Sniffer Mode

Information about Sniffer

The controller enables you to configure an access point as a network “sniffer”, which captures and forwards all the packets on a particular channel to a remote machine that runs packet analyzer software. These packets contain information on time stamps, signal strength, packet sizes, and so on.

Sniffers allow you to monitor and record network activity, and detect problems.

The packet analyzer machine configured receives the 802.11 traffic encapsulated using the Airopeek protocol from the controller management IP address with source port UDP/5555 and destination UDP/5000.

You must use **Clear** in AP mode to return the AP back to client-serving mode, for example the local mode or FlexConnect mode depending on the remote site tag configuration.

Prerequisites for Sniffer

To perform sniffing, you need the following hardware and software:

- A dedicated access point—An access point configured as a sniffer cannot simultaneously provide wireless access service on the network. To avoid disrupting coverage, use an access point that is not part of your existing wireless network.
- A remote monitoring device—A computer capable of running the analyzer software.
- Software and supporting files, plug-ins, or adapters—Your analyzer software may require specialized files before you can successfully enable.

Restrictions on Sniffer

- Supported third-party network analyzer software applications are as follows:
  - Wildpackets Omnipeek or Airopeek
  - AirMagnet Enterprise Analyzer
  - Wireshark
- The latest version of Wireshark can decode the packets by going to the Analyze mode. Select **decode as**, and switch UDP5555 to decode as PEEKREMOTE..
- Sniffer mode is not supported when the controller L3 interface is the Wireless Management Interface (WMI).
- When an AP or a radio operates in the sniffer mode, irrespective of its current channel width settings, the AP sniffs or captures only on the primary channel.

How to Configure Sniffer

Configuring an Access Point as Sniffer (GUI)

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 On the **General** tab, update the name of the AP. The AP name can be ASCII characters from 33 to 126, without leading and trailing spaces.

Step 3 Specify the physical location where the AP is present.

Step 4 Choose the **Admin Status** as **Enabled** if the AP is to be in enabled state.

Step 5 Choose the mode for the AP as *Sniffer*.

Step 6 In the **Tags** section, specify the appropriate policy, site, and RF tags that you created on the **Configuration** > **Tags & Profiles** > **Tags** page.

Note If the AP is in sniffer mode, you do not want to assign any tag.

Step 7 Click **Update & Apply to Device**.

Step 8 Choose the mode for the AP as **Clear** to return the AP back to the client-serving mode depending on the remote site tag configuration.

Configuring an Access Point as Sniffer (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device>enable`	Enables privileged EXEC mode.
Step 2	**ap name** *ap-name* **mode sniffer** **Example:** `Device# ap name access1 mode sniffer`	Configures the access point as a sniffer. Where, *ap-name* is the name of the Cisco lightweight access point. Use the **no** form of this command to disable the access point as a sniffer.

Enabling or Disabling Sniffing on the Access Point (GUI)

Before you begin

Change the access point AP mode to sniffer mode.

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Access Points**.

Step 2 On the **Access Points** page, click the AP name from the 5 GHz or 2.4 GHz list.

Step 3 In the **Edit Radios** > **Configure** > **Sniffer Channel Assignment** section, check the **Sniffer Channel Assignment** checkbox to enable.

Uncheck the checkbox to disable sniffing on the access point.

Step 4 From the **Sniff Channel** drop-down list, select the channel.

Step 5 Enter the IP address in the **Sniffer IP** field.

Step 6 Click **Update & Apply to Device**.

Enabling or Disabling Sniffing on the Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**ap name** *ap-name* **dot11 {24ghz | 5ghz | 6ghz} slot 3 sniff** *channel server-ip-address* **Example:** `Device# ap name access1 dot11 6ghz slot 3 sniff 1 9.9.48.5`	Enables sniffing on the access point. • *channel* is the valid channel to be sniffed. For 802.11a, the range is 36 to 165. For 802.11b, the range is 1 to 14. • *server-ip-address* is the IP address of the remote machine running Omnipeek, Airopeek, AirMagnet, or Wireshark software.
Step 3	**ap name** *ap-name* **dot11 {24ghz | 5ghz | 6ghz} slot 3 no sniff** *channel server-ip-address* **Example:** `Device#ap name access1 dot11 6ghz slot 3 sniff 1 9.9.48.5`	Disables sniffing on the access point.

Verifying Sniffer Configurations

Table 1: Commands for verifying sniffer configurations

Commands	Description
show ap name *ap-name* **config dot11** {**24ghz** | **5ghz** | **dual-band**}	Displays the sniffing details.
show ap name *ap-name* **config slot** *slot-ID*	Displays the sniffing configuration details. *slot-ID* ranges from 0 to 3. All access points have slot 0 and 1.

Examples for Sniffer Configurations and Monitoring

This example shows how to configure an access point as Sniffer:

```
Device# ap name access1 mode sniffer
```

This example shows how to enable sniffing on the access point:

```
Device# ap name access1 sniff dot11b 1 9.9.48.5
```

This example shows how to disable sniffing on the access point:

```
Device# ap name access1 no sniff dot11b
```

This example shows how to display the sniffing configuration details:

```
Device# show ap name access1 config dot11 24ghz
Device# show ap name access1 config slot 0
```