

在Catalyst 9800无线控制器上配置AP数据包捕获

目录

[简介](#)

[背景信息](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

简介

本文档介绍如何使用接入点(AP)数据包捕获功能。

背景信息

此功能仅适用于Cisco IOS AP (如AP 3702) ，因此在Cisco IOS XE版本17.3之后不再使用。

此解决方案由采用DNAC的智能捕获取代，或者通过将AP设置为嗅探器模式作为替代方案。

AP数据包捕获功能使您能够轻而易举地通过空中执行数据包捕获。启用此功能后，所有指定无线数据包和帧的副本会通过空中从/接收到/来自AP的特定无线mac地址，然后转发到文件传输协议(FTP)服务器，您可以在其中将其下载为.pcap文件，并使用首选数据包分析工具将其打开。

启动数据包捕获后，客户端所关联的AP将在FTP服务器上创建新的.pcap文件(确保为FTP登录指定的用户名具有写入权限)。如果客户端漫游，新AP将在FTP服务器上创建新的.pcap文件。如果客户端在服务集标识符(SSID)之间移动，则AP会保持数据包捕获处于活动状态，这样当客户端关联到新SSID时，您就可以看到所有管理帧。

如果您在开放式SSID上进行捕获(无安全性)，您可以看到数据包的内容，但是如果客户端与安全SSID(受密码保护的SSID或802.1x安全性)关联，则数据包的数据部分将被加密，并且无法以明文显示。

先决条件

要求

Cisco 建议您了解以下主题：

- 对无线控制器的命令行界面(CLI)或图形用户界面(GUI)访问。
- FTP 服务器

- .pcap文件

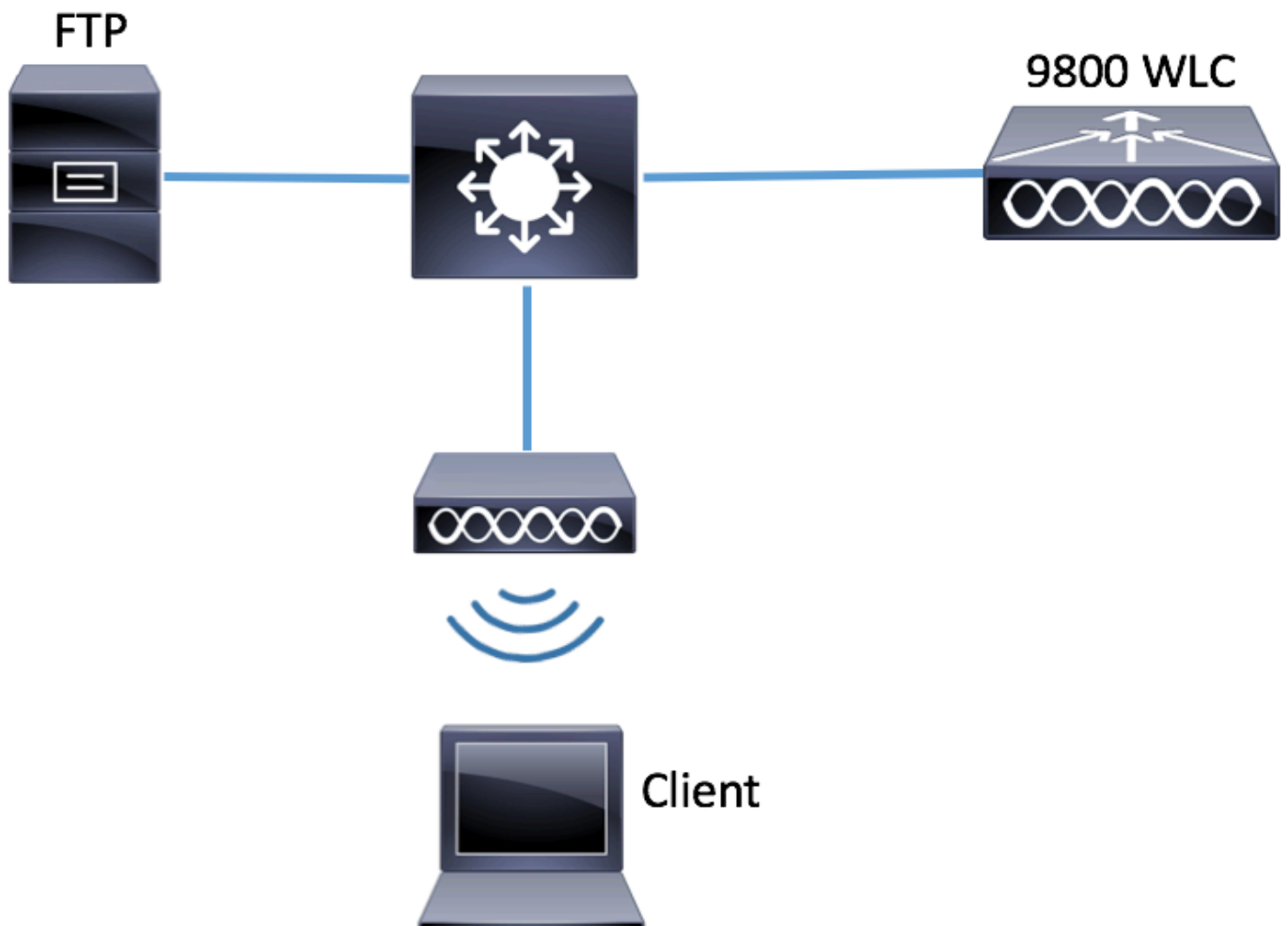
使用的组件

- 9800 WLC v16.10
- AP 3700
- FTP 服务器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图



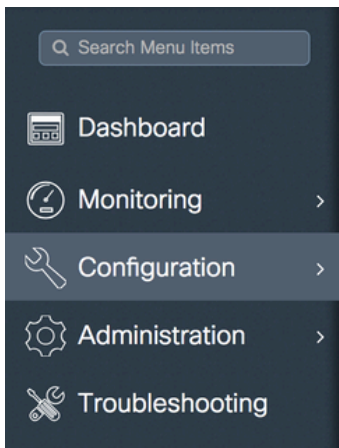
配置

在配置之前，检查无线客户端可以连接到哪些AP。

步骤1:验证与无线客户端可用于连接的AP关联的当前站点标记。

GUI:

导航到**配置>无线>接入点**



Access Points

▼ All Access Points

Number of AP(s): 1

AP Name "Is equal to" 3702-02

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 :

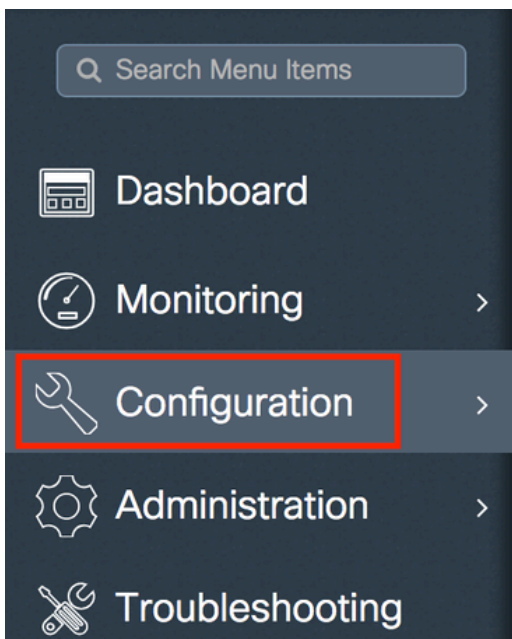
```
# show ap tag summary | inc 3702-02
```

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

第二步：检查与该站点标签关联的AP加入配置文件

GUI:

导航到配置>标签和配置文件>标签>站点>站点标签名称



Manage Tags

Policy

Site

RF

A

+ Add

× Delete

Site Tag Name

ST1

ST2

default-site-tag

注意关联的AP加入配置文件

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
```

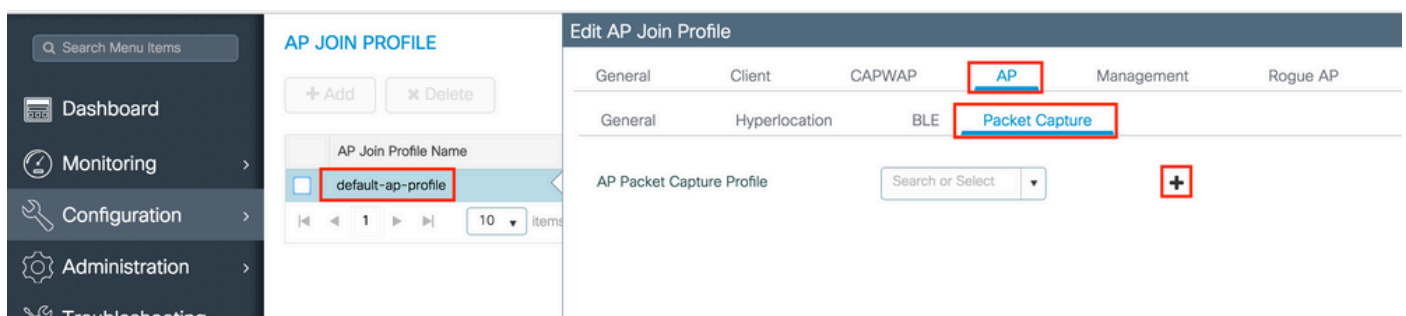
```
Local-site : Yes
```

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

第三步：在AP加入配置文件中添加数据包捕获设置

GUI:

导航到 **Configuration > Tags & Profiles > AP Join > AP Join Profile Name > AP > Packet Capture** 并添加新的AP Packet Capture Profile。



为数据包捕获配置文件选择名称，输入AP向其发送数据包捕获的FTP服务器详细信息。另请确保选

择要监控的数据包类型。

缓冲区大小= 1024-4096

持续时间= 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

Cancel Save Delete

保存捕获配置文件后，单击Update & Apply to Device。

FTP Details

Server IP 172.16.0.6

Cancel Update & Apply to Device

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
```

第四步：确保您想要监控的无线客户端已关联到任何SSID以及分配了标记的AP，其中AP加入配置文件已分配了数据包捕获设置，否则无法启动捕获。

提示:如果要对客户端无法连接到SSID的原因进行故障排除，您可以连接到正常工作的SSID，然后漫游到出现故障的SSID，捕获会跟随客户端并捕获其所有活动。

GUI:

导航到监控>无线>客户端

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	

10 items per page

CLI :

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

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

第五步：开始捕获

GUI:

导航到故障排除> AP数据包捕获



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

输入要监控的客户端的mac地址并选择**Capture Mode(捕获模式)**。**自动**表示无线客户端连接的每个AP自动创建一个新的.pcap文件。**静态**允许您选择一个特定的AP来监控无线客户端。

使用**Start (开始)**启动**捕获**。

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	10 items per page	

然后您可以看到捕获的当前状态：

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

10 items per page
1 - 1 of 1 items

CLI :

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

第六步：停止捕获

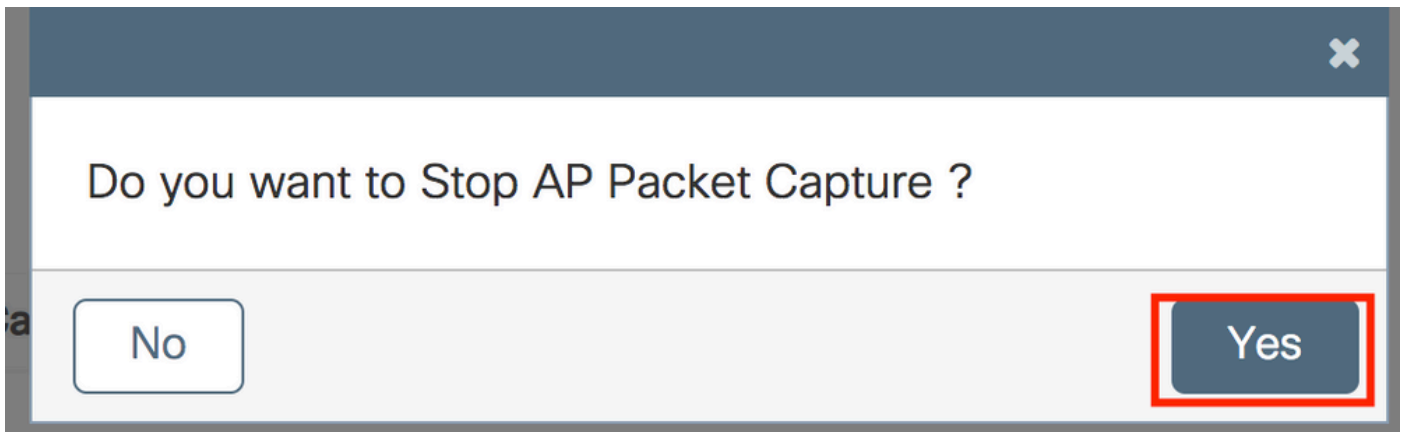
捕获所需行为后，通过GUI或CLI停止捕获：

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

10 items per page
1 - 1 of 1 items

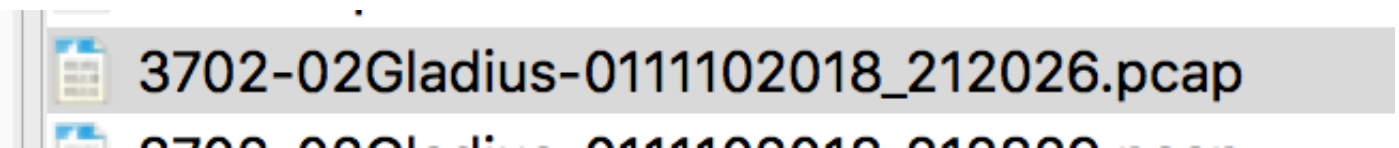


CLI :

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

步骤 7.从FTP服务器收集.pcap文件

您必须找到名称为<ap-name><9800-wlc-name>-<##-file><day><month><year>_<hour><minute><second>.pcap的文件



步骤 8您可以使用首选的数据包分析工具打开该文件。

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

验证

您可以使用这些命令验证数据包捕获功能的配置。

```
# 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

故障排除

您可以按照以下步骤对此功能进行故障排除：

步骤1:启用调试条件

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

第二步：重现该行为

第三步：检查当前控制器时间，以便能够及时跟踪日志

```
# show clock
```

第四步：收集日志

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

第五步：将日志条件恢复为默认值。

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

注意：在故障排除会话结束后，请务必设置日志级别，以避免生成不必要的日志。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。