AP Connectivity to Controller

- CAPWAP, on page 1
- Preferred Mode, on page 6
- IPv6 CAPWAP UDP Lite, on page 8
- Data Encryption, on page 10
- VLAN Tagging for CAPWAP Frames from Access Points, on page 13
- Discovering and Joining Controllers, on page 15
- Authorizing Access Points, on page 26
- AP Wired 802.1X Supplicant, on page 33
- Configuring a Static IP Address on a Lightweight Access Point, on page 41
- Troubleshooting the Access Point Join Process, on page 43

CAPWAP

Cisco lightweight access points use the IETF standard Control and Provisioning of Wireless Access Points Protocol (CAPWAP) to communicate with the controller and other lightweight access points on the network.

CAPWAP, which is based on LWAPP, is a standard, interoperable protocol that enables a controller to manage a collection of wireless access points. CAPWAP is implemented in controller 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 controllers to interoperate with third-party access points in the future

LWAPP-enabled access points can discover and join a CAPWAP controller, and conversion to a CAPWAP controller is seamless. For example, the controller discovery process and the firmware downloading process when using CAPWAP are the same as when using LWAPP. The one exception is for Layer 2 deployments, which are not supported by CAPWAP.

You can deploy CAPWAP controllers and LWAPP controllers on the same network. The CAPWAP-enabled software allows access points to join either a controller running CAPWAP or LWAPP.

The following are some guidelines that you must follow for access point communication protocols:

- If your firewall is currently configured to allow traffic only from access points using LWAPP, you must change the rules of the firewall to allow traffic from access points using CAPWAP.

- Ensure that the CAPWAP UDP ports 5246 and 5247 (similar to the 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 controller.
- If access control lists (ACLs) are in the control path between the controller and its access points, you need to open new protocol ports to prevent access points from being stranded.

This section contains the following subsections:

Restrictions for Access Point Communication Protocols

- Rate-limiting is applicable to all traffic destined to the CPU from either direction (wireless or wired). We recommend that you always run the controller with the default **config advanced rate enable** command in effect to rate limit traffic to the controller and protect against denial-of-service (DoS) attacks. You can use the **config advanced rate disable** command to stop rate-limiting of Internet Control Message Protocol (ICMP) echo responses for testing purposes. However, we recommend that you reapply the **config advanced rate enable** command after testing is complete.
- Ensure that the controllers are configured with the correct date and time. If the date and time configured on the controller precedes the creation and installation date of certificates on the APs, the AP fails to join the controller.
- The sender fragments the IPv6 UDP packets, which are then reassembled at the end device. APs do not support IPv6 reassembly and therefore IPv6 UDP packets are not recognized in the AP datapath.

  This issue does not impact IPv6 TCP because of TCP design. The MSS parameter is a part of the options in the TCP initial handshake that specifies the largest amount of data that a TCP speaker can receive in a single TCP segment. Each direction of TCP traffic uses its own MSS value because this is a receiver-specified value.
- Do not use the following IP addresses with Cisco Wave 2 APs in the network to avoid the AP from dropping packets:
  - 10.128.128.126
  - 10.128.128.127
  - 10.128.128.128
  - 6.0.0.7

Viewing CAPWAP Maximum Transmission Unit Information

See the maximum transmission unit (MTU) for the CAPWAP path on the controller by entering this command:

show ap config general *Cisco_AP*

The MTU specifies the maximum size of any packet (in bytes) in a transmission.

Information similar to the following appears:

```
Cisco AP Identifier.............................. 9
Cisco AP Name.................................... Maria-1250
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-A     802.11a:-A
```

```
AP Country code.............................. US  - United States
AP Regulatory Domain......................... 802.11bg:-A    802.11a:-A
Switch Port Number .......................... 1
MAC Address.................................. 00:1f:ca:bd:bc:7c
IP Address Configuration..................... DHCP
IP Address................................... 1.100.163.193
IP NetMask................................... 255.255.255.0
CAPWAP Path MTU.............................. 1485
```

Debugging CAPWAP

Use these commands to obtain CAPWAP debug information:

- **debug capwap events** {**enable** | **disable**}—Enables or disables debugging of CAPWAP events.
- **debug capwap errors** {**enable** | **disable**}—Enables or disables debugging of CAPWAP errors.
- **debug capwap detail** {**enable** | **disable**}—Enables or disables debugging of CAPWAP details.
- **debug capwap info** {**enable** | **disable**}—Enables or disables debugging of CAPWAP information.
- **debug capwap packet** {**enable** | **disable**}—Enables or disables debugging of CAPWAP packets.
- **debug capwap payload** {**enable** | **disable**}—Enables or disables debugging of CAPWAP payloads.
- **debug capwap hexdump** {**enable** | **disable**}—Enables or disables debugging of the CAPWAP hexadecimal dump.
- **debug capwap dtls-keepalive** {**enable** | **disable**}—Enables or disables debugging of CAPWAP DTLS data keepalive packets.

Link Latency

You can configure link latency on the controller to measure the link between an access point and the controller. This feature can be used with all access points joined to the controller but is especially useful for FlexConnect and OfficeExtend access points, for which the link could be a slow or unreliable WAN connection. Specifically for Cisco OEAPs, the least latency controller join feature can be used to guide the AP's controller selection.

The following are some guidelines for link latency:

- Link latency monitors the round-trip time of the CAPWAP heartbeat packets (echo request and response) from the access point to the controller and back. This time can vary due to the network link speed and controller processing loads. The access point timestamps the outgoing echo requests to the controller and the echo responses received from the controller. The access point sends this delta time to the controller as the system round-trip time. The access point sends heartbeat packets to the controller at a default interval of 30 seconds.

Note Link latency calculates the CAPWAP response time between the access point and the controller. It does not measure network latency or ping responses.

- The controller displays the current round-trip time as well as a running minimum and maximum round-trip time. The minimum and maximum times continue to run as long as the controller is up or can be cleared and allowed to restart.

- You can configure link latency for a specific access point using the controller GUI or CLI or for all access points joined to the controller using the CLI.

This section contains the following subsections:

Restrictions for Link Latency

- Link latency is supported for use only with FlexConnect access points in connected mode. FlexConnect access points in standalone mode are not supported.

Configuring Link Latency (GUI)

Procedure

Step 1 Choose **Wireless > Access Points > All APs** to open the All APs page.

Step 2 Click the name of the access point for which you want to configure link latency.

Step 3 Choose the **Advanced** tab to open the All APs > Details for (Advanced) page.

Step 4 Select the **Enable Link Latency** check box to enable link latency for this access point or unselect it to prevent the access point from sending the round-trip time to the controller after every echo response is received. The default value is unselected.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Step 7 When the All APs page reappears, click the name of the access point again.

Step 8 When the All APs > Details for page reappears, choose the **Advanced** tab again. The link latency and data latency results appear below the Enable Link Latency check box:

- **Current**—The current round-trip time (in milliseconds) of CAPWAP heartbeat packets or data packets from the access point to the controller and back.
- **Minimum**—Since link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets or data packets from the access point to the controller and back.
- **Maximum**—Since link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets or data packets from the access point to the controller and back.

Step 9 To clear the current, minimum, and maximum link latency and data latency statistics on the controller for this access point, click **Reset Link Latency**.

Step 10 After the page refreshes and the All APs > Details for page reappears, choose the **Advanced** tab. The updated statistics appear in the Minimum and Maximum text boxes.

Configuring Link Latency (CLI)

Procedure

Step 1 Enable or disable link latency for a specific access point or for all access points currently associated to the controller by entering this command:

config ap link-latency {**enable** | **disable**} {*Cisco_AP* | **all**}

The default value is disabled.

Note The **config ap link-latency** {**enable** | **disable**} **all** command enables or disables link latency only for access points that are currently joined to the controller. It does not apply to access points that join in the future.

Step 2 See the link latency results for a specific access point by entering this command:

show ap config general *Cisco_AP*

Information similar to the following appears:

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP1
...
AP Link Latency.................................. Enabled
 Current Delay................................... 1 ms
 Maximum Delay................................... 1 ms
 Minimum Delay................................... 1 ms
 Last updated (based on AP Up Time)............ 0 days, 05 h 03 m 25 s
```

The output of this command contains the following link latency results:

- **Current Delay**—The current round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.
- **Maximum Delay**—Since link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.
- **Minimum Delay**—Since link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.

Step 3 Clear the current, minimum, and maximum link latency statistics on the controller for a specific access point by entering this command:

config ap link-latency reset *Cisco_AP*

Step 4 See the results of the reset by entering this command:

show ap config general *Cisco_AP*

Preferred Mode

Preferred mode allows an administrator to configure CAPWAP L3 transport (IPv4 and IPv6) through which APs join the controller (based on its primary/secondary/tertiary configuration).

There are two levels of preferred mode

- AP Group specific
- Global Configuration

Guidelines for Configuring Preferred Mode

The following preferred mode configurations are available:

- AP-Group specific preferred mode is pushed to an AP only when the preferred mode of AP-Group is configured and the AP belongs to that group.
- Global preferred mode is pushed to default-group APs and to those AP-Groups on which the preferred mode is not configured.
- By default, values of preferred mode for AP-Group and Global is set to un-configured and IPv4 respectively.
- If an AP, with an configured preferred mode, tries to join the controller and fails, then it will fall back to choose AP-manager of the other transport and joins the same controller. When both transports fail, AP will move to next discovery response.
- In such a scenario, Static IP configuration will take precedence over prefer mode. For example:
  - On the controller, the preferred mode is configured with an IPv4 address.
  - On the AP, Static IPv6 is configured using CLI or GUI.
  - The AP will join the controller using IPv6 transport mode.
- The controllers CLI provides an XML support of preferred mode.

Configuring CAPWAP Preferred Mode (GUI)

Procedure

Step 1 Choose **Controller** > **General** to open the Global Configuration page. Select the **CAPWAP Preferred Mode** list box and select either IPv4 or IPv6 as the global CAPWAP Preferred mode.

Note By default, the controller is configured with an CAPWAP preferred mode IPv4 address.

Step 2 Choose **WLAN** > **Advanced** > **APGroup** > **General Tab** and select the **CAPWAP Preferred Mode** checkbox to configure an AP-Group with an IPv4 or IPv6 CAPWAP Preferred Mode.

Step 3 Choose **Wireless** > **ALL APs** > **General Tab** to check the APs CAPWAP setting. Refer to the **IP Config** section to view if the AP's CAPWAP Preferred Mode is applied globally or for an AP-Group.

Step 4 Choose **Monitor** > **Statistics** > **Preferred Mode** to help users to check if the preferred mode command is pushed successfully to an AP.

- Preferred mode of Global/AP Groups: The name of the AP that is configured with either IPv4, IPv6 or global.
- Total: The total count of APs configured with preferred mode.
- Success: Counts the number of times the AP was successfully configured with the preferred mode.
- Unsupported: APs that are not capable of joining in with IPv6 CAPWAP.
- Already Configured: Counts the attempts made to configure an already configured AP.
- Per-AP Group Configured: Preferred mode configured on per AP-Group.
- Failure: Counts the number of times the AP was failed to get configured with the preferred mode.

Configuring CAPWAP Preferred Mode (CLI)

Procedure

Step 1 Use this command to configure preferred mode of AP-Group and all APs. Global preferred mode will not be applied on APs whose AP-Group preferred mode is already configured. On successful configuration, the AP will restart CAPWAP and join with the configured preferred mode after choosing a controller based on its primary/secondary/tertiary configuration.

config ap preferred-mode {**ipv4** | **ipv6**} {*apgroup-name* | **all**}

Step 2 Use this command to disable (un-configure) the preferred mode on the AP.

config ap preferred-mode disable *apgroup-name*

Note APs that belong to *apgroup-name* will restart CAPWAP and join back the controller with global preferred mode.

Step 3 Use this command to view the statistics for preferred mode configuration. The statistics are not cumulative but will be updated for last executed configuration CLI of preferred mode.

show ap prefer-mode stats

Step 4 Use this command to view the preferred mode configured for all AP-Groups.

show wlan apgroups

Step 5 Use this command to view the global preferred mode configured.

show network summary

Step 6 Use this command to view to check if the preferred mode command is pushed to an AP from global configuration or from an AP-Group specific configuration.

show ap config general *ap-name*

```
(Cisco Controller) >show ap config general AP-3702E

Cisco AP Identifier.............................. 2
Cisco AP Name.................................... AP-3702E
```

```
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-A     802.11a:-A
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-A
Switch Port Number .............................. 1
MAC Address...................................... bc:16:65:09:4e:fc
IPv6 Address Configuration....................... SLAAC
IPv6 Address..................................... 2001:9:2:35:be16:65ff:fe09:4efc
IPv6 Prefix Length............................... 64
Gateway IPv6 Addr................................ fe80::a2cf:5bff:fe51:c4ce
NAT External IP Address.......................... None
CAPWAP Path MTU.................................. 1473
Telnet State..................................... Globally Enabled
Ssh State........................................ Globally Enabled
Cisco AP Location................................ default location
Cisco AP Floor Label............................. 0
Cisco AP Group Name.............................. default-group
Primary Cisco Switch Name........................ amb
Primary Cisco Switch IP Address.................. 9.2.35.25
.....................................
.....................................
.....................................
.....................................
.....................................
Ethernet Port Speed.............................. Auto
AP Link Latency.................................. Disabled
Rogue Detection.................................. Enabled
AP TCP MSS Adjust................................ Disabled
IPv6 Capwap UDP Lite............................. Enabled
Capwap Prefer Mode............................... Ipv6 (Global Config)
Hotspot Venue Group.............................. Unspecified
Hotspot Venue Type............................... Unspecified
DNS server IP ........................... Not Available
```

IPv6 CAPWAP UDP Lite

The UDP Lite feature, which is an enhancement to the existing IPv6 functionality, supports the UDP Lite protocol. This feature is only applicable to the IPv6 addresses of the controller and APs. IPv6 mandates complete payload checksum for UDP. The UDP Lite feature minimizes the performance impact on the controller and AP by restricting the checksum calculation coverage for the UDP Lite header to 8 bytes only.

This feature impacts intermediate firewalls to allow UDP Lite protocol (protocol ID of 136) packets. Existing firewalls might not provide the option to open specific ports on UDP Lite protocol. In such cases, the administrator must open up all the ports on UDP Lite.

Configuring UDP Lite Globally (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points > Global Configuration** to open the Global Configuration page.

Step 2 Under the **Global UDP Lite** section, select the **UDP Lite** checkbox to enable UDP Lite globally.

Note IPv6 UDP Lite is not applicable for APs connected with CAPWAPv4 tunnel. They are applicable only for APs joining the controller using CAPWAPv6 tunnel.

Step 3 Click **Apply** to set the global UDP Lite configuration.

Step 4 If desired, you can choose to override the global UDP Lite configuration by unselecting the Global IPv6 UDP Lite mentioned in Step 2.

Note Switching between UDP and UDP Lite causes the AP to disjoin and rejoin.

Step 5 Click **Save Configuration** to save your changes.

Configuring UDP Lite on AP (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points > All APs** to open the All APs page.

Step 2 Select an **AP Name** with an IPv6 address and click on it to open the **Details** page of the selected AP.

Step 3 Under the **Advanced** tab, select the **UDP Lite** checkbox to enable UDP Lite for the selected AP.

Note This field is displayed only for APs that have joined the controller over CAPWAPv6 tunnel. The Web UI page does not display this field for APs joining the controller over the CAPWAPv4 tunnel .

Step 4 Click **Apply** to commit your changes.

Step 5 Click **Save Configuration** to save your changes.

Configuring the UDP Lite (CLI)

Procedure

Step 1 Use this command to enable UDP Lite globally.

config ipv6 capwap udplite enable *all*

Step 2 Use this command to enable UDP Lite on a selected AP.

config ipv6 capwap udplite enable *ap-name*

Step 3 Use this command to disable UDP Lite globally.

config ipv6 capwap udplite disable *all*

Step 4 Use this command to disable UDP Lite on a selected AP.

config ipv6 capwap udplite disable *ap-name*

Step 5 Use this command to view the status of UDP Lite on a controller.

show ipv6 summary

```
(Cisco Controller) >show ipv6 summary

Global Config.............................. Disabled
Reachable-lifetime value................... 300
Stale-lifetime value....................... 86400
Down-lifetime value........................ 30
RA Throttling.............................. Disabled
RA Throttling allow at-least............... 1
RA Throttling allow at-most................ 1
RA Throttling max-through.................. 10
RA Throttling throttle-period.............. 600
RA Throttling interval-option.............. passthrough
NS Mulitcast CacheMiss Forwarding.......... Disabled
NA Mulitcast Forwarding.................... Enabled
IPv6 Capwap UDP Lite....................... Enabled
Operating System IPv6 state ............... Disabled
```

Data Encryption

Controllers enable you to encrypt CAPWAP control packets (and optionally, CAPWAP data packets) that are sent between the AP and the controller using Datagram Transport Layer Security (DTLS). DTLS is a standards-track Internet Engineering Task Force (IETF) protocol based on TLS. CAPWAP control packets are management packets exchanged between a controller and an access point while CAPWAP data packets encapsulate forwarded wireless frames. CAPWAP control and data packets are sent over separate UDP ports: 5246 (control) and 5247 (data). If an access point does not support DTLS data encryption, DTLS is enabled only for the control plane, and a DTLS session for the data plane is not established.

Table 1: DTLSv1.2 for CAPWAP Support Information

Release	Support Information
8.2	Not supported
8.3.11x.0 or a later release	Supported in controller and Cisco Wave 2 AP
Any release	Not supported in Cisco Wave 1 AP

Note Cisco Wave 1 APs supports TLS v1.0 only.

The following are supported for web authentication and WebAdmin based on the configuration:

- TLSv1.2.
- TLSv1.0
- SSLv3
- SSLv2

Note Controllers support only static configuration of gateway. Therefore, the ICMP redirect to change IP address of the gateway is not considered.

Cipher Suites Supported by APs

- Cipher suites supported by Cisco Aironet 4800, 3800, 2800, 1800, and 1560 Series APs:
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DH_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DH_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- Cipher suites supported by Cisco Aironet 3700, 2700, 3600, 2600 Series, and 802 APs:
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA256

Restrictions on Data Encryption

- The following access points support DTLS data encryption with hardware-based encryption: 1540, 1560, 1570, 1700, 1815, 2700, 2800, 3700, 3800, and 4800.
- DTLS data encryption is not supported on Cisco Aironet 700, 800, 1530 Series APs.
- Cisco Wave 1 APs does not support TLS v1.2.
- In Cisco Aironet 18xx Series APs, only software DTLS data encryption is supported with limited throughput performance. Hardware encryption is not supported.

- DTLS data encryption is enabled automatically for OfficeExtend access points but disabled by default for all other access points. Most access points are deployed in a secure network within a company building, so data encryption is not necessary. In contrast, the traffic between an OfficeExtend access point and the controller travels through an unsecure public network, so data encryption is more important for these access points. When data encryption is enabled, traffic is encrypted at the access point before it is sent to the controller and at the controller before it is sent to the client.
- Encryption limits throughput at both the controller and the access point, and maximum throughput is desired for most enterprise networks.
- You can use the controller to enable or disable DTLS data encryption for a specific access point or for all APs.
- Some AP models have hardware-based DTLS support, but some do not. The APs that do not have hardware-based DTLS support will have significantly reduced throughput if Data DTLS is enabled.
- Central switching is not supported on Cisco vWLC and therefore Data DTLS is not supported on Cisco vWLC.
- For Cisco 5520 and 8540 Wireless Controllers, data DTLS is available without the need for an additional license.
- If your controller does not have a data DTLS license and if the access point associated with the controller has DTLS enabled, the data path will be unencrypted.

Configuring Data Encryption (GUI)

Ensure that the base license is installed on the Cisco WLC. Once the license is installed, you can enable data encryption for the access points.

Procedure

Step 1 Choose **Wireless** > **Access Points** > **All APs** to open the **All APs** page.

Step 2 Click the name of the AP for which you want to enable data encryption.

Step 3 Choose the **Advanced** tab to open the All APs > Details for (Advanced) page.

Step 4 Check the **Data Encryption** check box to enable data encryption for this access point or unselect it to disable this feature. The default value is unselected.

Note Changing the data encryption mode requires the access points to rejoin the controller.

Step 5 Save the configuration.

Configuring Data Encryption (CLI)

Note In images without a DTLS license, the **config** or **show** commands are not available.

To enable DTLS data encryption for access points on the controller using the controller CLI, follow these steps:

Procedure

Step 1 Enable or disable data encryption for all access points or a specific access point by entering this command:

config ap link-encryption {**enable** | **disable**} {**all** | *Cisco_AP*}

The default value is disabled.

Note Changing the data encryption mode requires the access points to rejoin the controller.

Step 2 When prompted to confirm that you want to disconnect the access point(s) and attached client(s), enter **Y**.

Step 3 Enter the **save config** command to save your configuration.

Step 4 See the encryption state of all access points or a specific access point by entering this command:

show ap link-encryption {**all** | *Cisco_AP*}

This command also shows authentication errors, which tracks the number of integrity check failures, and replay errors, which tracks the number of times that the access point receives the same packet.

Step 5 See a summary of all active DTLS connections by entering this command:

show dtls connections

Note If you experience any problems with DTLS data encryption, enter the **debug dtls** {**all** | **event** | **trace** | **packet**} {**enable** | **disable**} command to debug all DTLS messages, events, traces, or packets.

Step 6 Enable new cipher suites for DTLS connection between AP and controller by entering this command:

config ap dtls-cipher-suite {**RSA-AES256-SHA256** | **RSA-AES256-SHA** | **RSA-AES128-SHA**}

Note If you choose to use the **RSA-AES256-SHA256** option, ensure that you set the DTLS version to **dtls_all** in the next step.

Step 7 Configure the DTLS version by entering this command:

config ap dtls-version {**dtls1.0** | **dtls1.2** | **dtls_all**}

Step 8 See the summary of DTLS cipher suite by entering this command:

show ap dtls-cipher-suite

VLAN Tagging for CAPWAP Frames from Access Points

You can configure VLAN tagging on the Ethernet interface either directly on the AP console or through the controller. The configuration is saved in the flash memory and all CAPWAP frames use the VLAN tag as configured, along with all the locally switched traffic, which is not mapped to a VLAN.

For more information about which APs support CAPWAP VLAN Tagging, see Feature Matrix for Wave 2 and 802.11ax (Wi-Fi 6) Access Points.

This section contains the following subsections:

Configuring VLAN Tagging for CAPWAP Frames from Access Points (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **All APs** to open the **All APs** page.

Step 2 Click the AP name from the list of AP names to open the Details page for the AP.

Step 3 Click the **Advanced** tab.

Step 4 In the **VLAN Tagging** area, check the **VLAN Tagging** check box.

Step 5 In the **Trunk VLAN ID** field, enter an ID.

If the AP is unable to route traffic through the specified trunk VLAN after about 10 minutes, the AP performs a recovery procedure by rebooting and sending CAPWAP frames in untagged mode to try and reassociate with the controller. The controller sends a trap to a trap server such as the Cisco Prime Infrastructure, which indicates the failure of the trunk VLAN.

If the AP is unable to route traffic through the specified trunk VLAN, it untags the packets and reassociates with the controller. The controller sends a trap to a trap server such as the Cisco Prime Infrastructure, which indicates the failure of the trunk VLAN.

If the trunk VLAN ID is 0, the AP untags the CAPWAP frames.

The VLAN Tag status is displayed showing whether the AP tags or untags the CAPWAP frames.

Step 6 Click **Apply**.

Step 7 You are prompted with a warning message saying that the configuration will result in a reboot of the AP. Click **OK** to continue.

Step 8 Click **Save Configuration**.

What to do next

After the configuration, the switch or other equipment connected to the Ethernet interface of the AP must also be configured to support tagged Ethernet frames.

Configuring VLAN Tagging for CAPWAP Frames from Access Points (CLI)

Procedure

Step 1 Configure VLAN tagging for CAPWAP frames from APs by entering this command:

config ap ethernet tag {**disable** | **id** *vlan-id*} {*ap-name* | **all**}

Step 2 You can see VLAN tagging information for an AP or all APs by entering this command:

show ap ethernet tag {**summary** | *ap-name*}

What to do next

After the configuration, the switch or other equipment connected to the Ethernet interface of the AP must also be configured to support tagged Ethernet frames.

Discovering and Joining Controllers

This section contains the following subsections:

Controller Discovery Process

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

The following are some guidelines for the controller discovery process:

- 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 controller.
- Access points must be discovered by a controller before they can become an active part of the network. The lightweight access points support the following controller discovery processes:
  - Layer 3 CAPWAP or LWAPP discovery—This feature can be enabled on different subnets from the access point and uses either IPv4 or IPv6 addresses and UDP packets rather the MAC addresses used by Layer 2 discovery.
  - CAPWAP Multicast Discovery—Broadcast does not exist in IPv6 address. Access point sends CAPWAP discovery message to all the controllers multicast address (FF01::18C). The controller receives the IPv6 discovery request from the AP only if it is in the same L2 segment and sends back the IPv6 discovery response.
  - Locally stored controller IPv4 or IPv6 address discovery—If the access point was previously associated to a controller, the IPv4 or IPv6 addresses of the primary, secondary, and tertiary controllers are stored in the access point's nonvolatile memory. This process of storing controller IPv4 or IPv6 addresses on an access point for later deployment is called *priming the access point*.
  - DHCP server discovery using option 43—This feature uses DHCP option 43 to provide controller IPv4 addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability.

Note You can configure up to three IP addresses in the hexadecimal string.

- DHCP server discovery using option 52 —This feature uses DHCP option 52 to allow the AP to discover the IPv6 address of the controller to which it connects. As part of the DHCPv6 messages, the DHCP server provides the controllers management with an IPv6 address.
- DNS discovery—The access point can discover controllers through your domain name server (DNS). You must configure your DNS to return controller IPv4 and IPv6 addresses in response to CISCO-LWAPP-CONTROLLER.*localdomain* or CISCO-CAPWAP-CONTROLLER.*localdomain*, where *localdomain* is the access point domain name.

  When an access point receives an IPv4/IPv6 address and DNSv4/DNSv6 information from a DHCPv4/DHCPv6 server, it contacts the DNS to resolve CISCO-LWAPP-CONTROLLER.*localdomain* or CISCO-CAPWAP-CONTROLLER.*localdomain*. When the DNS sends a list of controller IP addresses, which may include either IPv4 addresses or IPv6 addresses or both the addresses, the access point sends discovery requests to the controllers.
- To configure the IP addresses that the controller sends in its CAPWAP discovery responses, use the **config network ap-discovery nat-ip-only** {**enable** | **disable**} command.

Note If you disable **nat-ip-only**, the controller sends all active AP-Manager interfaces with their non-NAT IP in discovery response to APs.

If you enable **nat-ip-only**, the controller sends all active AP-Manager interfaces with NAT IP if configured for the interface, else non-NAT IP.

We recommend that you configure the interface as AP-Manager interface with NAT IP or non-NAT IP keeping these scenarios in mind because the AP chooses the least loaded AP-Manager interface received in the discovery response.

Guidelines and Restrictions on Controller Discovery Process

- Ensure that the controller is set to the current time. If the controller is set to a time that has already occurred, the access point might not join the controller because its certificate may not be valid for that time.
- Cisco 2800 and 3800 Series APs replaces the underscore with a hypen in hostname field of DHCP Discover packet. For more information about this behavior, see **RFC1035**.
- To avoid downtime restart CAPWAP on AP while configuring Global HA, so that AP goes back and joins the backup primary controller. This starts a discovery with the primary controller in the back ground. If the discovery with primary is successful, it goes back and joins the primary again.

Using DHCP Option 43 and DHCP Option 60

Cisco access points use the type-length-value (TLV) format for DHCP option 43. DHCP servers must may be programmed to return the option based on the access point's DHCP Vendor Class Identifier (VCI) string (DHCP option 60).

The format of the TLV block is as follows:

- Type: 0xf1 (decimal 241)

- Length: Number of controller IP addresses * 4
- Value: List of the IP addresses of controller management interfaces

See the product documentation for your DHCP server for instructions on configuring DHCP option 43. For more information about DHCP option 43, see https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/97066-dhcp-option-43-00.html.

If the AP is ordered with the Service Provider Option - AIR-OPT60-DHCP selected, the VCI string for that AP will be different than those listed above. The VCI string will have the “ServiceProvider”. For example, a 3600 with this option will return this VCI string: "Cisco AP c3600-ServiceProvider".

Note The controller IP address that you obtain from the DHCP server should be a unicast IP address. Do not configure the controller IP address as a multicast address when configuring DHCP Option 43.

Backup Controllers

A single controller at a centralized location can act as a backup for access points when they lose connectivity with the primary controller in the local region. Centralized and regional controllers do not need to be in the same mobility group. You can specify a primary, secondary, and tertiary controller for specific access points in your network. Using the controller GUI or CLI, you can specify the IP addresses of the backup controllers, which allows the access points to fail over to controllers outside of the mobility group.

The following are some guidelines for configuring backup controllers:

- You can configure primary and secondary backup controllers (which are used if primary, secondary, or tertiary controllers are not specified or are not responsive) for all access points connected to the controller as well as various timers, including heartbeat timers and discovery request timers. To reduce the controller failure detection time, you can configure the fast heartbeat interval (between the controller and the access point) with a smaller timeout value. When the fast heartbeat timer expires (at every heartbeat interval), the access point determines if any data packets have been received from the controller within the last interval. If no packets have been received, the access point sends a fast echo request to the controller.
- The access point maintains a list of backup controllers and periodically sends primary discovery requests to each entry on the list. When the access point receives a new discovery response from a controller, the backup controller list is updated. Any controller that fails to respond to two consecutive primary discovery requests is removed from the list. If the access point’s local controller fails, it chooses an available controller from the backup controller list in this order: primary, secondary, tertiary, primary backup, and secondary backup. The access point waits for a discovery response from the first available controller in the backup list and joins the controller if it receives a response within the time configured for the primary discovery request timer. If the time limit is reached, the access point assumes that the controller cannot be joined and waits for a discovery response from the next available controller in the list.
- When an access point's primary controller comes back online, the access point disassociates from the backup controller and reconnects to its primary controller. The access point falls back only to its primary controller and not to any available secondary controller for which it is configured. For example, if an access point is configured with primary, secondary, and tertiary controllers, it fails over to the tertiary controller when the primary and secondary controllers become unresponsive. If the secondary controller comes back online while the primary controller is down, the access point does not fall back to the secondary controller and stays connected to the tertiary controller. The access point waits until the primary controller comes back online to fall back from the tertiary controller to the primary controller. If the

tertiary controller fails and the primary controller is still down, the access point then falls back to the available secondary controller.

This section contains the following subsections:

Restrictions for Configuring Backup Controllers

- You can configure the fast heartbeat timer only for access points in local and FlexConnect modes.

Configuring Backup Controllers (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration** to open the Global Configuration page.

Step 2 From the Local Mode AP Fast Heartbeat Timer State drop-down list, choose **Enable** to enable the fast heartbeat timer for access points in local mode or choose **Disable** to disable this timer. The default value is Disable.

Step 3 If you chose Enable in Step 2, enter the Local Mode AP Fast Heartbeat Timeout text box to configure the fast heartbeat timer for access points in local mode. Specifying a small heartbeat interval reduces the amount of time it takes to detect a controller failure.

The range for the AP Fast Heartbeat Timeout value for Cisco 8540 Controllers is 10–15 (inclusive) and is 1–10 (inclusive) for other controllers. The default value for the heartbeat timeout for Cisco 8540 Controllers is 10. The default value for other controllers is 1 second.

Step 4 From the FlexConnect Mode AP Fast Heartbeat Timer State drop-down list, choose **Enable** to enable the fast heartbeat timer for FlexConnect access points or choose **Disable** to disable this timer. The default value is Disable.

Step 5 If you enable FlexConnect fast heartbeat, enter the FlexConnect Mode AP Fast Heartbeat Timeout value in the FlexConnect Mode AP Fast Heartbeat Timeout text box. Specifying a small heartbeat interval reduces the amount of time it takes to detect a controller failure.

The range for the FlexConnect Mode AP Fast Heartbeat Timeout value for Cisco 8540 Controllers is 10–15 (inclusive) and is 1–10 for other controllers. The default value for the heartbeat timeout for Cisco 8540 Controllers is 10. The default value for other controllers is 1 second.

Step 6 In the AP Primary Discovery Timeout text box, a value between 30 and 3600 seconds (inclusive) to configure the access point primary discovery request timer. The default value is 120 seconds.

Step 7 If you want to specify a primary backup controller for all access points, enter the IPv4/IPv6 address of the primary backup controller in the Back-up Primary Controller IP Address (IPv4/IPv6) text box and the name of the controller in the Back-up Primary Controller Name text box.

Note The default value for the IP address is 0.0.0.0, which disables the primary backup controller.

Step 8 If you want to specify a secondary backup controller for all access points, enter the IPv4/IPv6 address of the secondary backup controller in the Back-up Secondary Controller IP Address (IPv4/IPv6) text box and the name of the controller in the Back-up Secondary Controller Name text box.

Note The default value for the IP address is 0.0.0.0, which disables the secondary backup controller.

Step 9 Click **Apply** to commit your changes.

Step 10 Configure primary, secondary, and tertiary backup controllers for a specific access point as follows:

a) Choose **Access Points** > **All APs** to open the All APs page.
b) Click the name of the access point for which you want to configure primary, secondary, and tertiary backup controllers.
c) Choose the **High Availability** tab to open the All APs > Details for (High Availability) page.
d) If desired, enter the name and IP address of the primary controller for this access point in the Primary Controller text boxes.

Note Entering an IP address for the backup controller is optional in this step and the next two steps. If the backup controller is outside the mobility group to which the access point is connected (the primary controller), then you need to provide the IP address of the primary, secondary, or tertiary controller, respectively. The controller name and IP address must belong to the same primary, secondary, or tertiary controller. Otherwise, the access point cannot join the backup controller.

e) If desired, enter the name and IP address of the secondary controller for this access point in the Secondary Controller text boxes.
f) If desired, enter the name and IP address of the tertiary controller for this access point in the Tertiary Controller text boxes.
g) Click **Apply** to commit your changes.

Step 11 Click **Save Configuration** to save your changes.

Configuring Backup Controllers (CLI)

Procedure

Step 1 Configure a primary controller for a specific access point by entering this command:

config ap primary-base *controller_name Cisco_AP* [*controller_ip_address*]

Note The *controller_ip_address* parameter in this command and the next two commands is optional. If the backup controller is outside the mobility group to which the access point is connected (the primary controller), then you need to provide the IP address of the primary, secondary, or tertiary controller, respectively. In each command, the *controller_name* and *controller_ip_address* must belong to the same primary, secondary, or tertiary controller. Otherwise, the access point cannot join the backup controller.

Step 2 Configure a secondary controller for a specific access point by entering this command:

config ap secondary-base *controller_name Cisco_AP* [*controller_ip_address*]

Step 3 Configure a tertiary controller for a specific access point by entering this command:

config ap tertiary-base *controller_name Cisco_AP* [*controller_ip_address*]

Step 4 Configure a primary backup controller for all access points by entering this command:

config advanced backup-controller primary *system name ip_addr*

Note This command is valid for both IPv4 and IPv6

Step 5 Configure a secondary backup controller for all access points by entering this command:

config advanced backup-controller secondary *system name ip_addr*

Note To delete a primary or secondary backup controller entry, enter *0.0.0.0* for the controller IPv4/IPv6 address.

Note This command is valid for both IPv4 and IPv6

Step 6 Enable or disable the fast heartbeat timer for local or FlexConnect access points by entering this command:

config advanced timers ap-fast-heartbeat {**local** | **flexconnect** | **all**} {**enable | disable**} *interval*

where **all** is both local and FlexConnect access points, and *interval* is a value between 10 and 15 seconds for Cisco 3504, 5520, and 8540 controllers, and 1 and 10 seconds for Cisco vWLC controllers. Specifying a small heartbeat interval reduces the amount of time that it takes to detect a controller failure. The default value is disabled.Configure the access point heartbeat timer by entering this command:

config advanced timers ap-heartbeat-timeout *interval*

where *interval* is a value between 1 and 30 seconds (inclusive). This value should be at least three times larger than the fast heartbeat timer. The default value is 30 seconds.

Caution Do not enable the fast heartbeat timer with the high latency link. If you have to enable the fast heartbeat timer, the timer value must be greater than the latency.

Step 7 Configure the access point primary discovery request timer by entering this command:

config advanced timers ap-primary-discovery-timeout *interval*

where *interval* is a value between 30 and 3600 seconds. The default value is 120 seconds.

Step 8 Configure the access point discovery timer by entering this command:

config advanced timers ap-discovery-timeout *interval*

where *interval* is a value between 1 and 10 seconds (inclusive). The default value is 10 seconds.

Step 9 Configure the 802.11 authentication response timer by entering this command:

config advanced timers auth-timeout *interval*

where *interval* is a value between 5 and 600 seconds (inclusive). The default value is 10 seconds.

Step 10 Save your changes by entering this command:

save config

Step 11 See an access point's configuration by entering these commands:

- **show ap config general** *Cisco_AP*
- **show advanced backup-controller**
- **show advanced timers**

Information similar to the following appears for the **show ap config general** *Cisco_AP* command for Primary Cisco Switch IP Address using IPv4:

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP5
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-AB    802.11a:-AB
```

```
AP Country code.............................. US  - United States
AP Regulatory Domain......................... 802.11bg:-A    802.11a:-N
Switch Port Number .......................... 1
MAC Address.................................. 00:13:80:60:48:3e
IP Address Configuration..................... DHCP
IP Address................................... 1.100.163.133
...
Primary Cisco Switch Name.................... 1-5520
Primary Cisco Switch IP Address.............. 192.0.2.1
Secondary Cisco Switch Name.................. 1-8540
Secondary Cisco Switch IP Address............ 198.51.100.1
Tertiary Cisco Switch Name................... 2-8540
Tertiary Cisco Switch IP Address............. 209.165.201.1
...
```

Information similar to the following appears for the **show ap config general** *Cisco_AP* command for Primary Cisco Switch IP Address using IPv6:

```
Cisco AP Identifier.......................... 1
Cisco AP Name................................ AP6
Country code................................. US - United States
Regulatory Domain allowed by Country......... 802.11bg:-A 802.11a:-A
AP Country code.............................. US - United States
AP Regulatory Domain......................... 802.11bg:-A 802.11a:-A
Switch Port Number .......................... 13
MAC Address.................................. 44:2b:03:9a:9d:30
IPv6 Address Configuration................... DHCPv6
IPv6 Address................................. 2001:9:5:96:295d:3b2:2db2:9b47
IPv6 Prefix Length........................... 128
Gateway IPv6 Addr............................ fe80::6abd:abff:fe8c:764a
NAT External IP Address...................... None
CAPWAP Path MTU.............................. 1473
Telnet State................................. Globally Disabled
Ssh State.................................... Globally Disabled
Cisco AP Location............................ _5500
Cisco AP Floor Label......................... 0
Cisco AP Group Name.......................... IPv6-Same_VLAN
Primary Cisco Switch Name.................... Mak_WLC_5500-HA
Primary Cisco Switch IP Address.............. 2001:9:5:95::11
```

Information similar to the following appears for the **show advanced backup-controller** command when configured using IPv4:

```
AP primary Backup Controller ................... controller1 10.10.10.10
AP secondary Backup Controller ............... 0.0.0.0
```

Information similar to the following appears for the **show advanced backup-controller** command when configured using IPv6:

```
AP primary Backup Controller ................... WLC_5500-2 fd09:9:5:94::11
AP secondary Backup Controller .................. vWLC 9.5.92.11
```

Information similar to the following appears for the **show advanced timers** command:

```
Authentication Response Timeout (seconds)........ 10
Rogue Entry Timeout (seconds).................... 1300
AP Heart Beat Timeout (seconds).................. 30
```

```
AP Discovery Timeout (seconds)................... 10
AP Local mode Fast Heartbeat (seconds)........... 10 (enable)
AP flexconnect mode Fast Heartbeat (seconds)........... disable
AP Primary Discovery Timeout (seconds)........... 120
```

Failover Priority for Access Points

If a controller has the maximum number of supported APs joined to it, the failover priority feature allows it to disconnect a lower priority AP, if a higher priority AP tries to join.

The default priority is 1, the lowest priority; set higher priorities on APs if you want to enable this feature.

The following are some guidelines for configuring failover priority for access points:

- You can configure your wireless network so that the backup controller embedded controller recognizes a join request from a higher-priority access point, and if necessary, disassociates a lower-priority access point as a means to provide an available port.
- Failover priority is not in effect during the regular operation of your wireless network. It takes effect only if there are more association requests after a controller an embedded controller failure than there are available backup controller slots.
- You can enable failover priority on your network and assign priorities to the individual access points.
- By default, all access points are set to priority level 1, which is the lowest priority level. Therefore, you need to assign a priority level only to those access points that warrant a higher priority.

This section contains the following subsections:

Configuring Failover Priority for Access Points (GUI)

Procedure

Step 1 Choose **Wireless > Access Points > Global Configuration** to open the Global Configuration page.

Step 2 From the Global AP Failover Priority drop-down list, choose **Enable** to enable access point failover priority or choose **Disable** to disable this feature and turn off any access point priority assignments. The default value is Disable.

Step 3 Click **Apply** to commit your changes.

Step 4 Click **Save Configuration** to save your changes.

Step 5 Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 6 Click the name of the access point for which you want to configure failover priority.

Step 7 Choose the **High Availability** tab. The All APs > Details for (High Availability) page appears.

Step 8 From the AP Failover Priority drop-down list, choose one of the following options to specify the priority of the access point:

- **Low**—Assigns the access point to the level 1 priority, which is the lowest priority level. This is the default value.
- **Medium**—Assigns the access point to the level 2 priority.

- **High**—Assigns the access point to the level 3 priority.
- **Critical**—Assigns the access point to the level 4 priority, which is the highest priority level.

Step 9 Click **Apply** to commit your changes.

Step 10 Click **Save Configuration** to save your changes.

Configuring Failover Priority for Access Points (CLI)

Procedure

Step 1 Enable or disable access point failover priority by entering this command:

config network ap-priority {**enable** | **disable**}

Step 2 Specify the priority of an access point by entering this command:

config ap priority {**1** | **2** | **3** | **4**} *Cisco_AP*

where 1 is the lowest priority level and 4 is the highest priority level. The default value is 1.

Step 3 Enter the **save config** command to save your changes.

Viewing Failover Priority Settings (CLI)

- Confirm whether access point failover priority is enabled on your network by entering this command:

  show network summary

  Information similar to the following appears:

```
RF-Network Name............................. mrf
Web Mode.................................... Enable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Shell (ssh).......................... Enable
Telnet...................................... Enable
Ethernet Multicast Mode..................... Disable
Ethernet Broadcast Mode..................... Disable
IGMP snooping............................... Disabled
IGMP timeout................................ 60 seconds
User Idle Timeout........................... 300 seconds
ARP Idle Timeout............................ 300 seconds
Cisco AP Default Master..................... Disable
AP Join Priority........................... Enabled

...
```

- See the failover priority for each access point by entering this command:

  show ap summary

  Information similar to the following appears:

```
Number of APs.................................. 2
Global AP User Name............................ user
Global AP Dot1x User Name...................... Not Configured

AP Name  Slots  AP Model           Ethernet MAC       Location   Port Country Priority
-------  -----  ------------------ -----------------  ---------  ---- ------- -------
ap:1252  2      AIR-LAP1252AG-A-K9 00:1b:d5:13:39:74  hallway 6  1    US      1
ap:1121  1      AIR-LAP1121G-A-K9  00:1b:d5:a9:ad:08  reception  1    US      3
```

To see the summary of a specific access point, you can specify the access point name. You can also use wildcard searches when filtering for access points.

AP Retransmission Interval and Retry Count

The controller and the APs exchange packets using the CAPWAP reliable transport protocol. For each request, a response is defined. This response is used to acknowledge the receipt of the request message. Response messages are not explicitly acknowledged; therefore, if a response message is not received, the original request message is retransmitted after the retransmit interval. If the request is not acknowledged after a maximum number of retransmissions, the session is closed and the APs reassociate with another controller.

This section contains the following subsections:

Restrictions for Access Point Retransmission Interval and Retry Count

- You can configure the retransmission intervals and retry count both at a global as well as a specific access point level. A global configuration applies these configuration parameters to all the access points. That is, the retransmission interval and the retry count are uniform for all access points. Alternatively, when you configure the retransmission level and retry count at a specific access point level, the values are applied to that particular access point. The access point specific configuration has a higher precedence than the global configuration.
- Retransmission intervals and the retry count do not apply for mesh access points.

Configuring the AP Retransmission Interval and Retry Count (GUI)

You can configure the retransmission interval and retry count for all APs globally or a specific AP.

Procedure

Step 1 To configure the controller to set the retransmission interval and retry count globally using the controller GUI, follow these steps:

a) Choose **Wireless > Access Points > Global Configuration**.

b) Choose one of the following options under the AP Transmit Config Parameters section:

- **AP Retransmit Count**—Enter the number of times you want the access point to retransmit the request to the controller. This parameter can take values between 3 and 8.
- **AP Retransmit Interval**—Enter the time duration between the retransmission of requests. This parameter can take values between 2 and 5.

c) Click **Apply**.

Step 2 To configure the controller to set the retransmission interval and retry count for a specific access point, follow these steps:

a) Choose **Wireless > Access Points > All APs**.

b) Click on the AP Name link for the access point on which you want to set the values.

The **All APs > Details** page appears.

c) Click the **Advanced Tab** to open the advanced parameters page.

d) Choose one of the following parameters under the AP Transmit Config Parameters section:

- **AP Retransmit Count**—Enter the number of times that you want the access point to retransmit the request to the controller. This parameter can take values between 3 and 8.
- **AP Retransmit Interval**—Enter the time duration between the retransmission of requests. This parameter can take values between 2 and 5.

e) Click **Apply**.

Configuring the Access Point Retransmission Interval and Retry Count (CLI)

You can configure the retransmission interval and retry count for all access points globally or a specific access point.

- Configure the retransmission interval and retry count for all access points globally by entering the this command:

  config ap retransmit {**interval** | **count**} *seconds* **all**

  The valid range for the **interval** parameter is between 2 and 5 seconds. The valid range for the **count** parameter is between 3 and 8.

- Configure the retransmission interval and retry count for a specific access point, by entering this command:

  config ap retransmit {**interval** | **count**} *seconds Cisco_AP*

  The valid range for the **interval** parameter is between 2 and 5 seconds. The valid range for the **count** parameter is between 3 and 8.

- See the status of the configured retransmit parameters on all or specific APs by entering this command:

  show ap retransmit all

Note Because retransmit and retry values cannot be set for access points in mesh mode, these values are displayed as N/A (not applicable).

- See the status of the configured retransmit parameters on a specific access point by entering this command:

  show ap retransmit *Cisco_AP*

Authorizing Access Points

When an AP joins a controller, that connection is mutually authenticated via X.509 certificates, that is, the controller authenticates the AP's certificate and the AP authenticates the controller's certificate.

All Cisco wireless controllers and all Cisco APs manufactured after July 18 2005, have manufacturing installed certificates (MICs).

By default, the controllers and APs authenticate each other via MICs. MICs generated before mid-2017 expire after 10 years, at which point, by default, the APs will no longer be able to join the controller. To allow the APs with expired MICs to join the controller, and/or APs to join a controller with an expired MIC, use the following command:

config ap cert-expiry-ignore mic enable

For more information, see this field notice: https://www.cisco.com/c/en/us/support/docs/field-notices/639/fn63942.html.

Authorizing Access Points against Local MAC Address

By default, the controller accepts AP authorization based on MIC and does not accept or require any other form of AP authorization. If you want to allow APs with SSCs to join, enable it, if you want APs with LSCs to join, enable it.

Mesh APs must be MAC authorized in addition to certificate authorized. For extra security, you can configure MAC authorization of other APs.

This section contains the following subsections:

Authorizing Access Points Using SSCs

Cisco APs manufactured prior to 2005 did not have MICs. Tools were provided to generate SSCs on older APs without MICs. Those tools and APs are no longer supported. All such SSCs expired on January 1, 2020. To allow the APs with the expired SSCs to join the controller, use the following command:

config ap cert-expiry-ignore ssc enable

This section contains the following subsections:

Authorizing Access Points for Virtual Controllers Using SSC

Virtual controllers use SSC certificates instead of Manufacturing Installed Certificates (MIC) used by physical controllers. You can configure the controller to allow an AP to validate the SSC of the virtual controller. When an AP validates the SSC, the AP checks if the hash key of the virtual controller matches the hash key stored in its flash. If a match is found, the AP associates with the controller. If a match is not found, the validation fails and the AP disconnects from the controller and restarts the discovery process. By default, hash validation is enabled. An AP must have the virtual controller hash key in its flash before associating with the virtual controller. If you disable hash validation of the SSC, the AP bypasses the hash validation and directly moves to the Run state. APs can associate with a physical controller, download the hash keys and then associate with a virtual controller. If the AP is associated with a physical controller and hash validation is disabled, the AP associates with any virtual controller without hash validation. The hash key of the virtual controller can be configured for a mobility group member. This hash key gets pushed to the APs, so that the APs can validate the hash key of the controller.

Note When a factory default AP tries to join the virtual controller, the SSC token does not get downloaded when AP joins initially. So once the AP gets registered with a controller, we need to reconfigure the SSC token to push it to the AP. The AP will then save the SSC token.

To push the SSC token to the AP, use the command

config certificate ssc auth-token *token*

Configuring SSC (GUI)

Procedure

Step 1 Choose **Security** > **Certificate** > **SSC** to open the Self Significant Certificates (SSC) page.

The SSC device certification details are displayed.

Step 2 Select the **Enable SSC Hash Validation** check box to enable the validation of the hash key.

Step 3 Click **Apply** to commit your changes.

Configuring SSC (CLI)

Procedure

Step 1 To configure hash validation of SSC, enter this command:

config certificate ssc hash validation {**enable** | **disable**}

Step 2 To see the hash key details, enter this command:

show certificate ssc

Authorizing Access Points Using MICs

You can configure controllers to use RADIUS servers to authorize access points using MICs. The controller uses an access point's MAC address as both the username and password when sending the information to a RADIUS server. For example, if the MAC address of the access point is 000b85229a70, both the username and password used by the controller to authorize the access point are 000b85229a70.

Authorizing Access Points Using LSCs

You can use an LSC if you want your own public key infrastructure (PKI) to provide better security, to have control of your certificate authority (CA), and to define policies, restrictions, and usages on the generated certificates.

The LSC CA certificate is installed on access points and controllers. You need to provision the device certificate on the access point. The access point gets a signed X.509 certificate by sending a certRequest to the controller. The controller acts as a CA proxy and receives the certRequest signed by the CA for the access point.

Guidelines and Restrictions

- Starting in Release 8.3.112.0, device certification is required to enable LSC. Due to this requirement, we recommend that you follow these guidelines:
  - Ensure that APs are provisioned with LSC for them to associate with LSC-enabled controllers.
  - Ensure that there is no mixed environment where some APs use MIC and some use LSC.
  - You do not have to specify the **Number of attempts to LSC** and **AP Ethernet MAC addresses**.

    For more information about this, see CSCve63755.
- When the CA server is in manual mode and if there is an AP entry in the LSC SCEP table that is pending enrollment, the controller waits for the CA server to send a pending response. If there is no response from the CA server, the controller retries a total of three times to get a response, after which the fallback mode comes into effect where the AP provisioning times out and the AP reboots and comes up with MIC.
- LSC on controller does not take password challenge. Therefore, for LSC to work, you must disable password challenge on the CA server.
- If you are using Cisco 3504 WLC and want to update device certificate, we recommend that you use Windows Server 2012 R2 as the certificate authority server. If you are using Windows Server 2008 R2 as the certificate authority server, there exists a known issue for which you must have a fix. For more information about this issue and the fix, see https://support.microsoft.com/en-us/help/2483564/renewal-request-for-an-scep-certificate-fails-in-windows-server-2008-r.

Configuring Locally Significant Certificates (GUI)

Procedure

Step 1 Choose **Security** > **Certificate** > **LSC** to open the Local Significant Certificates (LSC) - General page.

Step 2 In the CA Server URL text box, enter the URL to the CA server. You can enter either a domain name or an IP address.

Step 3 In the Params text boxes, enter the parameters for the device certificate. [Optional] The key size is a value from 2048 to 4096 (in bits), and the default value is 2048.

Step 4 Click **Apply** to commit your changes.

Step 5 To add the CA certificate into the controller's certificate database, hover your cursor over the blue drop-down arrow for the certificate type and choose **Add**.

Step 6 To add the device certificate into the controller's certificate database, hover your cursor over the blue drop-down arrow for the certificate type and choose **Add**.

Step 7 Select the **Enable LSC on Controller** check box to enable the LSC on the system.

Step 8 Click **Apply** to commit your changes.

Step 9 Choose the **AP Provisioning** tab to open the Local Significant Certificates (LSC) - AP Provisioning page.

Step 10 Select the **Enable** check box and click **Update** to provision the LSC on the access point.

Step 11 Click **Apply** to commit your changes.

Step 12 When a message appears indicating that the access points will be rebooted, click **OK**.

Step 13 In the **Number of Attempts to LSC** field, enter the number of times that the access point attempts to join the controller using an LSC before the access point reverts to the default certificate (MIC or SSC). The range is 0 to 255 (inclusive), and the default value is 3.

Note If you are using Release 8.3.112.0 or a later release, due to the requirement per CSCve63755, you do not have to perform this task. You must ensure that APs are provisioned with LSC prior to associating with LSC-enabled controllers.

Note If you set the number of retries to a nonzero value and the access point fails to join the controller using an LSC after the configured number of retries, the access point reverts to the default certificate. If you set the number of retries to 0 and the access point fails to join the controller using an LSC, the access point does not attempt to join the controller using the default certificate.

Note If you are configuring LSC for the first time, we recommend that you configure a nonzero value.

Step 14 Enter the access point MAC address in the **AP Ethernet MAC Addresses** field and click **Add** to add access points to the provision list.

Note If you are using Release 8.3.112.0 or a later release, due to the requirement per CSCve63755, you do not have to perform this task. You must ensure that APs are provisioned with LSC prior to associating with LSC-enabled controllers.

Note To remove an access point from the provision list, hover your cursor over the blue drop-down arrow for the access point and choose **Remove**.

Note If you configure an access point provision list, only the access points in the provision list are provisioned when you enable AP provisioning. If you do not configure an access point provision list, all access points with a MIC or SSC certificate that join the controller are LSC provisioned.

Step 15 Click **Apply** to commit your changes.

Step 16 Click **Save Configuration** to save your changes.

Configuring Locally Significant Certificates (CLI)

Procedure

Step 1 Configure the URL to the CA server by entering this command:

config certificate lsc ca-server *http://url:port/path*

where *url* can be either a domain name or IP address.

Note You can configure only one CA server. To configure a different CA server, delete the configured CA server using the **config certificate lsc ca-server delete** command, and then configure a different CA server.

Step 2 Configure the parameters for the device certificate by entering this command:

config certificate lsc subject-params *country state city orgn dept e-mail*

Note The common name (CN) is generated automatically on the access point using the current MIC/SSC format C*xxxx-MacAddr*, where *xxxx* is the product number.

Step 3 [Optional] Configure a key size by entering this command:

config certificate lsc other-params *keysize*

The *keysize* is a value from 2048 to 4096 (in bits), and the default value is 2048.

Step 4 Add the LSC CA certificate into the controller's certificate database by entering this command:

config certificate lsc ca-cert {**add** | **delete**}

Step 5 Add the LSC device certificate into the controller's certificate database by entering this command:

config certificate lsc device-cert {**add** | **delete**}

Step 6 Enable LSC on the system by entering this command:

config certificate lsc {**enable** | **disable**}

Step 7 Provision the LSC on the access point by entering this command:

config certificate lsc ap-provision {**enable | disable** }

Step 8 Configure the number of times that the access point attempts to join the controller using an LSC before the access point reverts to the default certificate (MIC or SSC) by entering this command:

config certificate lsc ap-provision revert-cert *retries*

where *retries* is a value from 0 to 255, and the default value is 3.

Note If you are using Release 8.3.112.0 or a later release, due to the requirement per CSCve63755, you do not have to perform this task. You must ensure that APs are provisioned with LSC prior to associating with LSC-enabled controllers.

Note If you set the number of retries to a nonzero value and the access point fails to join the controller using an LSC after the configured number of retries, the access point reverts to the default certificate. If you set the number of retries to 0 and the access point fails to join the controller using an LSC, the access point does not attempt to join the controller using the default certificate.

Note If you are configuring LSC for the first time, Cisco recommends that you configure a nonzero value.

Step 9 Add access points to the provision list by entering this command:

config certificate lsc ap-provision auth-list add *AP_mac_addr*

Note If you are using Release 8.3.112.0 or a later release, due to the requirement per CSCve63755, you do not have to perform this task. You must ensure that APs are provisioned with LSC prior to associating with LSC-enabled controllers.

Note To remove access points from the provision list, enter the **config certificate lsc ap-provision auth-list delete** *AP_mac_addr command.*

Note If you configure an access point provision list, only the access points in the provision list are provisioned when you enable AP provisioning (in *Step 8*). If you do not configure an access point provision list, all access points with a MIC or SSC certificate that join the controller are LSC provisioned.

Step 10 See the LSC summary by entering this command:

show certificate lsc summary

Information similar to the following appears:

```
LSC Enabled..................................... Yes
LSC CA-Server................................... http://10.0.0.1:8080/caserver

LSC AP-Provisioning............................. Yes
 Provision-List................................. Not Configured
 LSC Revert Count in AP reboots................. 3

LSC Params:
 Country........................................ US
 State.......................................... ca
 City........................................... ss
 Orgn........................................... org
 Dept........................................... dep
 Email.......................................... dep@co.com
 KeySize........................................ 2048

LSC Certs:
 CA Cert........................................ Not Configured
 RA Cert..................................... Not Configured
```

Step 11 See details about the access points that are provisioned using LSC by entering this command:

show certificate lsc ap-provision

Information similar to the following appears:

```
LSC AP-Provisioning..................... Yes
Provision-List.......................... Present

Idx  Mac Address
---  ------------
1  00:18:74:c7:c0:90
```

Authorizing Access Points (GUI)

Procedure

Step 1 Choose **Security** > **AAA** > **AP Policies** to open the **AP Policies** page.

Step 2 If you want the access point to accept self-signed certificates (SSCs), manufactured-installed certificates (MICs), or local significant certificates (LSCs), select the appropriate check box.

Step 3 If you want the access points to be authorized using a AAA RADIUS server, check the **Authorize MIC APs against auth-list or AAA** check box.

Step 4 If you want the access points to be authorized using an LSC, check the **Authorize LSC APs against auth-list** check box.

Enter the Ethernet MAC address for all APs except when in bridge mode (where you need to enter the radio MAC address).

Step 5 Click **Apply** to commit your changes.

Step 6 Follow these steps to add an access point to the controller's authorization list:

a) Click **Add** to access the **Add AP to Authorization List** area.
b) In the **MAC Address** field, enter the MAC address of the access point.
c) From the **Certificate Type** drop-down list, choose **MIC**, **SSC**, or **LSC**.
d) Click **Add**. The access point appears in the access point authorization list.

Note To remove an access point from the authorization list, hover your cursor over the blue drop-down arrow for the access point and choose **Remove**.

Note To search for a specific access point in the authorization list, enter the MAC address of the access point in the Search by MAC text box and click **Search**.

Authorizing Access Points (CLI)

Procedure

- Configure an access point authorization policy by entering this command:

  config auth-list ap-policy {**authorize-ap** {**enable** | **disable**} | **authorize-lsc-ap** {**enable** | **disable**}}

- Configure an access point to accept manufactured-installed certificates (MICs), self-signed certificates (SSCs), or local significant certificates (LSCs) by entering this command:

  config auth-list ap-policy {**mic | ssc** | **lsc** {**enable** | **disable**}}

- Configure the user name to be used in access point authorization requests.

  config auth-list ap-policy {**authorize-ap username** {**ap_name** | **ap_mac** | **both**}}

- Add an access point to the authorization list by entering this command:

  config auth-list add {**mic** | **ssc** | **lsc**} *ap_mac* [*ap_key*]

  where *ap_key* is an optional key hash value equal to 20 bytes or 40 digits.

Note To delete an access point from the authorization list, enter this command: **config auth-list delete ap_mac**.

- See the access point authorization list by entering this command:

  show auth-list

Plug and Play (PnP)

PnP solution provides staging parameters to the AP before it joins a controller. Using this staging configuration, the AP gets the runtime configuration when it joins the controller. PNP is activated on AP only if the AP is fresh out-of-box or reset to the factory default. PnP is not initiated after the AP connects to the controller for the first time.

PnP IPv4 functionality is supported on Cisco Aironet 700, 1700, 2700, and 3700 series APs.

Both PnP IPv4 and IPv6 functionalities are supported on Cisco Wave 2 802.11ax Wi-Fi6 APs. For more information about specifc APs that support PnP, see https://www.cisco.com/c/en/us/td/docs/wireless/access_point/feature-matrix/ap-feature-matrix.html.

AP PnP Scenarios

- On-Premise Redirection—Customer hosting the PNP server in the customer-internal network. APs discover the PnP server using the DHCP option or DNS resolution.

Note For AP time sync with the controller, configure the controller NTP server with a reachable NTP IP address. APs do not support FQDN in a day0 scenario.

- Cloud Redirection—APs are connected to the third-party network where customers do not have control over the DHCP or DNS, or do not host the PNP server. In this scenario, AP connects to the Cisco Cloud redirect service to get either the controller or PnP address. The controller address is configured in the redirect service for customers without the PnP server.

For more information about PnP, see the documentation for *Wireless Plug and Play Deployment Guide* at http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-4/b_wireless_plug_and_play_deployment_guide.html.

AP Wired 802.1X Supplicant

IEEE 802.1X port-based authentication is configured on a device to prevent unauthorized devices (supplicants) from gaining access to the network. The device can combine the function of an access point, depending on the fixed configuration or installed modules.

Here, the Cisco switch is the authenticator; the Cisco AP is the supplicant, and the RADIUS/ISE server the authentication server. You may enable one of the three protocols—EAP-TLS, EAP-PEAP, or EAP-FAST on the controller to authenticate the supplicant devices (APs).

The EAP-TLS protocol uses the client certificate to authenticate the device. On the other hand, the EAP-PEAP protocol uses the client key exchange to authenticate the AP. This is after the AP is provisioned with the LSC certificate to validate the server certificate.

Cisco APs use the LSC provisioning method to download the vendor device and CA certificate to the AP. These certificates help authenticate the Cisco AP to use the switch port with EAP-TLS or PEAP protocol for data traffic.

The deployment occurs in two stages.

First, the Cisco APs are configured with 802.1X credentials, EAP method, and the LSC from the controller. In the second stage, the AP 802.1X enabled switch port passes the 802.1X authentication process to join the controller and begin serving data traffic.

Note Each time the dot1x user or the EAP method is changed the AP will restart the authentication process.

You can configure global authentication settings that all access points that are currently associated with the controller and any that associate in the future. You can also override the global authentication settings and assign unique authentication settings for a specific access point.

After the 802.1X authentication is configured on the switch, it allows 802.1X authenticated device traffic only.

There are two modes of authentication models:

- Global authentication—authentication setup for all APs
- AP Level authentication—authentication setup for a particular AP

The switch by default authenticates one device per port. This limitation is not present in the Cisco Catalyst Switches. The host mode type configured on the switch determines the number and type of endpoints allowed on a port. The host mode options are:

- Single host mode-a single IP or MAC address is authenticated on a port. This is set as the default.
- Multi-host mode-authenticates the first MAC address and then allows an unlimited number of other MAC addresses. Enable the host mode on the switch ports if connected AP has been configured with local switching mode. It allows the client's traffic pass the switch port. If you want a secured traffic path, then enable dot1x on the WLAN to protect the client data.

  The feature supports AP in local mode, FlexConnect mode, sniffer mode, and monitor mode. It also supports WLAN in central switching and local switching modes.

Note In FlexConnect mode, ensure that the VLAN support is enabled on the AP the correct native VLAN is configured on it.

Table 2: Deployment Options

802.1X on AP	Switch	Result
DISABLED	ENABLED	AP does not join the controller
ENABLED	DISABLED	AP joins the controller. After failing to receive EAP responses, fallbacks to non-dot1x CAPWAP discovery automatically
ENABLED	ENABLED	AP joins the controller, post port-Authentication

In a situation where the credentials on the AP need correction, disable the Switch port Dot1x Authentication, and re-enable the port authentication after updating the credentials.

This section contains the following subsections:

Prerequisites for Configuring Wired 802.1X Authentication for Access Points

Procedure

Step 1 If the AP is new, do the following:

a) Boot the AP with the installed lightweight AP image.

b) If you choose not to follow this suggested flow and instead enable 802.1X authentication on the switch port connected to the AP prior to the AP joining the controller, enter this command:

capwap ap dot1x username *username* **password** *password*

Note If you choose to follow this suggested flow and enable 802.1X authentication on the switch port after the AP has joined the controller and received the configured 802.1X credentials, you do not need to enter this command.

Note This command is available only for access points that are running the applicable recovery image.

Connect the AP to the switch port.

Note While ISE communicates with AP (acting as supplicant), the password policy criteria needs to be applied to the ISE. As AP 802.1X supplicant follows an authenticator password policy and cannot have a password criteria of their own.

Step 2 Install the required software image on the controller and reboot the controller.

Step 3 Allow all access points to join the controller.

Step 4 Configure authentication on the controller.

Step 5 Configure the switch to allow authentication.

Restrictions for Authenticating Access Points

- Always disable the Bridge Protocol Data Unit (BPDU) guard on the switch port connected to the AP. Enabling the BPDU guard is allowed only when the switch puts the port in port fast mode.
- Cisco Wave 1 APs supports only EAP-FAST authentication method.
- Trunk ports, dynamic ports, or EtherChannel ports are not supported.
- Certificate revocation checks are not implemented on the AP.
- Limited to only one LSC certificate which can be downloaded or provisioned on the AP.
- Cisco APs in bridge mode or Flex+bridge mode is not supported.
- Network Edge Authentication Topology (NEAT) is not supported.
- Client Information Signaling Protocol (CISP) is not supported.
- Downgrade from Cisco Release 8.7 to earlier version changes the EAP method on the Cisco AP to EAP-FAST (default).

- The EAP method needs to be manually deleted and set to default EAP-FAST method when dot1x credentials are deleted. Enter one of the following commands to set the default method.
  - **config ap 802.1Xuser eap-method delete** {**eap-fast | eap-tls | peap**} *ap-name*—Sets the Cisco AP specific method to static EAP-FAST
  - **config ap 802.1Xuser eap-method delete** {**eap-fast | eap-tls | peap all**}—Sets the global EAP method to static EAP-FAST

Configuring 802.1X Authentication Protocols for All Access Points (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration** to open the **Global Configuration** page.

Step 2 Under 802.1x Supplicant Credentials, select the **802.1x Authentication** check box.

Step 3 In the Username text box, enter the username that is to be inherited by all access points that join the controller.

Step 4 In the Password and Confirm Password text boxes, enter the password that is to be inherited by all access points that join the controller.

Note You must enter a strong password in these text boxes. Strong passwords have the following characteristics:

- They are at least eight characters long
- They contain a combination of uppercase and lowercase letters, numbers, and symbols
- They are not a word in any language

Step 5 From the EAP Method drop down list, choose from the following protocol options:

- EAP-FAST
- EAP-TLS
- PEAP

Step 6 Click **Apply** to send the global authentication username and password to all access points that are currently joined to the controller and to any that join the controller in the future.

Step 7 Click **Save Configuration** to save your changes.

Configuring 802.1X Authentication Protocols for All Access Points (CLI)

Procedure

- Configure the global authentication username and password for all access points by entering this command:
  config ap 802.1Xuser add username *ap-username* **password** *ap-password* **all**

Note You must enter a strong password for the *ap-password* parameter. Strong passwords have the following characteristics:

- They are at least eight characters long.
- They contain a combination of uppercase and lowercase letters, numbers, and symbols.
- They are not a word in any language.

- Configure the 802.1x EAP method for all access points by entering this command

  config ap 802.1Xuser eap-method add {**eap-fast | eap-tls | peap** }**all**

- (Optional) Delete the EAP method explicitly after deleting dot1x credentials. Use the following delete command to set the default (EAP-FAST) method.
  - Set the global EAP method to static EAP-FAST:

    config ap 802.1Xuser eap-method delete {**eap-fast | eap-tls | peap**} **all**

- (Optional) Disable 802.1X authentication for all access points or for a specific access point by entering this command:

  config ap 802.1Xuser disable {**all** | *Cisco_AP*}

Note You can disable 802.1X authentication for a specific access point only if global 802.1X authentication is not enabled. If global 802.1X authentication is enabled, you can disable 802.1X for all access points only.

- View the authentication settings for all access points that join the controller by entering this command:

  show ap summary

  Information similar to the following appears:

```
Number of APs.................................. 1
Global AP User Name............................ globalap
Global AP Dot1x User Name...................... globalDot1x
```

- See the authentication status on the AP by entering this command:

  show authentication interface wired-port status

Configuring 802.1X Authentication Protocols for An Access Point (GUI)

Procedure

Step 1 Choose **Access Points** > **All APs** to open the All APs page.

Step 2 Click the name of the access point for which you want to override the authentication settings.

Step 3 Click the **Credentials** tab to open the All APs > Details for (Credentials) page.

Step 4 Under 802.1x Supplicant Credentials, select the **Over-ride Global Credentials** check box to prevent this access point from inheriting the global authentication username and password from the controller. The default value is unselected.

Step 5 In the Username, Password, and Confirm Password text boxes, enter the unique username and password that you want to assign to this access point.

Note The information that you enter is retained across controller and access point reboots and whenever the access point joins a new controller.

Note If you want to force this access point to use the controller's global authentication settings, unselect the **Over-ride Global Credentials** check box.

Step 6 From the EAP Method drop down list, choose from the following protocol options:

- EAP-FAST
- EAP-TLS
- PEAP

Step 7 Click **Apply** to send the global authentication username and password to all access points that are currently joined to the controller and to any that join the controller in the future.

Step 8 Click **Save Configuration** to save your changes.

Configuring 802.1X Authentication Protocols for An Access Point (CLI)

Procedure

- Override the global authentication settings and assign a unique username and password to a specific access point by entering this command:

  config ap 802.1Xuser add username *ap-username* **password** *ap-password Cisco_AP*

Note You must enter a strong password for the *ap-password* parameter. Strong passwords have the following characteristics:

- They are at least eight characters long.
- They contain a combination of uppercase and lowercase letters, numbers, and symbols.
- They are not a word in any language.

The authentication settings that you enter in this command are retained across controller and access point reboots and whenever the access point joins a new controller.

- Configure the 802.1x EAP method for a specific access point by entering this command:

  config ap 802.1Xuser eap-method add {**eap-fast | eap-tls | peap**} *ap-name*

- (Optional) Delete the EAP method explicitly after deleting dot1x credentials. Use the following delete commands to set the default (EAP-FAST) method.
  - **config ap 802.1Xuser eap-method delete** {**eap-fast | eap-tls | peap**} *ap-name*—Sets the Cisco AP specific method to static EAP-FAST
- Enter the **save config** command to save your changes.
- (Optional) Disable 802.1X authentication for all access points or for a specific access point by entering this command:

  config ap 802.1Xuser disable {**all** | *Cisco_AP*}

Note You can disable 802.1X authentication for a specific access point only if global 802.1X authentication is not enabled. If global 802.1X authentication is enabled, you can disable 802.1X for all access points only.

- See the authentication settings for a specific access point by entering this command:

  show ap config general *Cisco_AP*

Note The name of the access point is case sensitive.

Note If this access point is configured for global authentication, the AP Dot1x User Mode text boxes shows "Automatic." If the global authentication settings have been overwritten for this access point, the AP Dot1x User Mode text box shows "Customized."

- See the authentication status on the AP by entering this command:

  show authentication interface wired-port status

Configuring LSC Authentication State (GUI)

Use this procedure to configure the AP to use the LSC certificate when the controller is configured with 802.1x port authentication with a RADIUS server.

Procedure

Step 1 Choose **Security** > **Certificate** > **LSC** to open the **Local Significant Certificates (LSC)** page.

Step 2 Choose the **AP Provisioning** tab to open the **AP Provisioning** page.

Step 3 From the **LSC AP Auth State** drop down list, choose one of the options:

- 802.1x AP port authentication
- APWAP-DTLS
- 802.1x+CAPWAP-DTLS

Step 4 Click **Apply**.

Configuring LSC Authentication State (CLI)

Procedure

- Configure the LSC certificate authentication state by entering this command:
  config certificate lsc ap-auth-state {**capwap_dtls** | **dot1x_port_auth** | **both**}
- View the status of the LSC Certificate by entering this command:

  show certificate lsc summary

Adding AP to an LSC Provisioned Network

When you need to add new Cisco APs to an already active LSC-provisioned network, there are two methods to achieve this with no downtime:

Procedure

- Method One:
  1. Associate the new APs to a VLAN which is linked to the LSC provisioning controller.
  2. Download the LSC certificate and configuration on to the Cisco APs.
  3. Associate these APs to the production VLAN.
- Method Two:
  1. Connect the new APs to a dedicated switch port for provisioning LSC certificate.
  2. Download the LSC certificate and configuration on to the Cisco APs.
  3. Connect these APs to the production switch port.

Configuring the Switch for Authentication

To enable 802.1X authentication on a switch port, on the switch CLI, enter these commands:

- Switch# **configure terminal**
- Switch(config)# **dot1x system-auth-control**
- Switch(config)# **aaa new-model**
- Switch(config)# **aaa authentication dot1x default group radius**
- Switch(config)# **radius-server host** *ip_addr* **auth-port** *port* **acct-port** *port* **key** *key*
- Switch(config)# **interface fastethernet2/1**

- Switch(config-if)# **switchport mode access**
- Switch(config-if)# **dot1x pae authenticator**
- Switch(config-if)# **dot1x port-control auto**
- Switch(config-if)# **end**

Configuring a Static IP Address on a Lightweight Access Point

If you want to specify an IP address for an access point rather than having one assigned automatically by a DHCP server, you can use the controller GUI or CLI to configure a static IP address for the access point. Static IP addresses are generally used only for deployments with a limited number of APs.

An access point cannot discover the controller using domain name system (DNS) resolution if a static IP address is configured for the access point, unless you specify a DNS server and the domain to which the access point belongs.

Note If you configure an access point to use a static IP address that is not on the same subnet on which the access point's previous DHCP address was, the access point falls back to a DHCP address after the access point reboots. If the access point falls back to a DHCP address, enter the **show ap config general** *Cisco_AP* CLI command to show that the access point is using a fallback IP address. However, the GUI shows both the static IP address and the DHCP address, but it does not identify the DHCP address as a fallback address.

Configuring a Static IP Address (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 2 Click the name of the access point for which you want to configure a static IP address. The All APs > Details for (General) page appears.

Step 3 Under IP Config, select the **Static IP (IPv4/IPv6)** check box if you want to assign a static IP address to this access point. The default value is unselected.

Note The static IP configured on the AP will take precedence over the preferred mode configured on the AP. For example: If AP has static IPV6 address and prefer-mode is set to IPV4, then the AP will join over IPv6.

Step 4 Enter the static IPv4/IPv6 address of the access point, subnet mask/ prefix length assigned to the access point IPv4/IPv6 address, and the IPv4/IPv6 gateway of the access point in the corresponding text boxes.

Step 5 Click **Apply** to commit your changes. The access point reboots and rejoins the controller, and the static IPv4/IPv6 address that you specified in Step 4 is sent to the access point.

Step 6 After the static IPv4/IPv6 address has been sent to the access point, you can configure the DNS server IP address and domain name as follows:

a) In the DNS IP Address text box, enter the IPv4/IPv6 address of the DNS server.
b) In the Domain Name text box, enter the name of the domain to which the access point belongs.

c) Click **Apply** to commit your changes.
d) Click **Save Configuration** to save your changes.

Configuring a Static IP Address (CLI)

Procedure

Step 1 Configure a static IP address on the access point by entering this command:

For IPv4—**config ap static-ip enable** *Cisco_AP ip_address mask gateway*

For IPv6—**config ap static-ip enable** *Cisco_AP ip_address prefix_length gateway*

Note To disable static IP for the access point, enter the **config ap static-ip disable** *Cisco_AP* command.

Note The static IP configured on the AP takes precedence over the preferred mode that is configured on the AP. For example: If AP has static IPv6 address and prefer-mode is set to IPv4, then the AP will join over IPv6.

Step 2 Enter the **save config** command to save your changes.

The access point reboots and rejoins the controller, and the static IP address that you specified in Step 1 is pushed to the access point.

Step 3 After the static IPv4/IPv6 address has been sent to the access point, you can configure the DNSv4/DNSv6 server IP address and domain name as follows:

a) To specify a DNSv4/DNSv6 server so that a specific access point or all access points can discover the controller using DNS resolution, enter this command:

config ap static-ip add nameserver {*Cisco_AP* | **all**} *ip_address*

Note To delete a DNSv4/DNSv6 server for a specific access point or all access points, enter the **config ap static-ip delete nameserver** {*Cisco_AP* | **all**} command.

b) To specify the domain to which a specific access point or all access points belong, enter this command:

config ap static-ip add domain {*Cisco_AP* | **all**} *domain_name*

Note To delete a domain for a specific access point or all access points, enter this command: **config ap static-ip delete domain** {*Cisco_AP* | **all**}.

c) Enter the **save config** command to save your changes.

Step 4 See the IPv4/IPv6 address configuration for the access point by entering this command:

- For IPv4:

  show ap config general *Cisco_AP*

  Information similar to the following appears:

```
show ap config general <Cisco_AP>

Cisco AP Identifier.............................. 4
Cisco AP Name.................................... AP6
...
```

```
IP Address Configuration..................... Static IP assigned
IP Address................................... 10.10.10.118
IP NetMask................................... 255.255.255.0
Gateway IP Addr.............................. 10.10.10.1

Domain....................................... Domain1
Name Server.................................. 10.10.10.205
...
```

- For IPv6:

  show ap config general *Cisco_AP*

  Information similar to the following appears:

```
show ap config general <Cisco_AP>

Cisco AP Identifier.............................. 16
Cisco AP Name.................................... AP2602I-A-K9-1
...
IPv6 Address Configuration....................... DHCPv6
IPv6 Address..................................... 2001:9:2:16:1ae:a1da:c2c7:44b
IPv6 Prefix Length............................... 128
Gateway IPv6 Addr................................ fe80::c60a:cbff:fe79:53c4
NAT External IP Address.......................... None

...
IPv6 Capwap UDP Lite............................. Enabled
Capwap Prefer Mode............................... Ipv6 (ApGroup Config)
Hotspot Venue Group.............................. Unspecified
Hotspot Venue Type............................... Unspecified
DNS server IP ..................... Not Available
```

Troubleshooting the Access Point Join Process

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

Controller software release 5.2 or later releases enable you to 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 controller 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 controller 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 controller, the controller collects information for all access points that send a discovery message to this controller and maintains information for any access points that have successfully joined this controller.

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

You can view join-related information for the following numbers of access points:

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

If any of these conditions are met and the access point has not yet joined a controller, 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.

Note The access point joins the controller with a DHCP address from an internal DHCP pool configured on WLC. When the DHCP lease address is deleted in WLC, the access point reloads with the following message:

AP Rebooting: Reset Reason - Admin Reload. This is a common behavior in Cisco Wave 1 and Wave 2 APs.

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

When the access point joins a controller for the first time, the controller 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 controller, and the global syslog server IP address configuration on the controller has been changed using the **config ap syslog host global** *syslog_server_IP_address* command. In this case, the controller pushes the new global syslog server IP address to the access point.
- The access point is still connected to the same controller, and a specific syslog server IP address has been configured for the access point on the controller using the **config ap syslog host specific** *Cisco_AP syslog_server_IP_address* command. In this case, the controller pushes the new specific syslog server IP address to the access point.
- The access point gets disconnected from the controller, and the syslog server IP address has been configured from the access point CLI using the **lwapp ap log-server** *syslog_server_IP_address* command. This command works only if the access point is not connected to any controller.
- The access point gets disconnected from the controller and joins another controller. In this case, the new controller 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, provided the access point can reach the syslog server IP address.

You can configure the syslog server for access points using the controller GUI and view the access point join information using the controller GUI or CLI.

When the name of the access point is modified using the **config ap name** *new_name old_name* command, then the new AP name is updated. You can view the new AP name updated in both the **show ap join stats summary all** as well as the **show ap summary** commands.

Note When an AP in a Release 8.0 image tries to join Cisco WLC, Release 8.3 (having Release 8.2 as the primary image and Release 8.2.1 as the secondary image on Flash), the AP goes into a perpetual loop. (Note that the release numbers are used only as an example to illustrate the scenario of three different images and does not apply to the releases mentioned.) This loop occurs due to version mismatch. After the download, when the AP compares its image with the Cisco WLC image, there will be a version mismatch. The AP will start the entire process again, resulting in a loop.

Configuring the Syslog Server for Access Points (CLI)

Procedure

Step 1 Perform one of the following:

- To configure a global syslog server for all access points that join this controller, enter this command:

  config ap syslog host global *syslog_server_IP_address*

  Note By default, the global syslog server IPv4/IPv6 address for all access points is 255.255.255.255. Make sure that the access points can reach the subnet on which the syslog server resides before configuring the syslog server on the controller. If the access points cannot reach this subnet, the access points are unable to send out syslog messages.

  Note Only one Syslog Server is used for both IPv4 and IPv6.

- To configure a syslog server for a specific access point, enter this command:

  config ap syslog host specific *Cisco_AP syslog_server_IP_address*

  Note By default, the syslog server IPv4/IPv6 address for each access point is 0.0.0.0, which indicates that the access point is not yet set. When the default value is used, the global access point syslog server IP address is pushed to the access point.

Step 2 Enter the **save config** command to save your changes.

Step 3 See the global syslog server settings for all access points that join the controller by entering this command:

show ap config global

Information similar to the following appears:

```
AP global system logging host..................... 255.255.255.255
```

Step 4 See the syslog server settings for a specific access point by entering this command:

show ap config general *Cisco_AP*

Viewing Access Point Join Information

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

Viewing Access Point Join Information (GUI)

Procedure

Step 1 Choose **Monitor** > **Statistics** > **AP Join** to open the AP Join Stats page.

This page lists all of the access points that are joined to the controller or that have tried to join. It shows the radio MAC address, access point name, current join status, Ethernet MAC address, IP address, and last join time for each access point.

The total number of access points appears in the upper right-hand corner of the page. If the list of access points spans multiple pages, you can view these pages by clicking the page number links. Each page shows the join statistics for up to 25 access points.

Note If you want to remove an access point from the list, hover your cursor over the blue drop-down arrow for that access point and click **Remove**.

Note If you want to clear the statistics for all access points and start over, click **Clear Stats on All APs**.

Step 2 If you want to search for specific access points in the list of access points on the AP Join Stats page, follow these steps to create a filter to display only access points that meet certain criteria (such as MAC address or access point name).

Note This feature is especially useful if your list of access points spans multiple pages, preventing you from viewing them all at once.

a) Click **Change Filter** to open the Search AP dialog box.
b) Select one of the following check boxes to specify the criteria used when displaying access points:

- **MAC Address**—Enter the base radio MAC address of an access point.
- **AP Name**—Enter the name of an access point.

Note When you enable one of these filters, the other filter is disabled automatically.

c) Click **Find** to commit your changes. Only the access points that match your search criteria appear on the AP Join Stats page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC Address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

Note If you want to remove the filter and display the entire access point list, click **Clear Filter**.

Step 3 To see detailed join statistics for a specific access point, click the radio MAC address of the access point. The AP Join Stats Detail page appears.

This page provides information from the controller's perspective on each phase of the join process and shows any errors that have occurred.

Viewing Access Point Join Information (CLI)

Use these CLI commands to see access point join information:

- See the MAC addresses of all the access points that are joined to the controller or that have tried to join by entering this command:

  show ap join stats summary all

- See the last join error detail for a specific access point by entering this command:

  show ap join stats summary *ap_mac*

  where *ap_mac* is the MAC address of the 802.11 radio interface.

Note To obtain the MAC address of the 802.11 radio interface, enter the **show interfaces Dot11Radio 0** command on the access point.

Information similar to the following appears:

```
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
```

- See all join-related statistics collected for a specific access point by entering this command:

  show ap join stats detailed *ap_mac*

  Information similar to the following appears:

```
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
```

- Clear the join statistics for all access points or for a specific access point by entering this command:

  clear ap join stats {**all** | *ap_mac*}