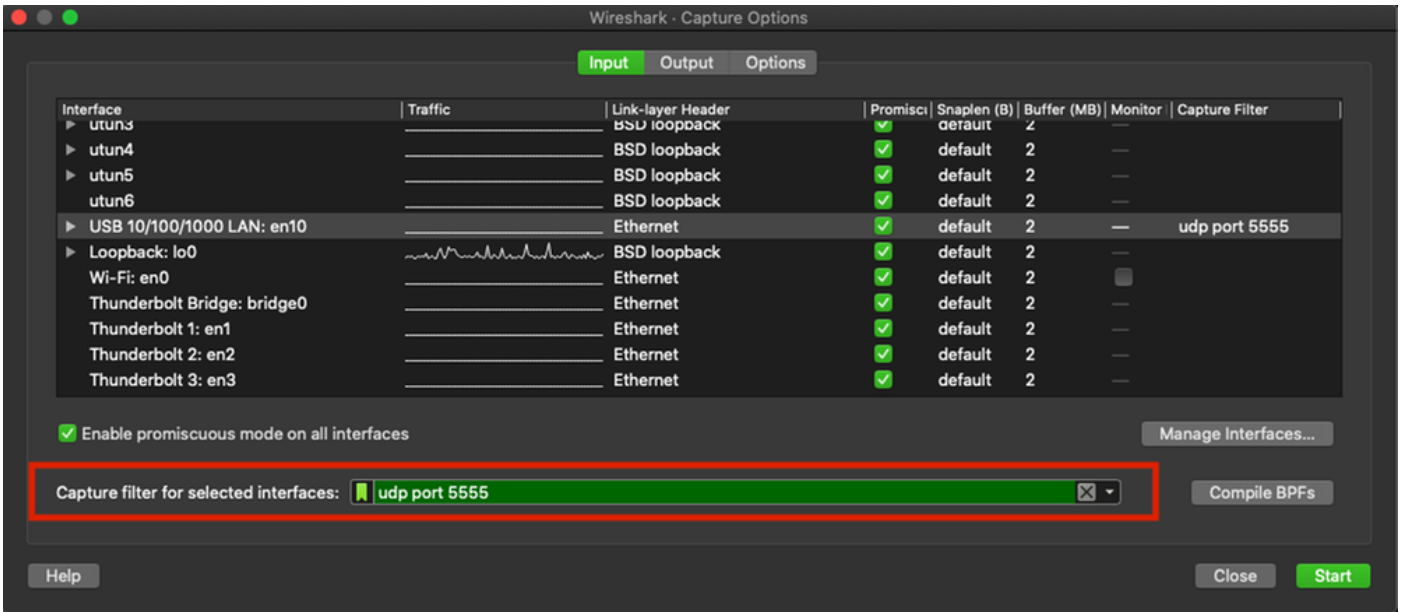
ةروصلال يف حضوم وه امك، Wireshark نم طاقلا تاريخ ةمئاق ةنوقي ا دح 2. ةوطخلا



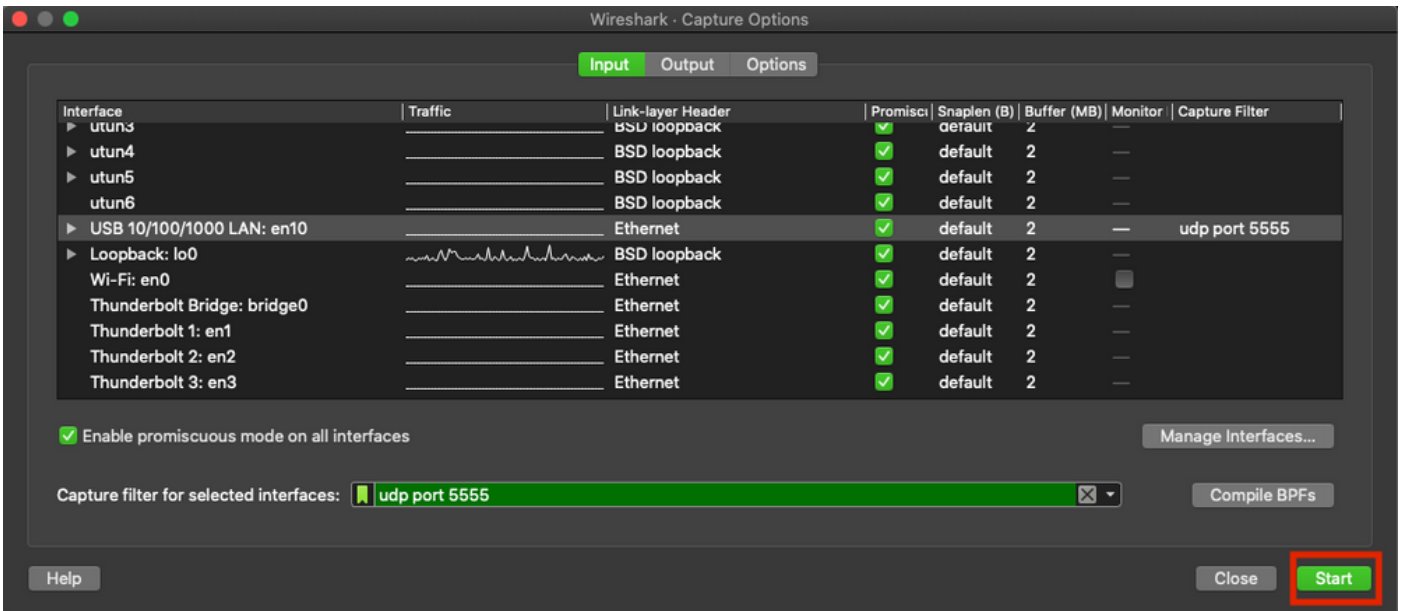
ردصمك ةمئاقلا نم ةيكل لسل ةهجال دح. ةقثب نم ةذفان ءارجلا اذه ضرعي 3. ةوطخلا ةروصلال يف حضوم وه امك، طاقلا لال



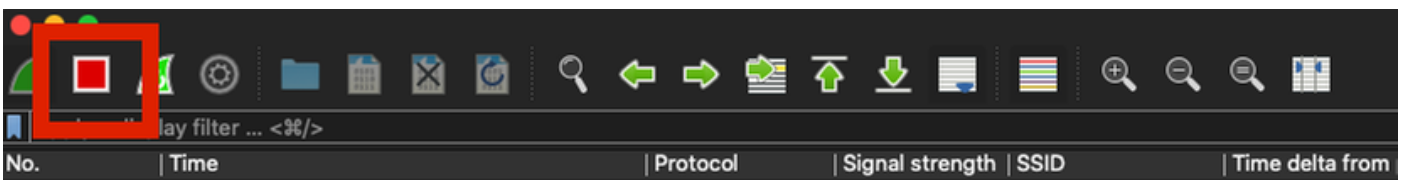
وه امك، udp port 555 بتك، لقحلا ع برم: ةدحمل تاهاجاول طاقلا لال حشرم تحت 4. ةوطخلا ةروصلال يف حضوم



ةروصلال يف حضوم وه امك ،ءدب لىل ع رقنا .5 ةوطخلال



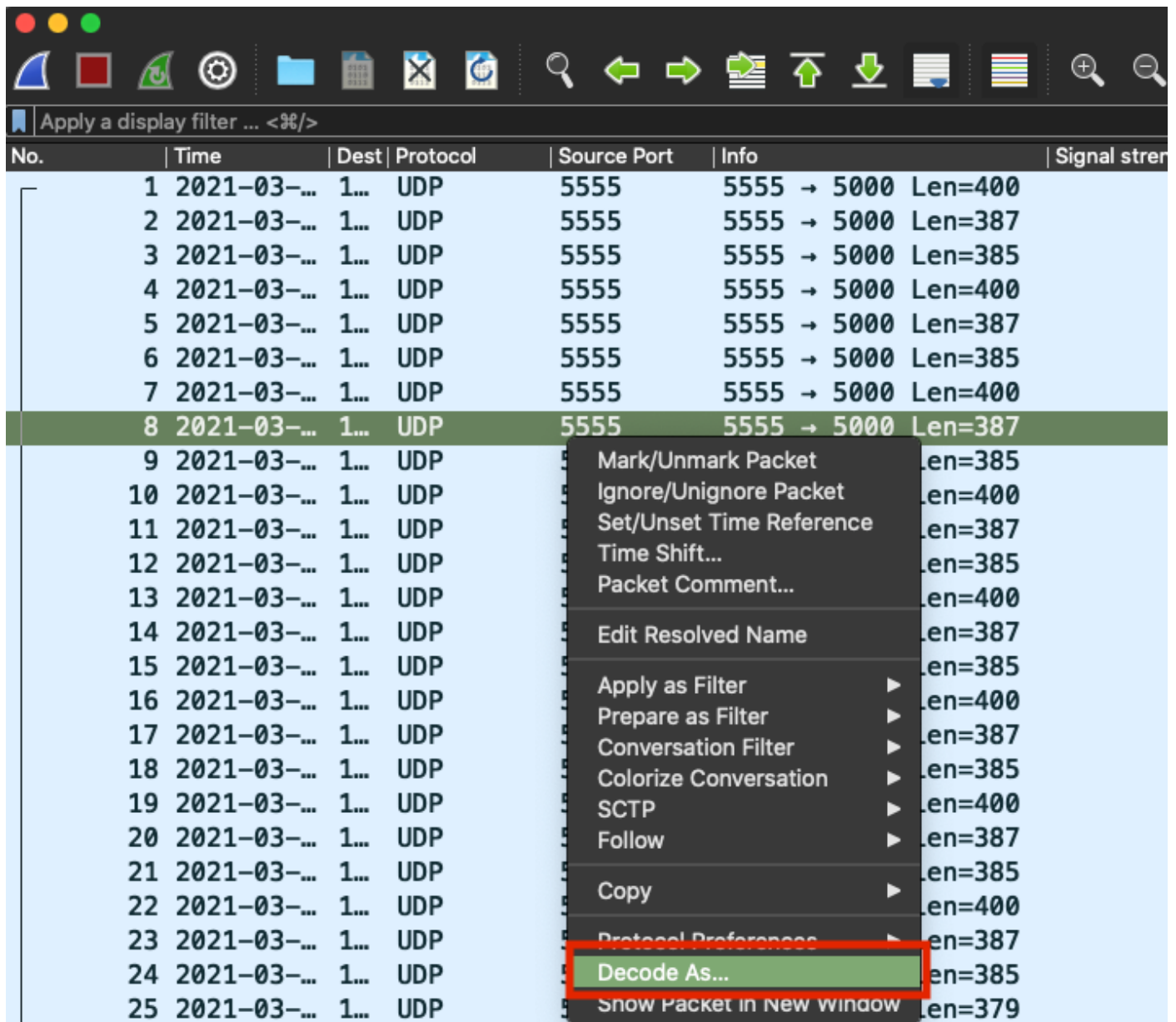
نم فاقى رز ددحو ةبولطلم تامولعمل عمج ب Wireshark موقى لىل رظتنا .6 ةوطخلال
ةروصلال يف حضوم وه امك ،Wireshark.



لثم ريفشلتال مدختست (WLAN) ةىكللساللا ةىلحملال ةكبلشلال تناك اذا :حيملت
لاصلتال ةحفاصم دىصى طاقتللالا نا نم دكأتف ،اقبسم كرتشملا حاتفملا
أدب اذا كلذب مايقوللا نكمىو .بولطلملا لىملاو لوصولال ةطقن نىب هاجتاللا ةىعابرلا
اذا و (WLAN) ةىكللساللا ةىلحملال ةكبلشلاب زاهللا نارتقا لبق OTA PCAP لىغشت
طاقتللالا لىغشت ءانثا هتقداصم دىعأو هىلعل قدصم رىغ لىملا ناك

رطس ددح ،مزلال زىمرت ك ف لچأ نم .اىئاقلت مزحلال زىمرت ك فب Wireshark موقى ال .7 ةوطخلال
وه امك ،.ك زىمرتال ك ف ددحو ،تاراىللا ضرعل نميال سواملا رزب رقنلا مدختسا ،طاقتللالا نم

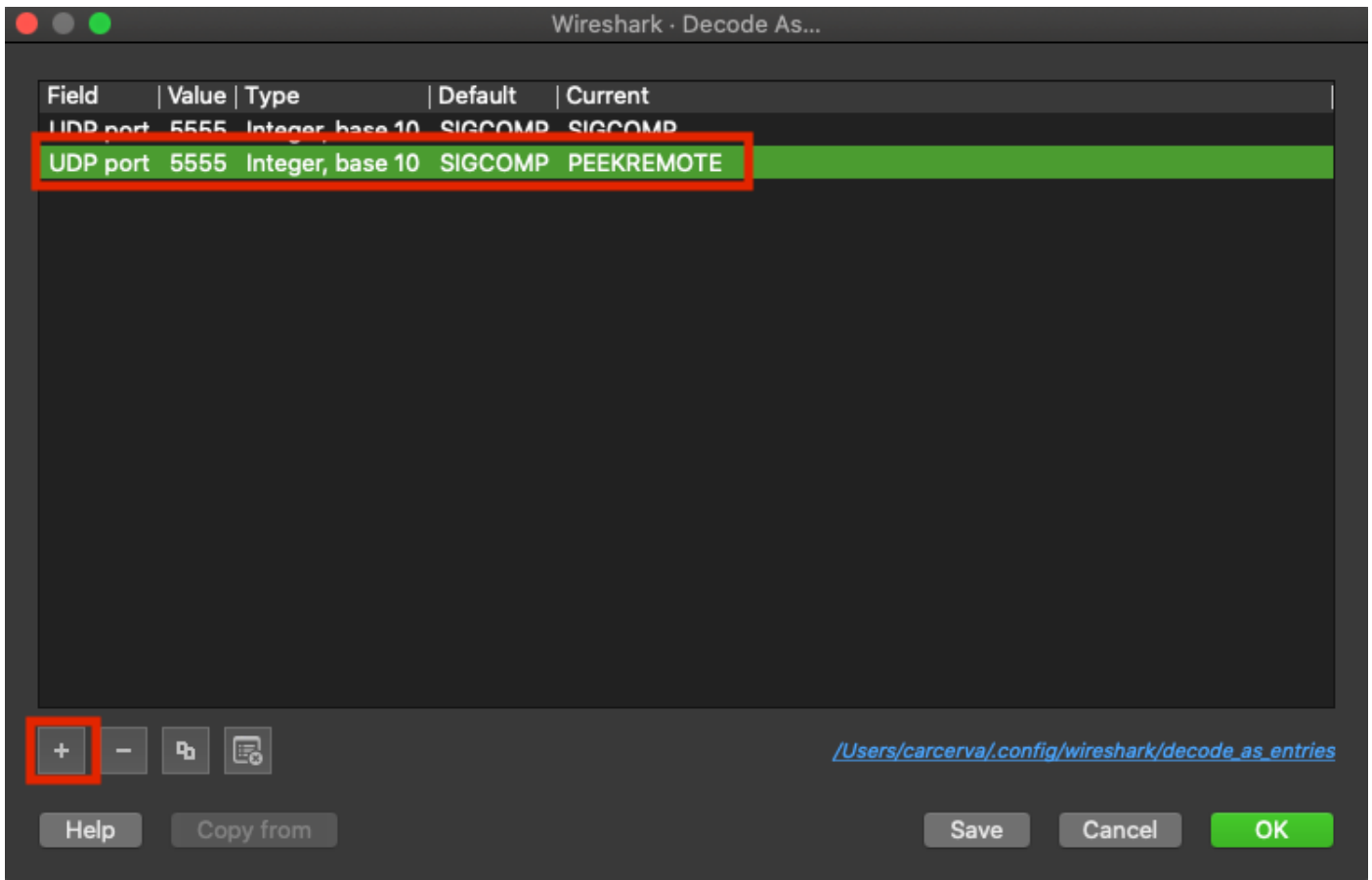
ةروصلال ي ف حضموم.



No.	Time	Dest	Protocol	Source Port	Info	Signal stren
1	2021-03-...	1...	UDP	5555	5555 → 5000 Len=400	
2	2021-03-...	1...	UDP	5555	5555 → 5000 Len=387	
3	2021-03-...	1...	UDP	5555	5555 → 5000 Len=385	
4	2021-03-...	1...	UDP	5555	5555 → 5000 Len=400	
5	2021-03-...	1...	UDP	5555	5555 → 5000 Len=387	
6	2021-03-...	1...	UDP	5555	5555 → 5000 Len=385	
7	2021-03-...	1...	UDP	5555	5555 → 5000 Len=400	
8	2021-03-...	1...	UDP	5555	5555 → 5000 Len=387	
9	2021-03-...	1...	UDP		en=385	
10	2021-03-...	1...	UDP		en=400	
11	2021-03-...	1...	UDP		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		en=385	
16	2021-03-...	1...	UDP		en=400	
17	2021-03-...	1...	UDP		en=387	
18	2021-03-...	1...	UDP		en=385	
19	2021-03-...	1...	UDP		en=400	
20	2021-03-...	1...	UDP		en=387	
21	2021-03-...	1...	UDP		en=385	
22	2021-03-...	1...	UDP		en=400	
23	2021-03-...	1...	UDP		en=387	
24	2021-03-...	1...	UDP		en=385	
25	2021-03-...	1...	UDP		en=379	

- Mark/Unmark Packet
- Ignore/Unignore Packet
- Set/Unset Time Reference
- Time Shift...
- Packet Comment...
- Edit Resolved Name
- Apply as Filter
- Prepare as Filter
- Conversation Filter
- Colorize Conversation
- SCTP
- Follow
- Copy
- Protocol Preferences
- Decode As...**
- Show Packet in New Window

تارايخال هذه ددح، ديدج لخدم ةفاضاب مقو ةفاضال رز ددح. ةقثب نم ةذفان رهظت 8 ةوطخال نم PEEKREMOTE و، يضا رتفالال نم SIGCOMP و، ةم يلال نم 5555، لجال نم UDP ذف نم ةروصلال ي ف حضموم وه امك، يلال.



لحلحتالءدبل ةزهاج نوكتو مزحلا زيمرت ك ف متي .OK قوف رقناو 9 ةوطخال

ةحصلال نم ققحتال

ححص لكشب نيوكتال لمع ديكأتل مسقلا اذه مدختسا

in order to ل 9800 gui نم بولسأ sniffer في ل ap تدكأ

> نيوكتال ل لقتنا ، 9800 WLC زارط (GUI) ةيموسرلا مدختسمل ةهجاو في 1 ةوطخال
لوصول طاقن عيجم > لوصول طاقن > يكلسال

نم ءاوتح| ددحو ، ثحبلا ةادا ضرعل لفسأل مهسلا رزرقنا . لوصول ةطقن في ثحبا 2 ةوطخال
ةوصول في حضورم وه امك ، لوصول ةطقن مسا بتكاو ، ةلدسنملا ةمئاقلا



Search Menu Items



Dashboard



Monitoring



Configuration



Administration



Licensing



Troubleshooting

Configuration > Wireless > Access Points

All Access Points

Number of AP(s): 1

AP Name	AP	Admin Status	IP Address
2802-carcerva-sniffer	Contains sniffer	<input checked="" type="checkbox"/>	172.16.0.125

5 GHz Radios

حضوره و امك، sniffer، و ه بولسأ ap ل او checkmark in green ل عم عضو Admin تقود. 3. و طخلال ا ف ةروصلال ف.



Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Licensing

Troubleshooting

Configuration > Wireless > Access Points

All Access Points

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address	Base Radio MAC	AP Mode	Operation Status	Configuration Status	Policy Tag	Site Tag
2802-carcerva-sniffer	AIR-AP2802I-B-K9	2	<input checked="" type="checkbox"/>	172.16.0.125	a03d.6f92.9400	Sniffer	Registered	Healthy	webauth_test	default-site-tag

in order to رماوأل هذه ل فغش تب مق. 9800 CLI ل نم بولسأ sniffer ف ap ل ادكأ

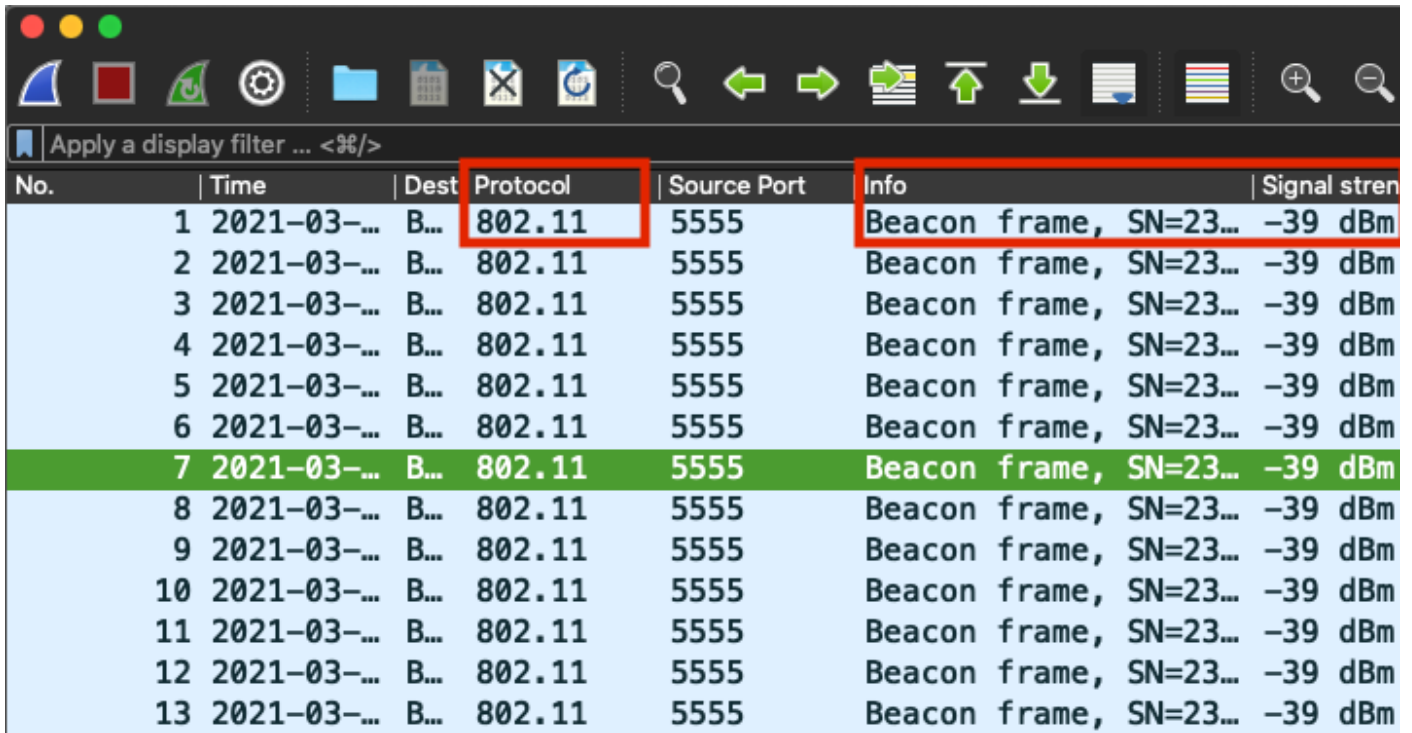
```
carcerva-9k-upg#show ap name 2802-carcerva-sniffer config general | i Administrative
Administrative State : Enabled
```

```
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

يُرت كانهو 802.11 إلى UDP نم لوكوتوربل ريغتي Wireshark. لي مزحل زيمرت ك ف ديكأتل ةروصل اي حضورم وه امك Beacon تاراطا.



No.	Time	Dest	Protocol	Source Port	Info	Signal stren
1	2021-03-...	B...	802.11	5555	Beacon frame, SN=23...	-39 dBm
2	2021-03-...	B...	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-...	B...	802.11	5555	Beacon frame, SN=23...	-39 dBm
6	2021-03-...	B...	802.11	5555	Beacon frame, SN=23...	-39 dBm
7	2021-03-...	B...	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

اهحالص او ءاطخال فاشكتسا

اهحالص او نيوكتل ءاطخال فاشكتسال اهم ادختسا كنكمي تامولعم مسقلا اذه رفوي

لوصول ةطقن نم تانايب اي Wireshark ي قلتل ال : ةلكشمل

ةيكلسال ال ةرادال ةهجو ةطساوب هيل لوصول ال باق Wireshark م داخ نوكي نا بجي : لجال في مكحتل رصنع نم WMI و Wireshark م داخ ني لوصول ةي ناكم ديكأت ءاچرل (WMI). ةيكلسال ال ةلحمل ةك بشل (WLC).

ةلص تاذا تامولعم

- [Cisco Catalyst 9800 Series Wireless Controller Software, Cisco IOS XE Amsterdam, رادصل ال - 17.3.x](#) : لصف الو : Sniffer
- [ةيكلسال ال 802.11 ةبقارم تاي ساسا](#)
- [Cisco Systems - تادنتس مل او ي نقتل م عدل](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل دن تسمل