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.

Note It is recommended not to use the AP command to change the CAPWAP mode.

Information About XOR Radio Role Sniffer Support

The XOR radio in APs like Cisco 2800, 3800, 4800, and the 9100 series AP models support sniffer role in single radio interface.

The XOR radio offers the ability to operate as a single radio interface in many modes. This eliminates the need to place the entire AP into a mode. When this concept is applied to a single radio level, it is termed as role.

From this release onwards, Sniffer is the new supported role along with the Client Serving and Monitor roles.

Note The radio role is supported in Local and FlexConnect modes.

Feature History for Sniffer Mode

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Table 1: Feature History for Sniffer Mode

Release	Feature	Feature Information
Cisco IOS XE 17.8.1	XOR Radio Role Sniffer Support on the Access Point	The XOR radio in APs like Cisco 2800, 3800, 4800, and the 9100 series AP models support sniffer role in single radio interface.

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.

Note As both Cisco Catalyst 9166I and 9166D APs have XOR radios, a Board Device File (BDF) has to be loaded to initialize radio 2 for the radios of these APs to work as expected. While the BDF is being loaded and for the file to be loaded correctly, the firmware has to be made non-operational and radios have to be reset. This operation of radio reset due to firmware being non-operational for the purposes of loading the BDFs is deliberate and is an expected behavior. This operation can be observed in both the controller and Cisco Catalyst Center. We recommend that you ignore the core dump that is generated due to this deliberate operation.

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.

Note All the radios will be set to manual mode when you change the AP mode to Sniffer mode. Simultaneously, a warning message will be displayed informing you to convert the radio submode back to AUTO, if required, while changing the mode from Sniffer to other.

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 6 GHz, 5 GHz, or 2.4 GHz list.

Step 3 In the **Role Assignment** section, select the **Assignment Method** as *Sniffer*.

Step 4 In the **Sniffer Channel Assignment** section, check the **Sniffer Channel Assignment** checkbox to enable.

Uncheck the checkbox to disable sniffing on the access point.

Step 5 From the **Sniff Channel** drop-down list, select the channel.

Note By default, the **Snif Channel** is set to *36* for the **5 GHz** and *1* for the **2.4 GHz**.

Step 6 Enter the IP address in the **Sniffer IP** field.

To validate the IP address, click **Update & Apply to Device**. If the IP address is valid, the **Sniffer IP Status** displays *Valid*.

Step 7 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* **sniff** {**dot11 6Ghz slot** *3 channel server-ip-address* | **dot11a** *channel server-ip-address* | **dot11b** *channel server-ip-address* | **dual-band** *channel server-ip-address*} **Example:** `Device# ap name access1 sniff dot11b 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. For dot11 6Ghz, the range is between 1 and 233. • *server-ip-address* is the IP address of the remote machine running Omnipeek, Airopeek, AirMagnet, or Wireshark software.
Step 3	**ap name** *ap-name* **no sniff** {**dot116Ghz** | **dot11a** | **dot11b** | **dual-band**} **Example:** `Device#ap name access1 no sniff dot116ghz`	Disables sniffing on the access point.

Configuring XOR Radio Role Sniffer Support on the Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**ap name** *ap-name* **dot11 {dual-band} shutdown** **Example:** `Device# ap name AP687D.B45C.189C dot11 dual-band shutdown`	Shutdown the XOR radio.
Step 3	**ap name** *ap-name* **dot11 {dual-band} role manual {client-serving}** **Example:** `Device# ap name ap-name dot11 dual-band role manual client-serving`	Converts the XOR radio role to manual.

	Command or Action	Purpose
Step 4	**ap name** *ap-name* **dot11 {dual-band} band {5ghz** | **24ghz}** **Example:** `Device# ap name  AP687D.B45C.189C dot11 dual-band band 5ghz`	Configures XOR radio to manually operate in a specific band.
Step 5	**ap name** *ap-name* **dot11 {dual-band} radio role manual sniffer channel** *channel-number* **ip** *ip-address* **Example:** `Device# ap name AP687D.B45C.189C dot11 dual-band radio role manual sniffer channel 100 ip 9.4.197.85`	Enables XOR radio role Sniffer support on AP from the controller. Where, • *ap-name* is the name of the Cisco lightweight access point. • *channel-number* is the channel number.
Step 6	**ap name** *ap-name* **no dot11 {dual-band} shutdown** **Example:** `Device# ap name AP687D.B45C.189C no dot11 dual-band shutdown`	Unshuts the XOR radio.
Step 7	**end** **Example:** `Device# end`	Returns to privileged EXEC mode. **Note** When configuring the radio to work as a Sniffer in the 5-GHz band, you will need to change the band of the radio manually as in **Step 4**.

Verifying Sniffer Configurations

Table 2: Commands for verifying sniffer configurations

Commands	Description
show ap name *ap-name* **config dot11** {**24ghz** | **5ghz** | **6ghz** | **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.

Verifying XOR Radio Role Sniffer Configuration

To verify the XOR radio role sniffer configuration for a given AP, use the following command:

```
Device# show ap name AP687D.B45C.189C config slot 0

Sniffing                                        : Enabled
Sniff Channel                                   : 6
Sniffer IP                                      : 9.4.197.85
Sniffer IP Status                               : Valid
ATF Mode                                        : Disable
ATE Optimization                                : N/A
AP Submode                                      : Not Configured
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : information
Software Version                                : 17.9.0.18
Boot Version                                    : 1.1.2.4
Mini IOS Version                                : 0.0.0.0
Stats Reporting Period                          : 60
primary_discovery_timer                         : 120
LED State                                       : Enabled
LED Flash State                                 : Enabled
LED Flash Timer                                 : 0
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : PoE/Full Power
Number of Slots                                 : 4
AP Model                                        : C9136I-B
IOS Version                                     : 17.9.0.18
Reset Button                                    : Disabled
AP Serial Number                                : FOC25322JJZ
AP Certificate Type                             : Manufacturer Installed Certificate
AP Certificate Expiry-time                      : 08/09/2099 20:58:26
AP Certificate issuer common-name               : High Assurance SUDI CA
AP Certificate Policy                           : Default
AP CAPWAP-DTLS LSC Status
    Certificate status        : Not Available
AP 802.1x LSC Status
    Certificate status        : Not Available
AP User Name                                    : admin
AP 802.1X User Mode                             : Global
AP 802.1X User Name                             : Not Configured
Cisco AP System Logging Host                    : 255.255.255.255
AP Up Time                                      : 4 hours 20 minutes 55 seconds
AP CAPWAP Up Time                               : 4 hours 16 minutes 17 seconds
Join Date and Time                              : 01/19/2022 03:06:12

Attributes for Slot 0
  Radio Type                                    : 802.11ax - 2.4 GHz
  Radio Mode                                    : Sniffer
  Radio Role                                    : Sniffer
  Maximum client allowed                        : 400
  Radio Role Op                                 : Manual
  Radio SubType                                 : Main
  Administrative State                          : Enabled
  Operation State                               : Up
```

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
```