

Configurar a captura de pacotes AP nos controladores sem fio Catalyst 9800

Contents

[Introduction](#)

[Informações de Apoio](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuração](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve como usar o recurso de Captura de Pacotes do Ponto de Acesso (AP).

Informações de Apoio

O recurso está disponível apenas para APs Cisco IOS (como AP 3702) e, portanto, foi preterido após o Cisco IOS XE versão 17.3.

Essa solução é substituída pelo Intelligent Capture com DNAC, ou como alternativa, definindo o AP para o modo sniffer.

O recurso de captura de pacote AP permite que você realize capturas de pacote pelo ar com pouco esforço. Quando o recurso está habilitado, uma cópia de todos os pacotes e quadros sem fio especificados enviados e recebidos de/para APs de/para um endereço MAC sem fio específico pelo ar é encaminhada para um servidor FTP, de onde você pode baixá-lo como arquivo .pcap e abri-lo com sua ferramenta preferencial de análise de pacotes.

Uma vez iniciada a captura do pacote, o AP ao qual o cliente está associado cria um novo arquivo .pcap no servidor FTP (certifique-se de que o nome de usuário especificado para login de FTP tenha direitos de gravação). Se o cliente faz roaming, o novo AP cria um novo arquivo .pcap no servidor FTP. Se o cliente se mover entre os Service Set Identifiers (SSIDs), o AP manterá a captura do pacote ativa para que você possa ver todos os quadros de gerenciamento quando o cliente se associar ao novo SSID.

Se você fizer a captura em um SSID aberto (sem segurança), poderá ver o conteúdo dos pacotes de dados, mas se o cliente estiver associado a um SSID protegido por senha (um SSID protegido por senha ou segurança 802.1x), a parte de dados dos pacotes de dados será criptografada e não poderá ser vista em texto claro.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso à interface de linha de comando (CLI) ou à interface gráfica de usuário (GUI) dos controladores sem fio.
- servidor FTP
- arquivos .pcap

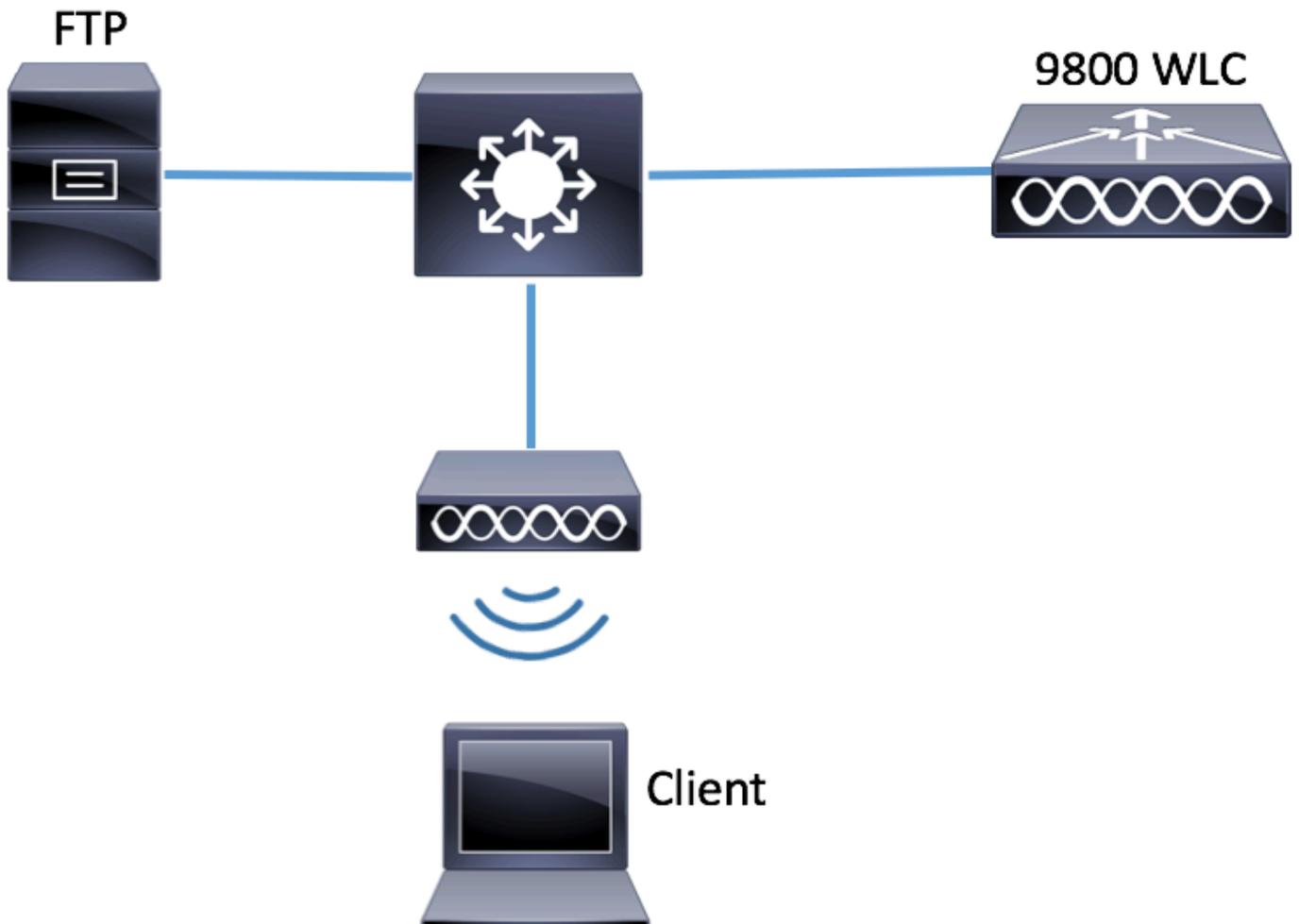
Componentes Utilizados

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

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.

Configuração

Diagrama de Rede



Configurações

Antes da configuração, verifique quais seriam os APs aos quais o cliente sem fio poderia se conectar.

Etapa 1. Verifique a marca Site atual associada aos APs que o cliente sem fio pode usar para se conectar.

GUI:

Navegue até **Configuração > Sem fio > Pontos de acesso**

The screenshot shows the 'Access Points' configuration page in a network management GUI. A sidebar on the left 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 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

Etapa 2. Verifique o perfil de ingresso no AP associado a essa etiqueta de site

GUI:

Navegue até **Configuration > Tags & Profiles > Tags > Site > Site Tag Name**

The screenshot shows the Cisco GUI interface for managing tags. 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 content area is titled 'Manage Tags' and has a breadcrumb trail: Policy > Site (highlighted with a red box) > RF > A. Below the breadcrumb are '+ Add' and 'x Delete' buttons. A table lists site tags with checkboxes:

	Site Tag Name
<input type="checkbox"/>	ST1
<input type="checkbox"/>	ST2
<input type="checkbox"/>	default-site-tag (highlighted with a red box)

Anote o perfil de ingresso do AP associado

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
```

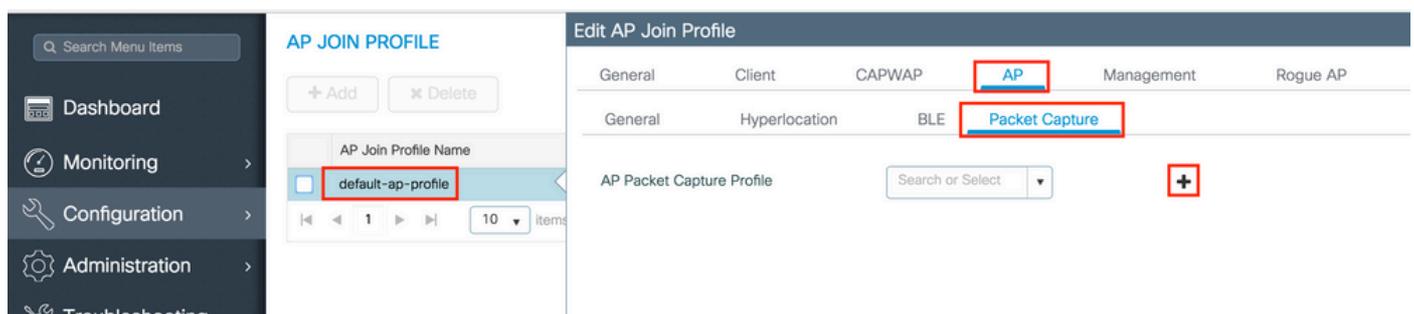
```
Local-site : Yes
```

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

Etapa 3. Adicione as configurações de Captura de pacotes no perfil de junção AP

GUI:

Navegue para **Configuration > Tags & Profiles > AP Join > AP Join Profile Name > AP > Packet Capture** e adicione um novo **AP Packet Capture Profile**.



Selecione um Nome para o Perfil de Captura de Pacotes, insira os detalhes do servidor FTP para

o qual os APs enviam a captura de pacotes. Certifique-se também de selecionar os tipos de pacotes que deseja monitorar.

Tamanho do buffer = 1024-4096

Duração = 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

Depois que o perfil Capture for salvo, clique em **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

Etapa 4. Certifique-se de que o cliente sem fio que você deseja monitorar já esteja associado a qualquer um dos SSIDs e a um dos APs que atribuiu a Tag onde o perfil de junção de AP com as configurações de captura de pacote foram atribuídas, caso contrário, a captura não poderá ser iniciada.

Dica: Se você quiser solucionar o problema do motivo pelo qual um cliente não consegue se conectar a um SSID, você poderá se conectar a um SSID que funciona bem e depois ir para o SSID com falha, a captura seguirá o cliente e capturará toda a sua atividade.

GUI:

Navegue até **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

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
```

Etapa 5. Iniciar a captura

GUI:

Navegue até 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

Insira o endereço mac do cliente que deseja monitorar e selecione o **Modo de captura. Automático** significa que cada AP ao qual o cliente sem fio se conecta cria um novo arquivo .pcap automaticamente. **Static** permite escolher um AP específico para monitorar o cliente sem fio.

Inicie a captura com **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		

Em seguida, você pode ver o estado atual da 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
```

Etapa 6. Parar a captura

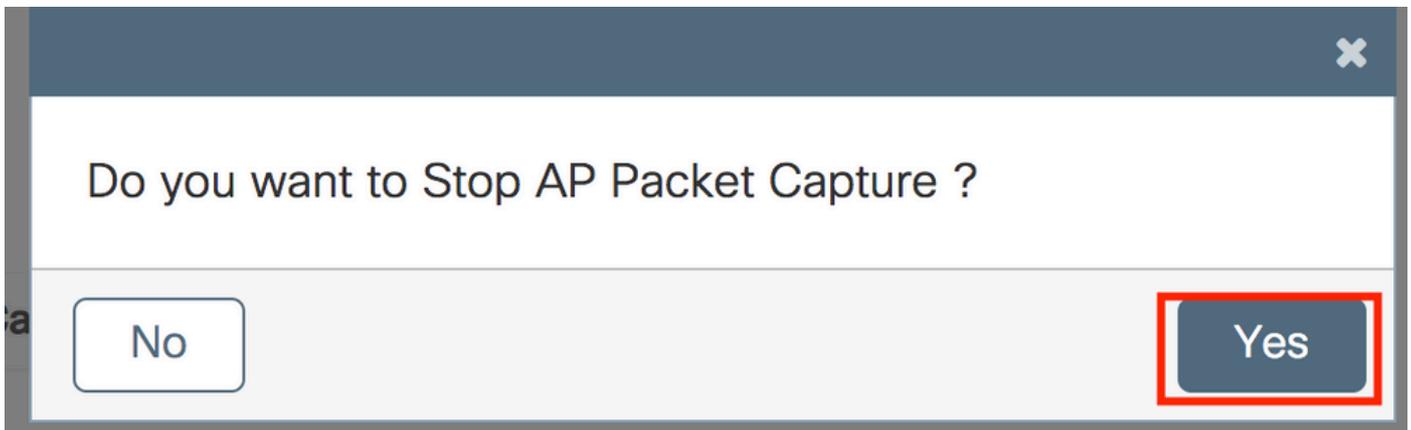
Depois que o comportamento desejado for capturado, interrompa a captura pela GUI ou CLI:

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

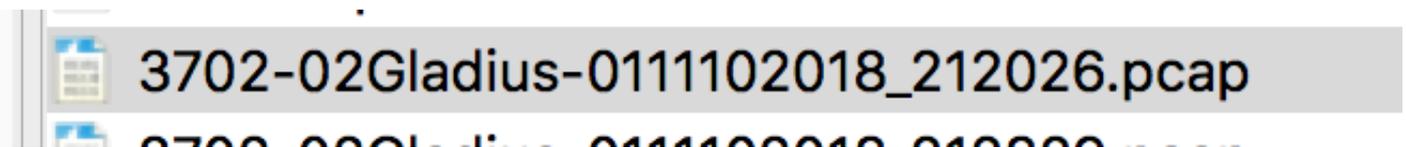


CLI:

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

Passo 7. Colete o arquivo .pcap do servidor FTP

Você deve localizar um arquivo com o nome <ap-name><9800-wlc-name>-<##-file><day><month><year>_<hour><minute><second>.pcap



Etapa 8. Você pode abrir o arquivo com a ferramenta de análise de pacote de sua preferência.

No.	Time	Source MAC	Destination MAC	Source	Destination	Info
223	16:21:16.603957			11.11.0.10	11.11.0.1	Echo (ping) req
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) req
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) req
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) req
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

Verificar

Você pode usar esses comandos para verificar a configuração do recurso de captura de pacotes.

```
# 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

Você pode seguir estas etapas para solucionar esse recurso:

Etapa 1. Habilitar condição de depuração

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

Etapa 2. Reproduzir o comportamento

Etapa 3. Verificar a hora atual do controlador para poder acompanhar a hora de logon

```
# show clock
```

Etapa 4. Coletar os logs

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

Etapa 5. Defina novamente a condição de logs para os padrões.

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

Observação: é muito importante que, após uma sessão de solução de problemas, você redefina os níveis dos logs para evitar a geração de logs desnecessários.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.