Configuring the Switch for Access Point Discovery

Finding Feature Information

Your software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring the Switch for Access Point Discovery

- Ensure that the Control and Provisioning of Wireless Access Points (CAPWAP) UDP ports 5246 and 5247 (similar to the Lightweight Access Point Protocol (LWAPP) UDP ports 12222 and 12223) are enabled and are not blocked by an intermediate device that could prevent an access point from joining the switch.
- If access control lists (ACLs) are in the control path between the switch and its access points, you must open new protocol ports to prevent access points from being stranded.
- If an access point is in the UP state and its IP address changes, the access point tears down the existing CAPWAP tunnel and rejoins the switch.

- Access points must be discovered by a switch before they can become an active part of the network. The lightweight access points support the following switch discovery processes:
  - Layer 3 CAPWAP discovery—You can enable this feature on different subnets from the access point. This feature uses IP addresses and UDP packets rather the MAC addresses used by Layer 2 discovery.
  - Locally stored switch IP address discovery—If the access point was previously associated to a switch, the IP addresses of the primary, secondary, and tertiary switchs are stored in the access point's nonvolatile memory. This process of storing switch IP addresses on an access point for later deployment is called *priming the access point*.
  - DHCP server discovery—This feature uses DHCP option 43 to provide switch IP addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability.
  - DNS discovery—The access point can discover switchs through your domain name server (DNS). You must configure your DNS to return switch IP addresses in response to CISCO-CAPWAP-CONTROLLER.*localdomain*, where *localdomain* is the access point domain name. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-CAPWAP-CONTROLLER.*localdomain*. When the DNS sends a list of switch IP addresses, the access point sends discovery requests to the switchs.

Restrictions for Configuring the Switch for Access Point Discovery

- Ensure that the switchs are configured with the correct date and time. If the date and time configured on the switch precedes the creation and installation date of certificates on the access points, the access point fails to join the switch.
- During the discovery process, access points that are supported by the Cisco switch, such as the 1140, 1260, 3500, 1040,1600, 2600, or 3600 query only for Cisco switchs.

Information About Configuring the Switch for Access Point Discovery

In a CAPWAP environment, a lightweight access point discovers a switch by using CAPWAP discovery mechanisms and then sends a CAPWAP join request to the switch. The switch sends a CAPWAP join response to the access point that allows the access point to join the switch. When the access point joins the switch, the switch manages its configuration, firmware, control transactions, and data transactions.

Access Point Communication Protocols

Cisco lightweight access points use the IETF standard CAPWAP to communicate with the switch and other lightweight access points on the network.

CAPWAP, which is based on LWAPP, is a standard, interoperable protocol that enables a switch to manage a collection of wireless access points. CAPWAP is implemented in switch for these reasons:

- To provide an upgrade path from Cisco products that use LWAPP to next-generation Cisco products that use CAPWAP
- To manage RFID readers and similar devices
- To enable switchs to interoperate with third-party access points in the future

Viewing Access Point Join Information

Join statistics for an access point that sends a CAPWAP discovery request to the switch at least once are maintained on the switch even if the access point is rebooted or disconnected. These statistics are removed only when the switch is rebooted or when you choose to clear the statistics.

Troubleshooting the Access Point Join Process

Access points can fail to join a switch for many reasons such as a RADIUS authorization is pending, self-signed certificates are not enabled on the switch, the access point and switch's regulatory domains do not match, and so on.

You can configure the access points to send all CAPWAP-related errors to a syslog server. You do not need to enable any debug commands on the switch because all of the CAPWAP error messages can be viewed from the syslog server itself.

The state of the access point is not maintained on the switch until it receives a CAPWAP join request from the access point, so it can be difficult to determine why the CAPWAP discovery request from a certain access point was rejected. In order to troubleshoot such joining issues without enabling CAPWAP debug commands on the switch, the switch collects information for all access points that send a discovery message to this switch and maintains information for any access points that have successfully joined this switch.

The switch collects all join-related information for each access point that sends a CAPWAP discovery request to the switch. Collection begins when the first discovery message is received from the access point and ends when the last configuration payload is sent from the switch to the access point.

When the switch is maintaining join-related information for the maximum number of access points, it does not collect information for any more access points.

You can also configure a DHCP server to return a syslog server IP address to the access point using option 7 on the server. The access point then starts sending all syslog messages to this IP address.

You can configure the syslog server IP address through the access point CLI, if the access point is not connected to the switch by entering the **capwap ap log-server** *syslog_server_IP_address* command.

When the access point joins a switch for the first time, the switch pushes the global syslog server IP address (the default is 255.255.255.255) to the access point. After that, the access point sends all syslog messages to this IP address, until it is overridden by one of the following scenarios:

- The access point is still connected to the same switch, and you changed the global syslog server IP address configuration on the switch by using the **ap syslog host** *Syslog_Server_IP_Address* command. In this case, the switch pushes the new global syslog server IP address to the access point.
- The access point is still connected to the same switch, and you configured a specific syslog server IP address for the access point on the switch by using the **ap name** *Cisco_AP* **syslog host** *Syslog_Host_IP_Address* command. In this case, the switch pushes the new specific syslog server IP address to the access point.

- The access point gets disconnected from the switch, and you configured the syslog server IP address from the access point CLI by using the **capwap ap log-server** *syslog_server_IP_address* command. This command works only if the access point is not connected to any switch.
- The access point gets disconnected from the switch and joins another switch. In this case, the new switch pushes its global syslog server IP address to the access point.

Whenever a new syslog server IP address overrides the existing syslog server IP address, the old address is erased from persistent storage, and the new address is stored in its place. The access point also starts sending all syslog messages to the new IP address, if the access point can reach the syslog server IP address.

How to Configure Access Point Discovery

Configuring the Syslog Server for Access Points (GUI)

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

The **All APs** page is displayed showing a list of access points that are associated with the switch and their current settings.

Step 2 From the **Show** drop-down list, choose **Quick Filter**.

The filter options (text boxes) appear in each of the column header in the table.

Step 3 Enter a keyword in the corresponding text boxes to specify the filter criteria based on which you want to search, and click the **Filter** icon.

Configuring the Syslog Server for Access Points (CLI)

SUMMARY STEPS

1. **show ap config global**
2. **show ap name** *Cisco_AP* **config general**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show ap config global** **Example:** `Switch# show ap config global`	Displays the global syslog server settings for all access points that join the switch.
Step 2	**show ap name** *Cisco_AP* **config general** **Example:** `Switch# show ap name AP03 config general`	Displays the syslog server settings for a specific access point.

Monitoring Access Point Join Information (CLI)

Note The procedure to perform this task using the switch GUI is not currently available.

SUMMARY STEPS

1. **enable**
2. **show ap join stats summary**
3. **show ap mac-address** *mac_address* **join stats summary**
4. **show ap mac-address** *mac_address* **join stats detailed**
5. **clear ap join statistics**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch# enable`	Enters privileged EXEC mode.
Step 2	**show ap join stats summary** **Example:** `Switch# show ap join stats summary`	Displays the MAC addresses of all the access points that are joined to the switch or that have tried to join.
Step 3	**show ap mac-address** *mac_address* **join stats summary** **Example:** `Switch# show ap mac-address 000.2000.0400 join stats summary`	Displays all the statistics for the AP including the last join error detail.
Step 4	**show ap mac-address** *mac_address* **join stats detailed** **Example:** `Switch# show ap mac-address 000.2000.0400 join stats detailed`	Displays all join-related statistics collected for a specific access point.
Step 5	**clear ap join statistics** **Example:** `Switch# clear ap join statistics`	Clears the join statistics for all access points. **Note** To clear the join statistics that correspond to specific access points, enter the **clear ap mac-address** *mac_address* **join statistics** command.

Related Topics

Displaying the MAC Addresses of all Access Points: Example, on page 6
DHCP Option 43 for Lightweight Cisco Aironet Access Points Configuration Example, on page 8

Searching for Access Point Radios (GUI)

Step 1 Choose **Monitor** > **Wireless** > **Access Points** and click **802.11a/n/ac Statistics** or **802.11b/g/n Statistics**.

The 802.11 Radio pages are displayed. These pages show all of the 802.11a/n/ac or 802.11b/g/n access point radios that are associated with the switch and their current settings.

Note In a Cisco converged access environment, the 802.11a/n/ac and 802.11b/g/n radios should not be differentiated based on their Base Radio MAC addresses, because they might have the same addresses. Instead, the radios should be differentiated based on their physical addresses.

Step 2 From the **Show** drop-down list, choose **Quick Filter**.

The filter options (text boxes) appear in each of the column header in the table.

Step 3 Enter a keyword in the corresponding text boxes to specify the filter criteria based on which you want to search, and click the **Filter** icon.

Monitoring the Interface Details (GUI)

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

The **All APs** page is displayed showing a list of access points that are associated with the switch.

Step 2 Click the access point name.

The **AP > Edit** page is displayed.

Step 3 Click the **Interface** tab.

The interface details are displayed.

Configuration Examples for Configuring the Switch for Access Point Discovery

Displaying the MAC Addresses of all Access Points: Example

This example shows how to display MAC addresses of all the access points that are joined to the switch:

```
Switch# show ap join stats summary
Number of APs.................................... 4

Base Mac          EthernetMac       AP Name IP Address    Status
----------------- ----------------- ------- ------------- ----------
00:0b:85:57:bc:c0 00:0b:85:57:bc:c0 AP1130  10.10.163.217 Joined
00:1c:0f:81:db:80 00:1c:63:23:ac:a0 AP1140  10.10.163.216 Not joined
```

```
00:1c:0f:81:fc:20 00:1b:d5:9f:7d:b2 AP1     10.10.163.215 Joined
00:21:1b:ea:36:60 00:0c:d4:8a:6b:c1 AP2     10.10.163.214 Not joined
```

This example shows how to display the last join error details for a specific access point:

```
Switch# show ap mac-address 000.2000.0400 join stats summary
Is the AP currently connected to controller..... Yes
Time at which the AP joined this
controller last time..... Aug 21 12:50:36.061
Type of error
that occurred last..... AP got or has been disconnected
Reason for error
that occurred last..... The AP has been reset by the controller
Time at which the last join error occurred..... Aug 21 12:50:34.374
```

This example shows how to display all join-related statistics collected for a specific access point:

```
Switch# show ap mac-address 000.2000.0400 join stats detailed
Discovery phase statistics
- Discovery requests received..... 2
- Successful discovery responses sent..... 2
- Unsuccessful discovery request processing..... 0
- Reason for last unsuccessful discovery attempt..... Not applicable
- Time at last successful discovery attempt..... Aug 21 12:50:23.335
- Time at last unsuccessful discovery attempt..... Not applicable

Join phase statistics
- Join requests received..... 1
- Successful join responses sent..... 1
- Unsuccessful join request processing..... 1
- Reason for last unsuccessful join attempt.....      RADIUS authorization
                                                      is pending
                                                      for the AP
- Time at last successful join attempt..... Aug 21 12:50:34.481
- Time at last unsuccessful join attempt..... Aug 21 12:50:34.374

Configuration phase statistics
- Configuration requests received..... 1
- Successful configuration responses sent..... 1
- Unsuccessful configuration request processing..... 0
- Reason for last unsuccessful configuration attempt.. Not applicable
- Time at last successful configuration attempt..... Aug 21 12:50:34.374
- Time at last unsuccessful configuration attempt..... Not applicable

Last AP message decryption failure details
- Reason for last message decryption failure..... Not applicable

Last AP disconnect details
- Reason for last AP connection failure..... The AP has been reset by
                                                      the controller
Last join error summary
- Type of error that occurred last..... AP got or has been
                                                      disconnected
- Reason for error that occurred last..... The AP has been reset
                                                      by the controller
- Time at which the last join error occurred..... Aug 21 12:50:34.374
```

DHCP Option 43 for Lightweight Cisco Aironet Access Points Configuration Example

For more information about the AP join process, see *DHCP OPTION 43 for Lightweight Cisco Aironet Access Points Configuration Example* at http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/97066-dhcp-option-43-00.html.

Configuring AP Pass Through

Information About AP Pass Through

AP pass through allows all the access points connected to Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches to join another controller on the network.

Prior to this release, all access points connected Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches would be terminated on the switch when the wireless management vlan is turned on. Unsupported access points connected to the switch were unable join a controller on a different vlan. AP pass through allows the connected AP to join another wireless controller on the network by assigning different vlan.

The advantages of AP pass through are:

- Allows partial deployment of Cisco New Generation Wireless Controllers where some APs are connected to Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches but other APs continue to join other controllers on the network.
- The APs that are not supported on the Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches are allowed to join other controllers on the network.
- The wireless LAN controller is used to provide access to both wired and wireless guests. AP Pass through allows the AP to pass through Cisco Catalyst 3850 Series Switches and Cisco Catalyst 3650 Series Switches to join any other controller when wired guest accessing is turned on.

Configuring AP Pass Through

All access points on VLANs other than the one with supported access points will be put into the AP pass-through mode and will not terminate on theSwitch.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 2	**wireless management interface vlan** *vlan_id* **Example:**	Configures the ports that are connected to the supported access points with the wireless management VLAN

	Command or Action	Purpose
	`Switch(config)# wireless management interface vlan10`	
Step 3	**interface GigabitEthernet1/0/1** **Example:** `Switch(config)# interface TenGigabitEthernet1/0/1`	Sets the 10-Gigbit Ethernet interface. The command prompt changes from (config)# to (config-if)#.
Step 4	**description Supported AP switchport access** *vlan_id* **Example:** `Switch(config-if)# switchport access vlan10`	Specifies the VLAN for which this access port will carry traffic
Step 5	**description Unsupported AP switchport access** *vlan_id* **Example:** `Switch(config-if)# switchport access vlan20`	Configures the ports that are connected to the unsupported access points with a vlan other than the wireless management VLAN.