

Configuración de la captura de paquetes AP en los controladores inalámbricos Catalyst 9800

Contenido

[Introducción](#)

[Antecedentes](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuración](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo utilizar la función de captura de paquetes del punto de acceso (AP).

Antecedentes

Esta función solo está disponible para los AP del IOS de Cisco (como AP 3702) y, por lo tanto, se ha dejado de utilizar después de la versión 17.3 del IOS XE de Cisco.

Esta solución es reemplazada por la captura inteligente con DNAC, o como alternativa configurando el AP en modo sniffer.

La función Captura de paquetes AP le permite realizar capturas de paquetes en el aire con poco esfuerzo. Cuando la función está habilitada, una copia de todos los paquetes inalámbricos especificados y las tramas enviadas y recibidas desde/hacia AP desde/hacia una dirección MAC inalámbrica específica por el aire, se reenvía a un servidor de Protocolo de transferencia de archivos (FTP), donde puede descargarlo como archivo .pcap y abrirlo con su herramienta de análisis de paquetes preferida.

Una vez que se inicia la captura de paquetes, el AP al que está asociado el cliente crea un nuevo archivo .pcap en el servidor FTP (asegúrese de que el nombre de usuario especificado para el inicio de sesión FTP tenga derechos de escritura). Si el cliente se desplaza, el nuevo AP crea un nuevo archivo .pcap en el servidor FTP. Si el cliente se mueve entre los identificadores del conjunto de servicios (SSID), el AP mantiene activa la captura de paquetes para que pueda ver todas las tramas de administración cuando el cliente se asocie al nuevo SSID.

Si realiza la captura en un SSID abierto (sin seguridad), podrá ver el contenido de los paquetes de datos, pero si el cliente está asociado a un SSID seguro (un SSID protegido por contraseña o seguridad 802.1x), la parte de datos de los paquetes de datos se cifrará y no podrá verse en texto sin formato.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Interfaz de línea de comandos (CLI) o interfaz gráfica de usuario (GUI) para acceder a los controladores inalámbricos.
- Servidor FTP
- .pcap, archivos

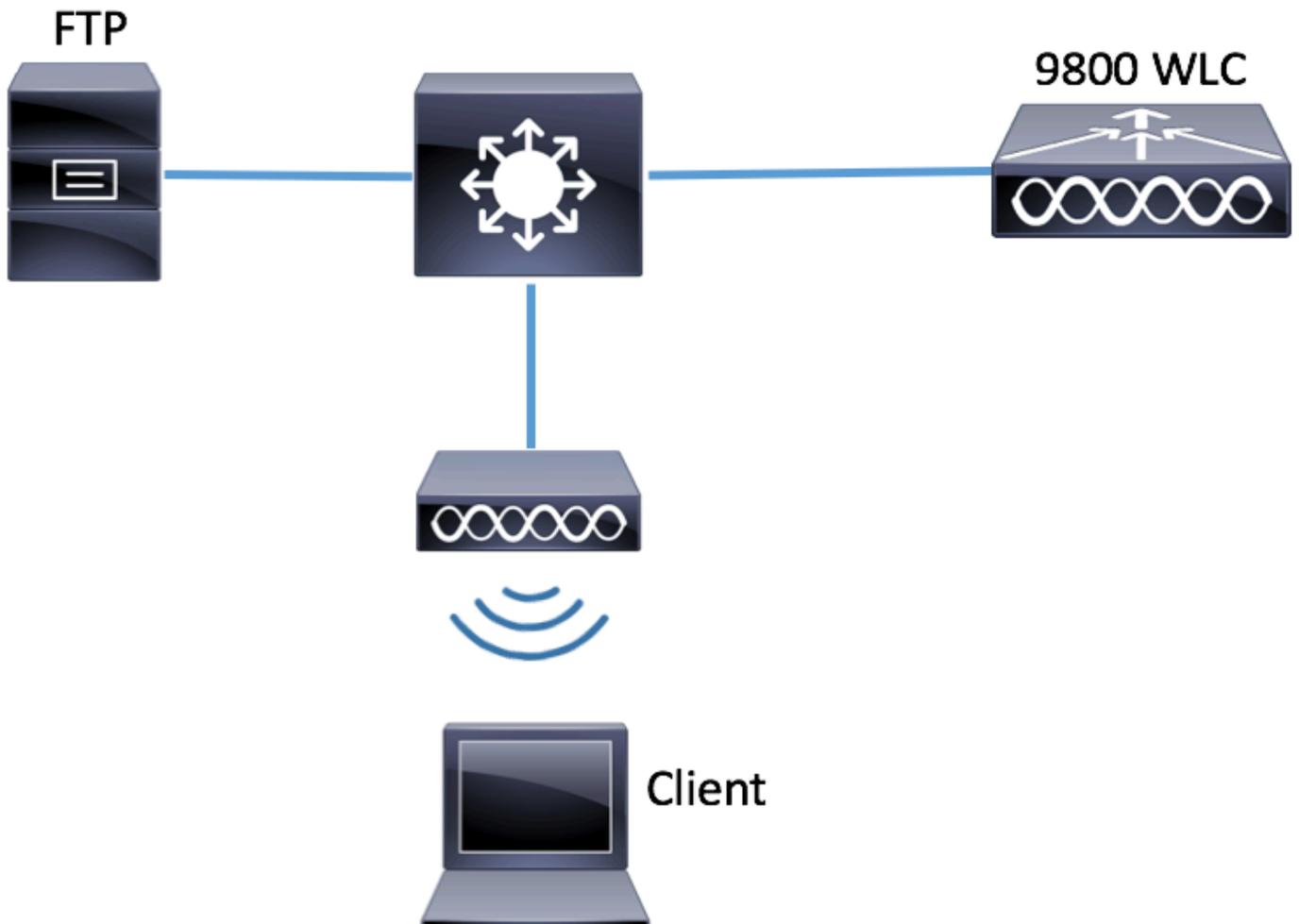
Componentes Utilizados

- 9800 WLC v16.10
- AP 3700
- Servidor FTP

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configuración

Diagrama de la red



Configuraciones

Antes de la configuración, verifique cuáles serían los AP a los que el cliente inalámbrico podría conectarse.

Paso 1. Verifique la etiqueta Site actual asociada a los AP que el cliente inalámbrico podría utilizar para conectarse.

GUI:

Vaya a **Configuration > Wireless > Access Points** .

The screenshot shows the 'Access Points' configuration page in a network management GUI. The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main content area shows a search filter for 'AP Name "Is equal to" 3702-02'. Below the search, a table lists the details of 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

Paso 2. Compruebe el perfil de unión de PA asociado a esa etiqueta de sitio

GUI:

Vaya a Configuration > Tags & Profiles > Tags > Site > Site Tag Name

The screenshot shows the 'Manage Tags' interface. On the left is a dark sidebar with a search bar and menu items: Dashboard, Monitoring, Configuration (highlighted with a red box), Administration, and Troubleshooting. The main area is titled 'Manage Tags' and has tabs for Policy, Site (highlighted with a red box), RF, and A. Below the tabs are '+ Add' and 'x Delete' buttons. A table lists site tags: 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

Tome nota del perfil de unión al PA asociado

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
```

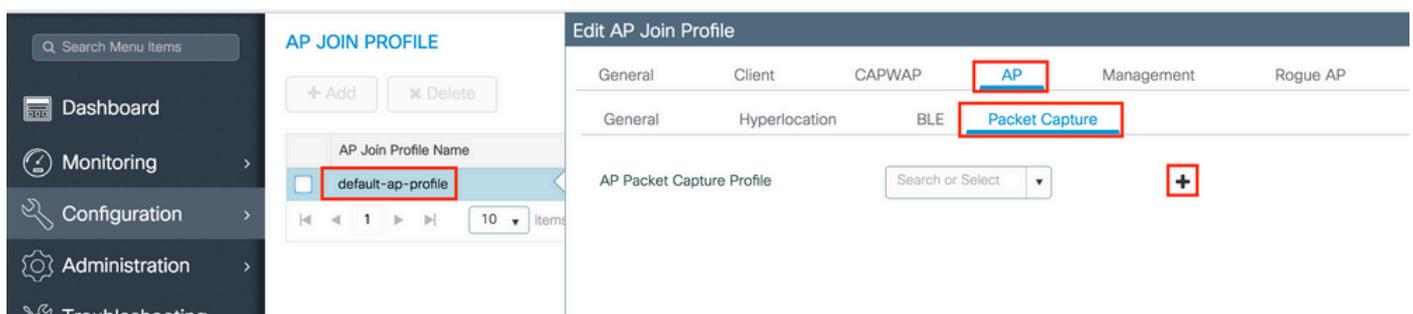
```
Local-site : Yes
```

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

Paso 3. Agregue la configuración de captura de paquetes en el perfil de unión a PA

GUI:

Navegue hasta **Configuration > Tags & Profiles > AP Join > AP Join Profile Name > AP > Packet Capture** y agregue un nuevo perfil de captura de paquetes AP.



Seleccione un nombre para el perfil de captura de paquetes e introduzca los detalles del servidor

FTP al que los AP envían la captura de paquetes. Asegúrese también de seleccionar el tipo de paquetes que desea monitorear.

Tamaño del búfer = 1024-4096

Duración = 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

Packet Classifiers

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"/>

TCP Port: 0

UDP:

UDP Port: 0

Una vez guardado el perfil de captura, haga clic en **Update & Apply to Device** .

FTP Details

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

ARP

IAPP

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

Paso 4. Asegúrese de que el cliente inalámbrico que desea monitorear ya esté asociado a cualquiera de los SSID y a uno de los AP que ha asignado la etiqueta donde se asignó el perfil de unión del AP con la configuración de captura de paquetes; de lo contrario, no se puede iniciar la captura.

Sugerencia: Si desea solucionar el problema por el que un cliente no puede conectarse a un SSID, puede conectarse a un SSID que funcione correctamente y luego desplazarse al SSID que falla, la captura sigue al cliente y captura toda su actividad.

GUI:

Vaya a **Monitoring > Wireless > Clients** .

Search Menu Items

Dashboard

Monitoring >

Configuration >

Administration >

Troubleshooting

Clients

Clients Sleeping Clients Excluded Clients

✕ Delete

Total Client(s) in the Network: 1

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

① 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	

10 items per page

CLI:

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

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

Paso 5. Iniciar la captura

GUI:

Vaya a Troubleshooting > 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

Introduzca la dirección MAC del cliente que desea supervisar y seleccione el **modo de captura**. **Auto** significa que cada AP al que se conecta el cliente inalámbrico, crea un nuevo archivo .pcap automáticamente. **Static** le permite elegir un AP específico para monitorear el cliente inalámbrico.

Inicie la captura con **Start**.

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

Currently Active Packet Capture Sessions

Client MAC Address	AP MAC Address	Mode
0 items per page		

A continuación, puede ver el estado actual de la captura:

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="button" value="Stop"/>

1 items per page 1 - 1 of 1 items

CLI:

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

Paso 6. Detener la captura

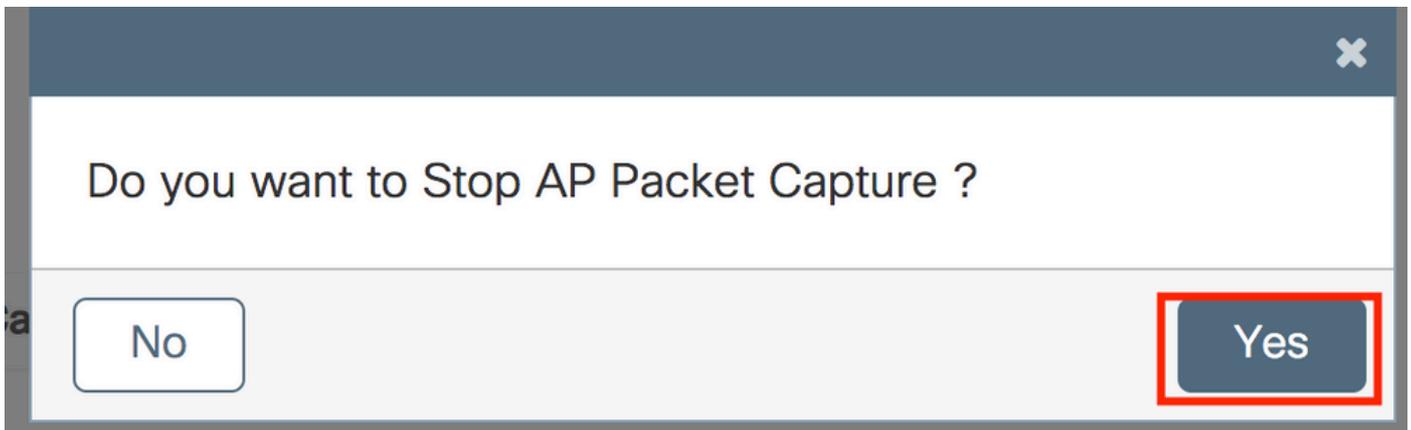
Una vez capturado el comportamiento deseado, detenga la captura mediante la GUI o la CLI:

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 type="button" value="Stop"/>

10 items per page 1 - 1 of 1 items

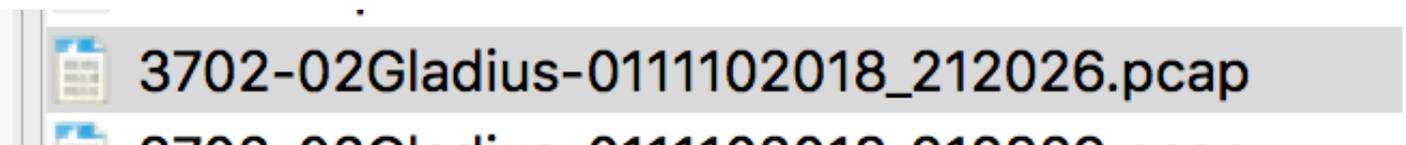


CLI:

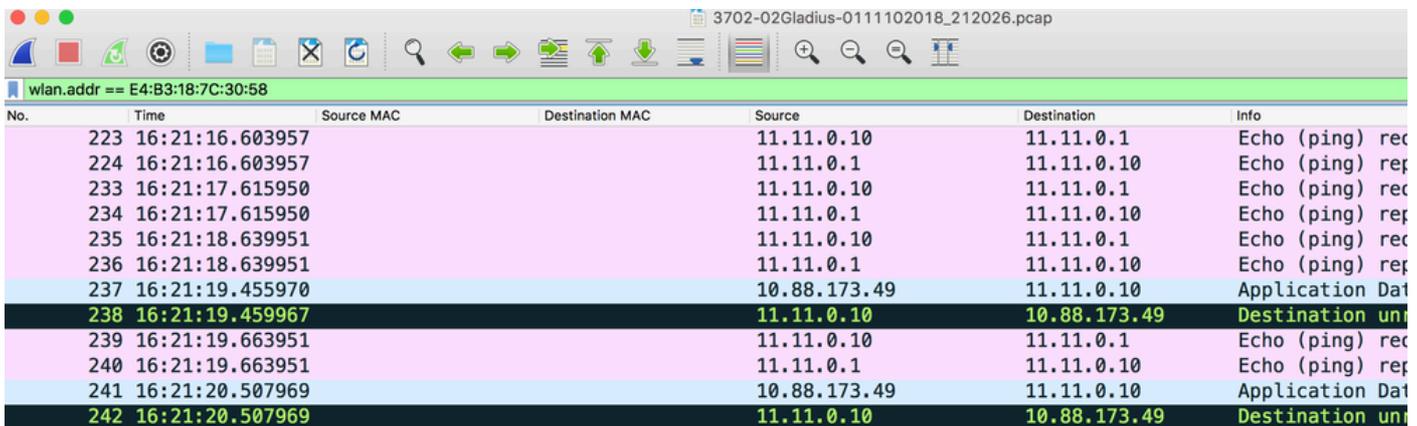
```
# ap packet-capture stop <E4B3.187C.3058> all
```

Paso 7. Recopile el archivo .pcap del servidor FTP

Debe encontrar un archivo con el nombre <ap-name><9800-wlc-name>-<###-file><day><month><year>_<hour><minute><second>.pcap



Paso 8. Puede abrir el archivo con la herramienta de análisis de paquetes que prefiera.



Verificación

Puede utilizar estos comandos para verificar la configuración de la función de captura de paquetes.

```
# 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
```

Troubleshoot

Puede seguir estos pasos para resolver problemas de esta función:

Paso 1. Habilitar condición de depuración

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

Paso 2. Reproducir el comportamiento

Paso 3. Compruebe la hora actual del controlador para poder realizar un seguimiento de la hora de inicio de sesión

```
# show clock
```

Paso 4. Recopilar los registros

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

Paso 5. Vuelva a establecer la condición de registros en los valores predeterminados.

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

Nota: Es muy importante que después de una sesión de troubleshooting establezca los niveles de logs para evitar la generación de logs innecesarios.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).