Access Points Modes

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
```

Introduction to Monitor Mode

To optimize the monitoring and location calculation of RFID tags, you can enable tracking optimization on up to four channels within the 2.4-GHz band of an 802.11b/g/x access point radio. This feature allows you to scan only the channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).

Note You can move an AP to a particular mode (sensor mode to local mode or flex mode) using the site tag with the corresponding mode. If the AP is not tagged to any mode, it will fall back to the mode specified in the default site tag.

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.

Enable Monitor Mode (GUI)

Procedure

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

Step 2 In the **Access Points** page, expand the **All Access Points** section and click the name of the AP to edit.

Step 3 In the **Edit AP** page, click the **General** tab and from the **AP Mode** drop-down list, choose **Monitor**.

Step 4 Click **Update & Apply to Device**.

Step 5 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.

Enable Monitor Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**ap name** *ap-name* **mode monitor** **Example:** `Device# ap name 3602a mode monitor`	Enables monitor mode for the access point.
Step 2	**ap name** *ap-name* **monitor tracking-opt** **Example:** `Device# ap name 3602a monitor tracking-opt`	Configures the access point to scan only the Dynamic Channel Assignment (DCA) channels supported by its country of operation.
Step 3	**ap name** *ap-name* **monitor-mode dot11b fast-channel** [*first-channel second-channel third-channel fourth-channel*] **Example:** `Device# ap name 3602a monitor dot11b 1 2 3 4`	Chooses up to four specific 802.11b channels to be scanned by the access point. In the United States, you can assign any value from 1 to 11 (inclusive) to the channel variable. Other countries support additional channels. You must assign at least one channel.
Step 4	**ap name** *ap-name* **dot11 6ghz slot** *3* **radio role manual monitor** **Example:** `Device# ap name cisco-ap dot11 6ghz slot 3 radio role manual monitor`	slot 3 radio role manual monitor Configures the 802.11 6-Ghz radio role manual monitor
Step 5	**show ap dot11 {24ghz | 5ghz | 6ghz} channel** **Example:** `Device# show ap dot11 5ghz channel`	Shows configuration and statistics of 802.11a or 802.11b or 6-GHz channel assignment.
Step 6	**show ap dot11 6ghz summary** **Example:** `Device# show ap dot11 6ghz summary`	Shows configuration and statistics summary of 6 the GHz band Cisco APs.

Feature History for Management Mode Migration in Cisco Catalyst Wireless 916X Access Points

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

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 3: Feature History for Management Mode Migration in Cisco Wireless Catalyst Wireless 916X Series Access Points

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.9.1	Management Mode Migration in Cisco Catalyst Wireless 916X Series Access Points	This feature allows you to convert the AP mode between DNA Management mode and Meraki Management mode, depending on your requirements. **Note** The document explains the conversion from DNA Management mode to Meraki Management mode and not vice versa.

Information About Management Mode Migration in Cisco Catalyst Wireless 916X Series Access Points

Cisco Catalyst Wireless 916x APs (CW9164I-x and CW9166I-x) support both cloud and controller architecture. You can migrate between cloud and controller deployments, depending on your requirements. The CW916x APs join and operate either in the DNA Management mode or in the Meraki Management mode. You can configure the management mode migration with the help of CLI commands in the privileged EXEC mode, at the AP level, and from the controller GUI.

CW916x APs support dual-band slot 3 radios, which in turn support both 6-GHz and 5-GHz bands.

Note The section explains the migration from DNA Management mode to the Meraki Management mode and not vice versa.

Regulatory Domain

For regulatory domain support, Cisco Catalyst 916x (CW916x) supports Rest of the World (RoW) and a few other fixed domains as shown here:

- -B
- -E
- -A
- -Z
- -Q
- -I
- -R

During the AP join flow, the regulatory domain details and the details of the country that is configured is passed on to the controller from the AP. The controller assigns or validates the right country of operation.

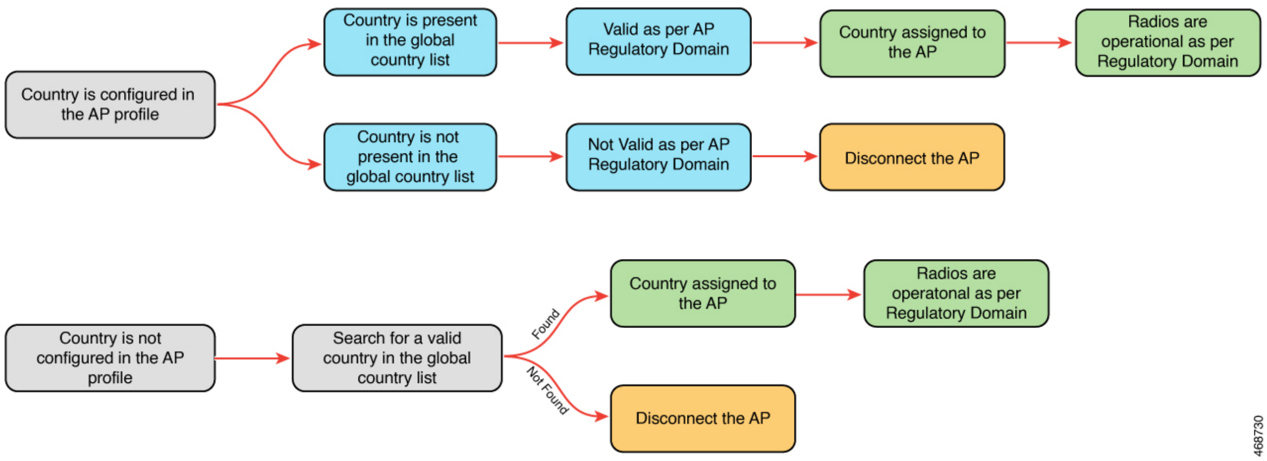
After the country is validated based on the decision tree, the controller informs the AP about which country the AP should be configured with.

The following are the scenarios that determine the country that an AP should be configured with:

AP Configured with Non-RoW Regulatory Domain

Case 1: AP does not report a country as part of the join procedure.

AP Does Not Report a Country as Part of the Join Procedure

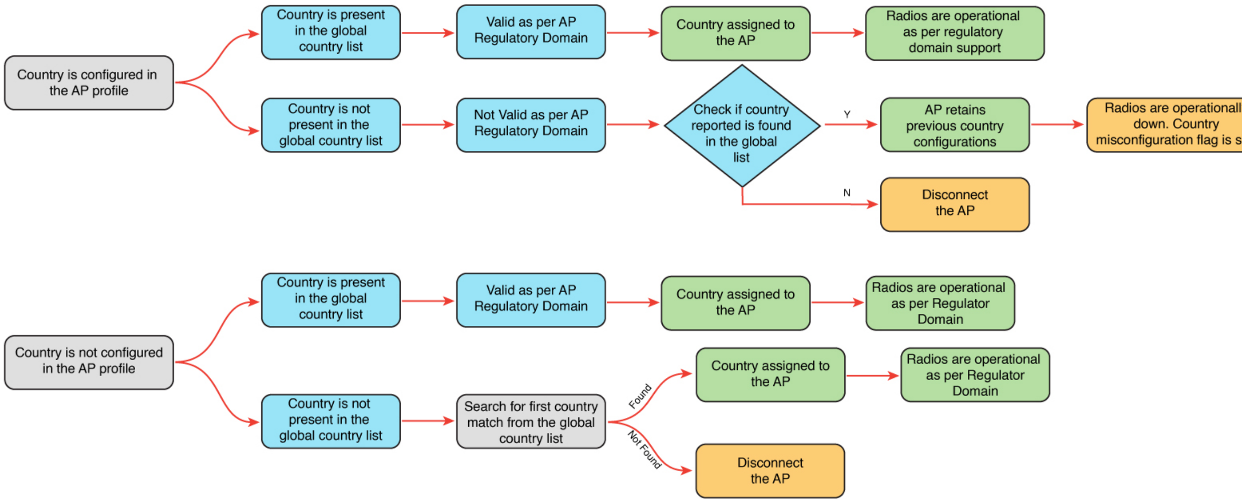

Country is configured in the AP profile
Country is present in the global country list
Valid as per AP Regulatory Domain
Country assigned to the AP
Radios are operational as per Regulatory Domain
Country is not present in the global country list
Not Valid as per AP Regulatory Domain
Disconnect the AP
Country is not configured in the AP profile
Search for a valid country in the global country list
Found
Not Found
Country assigned to the AP
Radios are operatonal as per Regulatory Domain
Disconnect the AP
468730

In the non-RoW regulatory domain, when an AP does not report a country as part of the join procedure, the following takes place:

- AP profile has a country configured.
    - If the country configured in the AP profile is present in the global country list, and is valid as per the AP regulatory domain, the country that is configured in the AP profile is assigned to the AP. Radios become operational as per the country or regulatory domain support.
    - If the country configured the AP profile is not present in the global country list, and is not valid as per the AP regulatory domain, the AP is disconnected.
- AP profile does not have a country configured. Find a valid country from the global country list (the first match), as per the AP regulatory domain.
    - If the country is found, the country is assigned to the AP and the radios become operational as per the country or regulatory domain support.
    - If the country is not found, the AP is disconnected.

Case 2: AP reports a country as part of the join procedure.

AP Reports Country as Part of the Join Procedure


Country is configured in the AP profile
Country is present in the global country list
Valid as per AP Regulatory Domain
Country assigned to the AP
Radios are operational as per regulatory domain support
Country is not present in the global country list
Not Valid as per AP Regulatory Domain
Check if country reported is found in the global list
Y
AP retains previous country configurations
Radios are operationall down. Country misconfiguration flag is s
N
Disconnect the AP
Country is not configured in the AP profile
Country is present in the global country list
Valid as per AP Regulatory Domain
Country assigned to the AP
Radios are operational as per Regulator Domain
Country is not present in the global country list
Search for first country match from the global country list
Found
Country assigned to the AP
Radios are operational as per Regulator Domain
Not Found
Disconnect the AP

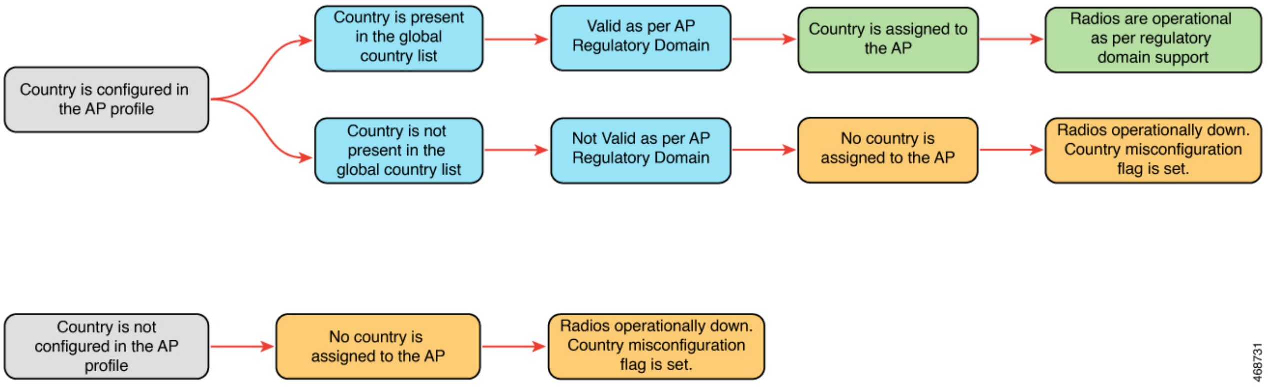
In the non-RoW regulatory domain, when an AP reports a country as part of the join procedure, the following takes place:

- The AP profile has a country configured.
  - If the country configured in the AP profile is present in the global country list, and it is valid as per the AP regulatory domain, the country that is configured in the AP profile is assigned to the AP. Radios become operational as per the country or regulatory domain support.
  - If the country configured in the AP profile is not present in the global country list, and is not valid as per the AP regulatory domain, check the global country list to confirm if the country is present in the list. If the country is present in the global list, the AP retains the previous country configuration and the radios are not operational with the country misconfiguration flag set. If the country is not located in the global list, the AP is disconnected.
- The AP profile does not have a country configured.
  - If the country reported by the AP is found in the global country list, and is valid as per the AP regulatory domain, the country is assigned to the AP and the radios become operational as per the country or regulatory domain support.
  - If the country is not present in the list, search for the first country match from the global list. If the country is found, the country is assigned to the AP and the radios become operational. If the country is not found, the AP is disconnected.

AP Configured with RoW Regulatory Domain

Case 1: The AP does not report a country as part of the join procedure.

AP Does Not Report a Country as Part of the Join Procedure

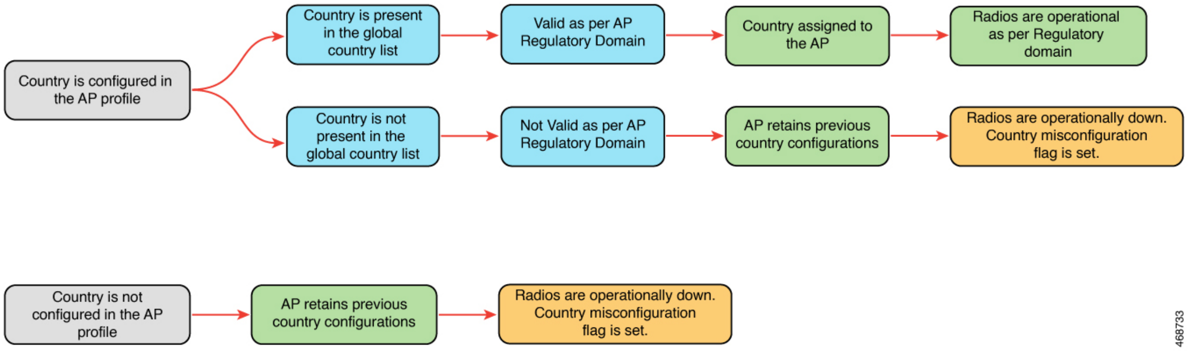

Country is configured in the AP profile
Country is present in the global country list
Valid as per AP Regulatory Domain
Country is assigned to the AP
Radios are operational as per regulatory domain support
Country is not present in the global country list
Not Valid as per AP Regulatory Domain
No country is assigned to the AP
Radios operationally down. Country misconfiguration flag is set.
Country is not configured in the AP profile
No country is assigned to the AP
Radios operationally down. Country misconfiguration flag is set.
468731

In the RoW regulatory domain, when an AP does not report a country as part of the join procedure, the following takes place:

- The AP profile has a country configured.
    - If the country configured in the AP profile is present in the global country list, and is valid as per the AP regulatory domain, country that is configured in the AP profile is assigned to the AP. Radios become operational as per the country or regulatory domain support.
    - If the country configured in the AP profile is not present in the global country list, and is not valid as per the AP regulatory domain, country is not assigned to the AP and radios are not operational, and the country misconfiguration flag is set.
- If the AP profile does not have a country configured, the country is not assigned to the AP and radios are not operational, and the country misconfiguration flag is set.

Case 2: The AP reports a country as part of the join procedure.

AP Reports a Country as Part of the Join Procedure


Country is configured in the AP profile
Country is present in the global country list
Valid as per AP Regulatory Domain
Country assigned to the AP
Radios are operational as per Regulatory domain
Country is not present in the global country list
Not Valid as per AP Regulatory Domain
AP retains previous country configurations
Radios are operationally down. Country misconfiguration flag is set.
Country is not configured in the AP profile
AP retains previous country configurations
Radios are operationally down. Country misconfiguration flag is set.
468733

In the RoW regulatory domain, when an AP reports a country as part of the join procedure, the following takes place:

- The AP profile has a country configured.

  - If the country configured in the AP profile is present in the global country list, and it is valid as per the AP regulatory domain, the country that is configured in the AP profile is assigned to the AP. Radios become operational as per the country or regulatory domain support.
  - If the country configured in the AP profile is not present in the global country list, and is not valid as per the AP regulatory domain, the AP retains the previous country configuration and the radios are not operational with the country misconfiguration flag set.

- The AP retains the previous country configuration and the radios are not operational with the country misconfiguration flag set.

Configuring Management Mode Migration (GUI)

Before you begin

The country code must be configured on the AP profile. To configure the country code, navigate to **Configuration** > **Tags & Profiles** > **AP Join** page. Click an AP profile to edit. In the **General** tab, select the country code from the drop-down list.

Procedure

Step 1 Choose **Configuration** > **Wireless** > **Migrate to Meraki Management Mode**.

Step 2 Select the required APs by clicking on the check box(es), from the displayed APs.
The **Migrate to Meraki Management Mode** button is enabled.

Step 3 Click **Migrate to Meraki Management Mode** button to perform a validation check on the selected APs. If the validation check is successful, the **Next** button is enabled.

Step 4 Click **Next** to start the process.

Step 5 On the **Confirm Management Mode Migration** window, do the following:

a. Select the **Agree and continue** check box.

b. Click **Yes** to confirm.

The **Management Mode Migration Successful** section displays the APs that were migrated to the Meraki management mode. The **Management Mode Migration Failed** section displays the APs that were retained in DNA management mode.

Step 6 Click **Restart Workflow** to restart the workflow for APs that did not migrate from DNA management mode to Meraki management mode.

Exporting Meraki Management Mode-Migrated APs (GUI)

You can export the details about the Meraki management mode-migrated APs either from the **Change to Meraki Persona** tab after the workflow is completed or from the **Previously changed APs** tab.

Procedure

	Command or Action	Purpose
Step 1	Choose **Configuration** > **Wireless** > **Migrate to Meraki Management Mode**.	
Step 2	Click the **Export** button to export the list of APs.	
Step 3	Select whether you want to export only the current page or all pages. Click **Yes** to continue.	
Step 4	On the **Export** window, select the export method. The available options are:	• **Serial Number** • **JSON** • **Export to Meraki Dashboard** **Note** We recommend the Export to Meraki Dashboard option as you can directly export the migrated APs information into the Meraki Dashboard.
Step 5	Click **Copy** to copy the migrated APs. Click **Download** and save the file location.	

Configuring the AP Management Mode (CLI)

Before you begin

- Ensure that the AP is Meraki-capable to run any of the EXEC commands. To view the list of Meraki-capable APs, use the **show ap management-mode meraki capability summary** command.

Note If the country code is misconfigured, the change of management mode will not be allowed for any of the EXEC commands, except the **force** command.

If the regulatory domain is misconfigured for any slot, the change of management mode is not allowed for any of the EXEC commands, except the **force** command.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter the password, if prompted.

	Command or Action	Purpose

Step 2	**ap name** *Cisco-AP-name* **management-mode meraki** [**force**] [**noprompt**]
	Example:
	`Device# ap name Cisco-AP-name management-mode meraki`
	`Device# ap name Cisco-AP-name management-mode meraki force`
	`Device# ap name Cisco-AP-name management-mode meraki noprompt`
	`Device# ap name Cisco-AP-name management-mode meraki force noprompt`
		Changes the AP management mode to Meraki.
		Here, **force** skips the validations at the controller and attempts Meraki management mode change at the AP.
		noprompt skips the user prompt for attempting AP management mode change.

Step 3	(Optional) **clear ap meraki stats** **Example:** `Device# clear ap meraki stats`	Clears the Meraki AP-related data.

Verifying the Management Mode Migration Details

To view the summary of the Meraki-capable AP information, run the following command:

```
Device# show ap management-mode meraki capability summary
AP Name                    AP Model            Radio MAC       MAC Address      AP Serial
 Number       Meraki Serial Number
-------------------------------------------------------------------------------------------

APXXXD.BXXX.1XXX          CW9162I           6XXd.bXXe.eXX0   6XXd.bXXe.eXX0   FOCXXXXXB90
            FOCXXXXXB90
```

To view the failure summary of the AP along with the migration attempt timestamp, run the following command:

```
Device# show ap management-mode meraki failure summary
AP Name              AP Model         Radio MAC        MAC Address      Conversion Attempt
        AP Serial Number       Meraki Serial Number   Reason Code
-------------------------------------------------------------------------------------------

APXXXD.BXXC.1       CW9162I           6XXd.bXXe.eXX0   6XXd.bXXe.eXX0   03/03/2022 17:17:42
 IST   FOCXXXXXB90            FOCXXXXXB90            Regulatory domain not set
```

To view the successful Meraki management mode migration attempts of all the APs, run the following command:

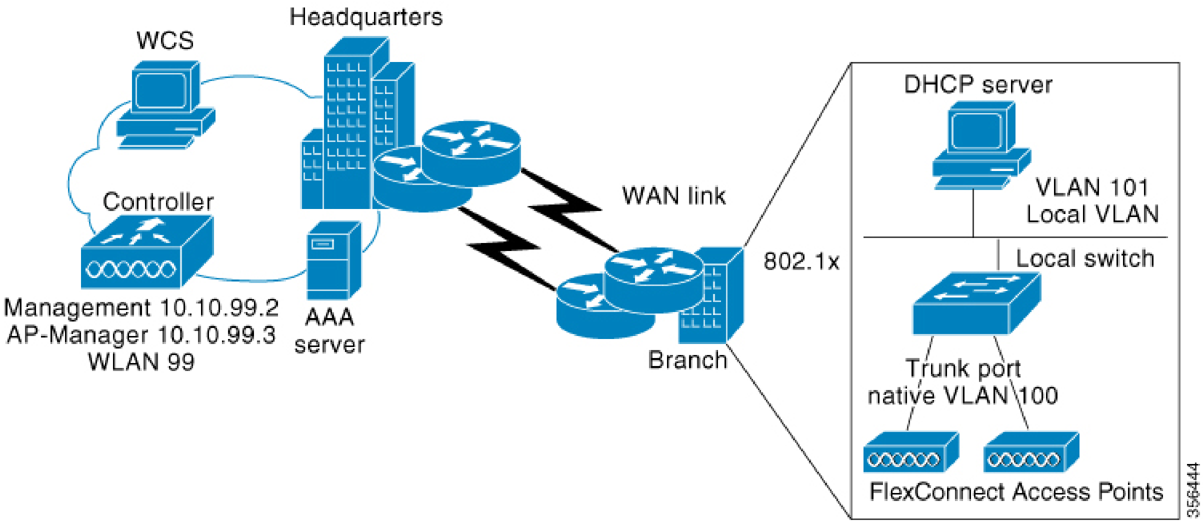
```
Device# show ap management-mode meraki change summary
AP Name                  AP Model          Radio MAC        MAC Address      Conversion
Timestamp       AP Serial Number        Meraki Serial Number
-------------------------------------------------------------------------------------------

APXXXX.3XXX.EXXX         CW9166I-B         1XXX.2XXX.1100   ccXX.3XXX.eXX0   05/02/2022
07:48:56 CST    KWC2XXXXX5G             Q5XX-4XXX-K7XX
```

Information About FlexConnect

FlexConnect is a wireless solution for branch office and remote office deployments. It enables customers to configure and control access points (AP) in a branch or remote office from the corporate office through a wide area network (WAN) link without deploying a controller in each office. The FlexConnect access points can also switch client data traffic locally and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller. FlexConnect access points support multiple SSIDs. In the connected mode, the FlexConnect access point can also perform local authentication.

Figure 1: FlexConnect Deployment



The controller software has a more robust fault tolerance methodology to FlexConnect access points. In previous releases, whenever a FlexConnect access point disassociates from a controller, it moves to the standalone mode. The clients that are centrally switched are disassociated. However, the FlexConnect access point continues to serve locally switched clients. When the FlexConnect access point rejoins the controller (or a standby controller), all the clients are disconnected and are authenticated again. This functionality has been enhanced and the connection between the clients and the FlexConnect access points are maintained intact and the clients experience seamless connectivity. When both the access point and the controller have the same configuration, the connection between the clients and APs is maintained.

After the client connection is established, the controller does not restore the original attributes of the client. The client username, current rate and supported rates, and listen interval values are reset to the default or new configured values only after the session timer expires.

The controller can send multicast packets in the form of unicast or multicast packets to an access point. In FlexConnect mode, an access point can receive only multicast packets.

In Cisco Catalyst 9800 Series Wireless Controller, you can define a flex connect site. A flex connect site can have a flex connect profile associate with it. You can have a maximum of 100 access points for each flex connect site.

FlexConnect access points support a 1-1 network address translation (NAT) configuration. They also support port address translation (PAT) for all features except true multicast. Multicast is supported across NAT boundaries when configured using the Unicast option. FlexConnect access points also support a many-to-one NAT or PAT boundary, except when you want true multicast to operate for all centrally switched WLANs.

Workgroup bridges and Universal Workgroup bridges are supported on FlexConnect access points for locally switched clients.

FlexConnect supports IPv6 clients by bridging the traffic to local VLAN, similar to an IPv4 operation. FlexConnect supports Client Mobility for a group of up to 100 access points.

An access point does not have to reboot when moving from local mode to FlexConnect mode and vice-versa.

FlexConnect Authentication

When an access point boots up, it looks for a controller. If it finds one, it joins the controller, downloads the latest software image and configuration from the controller, and initializes the radio. It saves the downloaded configuration in nonvolatile memory for use in standalone mode.

Note Once the access point is rebooted after downloading the latest controller software, it must be converted to the FlexConnect mode.

Note 802.1X is not supported on the AUX port for Cisco Aironet 2700 series APs.

A FlexConnect access point can learn the controller IP address in one of these ways:

- If the access point has been assigned an IP address from a DHCP server, it can discover a controller through the regular CAPWAP or LWAPP discovery process.

  Note OTAP is not supported.

- If the access point has been assigned a static IP address, it can discover a controller through any of the discovery process methods except DHCP option 43. If the access point cannot discover a controller through Layer 3 broadcast, we recommend DNS resolution. With DNS, any access point with a static IP address that knows of a DNS server can find at least one controller.
- If you want the access point to discover a controller from a remote network where CAPWAP or LWAPP discovery mechanisms are not available, you can use priming. This method enables you to specify (through the access point CLI) the controller to which the access point is to connect.

Note The LEDs on the access point change as the device enters different FlexConnect modes. See the hardware installation guide for your access point for information on LED patterns.

When a client associates to a FlexConnect access point, the access point sends all authentication messages to the controller and either switches the client data packets locally (locally switched) or sends them to the controller (centrally switched), depending on the WLAN configuration. With respect to client authentication (open, shared, EAP, web authentication, and NAC) and data packets, the WLAN can be in any one of the following states depending on the configuration and state of controller connectivity:

Note For the FlexConnect local switching, central authentication deployments, whenever passive client is enabled, the IP Learn timeout is disabled by default.

- central authentication, central switching—In this state, the controller handles client authentication, and all client data is tunneled back to the controller. This state is valid only in connected mode.

- central authentication, local switching—In this state, the controller handles client authentication, and the FlexConnect access point switches data packets locally. After the client authenticates successfully, the controller sends a configuration command with a new payload to instruct the FlexConnect access point to start switching data packets locally. This message is sent per client. This state is applicable only in connected mode.
- local authentication, local switching—In this state, the FlexConnect access point handles client authentication and switches client data packets locally. This state is valid in standalone mode and connected mode.

  In connected mode, the access point provides minimal information about the locally authenticated client to the controller. The following information is not available to the controller:

  - Policy type
  - Access VLAN
  - VLAN name
  - Supported rates
  - Encryption cipher

  Local authentication is useful where you cannot maintain a remote office setup of a minimum bandwidth of 128 kbps with the round-trip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 576 bytes. In local authentication, the authentication capabilities are present in the access point itself. Local authentication reduces the latency requirements of the branch office.
- Notes about local authentication are as follows:
  - Guest authentication cannot be done on a FlexConnect local authentication-enabled WLAN.
  - Local RADIUS on the controller is not supported.
  - Once the client has been authenticated, roaming is only supported after the controller and the other FlexConnect access points in the group are updated with the client information.
- authentication down, switch down—In this state, the WLAN disassociates existing clients and stops sending beacon and probe requests. This state is valid in both standalone mode and connected mode.
- authentication down, local switching—In this state, the WLAN rejects any new clients trying to authenticate, but it continues sending beacon and probe responses to keep existing clients alive. This state is valid only in standalone mode.

When a FlexConnect access point enters standalone mode, WLANs that are configured for open, shared, WPA-PSK, or WPA2-PSK authentication enter the “local authentication, local switching” state and continue new client authentications. This configuration is also correct for WLANs that are configured for 802.1X, WPA-802.1X, WPA2-802.1X, or Cisco Centralized Key Management, but these authentication types require that an external RADIUS server be configured.

Other WLANs enter either the “authentication down, switching down” state (if the WLAN was configured for central switching) or the “authentication down, local switching” state (if the WLAN was configured for local switching).

When FlexConnect access points are connected to the controller (rather than in standalone mode), the controller uses its primary RADIUS servers and accesses them in the order specified on the RADIUS Authentication Servers page or in the **config radius auth add** CLI command (unless the server order is overridden for a particular WLAN). However, to support 802.1X EAP authentication, FlexConnect access points in standalone mode need to have their own backup RADIUS server to authenticate clients.

Note A controller does not use a backup RADIUS server. The controller uses the backup RADIUS server in local authentication mode.

You can configure a backup RADIUS server for individual FlexConnect access points in standalone mode by using the controller CLI or for groups of FlexConnect access points in standalone mode by using either the GUI or CLI. A backup server configured for an individual access point overrides the backup RADIUS server configuration for a FlexConnect.

When web-authentication is used on FlexConnect access points at a remote site, the clients get the IP address from the remote local subnet. To resolve the initial URL request, the DNS is accessible through the subnet's default gateway. In order for the controller to intercept and redirect the DNS query return packets, these packets must reach the controller at the data center through a CAPWAP connection. During the web-authentication process, the FlexConnect access points allows only DNS and DHCP messages; the access points forward the DNS reply messages to the controller before web-authentication for the client is complete. After web-authentication for the client is complete, all the traffic is switched locally.

When a FlexConnect access point enters into a standalone mode, the following occurs:

- The access point checks whether it is able to reach the default gateway via ARP. If so, it will continue to try and reach the controller.

If the access point fails to establish the ARP, the following occurs:

- The access point attempts to discover for five times and if it still cannot find the controller, it tries to renew the DHCP on the ethernet interface to get a new DHCP IP.
- The access point will retry for five times, and if that fails, the access point will renew the IP address of the interface again, this will happen for three attempts.
- If the three attempts fail, the access point will fall back to the static IP and will reboot (only if the access point is configured with a static IP).
- Reboot is done to remove the possibility of any unknown error the access point configuration.

Once the access point reestablishes a connection with the controller, it disassociates all clients, applies new configuration information from the controller, and allows client connectivity again.

Guidelines and Restrictions for FlexConnect

- FlexConnect mode can support only 16 VLANs per AP.
- You can deploy a FlexConnect access point with either a static IP address or a DHCP address. In the context of DHCP, a DHCP server must be available locally and must be able to provide the IP address for the access point at bootup.
- FlexConnect supports up to 4 fragmented packets, or a minimum 576-byte maximum transmission unit (MTU) WAN link.

- Round-trip latency must not exceed 300 milliseconds (ms) between the access point and the controller, and CAPWAP control packets must be prioritized over all other traffic. In scenarios where you cannot achieve the 300-ms round-trip latency, configure the access point to perform local authentication.
- Client connections are restored only for locally switched clients that are in the RUN state when the access point moves from standalone mode to connected mode. After the access point moves, the access point's radio is also reset.
- When multiple APs come from standalone mode to connected mode on FlexConnect and all the APs send the client entry in hybrid-REAP payload to the controller. In this scenario, the controller sends disassociation messages to the WLAN client. However, the WLAN client comes back successfully and joins the controller.
- When APs are in standalone mode, if a client roams to another AP, the source AP cannot determine whether the client has roamed or is just idle. So, the client entry at source AP will not be deleted until idle timeout.
- The configuration on the controller must be the same between the time the access point went into standalone mode and the time the access point came back to connected mode. Similarly, if the access point is falling back to a secondary or backup controller, the configuration between the primary and the secondary or backup controller must be the same.
- A newly connected access point cannot be booted in FlexConnect mode.
- FlexConnect mode requires that the client send traffic before learning the client's IPv6 address. Compared to in local mode where the controller learns the IPv6 address by snooping the packets during Neighbor Discovery to update the IPv6 address of the client.
- 802.11r fast transition roaming is not supported on APs operating in local authentication.
- The primary and secondary controllers for a FlexConnect access point must have the same configuration. Otherwise, the access point might lose its configuration, and certain features, such as WLAN overrides, VLANs, static channel number, and so on, might not operate correctly. In addition, make sure you duplicate the SSID of the FlexConnect access point and its index number on both controllers.
- If you configure a FlexConnect access point with a syslog server configured on the access point, after the access point is reloaded and the native VLAN other than 1, at the time of initialization, a few syslog packets from the access point are tagged with VLAN ID 1.
- MAC filtering is not supported on FlexConnect access points in standalone mode. However, MAC filtering is supported on FlexConnect access points in connected mode with local switching and central authentication. Also, Open SSID, MAC Filtering, and RADIUS NAC for a locally switched WLAN with FlexConnect access points is a valid configuration, where MAC is checked by Cisco ISE.
- FlexConnect does not display any IPv6 client addresses in the Client Detail window.
- FlexConnect access points with locally switched WLANs cannot perform IP source guard and prevent ARP spoofing. For centrally switched WLANs, the wireless controller performs IP source guard and ARP spoofing.
- To prevent ARP spoofing attacks in FlexConnect APs with local switching, we recommend that you use ARP inspection.
- Proxy ARP for VM clients (with any wireless host) does not work since the client includes many IP addresses for the same MAC. To avoid this issue, disable the ARP-caching option in the Flex profile.

- When you enable local switching on policy profile for FlexConnect APs, the APs perform local switching. However, for the APs in local mode, central switching is performed.

  In a scenario where the roaming of a client between FlexConnect mode AP and Local mode AP is not supported, the client may not get the correct IP address due to VLAN difference after the move. Also, L2 and L3 roaming between FlexConnect mode AP and Local mode AP are not supported.

  FlexConnect local switching is not supported on Cisco Aironet Cisco 1810T and 1815T (Teleworker) Access Points.

- Cisco Centralized Key Management (CCKM) is not supported in FlexConnect standalone mode. Hence, CCKM enabled client will not be able to connect when AP is in FlexConnect standalone mode.
- For Wi-Fi Protected Access Version 2 (WPA2) in FlexConnect standalone mode or local authentication in connected mode or Cisco Centralized Key Management fast roaming in connected mode, only Advanced Encryption Standard (AES) is supported.
- For Wi-Fi Protected Access (WPA) in FlexConnect standalone mode or local-auth in connected mode or Cisco Centralized Key Management fast-roaming in connected mode, only Temporal Key Integrity Protocol (TKIP) is supported.
- WPA2 with TKIP and WPA with AES is not supported in standalone mode, local-auth in connected mode, and Cisco Centralized Key Management fast-roaming in connected mode.
- WPA with TKIP is supported in non-FIPS mode.
- Only open, WPA (PSK and 802.1x), and WPA2 (AES) authentication is supported on the Cisco Aironet 1830 Series and 1850 Series APs.
- Only 802.11r fast-transition roaming is supported on the Cisco Aironet 1830 Series and 1850 Series APs.
- AVC on locally switched WLANs is supported on second-generation APs.
- Local authentication fallback is not supported when a user is not available in the external RADIUS server.
- For WLANs configured for FlexConnect APs in local switching and local authentication, synchronization of dot11 client information is supported.
- DNS override is not supported on the Cisco Aironet 1830 Series and 1850 Series APs.
- The Cisco Aironet 1830 Series and 1850 Series APs do not support IPv6. However, a wireless client can pass IPv6 traffic across these APs.
- VLAN group is not supported in Flex mode under flex-profile.
- Configuring maximum number of allowed media streams on individual client or radio is not supported in FlexConnect mode.
- The WLAN client association limit will not work when the AP is in FlexConnect mode (connected or standalone) and is performing local switching and local authentication.
- A local switching client on FlexConnect mode will not get IP address for RLAN profile on the Cisco Aironet 1810 Series AP.
- Standard ACL is not supported on FlexConnect AP mode.
- IPv6 RADIUS Server is not configurable for FlexConnect APs. Only IPv4 configuration is supported.
- In Flex mode, IPv4 ACLs configured on WLAN gets pushed to AP but IPv6 ACLs does not.

- The client delete reason counters that are a part of the **show wireless stats client delete reasons** command, will be incremented only when the client record entry persists for join.

  For example, when an AP in the FlexConnect mode performs local authentication with ACL mismatch, then the AP deletes the client, and the controller does not create any client record.

- Cisco Centralized Key Management (CCKM) is supported in wave 1 APs in FlexConnect when you use local association.

- If the client roams from one AP to another and the roaming is successful, the following occurs:

  - The client does not send any traffic to the new AP.

  - The client's state is IP LEARN pending.

  - The client is deauthenticated after 180 seconds, if there is no traffic for the entire duration. In case the DHCP Required flag is set, the deauthentication occurs after 60 seconds.

- Using custom VLANs under the policy profile of the FlexConnect locally switched WLANs stops the SSID broadcast. In such scenarios, run the **shut** and **no shut** commands on the policy profile to start the SSID broadcast.

  SSIDs are broadcasted when you:

  - Perform VLAN name to id mapping under FlexConnect profile and map the custom VLAN name under the policy profile.

  - Use VLAN id or standard VLAN name, for example, VLANxxxx.

- In the FlexConnect mode, the group temporal key (GTK) timer is set to 3600 seconds by default on Cisco Wave 2 AP, and this value cannot be reconfigured.

- For Flex mode deployments, local association configured policy profiles are not supported at a given time on the WLAN. Only the local association command must be enabled.

- From Cisco IOS XE Amsterdam 17.1.1 release onwards, the police rate per client in the flex connect APs in the controller, is represented as **rate_out** for Ingress (input) and **rate_in** for Egress (output). To verify police rate on the flex AP, use the **show rate-limit client** command.

- FlexConnect APs do not forward the DHCP packets after Change of Authorization (CoA) and change of VLANs using 802.1X encryption. You must disconnect the client from the WLAN and reconnect the client to enable the client to get an IP address in the second VLAN.

- Cisco Wave 2 and Catalyst Wi-Fi6 APs in FlexConnect local switching mode do not support Layer2(PSK, 802.1X) + Layer3(LWA, CWA, redirection-based posturing) + Dynamic AAA override + NAC.

- In Cisco Catalyst 9136I APs, in FlexConnect local authentication, the ongoing session timeout for a client gets reset after every roam.

- Network access control (NAC) is not supported in FlexConnect local authentication.

- Multicast traffic on an AAA overridden VLAN is not supported. Using this configuration may result in potential traffic leaks between VLANs.

Configuring a Site Tag

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag site** *site-name* **Example:** `Device(config)# wireless tag site default-site-tag`	Configures site tag and enters site tag configuration mode.
Step 3	**flex-profile** *flex-profile-name* **Example:** `Device(config-site-tag)# flex-profile rr-xyz-flex-profile`	Maps a flex profile to a site tag.
Step 4	**ap-profile** *ap-profile* **Example:** `Device(config-site-tag)# ap-profile xyz-ap-profile`	Assigns an AP profile to the wireless site.
Step 5	**description** *site-tag-name* **Example:** `Device(config-site-tag)# description "default site tag"`	Adds a description for the site tag.
Step 6	**no local-site** **Example:** `Device(config-site-tag)# no local-site`	Moves the access point to FlexConnect mode.

Step 7	**end**
	Example:
	`Device(config-site-tag)# end`
		Saves the configuration, exits the configuration mode, and returns to privileged EXEC mode.

Step 8	**show wireless tag site summary** **Example:** `Device# show wireless tag site summary`	(Optional) Displays the summary of site tags.

Configuring a Policy Tag (CLI)

Follow the procedure given below to configure a policy tag:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**wireless tag policy** *policy-tag-name* **Example:** `Device(config-policy-tag)# wireless tag policy default-policy-tag`	Configures policy tag and enters policy tag configuration mode. **Note** When performing LWA, the clients connected to a controller gets disconnected intermittently before session timeout.
Step 4	**description** *description* **Example:** `Device(config-policy-tag)# description "default-policy-tag"`	Adds a description to a policy tag.

Step 5	**remote-lan** *name* **policy** *profile-policy-name* {**ext-module**| **port-id** }
	Example:
	`Device(config-policy-tag)# remote-lan rr-xyz-rlan-aa policy rr-xyz-rlan-policy1 port-id 2`
		Maps a remote-LAN profile to a policy profile.

Step 6	**wlan** *wlan-name* **policy** *profile-policy-name* **Example:** `Device(config-policy-tag)# wlan rr-xyz-wlan-aa policy rr-xyz-policy-1`	Maps a policy profile to a WLAN profile. **Note** Ensure that the WLAN profile is not used by any other profiles. If the AP uses the default profile, ensure that the **no central switching** command is configured on other profiles.

Step 7	**end**
	Example:
	`Device(config-policy-tag)# end`
		Exits policy tag configuration mode, and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 8	**show wireless tag policy summary** **Example:** `Device# show wireless tag policy summary`	(Optional) Displays the configured policy tags. **Note** To view detailed information about a policy tag, use the **show wireless tag policy detailed** *policy-tag-name* command.

Attaching a Policy Tag and a Site Tag to an Access Point (GUI)

Procedure

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

Step 2 Click the **Access Point** name.

Step 3 Go to the **Tags** section.

Step 4 Choose the **Policy Tag** from the **Policy** drop-down list.

Step 5 Choose the **Site Tag** from the **Site** drop-down list.

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

Attaching Policy Tag and Site Tag to an AP (CLI)

Follow the procedure given below to attach a policy tag and a site tag to an AP:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap F866.F267.7DFB`	Configures a Cisco AP and enters AP profile configuration mode. **Note** The *mac-address* should be a wired mac address.
Step 3	**policy-tag** *policy-tag-name* **Example:** `Device(config-ap-tag)# policy-tag rr-xyz-policy-tag`	Maps a policy tag to the AP.

	Command or Action	Purpose
Step 4	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag rr-xyz-site`	Maps a site tag to the AP.
Step 5	**rf-tag** *rf-tag-name* **Example:** `Device(config-ap-tag)# rf-tag rf-tag1`	Associates the RF tag.

Step 6	**end**
	Example:
	`Device(config-ap-tag)# end`
		Saves the configuration, exits configuration mode, and returns to privileged EXEC mode.

Step 7	**show ap tag summary** **Example:** `Device# show ap tag summary`	(Optional) Displays AP details and the tags associated to it.
Step 8	**show ap name** *<ap-name>* **tag info** **Example:** `Device# show ap name ap-name tag info`	(Optional) Displays the AP name with tag information.
Step 9	**show ap name** *<ap-name>* **tag detail** **Example:** `Device# show ap name ap-name tag detail`	(Optional) Displays the AP name with tag details.

Linking an ACL Policy to the Defined ACL (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Name** of the Flex Profile. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 In the **Policy ACL** tab, click **Add**.

Step 5 Select the ACL from the **ACL Name** drop-down list and click **Save**.

Step 6 Click **Apply to Device**.

Applying ACLs on FlexConnect

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile-name* **Example:** `Device(config)# wireless profile flex Flex-profile-1`	Configures a wireless flex profile and enters wireless flex profile configuration mode.
Step 3	**acl-policy** *acl-policy-name* **Example:** `Device(config-wireless-flex-profile)# acl-policy ACL1`	Configures an ACL policy. Access control lists (ACLs) perform packet filtering to control the movement of packets through a network.
Step 4	**exit** **Example:** `Device(config-wireless-flex-profile-acl)# exit`	Returns to wireless flex profile configuration mode.
Step 5	**native-vlan-id** **Example:** `Device(config-wireless-flex-profile)# native-vlan-id 25`	Configures native vlan-id information.
Step 6	**vlan** *vlan-name* **Example:** `Device(config-wireless-flex-profile)# vlan-name VLAN0169`	Configures a VLAN.
Step 7	**acl** *acl-name* **Example:** `Device(config-wireless-flex-profile-vlan)# acl ACL1`	Configures an ACL for the interface.
Step 8	**vlan-id***vlan-id* **Example:** `Device(config-wireless-flex-profile-vlan)# vlan-id 169`	Configures VLAN information.

Configuring FlexConnect

Configuring a Switch at a Remote Site

Procedure

Step 1 Attach the access point, which will be enabled for FlexConnect, to a trunk or access port on the switch.

Note The sample configuration in this procedure shows the FlexConnect access point connected to a trunk port on the switch.

Step 2 The following example configuration shows you how to configure a switch to support a FlexConnect access point.

In this sample configuration, the FlexConnect access point is connected to the trunk interface FastEthernet 1/0/2 with native VLAN 100. The access point needs IP connectivity on the native VLAN. The remote site has local servers or resources on VLAN 101. A DHCP pool is created in the local switch for both the VLANs in the switch. The first DHCP pool (NATIVE) is used by the FlexConnect access point, and the second DHCP pool (LOCAL-SWITCH) is used by the clients when they associate to a WLAN that is locally switched.

```
.
.
.
ip dhcp pool NATIVE
   network 209.165.200.224 255.255.255.224
   default-router 209.165.200.225
   dns-server 192.168.100.167
!
ip dhcp pool LOCAL-SWITCH
   network 209.165.201.224 255.255.255.224
   default-router 209.165.201.225
   dns-server 192.168.100.167
!
interface Gig1/0/1
 description Uplink port
 no switchport
 ip address 209.165.202.225 255.255.255.224
!
interface Gig1/0/2
 description the Access Point port
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 101
 switchport mode trunk
!
interface Vlan100
 ip address 209.165.200.225 255.255.255.224
!
interface Vlan101
 ip address 209.165.201.225 255.255.255.224
end
!
.
```

.
.

Configuring the Controller for FlexConnect

You can configure the controller for FlexConnect in two environments:

- Centrally switched WLAN
- Locally switched WLAN

The controller configuration for FlexConnect consists of creating centrally switched and locally switched WLANs. This table shows three WLAN scenarios.

Table 4: WLAN Scenarios

WLAN	Security	Authentication	Switching	Interface Mapping (GUEST VLAN)
Employee	WPA1+WPA2	Central	Central	Management (centrally switched GUEST VLAN)
Employee-local	WPA1+WPA2 (PSK)	Local	Local	101 (locally switched GUEST VLAN)
Guest-central	Web authentication	Central	Central	Management (centrally switched GUEST VLAN)
Employee-local-auth	WPA1+WPA2	Local	Local	101 (locally switched VLAN)

Configuring Local Switching in FlexConnect Mode (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy Profile** page, click the name of a policy profile to edit it or click **Add** to create a new one.

Step 3 In the **Add/Edit Policy Profile** window that is displayed, uncheck the **Central Switching** check box.

Step 4 Click **Update & Apply to Device**.

Configuring Local Switching in FlexConnect Mode (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	**no central switching** **Example:** `Device(config-wireless-policy)# no central switching`	Configures the WLAN for local switching.

Step 4	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring Central Switching in FlexConnect Mode (GUI)

Before you begin

Ensure that the policy profile is configured. If the policy profile is not configured, see *Configuring a Policy Profile (GUI)* section.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy Profile** page, select a policy.

Step 3 In the **Edit Policy Profile** window, in General Tab, use the slider to enable or disable **Central Switching**.

Step 4 Click **Update & Apply to Device**.

Configuring Central Switching in FlexConnect Mode

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Configures the WLAN for central switching.

Step 4	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring an Access Point for FlexConnect

For more information, see *Configuring a Site Tag (CLI)* topic in New Configuration Model chapter.

Configuring an Access Point for Local Authentication on a WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 In the **Policy Profile** page, select a policy profile name. The **Edit Policy Profile** window is displayed.

Step 3 In the General tab, deselect **Central Authentication** check box.

Step 4 Click **Update & Apply to Device**.

Configuring an Access Point for Local Authentication on a WLAN (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures WLAN policy profile and enters the wireless policy configuration mode.
Step 3	**no central authentication** **Example:** `Device(config-wireless-policy)# no central authentication`	Configures the WLAN for local authentication.

Step 4	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Connecting Client Devices to WLANs

Follow the instructions for your client device to create profiles to connect to the WLANs you created, as specified in the #unique_414 .

In the example scenarios (see #unique_414), there are three profiles on the client:

1. To connect to the *employee* WLAN, create a client profile that uses WPA or WPA2 with PEAP-MSCHAPV2 authentication. After the client is authenticated, the client is allotted an IP address by the management VLAN of the controller .

2. To connect to the *local-employee* WLAN, create a client profile that uses WPA or WPA2 authentication. After the client is authenticated, the client is allotted an IP address by VLAN 101 on the local switch.

3. To connect to the *guest-central* WLAN, create a client profile that uses open authentication. After the client is authenticated, the client is allocated an IP address by VLAN 101 on the network local to the access point. After the client connects, a local user can enter any HTTP address in the web browser. The user is automatically directed to the controller to complete the web authentication process. When the web login window appears, the user should enter the username and password.

Configuring FlexConnect Ethernet Fallback

Information About FlexConnect Ethernet Fallback

You can configure an AP to shut down its radio when the Ethernet link is not operational. When the Ethernet link comes back to operational state, you can configure the AP to set its radio back to operational state. This feature is independent of the AP being in connected or standalone mode. When the radios are shut down, the AP does not broadcast the WLANs, and therefore, the clients cannot connect to the AP, either through first association or through roaming.

Configuring FlexConnect Ethernet Fallback

Before you begin

This feature is not applicable to APs with multiple ports.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile-name* **Example:** `Device(config)# wireless profile flex test`	Configures a wireless flex profile and enters wireless flex profile configuration mode.
Step 3	**fallback-radio-shut** **Example:** `Device(config-wireless-flex-profile)# fallback-radio-shut`	Enables radio interface shutdown.

Step 4	**end**
	Example:
	`Device(config-wireless-flex-profile)# end`
		Exits configuration mode and returns to privileged EXEC mode.

Step 5	**show wireless profile flex detailed** *flex-profile-name* **Example:** `Device# show wireless profile flex detailed test`	(Optional) Displays detailed information about the selected profile.

Flex AP Local Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.

Step 2 In the **Flex** page, click the name of the **Flex Profile** or click **Add** to create a new one.

Step 3 In the **Add/Edit Flex Profile** window that is displayed, click the **Local Authentication** tab.

When local authentication and association is enabled in Access Point with Flex mode, the following occurs:

- AP handles the authentication.
- AP handles the rejection of client joins (in Mobility).

Note The controller does not increment statistics when AP rejects client association.

Step 4 Choose the server group from the **RADIUS Server Group** drop-down list.

Step 5 Use the **Local Accounting Radius Server Group** drop down to select the RADIUS server group.

Step 6 Check the **Local Client Roaming** check box to enable client roaming.

Step 7 Choose the profile from the **EAP Fast Profile** drop-down list.

Step 8 Choose to enable or disable the following:

- LEAP: Lightweight Extensible Authentication Protocol (LEAP) is an 802.1X authentication type for wireless LANs and supports strong mutual authentication between the client and a RADIUS server using a logon password as the shared secret. It provides dynamic per-user, per-session encryption keys.
- PEAP: Protected Extensible Authentication Protocol (PEAP) is a protocol that encapsulates the Extensible Authentication Protocol (EAP) within an encrypted and authenticated Transport Layer Security (TLS) tunnel.
- TLS: Transport Layer Security (TLS) is a cryptographic protocol that provide communications security over a computer network.
- RADIUS: Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service.

Step 9 In the **Users** section, click **Add**.

Step 10 Enter username and password details and click **Save**.

Step 11 Click **Save & Apply to Device**.

Flex AP Local Authentication (CLI)

Note The Cisco Catalyst 9800 Series Wireless Controller + FlexConnect local authentication + AP acting as RADIUS are not supported on Cisco COS and IOS APs.

Procedure

	Command or Action	Purpose
Step 1	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Creates a AAA authentication model.
Step 2	**aaa session-id common** **Example:** `Device(config)# aaa session-id common`	Ensures that all the session IDs information that is sent out from the RADIUS group for a given call are identical.
Step 3	**dot1x system-auth-control** **Example:** `Device(config)# dot1x system-auth-control`	Enables system authorization control for the RADIUS group.
Step 4	**eap profile** *name* **Example:** `Device(config)# eap profile aplocal-test`	Creates an EAP profile.
Step 5	**method fast** **Example:** `Device(config-eap-profile)# method fast`	Configures the FAST method on the profile.
Step 6	**exit** **Example:** `Device(config-radius-server)# exit`	Returns to configuration mode.
Step 7	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex default-flex-profile`	Configures the flex policy.
Step 8	**local-auth ap eap-fast** *name* **Example:** `Device(config-wireless-flex-profile)# local-auth ap eap-fast aplocal-test`	Configures EAP-FAST profile details.

	Command or Action	Purpose
Step 9	**local-auth ap leap** **Example:** `Device(config-wireless-flex-profile)# local-auth ap leap`	Configures the LEAP method.
Step 10	**local-auth ap peap** **Example:** `Device(config-wireless-flex-profile)# local-auth ap peap`	Configures the PEAP method.
Step 11	**local-auth ap username** *username* **Example:** `Device(config-wireless-flex-profile)# local-auth ap username test1 test1`	Configures username and password.
Step 12	**local-auth ap username** *username password* **Example:** `Device(config-wireless-flex-profile)# local-auth ap username test2 test2`	Configures another username and password.
Step 13	**exit** **Example:** `Device(config-wireless-flex-profile)# exit`	Returns to configuration mode.
Step 14	**wireless profile policy** *policy-profile* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures profile policy.
Step 15	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Disables the policy profile.
Step 16	**no central authentication** **Example:** `Device(config)# no central authentication`	Disables central (controller) authentication.
Step 17	**vlan-id** *vlan-id* **Example:** `Device(config)# vlan-id 54`	Configures VLAN name or VLAN ID.
Step 18	**no shutdown** **Example:** `Device(config)# no shutdown`	Enables the configuration.

Flex AP Local Authentication with External Radius Server

In this mode, an access point handles client authentication and switches client data packets locally. This state is valid in standalone mode and connected mode.

Procedure

	Command or Action	Purpose
Step 1	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Creates a AAA authentication model.
Step 2	**aaa session-id common** **Example:** `Device(config)# aaa session-id common`	Ensures that all the session ID's information that is sent out, from the RADIUS group for a given call are identical.
Step 3	**dot1x system-auth-control** **Example:** `Device(config)# dot1x system-auth-control`	Enables the system authorization control for the RADIUS group.
Step 4	**radius server** *server-name* **Example:** `Device(config)# radius server Test-SERVER1`	Specifies the RADIUS server name. **Note** To authenticate clients with freeradius over RADSEC, you should generate an RSA key longer than 1024 bit. Use the **crypto key generate rsa general-keys exportable label** *name* command to achieve this. Do not configure **key-wrap** option under the radius server and radius server group, as it may lead to clients getting stuck in authentication state.

Step 5	**address {ipv4 | ipv6}** *ip address* {**auth-port** *port-number* | **acct-port** *port-number* }
	Example:
	`Device(config-radius-server)# address ipv4 124.3.50.62 auth-port 1112 acct-port 1113`
	`Device(config-radius-server)# address ipv6 2001:DB8:0:20::15 auth-port 1812 acct-port 1813`
		Specifies the primary RADIUS server parameters.

	Command or Action	Purpose
Step 6	**key** *string* **Example:** `Device(config-radius-server)# key test123`	Specifies the authentication and encryption key used between the device and the RADIUS daemon running on the RADIUS server. **Note** The maximum number of characters allowed for the shared secret is 63.
Step 7	**radius server** *server-name* **Example:** `Device(config)# radius server Test-SERVER2`	Specifies the RADIUS server name.

Step 8	**address {ipv4 | ipv6}** *ip address* {**auth-port** *port-number* | **acct-port** *port-number* }
	Example:
	`Device(config-radius-server)# address ipv4 124.3.52.62 auth-port 1112 acct-port 1113`
	`Device(config-radius-server)# address ipv6 2001:DB8:0:21::15 auth-port 1812 acct-port 1813`
		Specifies the secondary RADIUS server parameters.

Step 9	**key** *string* **Example:** `Device(config-radius-server)# key test113`	Specifies the authentication and encryption key used between the device and the RADIUS daemon running on the RADIUS server.
Step 10	**exit** **Example:** `Device(config-radius-server)# exit`	Returns to configuration mode.
Step 11	**aaa group server radius** *server-group* **Example:** `Device(config)# aaa group server radius aaa_group_name`	Creates a RADIUS server group identification. **Note** *server-group* refers to the server group name. The valid range is from 1 to 32 alphanumeric characters.
Step 12	**radius server** *server-name* **Example:** `Device(config)# radius server Test-SERVER1`	Specifies the RADIUS server name.
Step 13	**radius server** *server-name* **Example:** `Device(config-radius-server)# radius server Test-SERVER2`	Specifies the RADIUS server name.

	Command or Action	Purpose
Step 14	**exit** **Example:** `Device(config-radius-server)# exit`	Exit from RADIUS server configuration mode.
Step 15	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex default-flex-profile`	Creates a new flex policy.
Step 16	**local-auth radius-server-group** *server-group* **Example:** `Device(config-wireless-flex-profile)# local-auth radius-server-group aaa_group_name`	Configures the authentication server group name.
Step 17	**exit** **Example:** `Device(config-wireless-flex-profile)# exit`	Returns to configuration mode.
Step 18	**wireless profile policy** *policy-profile* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures a WLAN policy profile.
Step 19	**shutdown** **Example:** `Device(config-wireless-policy)# shutdown`	Disables a policy profile.
Step 20	**no central authentication** **Example:** `Device(config-wireless-policy)# no central authentication`	Disables central (controller) authentication.
Step 21	**vlan-id** *vlan-id* **Example:** `Device(config-wireless-policy)# vlan-id 54`	Configures a VLAN name or VLAN Id.
Step 22	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables the configuration.

Configuration Example: FlexConnect with Central and Local Authentication

To see configuration example on how to configure a controller for FlexConnect central and local authentication, see the FlexConnect Configuration with Central and Local Authentication on Catalyst 9800 Wireless Controllers document.

NAT-PAT for FlexConnect

If you want to use a central DHCP server to service clients across remote sites, NAT-PAT should be enabled.

An AP translates the traffic coming from a client and replaces the client's IP address with its own IP address.

Note You must enable local switching, central DHCP, and DHCP required using the (**ipv4 dhcp required**) command to enable NAT and PAT.

Configuring NAT-PAT for a WLAN or a Remote LAN

Creating a WLAN

Follow the steps given here to create a WLAN.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan wlan-demo 1 ssid-demo`	Enters the WLAN configuration sub-mode. • *wlan-name*—Enter the profile name. The range is from 1 to 32 alphanumeric characters. • *wlan-id*—Enter the WLAN ID. The range is from 1 to 512. • *SSID-name*—Enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID.

	Command or Action	Purpose
		Note If you have already configured WLAN, enter *wlan wlan-name* command.
Step 3	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Shut down the WLAN.

Step 4	**end**
	Example:
	`Device(config-wlan)# end`
		Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring a Wireless Profile Policy and NAT-PAT (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Name** of the policy.

Step 4 Disable the **Central Switching** toggle button.

Step 5 Enable the **Central DHCP** toggle button.

Step 6 Enable the **Flex NAT/PAT** toggle button.

Step 7 In the **Advanced** tab, under the **DHCP** Settings, check the **IPv4 DHCP Required** check box.

Step 8 Click **Apply to Device**.

Configuring a Wireless Profile Policy and NAT-PAT

Follow the procedure given below to configure a wireless profile policy and NAT-PAT:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy nat-enabled-policy`	Configures the policy profile for NAT.

	Command or Action	Purpose
Step 3	**no central switching** **Example:** `Device(config-wireless-policy)# no central switching`	Configures the WLAN for local switching.
Step 4	**ipv4 dhcp required** **Example:** `Device(config-wireless-policy)# ipv4 dhcp required`	Configures the DHCP parameters for WLAN.
Step 5	**central dhcp** **Example:** `Device(config-wireless-policy)# central dhcp`	Configures the central DHCP for locally switched clients.
Step 6	**flex nat-pat** **Example:** `Device(config-wireless-policy)# flex nat-pat`	Enables NAT-PAT.
Step 7	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables policy profile.

Step 8	**end**
	Example:
	`Device(config-wireless-policy)# end`
		Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Mapping a WLAN to a Policy Profile

Follow the procedure given below to map a WLAN to a policy profile:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag policy** *policy-tag-name* **Example:** `Device(config)# wireless tag policy demo-tag`	Configures a policy tag and enters policy tag configuration mode.

	Command or Action	Purpose
Step 3	**wlan** *wlan-name* **policy** *profile-policy-name* **Example:** `Device(config-policy-tag)# wlan wlan-demo policy nat-enabled-policy`	Maps a policy profile to a WLAN profile.

Step 4	**end**
	Example:
	`Device(config-policy-tag)# end`
		Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring a Site Tag

Follow the procedure given below to configure a site tag:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag site** *site-name* **Example:** `Device(config)# wireless tag site flex-site`	Configures a site tag and enters site tag configuration mode.
Step 3	**no local-site** **Example:** `Device(config-site-tag)# no local-site`	Moves an access point to FlexConnect mode.

Step 4	**end**
	Example:
	`Device(config-site-tag)# end`
		Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Attaching a Policy Tag and a Site Tag to an Access Point (GUI)

Procedure

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

Step 2 Click the **Access Point** name.

Step 3 Go to the **Tags** section.

Step 4 Choose the **Policy Tag** from the **Policy** drop-down list.

Step 5 Choose the **Site Tag** from the **Site** drop-down list.

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

Attaching a Policy Tag and a Site Tag to an Access Point

Follow the procedure given below to attach a policy tag and a site tag to an access point:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap F866.F267.7DFB`	Configures Cisco APs and enters ap-tag configuration mode.
Step 3	**policy-tag** *policy-tag-name* **Example:** `Device(config-ap-tag)# policy-tag demo-tag`	Maps a policy tag to the AP.
Step 4	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag flex-site`	Maps a site tag to the AP.

Step 5	**end**
	Example:
	`Device(config-ap-tag)# end`
		Returns to privileged EXEC mode.

Split Tunneling for FlexConnect

If a client that connects over a WAN link that is associated with a centrally switched WLAN has to send traffic to a device present in the local site, this traffic should be sent over CAPWAP to the controller, and the same traffic is sent back to the local site either over CAPWAP or with the help of some off-band connectivity.

This process consumes WAN link bandwidth unnecessarily. To avoid this, you can use the Split Tunneling feature, which allows the traffic sent by a client to be classified based on the packet contents. The matching packets are locally switched and the rest of the traffic is centrally switched. The traffic that is sent by the client that matches the IP address of the device present in the local site can be classified as locally switched traffic, and the rest of the traffic as centrally switched.

To configure local split tunneling on an AP, ensure that you have enabled DCHP Required on the policy profile using the (**ipv4 dhcp required**) command. This ensures that the client that is associating with the split WLAN does DHCP.

Note Apple iOS clients need option 6 (DNS) to be set in DHCP offer for split tunneling to work.

Note

- FlexConnect split tunneling (vlan-based central switching for FlexConnect) on auto-anchor deployment is not supported.
- Split tunneling does not work on RLAN clients. When the **split-tunnel** option is enabled on RLAN, traffic denied by the split tunnel ACL is not translated based on the IP address, instead the traffic is sent back to the controller through CAPWAP.
- URL filter must not be configured with wildcard URLs such as * and *.*

Configuring Split Tunneling for a WLAN or Remote LAN

Defining an Access Control List for Split Tunneling (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **ACL**.

Step 2 Click **Add**.

Step 3 In the **Add ACL Setup** dialog box, enter the **ACL Name**.

Step 4 Choose the ACL type from the **ACL Type** drop-down list.

Step 5 Under the **Rules** settings, enter the **Sequence** number and choose the **Action** as either **permit** or **deny**.

Step 6 Choose the required source type from the **Source Type** drop-down list.

a) If you choose the source type as **Host**, then you must enter the **Host Name/IP**.

b) If you choose the source type as **Network**, then you must specify the **Source IP** address and **Source Wildcard** mask.

Step 7 Check the **Log** check box if you want the logs.

Step 8 Click **Add**.

Step 9 Add the rest of the rules and click **Apply to Device**.

Defining an Access Control List for Split Tunneling

Follow the procedure given below to define an Access Control List (ACL) for split tunneling:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip access-list extended** *name* **Example:** `Device(config)# ip access-list extended split_mac_acl`	Defines an extended IPv4 access list using a name, and enters access-list configuration mode.
Step 3	**deny ip any host** *hostname* **Example:** `Device(config-ext-nacl)# deny ip any host 9.9.2.21`	Allows the traffic to switch centrally.
Step 4	**permit ip any any** **Example:** `Device(config-ext-nacl)# permit ip any any`	Allows the traffic to switch locally.

Step 5	**end**
	Example:
	`Device(config-ext-nacl)# end`
		Exits configuration mode and returns to privileged EXEC mode.

Linking an ACL Policy to the Defined ACL

Follow the procedure given below to link an ACL policy to the defined ACL:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex flex-profile`	Configures the Flex profile and enters flex profile configuration mode.
Step 3	**acl-policy** *acl policy name* **Example:** `Device(config-wireless-flex-profile)# acl-policy split_mac_acl`	Configures an ACL policy for the defined ACL.

	Command or Action	Purpose

Step 4	**end**
	Example:
	`Device(config-wireless-flex-profile)# end`
		Exits configuration mode and returns to privileged EXEC mode.

Creating a WLAN

Follow the procedure given below to create a WLAN.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id SSID-name* **Example:** `Device(config)# wlan wlan-demo 1 ssid-demo`	Specifies the WLAN name and ID: • *wlan-name*—Enter the profile name. The range is from 1 to 32 alphanumeric characters. • *wlan-id*—Enter the WLAN ID. The range is from 1 to 512. • *SSID-name*—Enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID.
Step 3	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Step 4	**end**
	Example:
	`Device(config-wlan)# end`
		Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring a Wireless Profile Policy and a Split MAC ACL Name (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Name** of the policy.

Step 4 Enable the **Central Switching** toggle button.

Step 5 Enable the **Central DHCP** toggle button.

Step 6 In the **Advanced** tab, under the **DHCP** settings, check the **IPv4 DHCP Required** check box and enter the **DHCP Server IP Address**.

Step 7 Under the **WLAN Flex Policy** settings, choose the split MAC ACL from the **Split MAC ACL** drop-down list.

Step 8 Click **Apply to Device**.

Configuring a Wireless Profile Policy and a Split MAC ACL Name

Follow the procedure given below to configure a wireless profile policy and a split MAC ACL name:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy split-tunnel-enabled-policy`	Configures a WLAN policy profile and enters wireless policy configuration mode.
Step 3	**flex split-mac-acl** *split-mac-acl-name* **Example:** `Device(config-wireless-policy)# flex split-mac-acl split_mac_acl`	Configures a split MAC ACL name. **Note** You should use the same ACL name for linking the flex and the policy profile.
Step 4	**central switching** **Example:** `Device(config-wireless-policy)# central switching`	Configures WLAN for central switching.
Step 5	**central dhcp** **Example:** `Device(config-wireless-policy)# central dhcp`	Enables central DHCP for centrally switched clients.
Step 6	**ipv4 dhcp required** **Example:** `Device(config-wireless-policy)# ipv4 dhcp required`	Configures the DHCP parameters for a WLAN.
Step 7	**ipv4 dhcp server** *ip_address* **Example:**	Configures the override IP address of the DHCP server.

	Command or Action	Purpose
	`Device(config-wireless-policy)# ipv4 dhcp server 9.1.0.100`	
Step 8	**no shutdown** **Example:** `Device(config-wireless-policy)# no shutdown`	Enables a policy profile.

Mapping a WLAN to a Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.

Step 2 Click **Add**.

Step 3 Enter the **Name** of the Tag Policy.

Step 4 Under **WLAN-POLICY Maps** tab, click **Add** .

Step 5 Choose the WLAN Profile from the **WLAN Profile** drop-down list.

Step 6 Choose the Policy Profile from the **Policy Profile** drop-down list.

Step 7 Click the **Tick** Icon .

Step 8 Click **Apply to Device**.

Mapping WLAN to a Policy Profile

Follow the procedure given below to map WLAN to a policy profile.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag policy** *policy-tag-name* **Example:** `Device(config)# wireless tag policy split-tunnel-enabled-tag`	Configures a policy tag and enters policy tag configuration mode.
Step 3	**wlan** *wlan-name* **policy** *profile-policy-name* **Example:** `Device(config-policy-tag)# wlan wlan-demo policy split-tunnel-enabled-policy`	Maps a policy profile to a WLAN profile.

	Command or Action	Purpose

Step 4	**end**
	Example:
	`Device(config-policy-tag)# end`
		Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Configuring a Site Tag

Follow the procedure given below to configure a site tag:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless tag site** *site-name* **Example:** `Device(config)# wireless tag site flex-site`	Configures a site tag and enters site tag configuration mode.
Step 3	**no local-site** **Example:** `Device(config-site-tag)# no local-site`	**Local site** is not configured on the site tag.
Step 4	**flex-profile** *flex-profile-name* **Example:** `Device(config-site-tag)# flex-profile flex-profile`	Configures a flex profile.

Step 5	**end**
	Example:
	`Device(config-site-tag)# end`
		Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Attaching a Policy Tag and Site Tag to an Access Point

Follow the procedure given below to attach a policy tag and site tag to an access point.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**ap** *ethernet-mac-address* **Example:** `Device(config)# ap 188b.9dbe.6eac`	Configures an AP and enters ap tag configuration mode.
Step 3	**policy-tag** *policy-tag-name* **Example:** `Device(config-ap-tag)# policy-tag split-tunnel-enabled-tag`	Maps a policy tag to an AP.
Step 4	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag flex-site`	Maps a site tag to an AP.

Step 5	**end**
	Example:
	`Device(config-ap-tag)# end`
		Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

VLAN-based Central Switching for FlexConnect

In FlexConnect local switching, if the VLAN definition is not available in an access point, the corresponding client does not pass traffic. This scenario is applicable when the AAA server returns the VLAN as part of client authentication.

When a WLAN is locally switched in flex and a VLAN is configured on the AP side, the traffic is switched locally. When a VLAN is not defined in an AP, the VLAN drops the packet.

When VLAN-based central switching is enabled, the corresponding AP tunnels the traffic back to the controller. The controller then forwards the traffic to its corresponding VLAN.

Note

- For VLAN-based central switching, ensure that VLAN is defined on the controller.
- VLAN-based central switching is not supported by mac filter.
- For local switching, ensure that VLAN is defined on the policy profile and FlexConnect profile.
- VLAN-based central switching with central web authentication enabled in Flex profile is not supported.

Configuring VLAN-based Central Switching (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click the name of the policy profile.

Step 3 In the **Edit Policy Profile** window, perform these tasks:

a) Set **Central Switching** to **Disabled** state.
b) Set **Central DHCP** to **Disabled** state.
c) Set **Central Authentication** to **Enabled** state.

Step 4 Click the **Advanced** tab.

Step 5 Under **AAA Policy**, check the **Allow AAA Override** check box to enable AAA override.

Step 6 Under **WLAN Flex Policy**, check the **VLAN Central Switching** check box, to enable VLAN-based central switching on the policy profile.

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

Configuring VLAN-based Central Switching (CLI)

Follow the procedure given below to configure VLAN-based central switching.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy default-policy-profile`	Configures a wireless policy profile.
Step 3	**no central switching** **Example:** `Device(config-wireless-policy)# no central switching`	Configures a WLAN for local switching.
Step 4	**no central dhcp** **Example:** `Device(config-wireless-policy)# no central dhcp`	Configures local DHCP mode, where the DHCP is performed in an AP.
Step 5	**central authentication** **Example:** `Device(config-wireless-policy)# central authentication`	Configures a WLAN for central authentication.
Step 6	**aaa-override** **Example:**	Configures AAA policy override.

	Command or Action	Purpose
	`Device(config-wireless-policy)# aaa-override`	
Step 7	**flex vlan-central-switching** **Example:** `Device(config-wireless-policy)# flex vlan-central-switching`	Configures VLAN-based central switching.

Step 8	**end**
	Example:
	`Device(config-wireless-policy)# end`
		Returns to privileged EXEC mode.

Step 9	**show wireless profile policy detailed** *default-policy-profile* **Example:** `Device# show wireless profile policy detailed default-policy-profile`	(Optional) Displays detailed information of the policy profile.

OfficeExtend Access Points for FlexConnect

A Cisco OfficeExtend access point (OEAP) provides secure communications from a controller to a Cisco AP at a remote location, seamlessly extending the corporate WLAN over the Internet to an employee's residence. A user's experience at the home office is exactly the same as it would be at the corporate office. Datagram Transport Layer Security (DTLS) encryption between an access point and the controller ensures that all communications have the highest level of security.

Note Preconfigure the controller IP for a zero-touch deployment with OEAP. All other home users can use the same access point to connect for home use by configuring the local SSID from AP.

Note In releases prior to Cisco IOS XE Amsterdam 17.3.2, when an AP is converted to OEAP, the local DHCP server on the AP is enabled by default. If the DHCP server on home router has a similar configuration, a network conflict occurs and AP will not be able to join back to the controller. In such a scenario, we recommend that you change the default DHCP server on the Cisco AP using OEAP GUI.

Note For OEAP, when configuration changes are made from the OEAP GUI to the following: Radio Status, Radio Interface Status, 802.11 n-mode, 802.11 ac-mode, Bandwidth, and Channel Selection (2.4 GHz or 5 GHz), CAPWAP should be restarted for the configuration sync to take place between the AP and the controller. During this interval, the AP GUI may not respond until the AP rejoins the controller. We recommend that you wait for the AP to rejoin the controller (for about 1-2 minutes), before you make further changes from the OEAP GUI.

Note In Cisco OfficeExtend access point (Cisco OEAP), if the OEAP local DHCP server is enabled and the user configures DNS IP from OEAP GUI, the wireless and wired clients connected to Cisco OEAP will receive that IP as DNS server IP in DHCP ACK.

Configuring OfficeExtend Access Points

Follow the procedure given below to configure OfficeExtend access points.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile-name* **Example:** `Device(config)# wireless profile flex test`	Configures a wireless flex profile and enters wireless flex profile configuration mode.
Step 3	**office-extend** **Example:** `Device(config-wireless-flex-profile)# office-extend`	Enables the OfficeExtend AP mode for a FlexConnect AP.

Step 4	**end**
	Example:
	`Device(config-wireless-flex-profile)# end`
		Exits configuration mode and returns to privileged EXEC mode.
		Note After creating a flex profile, ensure that OEAP is in flex connect mode and mapped to its corresponding site tag.
		OfficeExtend is disabled by default. To clear the access point's configuration and return it to the factory-defaults, use the **clear ap config** *cisco-ap* command.

Disabling OfficeExtend Access Point

Follow the procedure given below to disable an OfficeExtend access point.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile-name* **Example:** `Device(config)# wireless profile flex test`	Configures a wireless flex profile and enters wireless flex profile configuration mode.
Step 3	**no office-extend** **Example:** `Device(config-wireless-flex-profile)# no office-extend`	Disables OfficeExtend AP mode for a FlexConnect AP.

Step 4	**end**
	Example:
	`Device(config-wireless-flex-profile)# end`
		Exits configuration mode and returns to privileged EXEC mode.

Support for OEAP Personal SSID

Information About OEAP Personal SSID Support

The Cisco OfficeExtend Access Point supports personal SSID. This enables a local home client to use the same OfficeExtend Access Point for local networking and internet connectivity. With the help of the OEAP personal SSID feature, you can enable or disable personal SSID, enable or disable Datagram Transport Layer Security (DTLS) encryption between an access point and the controller, and enable rogue detection, using the knobs that are present on the AP profile page in the GUI. The local network access and DTLS encryption are enabled by default. The configurations described in this chapter is applicable for OEAP or for APs in the OEAP mode.

Configuring OEAP Personal SSID (GUI)

Procedure

Step 1 Choose **Configuration** > **AP Tags & Profiles** > **AP Join**.

The **AP Join Profile** section displays all the AP Join profiles.

Step 2 To edit the configuration details of an AP Join profile, select APs in the OEAP mode.
The **Edit AP Join Profile** window is displayed.

Step 3 In the **General** tab, under the **OfficeExtend AP Configuration** section, configure the following:

a) Check the **Local Access** check box to enable the local network. By default, **Local Access** is enabled. After the AP joins the controller using AP join profile where local access is enabled, the AP will not broadcast the default personal SSID. Since the local access is enabled, you can login to the AP GUI and configure the personal SSID.

b) Check the **Link Encryption** check box to enable data DTLS. By default, **Link Encryption** is enabled.

c) Check the **Rogue Detection** check box to enable rogue detection. Rogue detection is disabled by default for OfficeExtend APs because these APs, deployed in a home environment, are likely to detect a large number of rogue devices.

Configuring OEAP Personal SSID (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *ap-profile* **Example:** `Device(config)# ap profile ap-profile`	Configures an AP profile and enters the AP profile configuration mode.
Step 3	**[no] oeap local-access** **Example:** `Device(config-ap-profile)# oeap local-access`	Enables the local access to AP. Local access consist of local AP GUI, LAN ports and personal SSID. The **no** form of this command disables the feature. If the local access is disabled, you will not be able to access the AP GUI, the local LAN port will be disabled, and personal SSID will not be broadcasted.
Step 4	**[no] oeap link-encryption** **Example:** `Device(config-ap-profile)# oeap link-encryption`	Enables DTLS encryption for OEAP APs or APs moving to the OEAP mode. The **no** form of this command disables the feature. This feature is enabled by default.
Step 5	**[no] oeap rogue-detection** **Example:** `Device(config-ap-profile)# no oeap rogue-detection`	Enables OEAP DTLS encryption in the AP profile configuration mode. This feature is disabled by default.

Viewing OEAP Personal SSID Configuration

To view the OEAP personal SSID configuration, run the following command.

```
Device# show ap profile name default-ap-profile detailed
.
.
.
OEAP Mode Config
Link Encryption : ENABLED
```

```
Rogue Detection : DISABLED
Local Access : ENABLED
```

Clearing Personal SSID from an OfficeExtend Access Point

To clear the personal SSID from an access point, run the following command:

ap name *Cisco_AP* **clear-personal-ssid**

Example: Viewing OfficeExtend Configuration

This example displays an OfficeExtend configuration:

```
Device# show ap config general

Cisco AP Name   : ap_name
=================================================

Cisco AP Identifier                             : 70db.986d.a860
Country Code                                    : Multiple Countries : US,IN
Regulatory Domain Allowed by Country            : 802.11bg:-A   802.11a:-ABDN
AP Country Code                                 : US  - United States
AP Regulatory Domain
  Slot 0                                        : -A
  Slot 1                                        : -D
MAC Address                                     : 002c.c899.7b84
IP Address Configuration                        : DHCP
IP Address                                      : 9.9.48.51
IP Netmask                                      : 255.255.255.0
Gateway IP Address                              : 9.9.48.1
CAPWAP Path MTU                                 : 1485
Telnet State                                    : Disabled
SSH State                                       : Disabled
Jumbo MTU Status                                : Disabled
Cisco AP Location                               : default location
Site Tag Name                                   : flex-site
RF Tag Name                                     : default-rf-tag
Policy Tag Name                                 : split-tunnel-enabled-tag
AP join Profile                                 : default-ap-profile
Primary Cisco Controller Name                   : uname-controller
Primary Cisco Controller IP Address             : 9.9.48.34
Secondary Cisco Controller Name                 : uname-controller1
Secondary Cisco Controller IP Address           : 0.0.0.0
Tertiary Cisco Controller Name                  : uname-ewlc2
Tertiary Cisco Controller IP Address            : 0.0.0.0
Administrative State                            : Enabled
Operation State                                 : Registered
AP Mode                                         : FlexConnect
AP Submode                                      : Not Configured
Office Extend Mode                              : Enabled
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : information
Software Version                                : 16.8.1.1
Boot Version                                    : 1.1.2.4
Mini IOS Version                                : 0.0.0.0
Stats Reporting Period                          : 0
LED State                                       : Enabled
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : PoE/Full Power (normal mode)
```

Proxy ARP

Proxy address resolution protocol (ARP) is the most common method for learning about MAC address through a proxy device. Enabling Proxy ARP known as ARP caching in Cisco Catalyst 9800 Series Wireless Controller means that the AP owning client is the destination of the ARP request, replies on behalf of that client and therefore does not send the ARP request to the client over the air. Access points not owning the destination client and receiving an ARP request through their wired connection will drop the ARP request. When the ARP caching is disabled, the APs bridge the ARP requests from wired-to-wireless and vice-versa increasing the air time usage and broadcasts over wireless.

The AP acts as an ARP proxy to respond to ARP requests on behalf of the wireless clients.

Enabling Proxy ARP for FlexConnect APs (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.

Step 2 Click **Add**.

Step 3 In the **General** tab, enter the **Name** of the Flex Profile and check the **ARP Caching** check box. The name can be ASCII characters from 32 to 126, without leading and trailing spaces.

Step 4 Click **Apply to Device**.

Enabling Proxy ARP for FlexConnect APs

Follow the procedure given below to configure proxy ARP for FlexConnect APs.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-policy* **Example:** `Device(config)# wireless profile flex flex-test`	Configures WLAN policy profile and enters wireless flex profile configuration mode.
Step 3	**arp-caching** **Example:** `Device(config-wireless-flex-profile)# arp-caching`	Enables ARP caching. **Note** Use the **no arp-caching** command to disable ARP caching.

	Command or Action	Purpose

Step 4	**end**
	Example:
	`Device(config-wireless-flex-profile)# end`
		Returns to privileged EXEC mode.

Step 5	**show running-config | section wireless profile flex** **Example:** `Device# show running-config | section wireless profile flex`	Displays ARP configuration information.
Step 6	**show wireless profile flex detailed** *flex-profile-name* **Example:** `Device# show wireless profile flex detailed flex-test`	(Optional) Displays detailed information of the flex profile.
Step 7	**show arp summary** **Example:** `Device# show arp summary`	(Optional) Displays ARP summary.

Overlapping Client IP Address in Flex Deployment

Overview of Overlapping Client IP Address in Flex Deployment

In flex deployments, you can use cookie cutter configuration across sites and branches which also includes local DHCP servers configured with the same subnet. In this topology, controllers detect multiple client sessions with the same IP as IP THEFT and clients are put in blocked list.

The Overlapping Client IP Address in Flex Deployment feature offers overlapping IP address across various flex sites and provides all the functionalities that are supported in flex deployments.

Enabling Overlapping Client IP Address in Flex Deployment (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex** and click **Add**.

Step 2 On the **Add Flex Profile** window and **General** tab.

Step 3 Check the **IP Overlap** check box to enable overlapping client IP Address in Flex deployment.

Step 4 Click **Apply to Device**.

Enabling Overlapping Client IP Address in Flex Deployment

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex flex1`	Configures a Flex profile and enters Flex profile configuration mode.
Step 3	[**no**] **ip overlap** **Example:** `Device(config-wireless-flex-profile)# [no] ip overlap`	Enables overlapping client IP address in flex deployment. **Note** By default, the configuration is disabled.

Verifying Overlapping Client IP Address in Flex Deployment (GUI)

Procedure

Step 1 Choose **Monitoring** > **Wireless** > **Clients**.

Step 2 Click the client in the table to view properties and statistics for each client.

Step 3 On the **Client** window and **General** tab, click **Client Statistics** tab to view the following details:

- Number of Bytes Received from Client
- Number of Bytes Sent to Client
- Number of Packets Received from Client
- Number of Packets Sent to Client
- Number of Policy Errors
- Radio Signal Strength Indicator
- Signal to Noise Ratio
- IP - Zone ID Mapping

Step 4 Click **OK**.

Verifying Overlapping Client IP Address in Flex Deployment

To verify if the overlapping client IP address in Flex deployment feature is enabled or not, use the following command:

```
Device# show wireless profile flex detailed flex1
Fallback Radio shut            : DISABLED
ARP caching                    : ENABLED
Efficient Image Upgrade        : ENABLED
OfficeExtend AP                : DISABLED
Join min latency               : DISABLED
IP overlap status              : DISABLED
```

To view additional details about the overlapping client IP address in Flex deployment feature, use the following command:

```
Device# show wireless device-tracking database ip

IP                                            ZONE-ID       STATE      DISCOVERY   MAC
------------------------------------------------------------------------------------------

  9.91.59.154                                 0x00000002  Reachable   IPv4 Packet
6038.e0dc.3182
  1000:1:2:3:90d8:dd1a:11ab:23c0              0x00000002  Reachable   IPv6 Packet
58ef.680d.c6c3
  1000:1:2:3:f9b5:3074:d0da:f93b              0x00000002  Reachable   IPv6 Packet
58ef.680d.c6c3
  2001:9:3:59:90d8:dd1a:11ab:23c0             0x00000002  Reachable   IPv6 NDP
58ef.680d.c6c3
  2001:9:3:59:f9b5:3074:d0da:f93b             0x00000002  Reachable   IPv6 NDP
58ef.680d.c6c3
  fe80::f9b5:3074:d0da:f93b                   0x80000001  Reachable   IPv6 NDP
58ef.680d.c6c3
```

To view APs in various site tags, use the following command:

```
Device# show ap tag summary
Number of APs: 5

AP Name AP Mac Site Tag Name Policy Tag Name RF Tag Name Misconfigured Tag Source
------------------------------------------------------------------------------------------
AP3802 70b3.17f6.37aa flex_ip_overlap-site-tag-auto-3 flex_ip_overlap_policy_tag_1
default-rf-tag No Static
AP-9117AX 0cd0.f894.0f8c default-site-tag default-policy-tag default-rf-tag No Default
AP1852JJ9 38ed.18ca.2b48 flex_ip_overlap-site-tag-auto-2 flex_ip_overlap_policy_tag_2
default-rf-tag No Static
AP1852I 38ed.18cc.61c0 flex_ip_overlap-site-tag-auto-1 flex_ip_overlap_policy_tag_1
default-rf-tag No Static
AP1542JJ9 700f.6a84.1b30 flex_ip_overlap-site-tag-auto-2 flex_ip_overlap_policy_tag_2
default-rf-tag No Static
```

To view APs in FlexConnect mode, use the following command:

```
Device# show ap status
AP Name     Status      Mode        Country
-------------------------------------------------------------------------
AP3802      Disabled   FlexConnect   IN
AP1852I     Enabled    FlexConnect   US
AP-9117AX   Enabled    FlexConnect   IN
AP1542JJ9   Disabled   FlexConnect   US
AP1852JJ9   Enabled    FlexConnect   US
```

Troubleshooting Overlapping Client IP Address in Flex Deployment

To verify the WNCD instance for each of the APs, use the following command:

```
Device# show wireless loadbalance ap affinity wncd 0
AP Mac          Discovery Timestamp    Join Timestamp          Tag
----------------------------------------------------------------------------
0cd0.f894.0f8c   10/27/20 22:11:05    10/27/20 22:11:14    default-site-tag
38ed.18ca.2b48   10/27/20 22:06:09    10/27/20 22:06:19    flex_ip_overlap-site-tag-auto-2
700f.6a84.1b30   10/27/20 22:25:03    10/27/20 22:25:13    flex_ip_overlap-site-tag-auto-2
```

Information About FlexConnect High Scale Mode

This feature helps to scale up the FlexConnect site capacity to accommodate 300 APs and 3000 802.1x clients per site. The FlexConnect site capability is scaled up by using the Pairwise Master Key (PMK) option to skip Extensible Authentication Protocol (EAP) exchange while performing client roaming.

When a client associates with an AP under an 802.1x authentication architecture, an EAP exchange takes place, followed by a four-way handshake to verify the encryption keys. Using PMK caching, an AP can cache the PMK identifier of the EAP exchange, and for the subsequent client join. In PMK caching, the EAP exchange process is eliminated, and the authentication time process is decreased.

The PMK propagation feature is disabled by default. Until Cisco IOS XE Cupertino 17.7.1, the wireless controller used to push the PMK cache to every FlexConnect AP in the site. From Cisco IOS XE Cupertino 17.8.1 onwards, when PMK propagation is enabled, the controller pushes the PMK cache only to selective FlexConnect APs. These FlexConnect APs then forward the PMK identifier to the other FlexConnect APs within the same site.

Enabling PMK Propagation (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *test-flex-profile* **Example:** `Device(config)#` **`wireless profile flex test-flex-profile`**	Creates a FlexConnect profile.
Step 3	**pmk propagate** **Example:** `Device(config-wireless-flex-profile)# pmk propogate`	Propagates PMK information to the other APs in the site. **Note** The PMK propagation feature is disabled by default.

Examples

```
Device# configure terminal
Device(config)# wireless profile flex test-flex-profile
Device(config-wireless-flex-profile)# pmk propagate
```

Flex Resilient with Flex and Bridge Mode Access Points

Information About Flex Resilient with Flex and Bridge Mode Access Points

The Flex Resilient with Flex and Bridge Mode Access Points describe how to set up a controller with Flex+Bridge mode Access Points (APs) and Flex Resilient feature. The Flex Resilient feature works only in Flex+Bridge mode APs. The feature resides in Mesh link formed between RAP - MAP, once the link is UP and RAP loses connection to the CAPWAP controller, both RAP and MAP continue to bridge the traffic. A child Mesh AP (MAP) maintains its link to a parent AP and continues to bridge till the parent link is lost. A child MAP cannot establish a new parent or child link till it reconnects to the CAPWAP controller.

Note Existing wireless clients in locally switching WLAN can stay connected with their AP in this mode. No new or disconnected wireless client can associate to the Mesh AP in this mode. Client traffic in Flex+Bridge MAP is dropped at RAP switchport for the locally switched WLANs.

Configuring a Flex Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.

Step 2 Click a **Flex Profile Name**. The **Edit Flex Profile** dialog box appears.

Step 3 Under the **General** tab, choose the **Flex Resilient** check box to enable the Flex Resilient feature.

Step 4 Under the **VLAN** tab, choose the required VLANs.

Step 5 (Optionally) Under the **Local Authentication** tab, choose the desired server group from the **Local Accounting RADIUS Server Group** drop-down list. Also, choose the **RADIUS** check box.

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

Configuring a Flex Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex new-flex-profile`	Configures a Flex profile and enters Flex profile configuration mode.
Step 3	**arp-caching** **Example:** `Device(config-wireless-flex-profile)# arp-caching`	Enables ARP caching.
Step 4	**description** *description* **Example:** `Device(config-wireless-flex-profile)# description "new flex profile"`	Enables default parameters for the Flex profile.
Step 5	**native-vlan-id** **Example:** `Device(config-wireless-flex-profile)# native-vlan-id 2660`	Configures native vlan-id information.
Step 6	**resilient** **Example:** `Device(config-wireless-flex-profile)# resilient`	Enables the resilient feature.
Step 7	**vlan-name** *vlan_name* **Example:** `Device(config-wireless-flex-profile)# vlan-name VLAN2659`	Configures VLAN name.
Step 8	**vlan-id** *vlan_id* **Example:** `Device(config-wireless-flex-profile)# vlan-id 2659`	Configures VLAN ID. The valid VLAN ID ranges from 1 to 4096.

Step 9	**end**
	Example:
	`Device(config-wireless-flex-profile)# end`
		Exits configuration mode and returns to privileged EXEC mode.

Configuring a Site Tag (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**wireless tag site** *site-name* **Example:** `Device(config)# wireless tag site new-flex-site`	Configures a site tag and enters site tag configuration mode.
Step 3	**flex-profile** *flex-profile-name* **Example:** `Device(config-site-tag)# flex-profile new-flex-profile`	Configures a flex profile.
Step 4	**no local-site** **Example:** `Device(config-site-tag)# no local-site`	**Local site** is not configured on the site tag.
Step 5	**site-tag** *site-tag-name* **Example:** `Device(config-site-tag)# site-tag new-flex-site`	Maps a site tag to an AP.

Step 6	**end**
	Example:
	`Device(config-site-tag)# end`
		Exits configuration mode and returns to privileged EXEC mode.

Configuring a Mesh Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**wireless profile mesh** *profile-name* **Example:** `Device(config)# wireless profile mesh Mesh_Profile`	Configures a Mesh profile and enters the Mesh profile configuration mode.

	Command or Action	Purpose
Step 3	**no ethernet-vlan-transparent** **Example:** `Device(config-wireless-profile-mesh)# no ethernet-vlan-transparent`	Disables VLAN transparency to ensure that the bridge is VLAN aware.

Step 4	**end**
	Example:
	`Device(config-wireless-profile-mesh)# end`
		Exits configuration mode and returns to privileged EXEC mode.

Associating Wireless Mesh to an AP Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**ap profile** *ap-profile-name* **Example:** `Device(config)# ap profile new-ap-join-profile`	Configures the AP profile and enters AP profile configuration mode.
Step 3	**mesh-profile** *mesh-profile-name* **Example:** `Device(config-ap-profile)# mesh-profile Mesh_Profile`	Configures the Mesh profile in AP profile configuration mode.
Step 4	**ssh** **Example:** `Device(config-ap-profile)# ssh`	Configures the Secure Shell (SSH).
Step 5	**mgmtuser username** *username* **password** {**0** | **8**} *password* **Example:** `Device(config-ap-profile)# mgmtuser username Cisco password 0 Cisco secret 0 Cisco`	Specifies the AP management username and password for managing all of the access points configured to the controller. • **0**: Specifies an UNENCRYPTED password. • **8**: Specifies an AES encrypted password. **Note** While configuring an username, ensure that special characters are not used as it results in error with bad configuration.

	Command or Action	Purpose

Step 6	**end**
	Example:
	`Device(config-ap-profile)# end`
		Exits configuration mode and returns to privileged EXEC mode.

Attaching Site Tag to an Access Point (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**ap** *mac-address* **Example:** `Device(config)# ap F866.F267.7DFB`	Configures Cisco APs and enters ap-tag configuration mode.
Step 3	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag new-flex-site`	Maps a site tag to the AP. **Note** Associating Site Tag causes the associated AP to reconnect.

Step 4	**end**
	Example:
	`Device(config-ap-tag)# end`
		Exits configuration mode and returns to privileged EXEC mode.

Configuring Switch Interface for APs (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode
Step 2	**interface** *interface-id* **Example:** `Device(config)# interface <int-id>`	Enters the interface to be added to the VLAN.
Step 3	**switchport trunk native vlan** *vlan-id* **Example:**	Assigns the allowed VLAN ID to the port when it is in trunking mode.

	Command or Action	Purpose
	`Device(config-if)# switchport trunk native vlan 2660`	
Step 4	**switchport trunk allowed vlan** *vlan-id* **Example:** `Device(config-if)# switchport trunk allowed vlan 2659,2660`	Assigns the allowed VLAN ID to the port when it is in trunking mode.
Step 5	**switchport mode trunk** **Example:** `Device(config-if)# switchport mode trunk`	Sets the trunking mode to trunk unconditionally. **Note** When the controller works as a host for spanning tree, ensure that you configure portfast trunk, using **spanning-tree portfast trunk** command, in the uplink switch to ensure faster convergence.

Step 6	**end**
	Example:
	`Device(config-if)# end`
		Exits configuration mode and returns to privileged EXEC mode.

Verifying Flex Resilient with Flex and Bridge Mode Access Points Configuration

To view the AP mode and model details, use the following command:

```
Device# show ap name <ap-name> config general | inc AP Mode
AP Mode                                         : Flex+Bridge
AP Model                                        : AIR-CAP3702I-A-K9
```

To view the MAP mode details, use the following command:

```
Device# show ap name MAP config general | inc AP Mode
AP Mode                                         : Flex+Bridge
AP Model                                        : AIR-CAP3702I-A-K9
```

To view the RAP mode details, use the following command:

```
Device# show ap name RAP config general | inc AP Mode
AP Mode                                         : Flex+Bridge
AP Model                                        : AIR-AP2702I-A-K9
```

To view if the Flex Profile - Resilient feature is enabled or not, use the following command:

```
Device# show  wireless profile flex detailed FLEX_TAG | inc resilient
Flex resilient                 : ENABLED
```

Feature History for OEAP Link Test

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

This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 5: Feature History for OEAP Link Test

Release	Feature	Feature Information
Cisco IOS XE Bengaluru 17.5.1	OEAP Link Test	The Cisco OEAP Link Test feature allows you to determine the DTLS upload, link latency, and jitter of the link between an AP and the controller.

Information About OEAP Link Test

The Cisco OEAP Link Test feature allows you to determine the DTLS upload speed of the link between an AP and the controller. This feature helps in identifying network bottlenecks and reasons for functionality failures. You can determine the link latency by running a test on demand.

A link test is used to determine the quality of the link between the controller and an AP in OEAP mode. The AP sends synthetic packets to the controller and the controller echoes them back to the AP, which can then estimate the link quality.

Feature Scenarios

Cisco OfficeExtend Access Point (OEAP) users are complaining of poor performance when connected to a teleworker AP.

Use Cases

This feature allows OEAP network admins to troubleshoot low throughput from the Cisco Catalyst 9800 Controller GUI by running OEAP link test.

The OEAP link test provides DTLS upload speed, link latency, and link jitter, all of which help the network administrators to narrow down the problem.

Configuring OEAP Link Test (CLI)

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode.
Step 2	**ap name** *ap-name* **network-diagnostic** **Example:** `Device# ap name ap18 network-diagnostic`	Triggers network diagnostics on an OfficeExtend AP.

Performing OEAP Link Test (GUI)

Procedure

Step 1 Choose **Monitoring** > **Wireless** > **AP Statistics**.

In the list of APs, a **Link Test** icon is displayed in the **AP Name** column for OEAP-capable APs.

Note The **Link Test** icon is displayed only if an AP is OEAP capable and is configured to operate as OEAP.

Step 2 Click **Link Test**.

A link test is run and the results are shown.

Verifying OEAP Link Test

The following example shows how to verify network diagnostics information:

```
Device# show FlexConnect office-extend diagnostics

Summary of OfficeExtend AP Link Latency

CAPWAP Latency Heartbeat

Current: current latency (ms)
Min: minimum latency (ms)
Max: maximum latency (ms)

Link Test

Upload: DTLS Upload (Mbps)
Latency: DTLS Link Latency (ms)
Jitter: DTLS Link Jitter (ms)

AP Name Last Latency Heartbeat from AP Current Max Min Last Link Test Run Upload Latency
Jitter
------------------------------------------------------------------------------------------
ap-18   1 minute 1 second             0       0   0   12/04/20 09:19:48  8      2
 0
```

Feature History for Cisco OEAP Split Tunneling

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

This feature is available in all the releases subsequent to the one in which it is introduced in, unless noted otherwise.

Table 6: Feature History for Cisco OEAP Split Tunneling

Release	Feature	Feature Information
Cisco IOS XE Cupertino 17.8.1	IPv6 Support	IPv6 addressing is supported on the Cisco OEAP Split Tunneling feature.
Cisco IOS XE Cupertino 17.7.1	Cisco OEAP Split Tunneling	The Split Tunneling feature in Cisco OfficeExtend Access Point (OEAP) provides a mechanism to classify client traffic, based on packet content, using access control lists (ACLs).

Information About Cisco OEAP Split Tunneling

The global pandemic has redefined the way people interact and work. The workplace has shifted from office cubicles to home desks, which requires applications that enable seamless collaboration among the workforce. For home-based workers, access to business services must be reliable, consistent, and secure. It should provide an experience that is similar to the office facility. Routing all of the traffic through the corporate network using traditional VPNs increases the traffic volume, slows down access to resources, and negatively impacts the remote user experience.

Cisco OEAP provides secure communications from a controller to an access point (AP) at a remote location, seamlessly extending the corporate WLAN over the internet to an employee's residence. Cisco OEAP provides segmentation of home and corporate traffic using the Split Tunnelling feature, which allows for home device connectivity without security risks to corporate policy.

Split tunnelling classifies the traffic sent by a client, based on packet content, using ACLs. Matching packets are switched locally from Cisco OEAP, and other packets are centrally switched over CAPWAP. Clients on a corporate SSID can talk to devices on a local network (printers, wireless devices on a personal SSID, and so on) directly without consuming WAN bandwidth, by sending packets over CAPWAP.

Traffic to Software as a Service (Saas) applications such as Cisco WebEx, Microsoft SharePoint, Microsoft Office365, Box, Dropbox, and so on that is required as part of the work routine, need not go through the corporate network, by using the Split Tunnelling feature.

The Cisco OEAP advertises two SSIDs, one corporate and one personal. Corporate SSID clients obtain their IP address from the central DHCP server in the corporate network. If split tunneling is enabled and a client wants to access a device in the home network, the AP performs NAT (PAT) translation between the wireless client corporate network subnet and the home network where the AP is located.

The personal SSID is configurable by a Cisco OEAP user. Clients will either get their IP address from the home router (when the AP personal SSID firewall is disabled) or from the internal AP DHCP server (when the AP personal SSID firewall is enabled). In the latter scenario, if the clients want to reach the home network devices, the AP perform sNAT (PAT) translation between the wireless client's internal network and the home network where the AP is located.

IPv6 Address Support

From Cisco IOS XE Cupertino 17.8.1, IPv6 addressing is supported. You can disable IPv6 addressing only by disabling the feature.

Note The end-to-end network should support IPv6, that is, both the corporate network (controller, corporate gateway, and so on) and the home network (wireless clients, home router, and so on) should support IPv6.

Prerequisites for Cisco OEAP Split Tunneling

- Cisco Wave 2 APs or Cisco Catalyst 9100AX Series Access Points
- URL filter list that matches the ACL name configured in split tunneling

Restrictions for Cisco OEAP Split Tunneling

- Cisco OEAPs are not supported when Cisco Embedded Wireless Controller on Catalyst Access Points (EWC) is used as a controller.
- Mesh topology is not supported.
- Clients connected on personal SSID or on home network (AP native VLAN) cannot discover devices on the corporate network.
- Split tunnelling is not supported in standalone mode.
- URL split tunnelling supports only up to 512 URLs.
- Action (deny or permit) can be specified only on the URL filter list, not for each individual entry.
- If URL-based ACL contains wild-card URLs, a maximum of 10 URLs are supported.
- The amount of snooped DNS IP addresses is limited as follows:
  - An AP can snoop 4095 IP addresses per DNS response, if IP addresses are less than 150,000.
  - An AP can snoop 10 IP addresses per DNS response, if IP addresses are between 150,000 and 200,000.
  - An AP can snoop five IP addresses per DNS response, if IP addresses are between 200,000 and 250,000.
  - An AP can snoop one IP address per DNS response, if IP addresses are greater than 250,000.
- A maximum of 128 IP address ACE (rules) can be used in the IP ACL for split tunnelling.
- URL-based split tunnelling only works with IPv4 addresses.
- The following restrictions are specific to IPv6 addressing
  - Multihoming (multiple router advertisement prefixes) is not supported (If a home network receives multiple prefixes, the one used by the AP that is connected to the controller is used.)
  - Roaming is not supported.
  - Filtering is not supported on the upstream traffic towards the wireless client.

- Split tunneling is disabled for clients with duplicate IPv6 addresses. Traffic for these clients is forwarded centrally to the controller.
- DHCPv6 prefix delegation is not supported for wireless clients.
- If the corporate prefix length is smaller than the home prefix length, split tunneling for a particular client is disabled.

Use Cases for Cisco OEAP Split Tunneling

Before Release 17.7.1, split tunneling used IP ACLs. This meant that cloud services such as Cisco Webex were accessed directly without going through the corporate network. The network administrator maintained the list of IP addresses that Cisco Webex used, which was a daunting task. From Release 17.7.1, using the Cisco OEAP Split Tunneling feature, the network administrator needs to provide only the DNS names that Cisco Webex uses. The AP ensures that traffic from these DNS names is routed directly to the internet without using the corporate network.

Workflow to Configure Cisco OEAP Split Tunneling

1. Create an IP address ACL or URL ACL
2. Add ACL to FlexConnect Profile
3. Enable Split Tunnelling on Policy Profile
4. Verify the Configuration

Create an IP Address ACL (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ip access-list extended** *name* **Example:** `Device(config)# ip access-list extended vlan_oeap`	Defines an extended IPv4 access list using a name. **Note** IP ACL can be used to define a default action if there is no match in the URL ACL.
Step 3	*seq-num* **deny ip any host** *hostname* **Example:**	Denies IP traffic from any host.

	Command or Action	Purpose
	`Device(config-ext-nacl)# 10 deny ip any 10.10.0.0 0.0.255.255`	
Step 4	*seq-num* **permit ip any any** *hostname* **Example:** `Device(config-ext-nacl)# 20 permit ip any any`	Permits IP traffic from any source or destination host.

Step 5	**end**
	Example:
	`Device(config-ext-nacl)# end`
		Exits configuration mode and returns to privileged EXEC mode.

Create a URL ACL (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**urlfilter list** *list-name* **Example:** `Device(config)# urlfilter list vlan_oeap`	Configures the URL filter list. The list name must not exceed 32 alphanumeric characters.
Step 3	**action permit** **Example:** `Device(config-urlfilter-params)# action permit`	Configures the action: Permit (traffic is allowed directly on the home network) or Deny (traffic is directed to the corporate network).
Step 4	**filter-type post-authentication** **Example:** `Device(config-urlfilter-params)# filter-type post-authentication`	Configures the URL list as post authentication filter.
Step 5	**url** *url-name* **Example:** `Device(config-urlfilter-params)# url wiki.cisco.com`	Configures a URL.
Step 6	**url** *url-name* **Example:** `Device(config-urlfilter-params)# url example.com`	(Optional) Configures a URL. Use this option when you want to add multiple URLs.

	Command or Action	Purpose

Step 7	**end**
	Example:
	`Device(config-urlfilter-params)# end`
		Exits configuration mode and returns to privileged EXEC mode.

Add an ACL to a FlexConnect Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex default-flex-profile`	Configures a FlexConnext profile.
Step 3	**acl-policy** *acl-policy-name* **Example:** `Device(config-wireless-flex-profile)# acl-policy vlan_oeap`	Configures an ACL policy.
Step 4	**urlfilter list** *url-filter* **Example:** `Device(config-wireless-flex-profile-acl)# urlfilter list vlan_oeap`	Configures a URL filter list.
Step 5	**exit** **Example:** `Device(config-wireless-flex-profile-acl)# exit`	Returns to FlexConnect profile configuration mode..
Step 6	**office-extend** **Example:** `Device(config-wireless-flex-profile)# office-extend`	Enables the OEAP mode for a FlexConnect AP.

Step 7	**end**
	Example:
	`Device(config-wireless-flex-profile)# end`
		Exits configuration mode and returns to privileged EXEC mode.

Enable Split Tunnelling in a Policy Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex default-flex-profile`	Configures a FlexConnect profile.
Step 3	**no central association** **Example:** `Device(config-wireless-flex-profile)# no central association`	Disables central association and enables local association for locally switched clients.
Step 4	**flex split-mac-acl** *split-mac-acl-name* **Example:** `Device(config-wireless-flex-profile)# flex split-mac-acl vlan_oeap`	Configures a split MAC ACL name. **Note** Ensure that you use the same *acl-policy-name* in the FlexConnect profile.

Step 5	**end**
	Example:
	`Device(config-wireless-flex-profile)# end`
		Exits configuration mode and returns to privileged EXEC mode.

Verifying the Cisco OEAP Split Tunnel Configuration

To verify the split tunneling DNS ACLs per wireless client on the AP side, use the following command:

```
Device# show split-tunnel client 00:11:22:33:44:55 access-list

Split tunnel ACLs for Client: 00:11:22:33:44:55

IP ACL: SplitTunnelACL

Tunnel packets Tunnel bytes NAT packets NAT bytes
             1          242           3       768

URL ACL: SplitTunnelACL

Tunnel packets Tunnel bytes NAT packets NAT bytes
             3          778           0         0

Resolved IPs for Client: 00:11:22:33:44:55 for Split tunnel
```

```
HIT-COUNT       URL             ACTION  IP-LIST

1               base1.com       deny.   20.0.1.1
                                        20.0.1.10

2               base2.com       deny.   20.0.1.2

3               base3.com       deny.   20.0.1.3
```

To verify the current binding between a WLAN and an ACL, use the following command:

```
Device# show split-tunnel mapping

VAP-Id       ACL Name
    0        SplitTunnelACL
```

To verify the content of the current URL ACL, use the following command:

```
Device# show flexconnect url-acl

ACL-NAME          ACTION      URL-LIST

SplitTunnelACL    deny        base.com
```

AP Survey Mode

To enable the Cisco Catalyst 9136 Series APs and other upcoming AP models for site survey at customer sites, a new AP command is introduced to help APs to switch to survey mode. When an AP is in survey mode, the AP GUI is enabled and is used for configuring the RF parameters for site survey investigation.

To enable survey mode on an AP, run the **ap-type site-survey** command from the AP CLI.

The following features in the AP GUI are hidden, when the AP is in the survey mode:

- WAN
- Firewall
- Network Diagnostics

Note To make the hidden features visible on the AP GUI, you must switch the AP back to the CAPWAP mode, by running the **ap-type capwap** command from the AP CLI. In CAPWAP mode, the AP GUI becomes available only when the **OfficeExtend AP** field is enabled in the flex profile page associated to that AP.

Note To access the AP survey mode from the GUI, you must enter the default login as 'admin' and the default password as 'admin' (both case sensitive).

When the AP is in survey mode, it broadcasts an SSID by default. The default password to connect to this SSID is 'password' (case sensitive).