



AP Packet Capture

- [AP client packet capture, on page 1](#)
- [Enable packet capture \(GUI\), on page 2](#)
- [Enable packet capture \(CLI\), on page 2](#)
- [Create AP packet capture profile and map to an AP join profile \(GUI\), on page 3](#)
- [Create AP packet capture profile and map to an AP join profile, on page 3](#)
- [Start or stop packet capture, on page 4](#)

AP client packet capture

An AP client packet capture is a diagnostic feature that

- enables packet capture on APs for the purpose of wireless client troubleshooting
- filters and captures packets on the channel and radio where the AP is operating, and
- uploads the captured packets to a file on an FTP server for later analysis (for example, in Wireshark).

Feature history

Table 1: Feature history for AP client packet capture

Feature name	Release information	Feature description
AP client packet capture	Cisco IOS XE 16.7.1	The AP client packet capture feature enables packet capture on APs, filters and captures packets on the channels and radios, and uploads the captured packets to a file.

This feature allows network engineers to analyze over-the-air traffic as observed by the AP, helping identify connectivity or performance issues experienced by wireless clients. For instance, when debugging why a client device cannot connect to a Wi-Fi network, engineers can use AP client packet capture to record and examine all packets exchanged between the client and the AP.

Limitations of AP client packet capture

The limitations of AP client packet capture include:

- You can perform packet capture for only one client at a time per site.
- You can start packet capture on a specific AP or a set of APs using static mode.

When you start packet capture in auto mode, the system selects nearby APs to capture packets for a specific client. In auto mode, you cannot start or stop packet capture on an individual AP. Use the **stop all** command to stop packet capture when it is started in auto mode.

- After the Single Sign-On (SSO) process is complete, the packet capture stops after a switchover.

Enable packet capture (GUI)

Enable packet capture on selected network interfaces.

Procedure

-
- Step 1** Choose **Troubleshooting > Packet Capture**.
 - Step 2** Click **Add**. Enter the name that identifies the capture point.
 - Step 3** From the **Filter** drop-down list, choose if you want to capture IPv4 or IPv6 packets. For IPv4, provide the source and destination addresses and the subnet mask. For IPv6, enter the source and destination addresses and the prefix length.
 - Step 4** Check the **Monitor Control Plane** check box to configure the control plane as an attachment point.
 - Step 5** Check the **DHCP** check box to enable **Inner Filter Protocol**.
 - Step 6** Enter the **Inner Filter MAC address** using one of the standard MAC address formats: xx:xx:xx:xx:xx:xx, xx-xx-xx-xx-xx-xx, or xxxx.xxxx.xxxx.
 - Step 7** Type the capture buffer size. The default buffer is 10 MB.
 - Step 8** Specify the session limit either in seconds or in the number of packets captured.
 - Step 9** Select the interfaces from which you want to capture packets, in the **Available** list. Click the arrow button to move it to the **Selected** list.
 - Step 10** Click **Apply to Device**.

Packet capture is active on the chosen interfaces, and captured packet data is available for analysis.

Enable packet capture (CLI)

Enable packet capture for a specified client.

Procedure

-
- Step 1** Enter privileged EXEC mode.

Example:

```
Device# enable
```

Step 2 Enable packet capture for the specified client on a set of nearby APs.

Example:

```
Device# ap packet-capture start client-mac-address auto
```

Packet capture is now enabled on your specified client.

```
Device# enable
```

```
Device# ap packet-capture start 0011.0011.0011 auto
```

Create AP packet capture profile and map to an AP join profile (GUI)

Add a packet capture profile to an AP join profile so you can monitor APs.

Procedure

-
- Step 1** Click **Configuration > Tags & Profiles > AP Join Profile**.
 - Step 2** Click **Add** to create a new AP Join Profile and enter the required details.
 - Step 3** In the **Add AP Join Profile** area, click **AP > Packet Capture**.
 - Step 4** Click the **Plus** icon to create a new Packet Capture profile or select a profile from the dropdown menu.
 - Step 5** Click **Save**.

The AP join profile now includes a packet capture profile. This change enables packet capture for associated APs.

Create AP packet capture profile and map to an AP join profile

Create and enable an AP packet capture profile, then associate it with a specific AP join profile to facilitate packet capture for targeted APs.

Packet capture profile configurations apply to individual APs. The packet capture profile is assigned to an access point profile, which is then mapped to a site tag.

When starting packet capture, APs apply the packet capture profile configurations associated with their site and AP join profile.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure an AP profile.

Example:

```
Device(config)# wireless profile ap packet-capture packet-capture-profile-name
```

Step 3 Configure an AP packet capture profile.

Example:

```
Device(config)# ap profile profile-name
```

Step 4 Enable packet capture in the AP profile.

Example:

```
Device(config-ap-profile)# packet-capture profile-name
```

Step 5 Exit the AP profile configuration mode.

Example:

```
Device(config-ap-profile)# end
```

Step 6 Check the detailed information for the selected AP packet capture profile.

Example:

```
Device# show wireless profile ap packet-capture detailed profile-name
```

The AP packet capture profile is successfully created and mapped to the selected AP join profile.

```
Device# configure terminal
Device(config)# wireless profile ap packet-capture test1
Device(config)# ap profile ap-profile1
Device(config-ap-profile)# packet-capture capture-profile
Device(config-ap-profile)# end
Device# show wireless profile ap packet-capture detailed test1
```

Start or stop packet capture

You can start or stop wireless packet capture for a specific client using CLI commands.

Procedure

Step 1 Enable packet capture for a specific client.

Example:

```
Device# ap packet-capture stop client-mac-address {auto | static | ap-name}
```

Step 2

Disable packet capture for a specific client.

Example:

```
Device# ap packet-capture stop client-mac-address {all | static | ap-name}
```

The system starts or stops packet capture for the selected client on the specified AP.

```
Device# ap packet-capture start 0011.0011.0011 auto
```

```
Device# ap packet-capture stop 0011.0011.0011 all
```

Start or stop packet capture