

AP Packet Capture configureren op Catalyst 9800 draadloze controllers

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configuratie](#)

[Netwerkdigram](#)

[Configuraties](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe de functie voor pakketvastlegging van access point (AP) moet worden gebruikt.

Achtergrondinformatie

Deze optie is alleen beschikbaar voor Cisco IOS AP's (zoals AP 3702) en wordt daarom afgekeurd na Cisco IOS XE versie 17.3.

Deze oplossing wordt vervangen door Intelligent Capture met DNAC, of als alternatief door het toegangspunt in te stellen op de snuffelmodus.

Met de functie AP Packet Capture kunt u pakketopnamen via de ether uitvoeren met weinig inspanning. Wanneer de functie is ingeschakeld, wordt een kopie van alle opgegeven draadloze pakketten en frames die van/naar AP's zijn verzonden en ontvangen van/naar een specifiek draadloos MAC-adres via de ether, doorgestuurd naar een FTP-server (File Transfer Protocol), waar u het bestand kunt downloaden als .pcap-bestand en het kunt openen met uw voorkeurspakketanalysetool.

Zodra het pakketvastlegging is gestart, maakt het toegangspunt waar de client aan is gekoppeld, een nieuw .pcap-bestand op de FTP-server (zorg ervoor dat de gebruikersnaam die voor FTP-aanmelding is opgegeven, schrijfrechten heeft). Als de client zwerft, maakt de nieuwe AP een nieuw .pcap bestand op de FTP server. Als de client zich tussen Service Set Identifiers (SSID's) beweegt, houdt het toegangspunt het pakketvastlegging levendig, zodat u alle beheerframes kunt zien wanneer de client aan de nieuwe SSID koppelt.

Als u de opname maakt op een open SSID (geen beveiliging), kunt u de inhoud van de gegevenspakketten zien, maar als de client is gekoppeld aan een beveiligde SSID (een met een wachtwoord beveiligde SSID of 802.1x beveiliging), dan wordt het gegevensgedeelte van de gegevenspakketten versleuteld en kan het niet worden gezien in duidelijke tekst.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toegang tot de draadloze controllers via Command Line Interface (CLI) of Graphic User Interface (GUI).
- FTP-server
- .pcap-bestanden

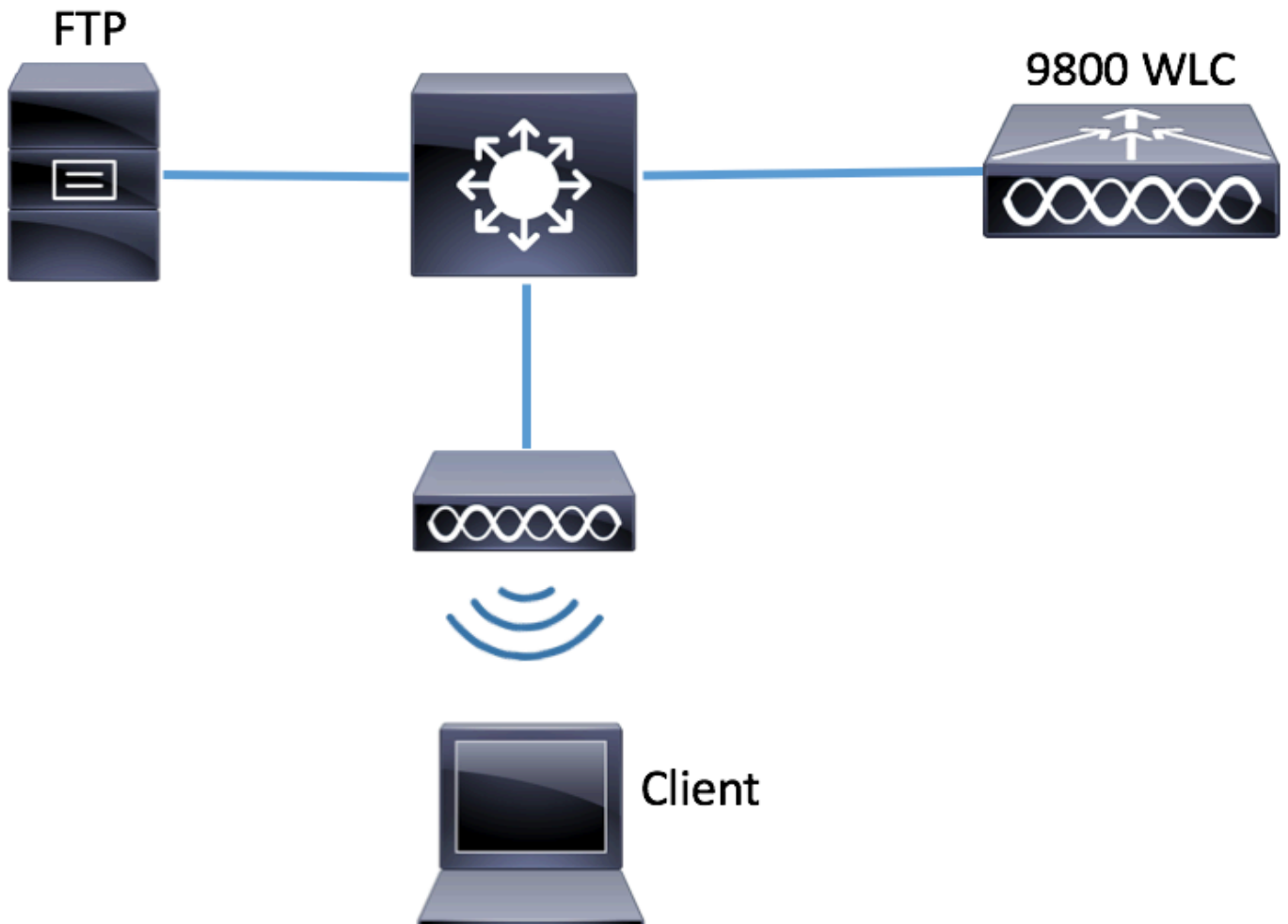
Gebruikte componenten

- 980 WLC v16.10
- AP. 3700
- FTP-server

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configuratie

Netwerkdigram



Configuraties

Controleer voor de configuratie welke toegangspunten worden gebruikt voor de verbinding van de draadloze client.

Stap 1. Controleer de huidige sitetag die is gekoppeld aan de toegangspunten die de draadloze client kan gebruiken voor de verbinding.

GUI:

Navigeren naar **configuratie > Draadloos > Access points**

The screenshot shows the GUI for Access Points configuration. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main content area displays the 'Access Points' configuration page. A search filter is applied: 'AP Name "Is equal to" 3702-02'. The table below shows the configuration for the selected AP.

AP Name	AP Model	Base Radio MAC	AP Mode	Admin Status	Operation Status	Policy Tag	Site Tag	RF Tag
3702-02	AIR-CAP3702I-A-K9	f07f.06ee.f590	Local	Enabled	Registered	default-policy-tag	default-site-tag	default-rf-tag

CLI:

show ap tag summary | inc 3702-02

3702-02 f07f.06e1.9ea0 **default-site-tag** default-policy-tag default-rf-tag No Default

Stap 2. Controleer het profiel van het toegangspunt dat aan die sitetag is gekoppeld

GUI:

Navigeren naar **Configuratie > Tags & profielen > Tags > Site > Site Tag naam**

The screenshot shows the GUI interface. On the left is a dark sidebar menu with a search bar and several menu items: Dashboard, Monitoring, Configuration (highlighted with a red box), Administration, and Troubleshooting. The main content area is titled 'Manage Tags' and features a tabbed interface with 'Policy', 'Site' (highlighted with a red box), 'RF', and 'A'. Below the tabs are '+ Add' and 'x Delete' buttons. A table lists 'Site Tag Name' entries: ST1, ST2, and 'default-site-tag' (highlighted with a red box).

Site Tag Name
<input type="checkbox"/> ST1
<input type="checkbox"/> ST2
<input type="checkbox"/> default-site-tag

Noteer het profiel voor de verbinding met het toegangspunt.

Edit Site Tag

Name*

default-site-tag

Description

default site tag

AP Join Profile

default-ap-profile ▼

Control Plane Name



Enable Local Site



CLI:

```
# show wireless tag site detailed default-site-tag
```

```
Site Tag Name : default-site-tag
```

```
Description : default site tag
```

```
-----  
AP Profile : default-ap-profile
```

```
Local-site : Yes
```

```
Image Download Profile: default-me-image-download-profile
```

Stap 3. Voeg de instellingen voor pakketvastlegging toe aan het profiel AP Join

GUI:

Navigeer naar **Configuration > Tags en profielen > AP Join > AP Join Profile Name > AP > Packet Capture** en voeg een nieuw **AP Packet Capture Profile** toe.

The screenshot shows the 'Edit AP Join Profile' interface. On the left, a sidebar menu includes 'Dashboard', 'Monitoring', 'Configuration', 'Administration', and 'Troubleshooting'. The main area is titled 'AP JOIN PROFILE' and contains a list of profiles with 'default-ap-profile' selected. On the right, the 'Edit AP Join Profile' panel has tabs for 'General', 'Client', 'CAPWAP', 'AP', 'Management', and 'Rogue AP'. The 'AP' tab is active, showing sub-tabs for 'General', 'Hyperlocation', and 'BLE'. The 'BLE' sub-tab is selected, displaying the 'AP Packet Capture Profile' field with a search icon and a plus sign.

Selecteer een naam voor het pakketopnameprofiel en voer de FTP-servergegevens in waarnaar

de AP's het pakketopnameprofiel verzenden. Zorg er ook voor dat u het soort pakketten selecteert dat u wilt controleren.

Buffergrootte = 1024-4096

Duur = 1-60

Create a new packet capture profile

Name*	Capture-all
Description	Enter Description
Buffer Size (KB)*	2048
Duration (min)*	10
Truncate Length (bytes)*	0

FTP Details

Server IP	172.16.0.6
File Path	/home/backup
UserName	backup
Password

Password Type: clear

TCP Port	0
UDP	<input type="checkbox"/>
UDP Port	0

802.11 Control	<input checked="" type="checkbox"/>
802.11 Management	<input checked="" type="checkbox"/>
802.11 Data	<input checked="" type="checkbox"/>
Dot1x	<input checked="" type="checkbox"/>
ARP	<input checked="" type="checkbox"/>
IAPP	<input checked="" type="checkbox"/>
IP	<input checked="" type="checkbox"/>
Broadcast	<input checked="" type="checkbox"/>
Multicast	<input checked="" type="checkbox"/>
TCP	<input checked="" type="checkbox"/>

Klik na het opslaan van het Capture profiel op **Update & Apply to Device**.

FTP Details

Server IP	172.16.0.6
-----------	------------

ARP	<input checked="" type="checkbox"/>
IAPP	<input checked="" type="checkbox"/>

CLI:

```
# config t
# wireless profile ap packet-capture Capture-all
```

```

# classifier arp
# classifier broadcast
# classifier data
# classifier dot1x
# classifier iapp
# classifier ip
# classifier tcp
# ftp password 0 backup
# ftp path /home/backup
# ftp serverip 172.16.0.6
# ftp username backup
# exit

# ap profile default-ap-profile
# packet-capture Capture-all
# end

# show wireless profile ap packet-capture detailed Capture-all

```

```

Profile Name : Capture-all
Description  :
-----

```

```

Buffer Size      : 2048 KB
Capture Duration : 10 Minutes
Truncate Length  : packet length
FTP Server IP    : 172.16.0.6
FTP path         : /home/backup
FTP Username     : backup

```

Packet Classifiers

```

802.11 Control   : Enabled
802.11 Mgmt      : Enabled
802.11 Data      : Enabled
Dot1x            : Enabled
ARP              : Enabled
IAPP             : Enabled
IP               : Enabled
TCP              : Enabled
TCP port         : all
UDP              : Disabled
UDP port         : all
Broadcast        : Enabled
Multicast        : Disabled

```

Stap 4. Zorg ervoor dat de draadloze client die u wilt bewaken al is gekoppeld aan een van de SSID's en aan een van de AP's die de tag heeft toegewezen aan het profiel waarin het AP-lid zich bij het pakket heeft aangesloten en aan de pakketopnamestaties zijn toegewezen, anders kan de opname niet worden gestart.

Tip: Als u de reden wilt oplossen waarom een client geen verbinding kan maken met een SSID, dan kunt u verbinding maken met een SSID dat prima werkt en dan zwerven naar de falende SSID, de opname volgt de client en neemt al zijn activiteit op.

GUI:

Naar **bewaking > Draadloos > Clients navigeren**

🔍 Search Menu Items

- 📊 Dashboard
- 🕒 Monitoring >
- 🔧 Configuration >
- ⚙️ Administration >
- 🔧 Troubleshooting

Clients

Clients
Sleeping Clients
Excluded Clients

Total Client(s) in the Network: 1

Client MAC Address "Is equal to" e4:b3:18:7c:30:58 ✕

ⓘ Only 'Contains' is supported while filtering two or more columns.

	Client MAC Address	IPv4/IPv6 Address	AP Name	WLAN	State	Protocol	User Name
<input type="checkbox"/>	e4:b3:18:7c:30:58	11.11.0.10	3702-02	3	Run	11ac	

⏪ < 1 > ⏩ 10 items per page

CLI:

```
# show wireless client summary | inc e4b3.187c.3058
```

```
e4b3.187c.3058 3702-02 3 Run 11ac
```

Stap 5. Start de vastlegging

GUI:

Naar probleemoplossing navigeren > AP Packet Capture



Troubleshooting

Ping and Trace Route



Check Ping-ability and Trace route info of a target destination through different sources

AP Packet Capture



AP Packet Capture for troubleshooting wireless clients

Voer het hoofdadres in van de client die u wilt bewaken en selecteer de **Capture Mode**. **Auto** betekent dat elke AP waarmee de draadloze client verbinding maakt, automatisch een nieuw .pcap bestand maakt. **Statisch** laat u één specifieke AP kiezen om de draadloze cliënt te controleren.

Start de opname met **Start**.

Q Search Menu Items

- Dashboard
- Monitoring >
- Configuration >
- Administration >
- Troubleshooting

Troubleshooting : AP Packet Capture

[← Back to TroubleShooting Menu](#)

Start Packet Capture

Client MAC Address*

Capture Mode Auto Static

✓ Start

Currently Active Packet Capture Sessions

	Client MAC Address	AP MAC Address	Mode
<< < 0 > >> <input style="width: 40px;" type="text" value="10"/> items per page			

Dan kunt u de huidige staat van de opname zien:

Currently Active Packet Capture Sessions

	Client MAC Address	AP MAC Address	Mode	Capture State	Site Tag Name	Stop AP Packet Capture
<input type="checkbox"/>	e4:b3:18:7c:30:58	f0:7f:06:ee:f5:90	Auto	Idle	default-site-tag	<input type="checkbox"/> Stop
<< < 1 > >> <input style="width: 40px;" type="text" value="10"/> items per page 1 - 1 of 1 items						

CLI:

```
# ap packet-capture start <E4B3.187C.3058> auto
```

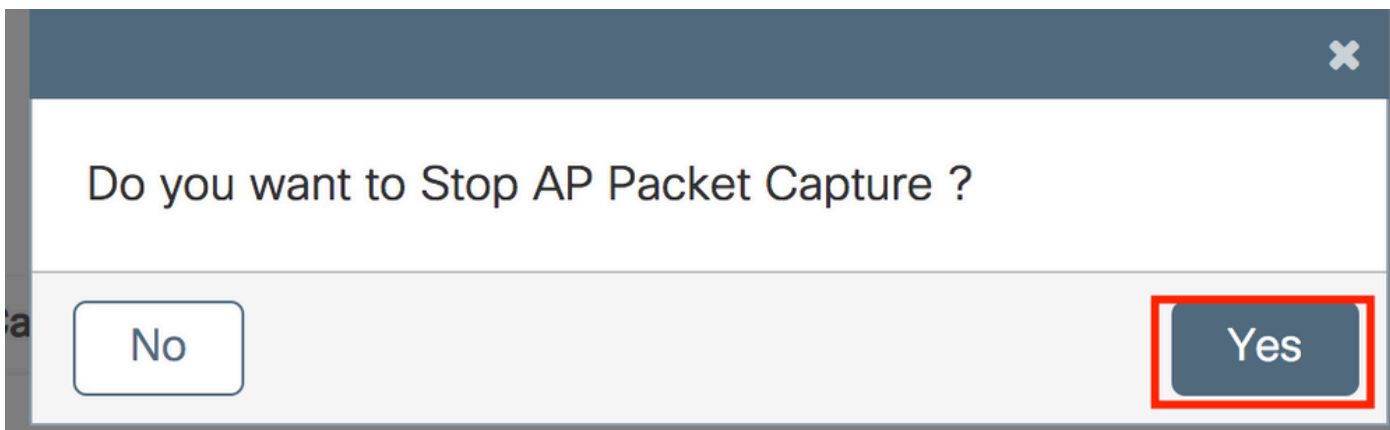
Step 6. Stop de vastlegging

Zodra het gewenste gedrag is opgenomen, moet u de opname stoppen door GUI of CLI:

GUI:

Currently Active Packet Capture Sessions

	Client MAC Address	AP MAC Address	Mode	Capture State	Site Tag Name	Stop AP Packet Capture
<input type="checkbox"/>	e4:b3:18:7c:30:58	f0:7f:06:ee:f5:90	Auto	Idle	default-site-tag	<input checked="" type="checkbox"/> Stop
<< < 1 > >> <input style="width: 40px;" type="text" value="10"/> items per page 1 - 1 of 1 items						

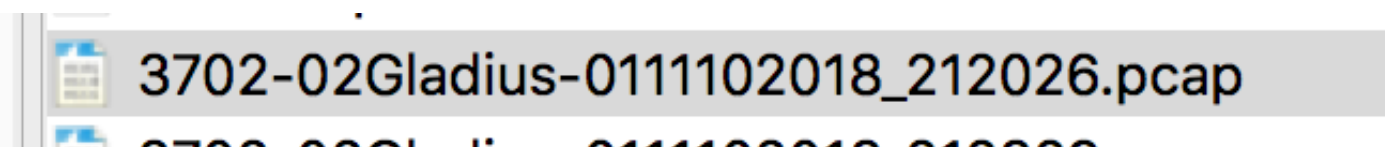


CLI:

```
# ap packet-capture stop <E4B3.187C.3058> all
```

Stap 7. Verzamel het .pcap bestand van de FTP server

U moet een bestand met een naam vinden als <ap-name><9800-wlc-name>-<###-file><day><month><year><hour><minuut><seconde>.pcap



Stap 8. U kunt het bestand openen met de tool voor pakketanalyse van uw voorkeur.

No.	Time	Source MAC	Destination MAC	Source	Destination	Info
223	16:21:16.603957			11.11.0.10	11.11.0.1	Echo (ping) rec
224	16:21:16.603957			11.11.0.1	11.11.0.10	Echo (ping) req
233	16:21:17.615950			11.11.0.10	11.11.0.1	Echo (ping) rec
234	16:21:17.615950			11.11.0.1	11.11.0.10	Echo (ping) req
235	16:21:18.639951			11.11.0.10	11.11.0.1	Echo (ping) rec
236	16:21:18.639951			11.11.0.1	11.11.0.10	Echo (ping) req
237	16:21:19.455970			10.88.173.49	11.11.0.10	Application Dat
238	16:21:19.459967			11.11.0.10	10.88.173.49	Destination un
239	16:21:19.663951			11.11.0.10	11.11.0.1	Echo (ping) rec
240	16:21:19.663951			11.11.0.1	11.11.0.10	Echo (ping) req
241	16:21:20.507969			10.88.173.49	11.11.0.10	Application Dat
242	16:21:20.507969			11.11.0.10	10.88.173.49	Destination un

Verifiëren

U kunt deze opdrachten gebruiken om de configuratie van de pakketopnamefunctie te verifiëren.

```
# show ap status packet-capture
```

```
Number of Clients with packet capture started : 1
```

```
Client MAC      Duration(secs)  Site tag name      Capture Mode
```

```
-----  
e4b3.187c.3058  600             default-site-tag   auto
```

```
# show ap status packet-capture detailed e4b3.187c.3058
```

```
Client MAC Address      : e4b3.187c.3058
Packet Capture Mode    : auto
Capture Duration       : 600 seconds
Packet Capture Site    : default-site-tag
```

Access Points with status

AP Name	AP MAC Addr	Status
-----	-----	-----
APf07f.06e1.9ea0	f07f.06ee.f590	Started

Problemen oplossen

U kunt deze stappen volgen om deze functie op te lossen:

Stap 1. debug-voorwaarde inschakelen

```
# set platform software trace wireless chassis active R0 wncmgrd all-modules debug
```

Stap 2. Het gedrag reproduceren

Stap 3. Controleer de huidige controller-tijd om de inlogtijd te kunnen volgen

```
# show clock
```

Stap 4. De logbestanden verzamelen

```
# show logging process wncmgrd internal | inc ap-packet-capture
```

Stap 5. Zet de standaardinstellingen voor de logbestanden terug.

```
# set platform software trace wireless chassis active R0 wncmgrd all-modules notice
```

Opmerking: het is erg belangrijk dat u na een probleemoplossing de logniveaus terugzet om de generatie van overbodige logbestanden te voorkomen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.