Using Access Point Communication Protocols

- Information About Access Point Communication Protocols, page 1
- Restrictions for Access Point Communication Protocols, page 2
- Configuring Data Encryption, page 2
- Viewing CAPWAP Maximum Transmission Unit Information, page 5
- Debugging CAPWAP, page 6
- Controller Discovery Process, page 6
- Verifying that Access Points Join the Controller, page 7

Information About Access Point Communication Protocols

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 only exceptions are that the Cisco Aironet 1040, 1140, 1260, 3500, and 3600 Series Access Points, which support only CAPWAP and join only controllers that run CAPWAP. For example, an 1130 series access point can join a controller running either CAPWAP or LWAPP where an1140 series access point can join only a controller that runs CAPWAP.
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.

### Restrictions for Access Point Communication Protocols

- On virtual controller platforms, per-client downstream rate limiting is not supported in FlexConnect central switching.
- 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 access points, the access point fails to join the controller.

### Configuring Data Encryption

Cisco 5500 Series Controllers enable you to encrypt CAPWAP control packets (and optionally, CAPWAP data packets) that are sent between the access point 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.

> **Note**

With Release 8.2, DTLSv1.2 for CAPWAP is not supported. The following are supported for web authentication and WebAdmin based on the configuration:

- TLSv1.2
- TLSv1.0
- SSLv3
- SSLv2
Cisco WLC supports only static configuration of gateway. Therefore, the ICMP redirect to change IP address of the gateway is not considered.

Guidelines for Data Encryption

- Cisco 1130 and 1240 series access points support DTLS data encryption with software-based encryption.
- Cisco 1040, 1140, 1250, 1260, 1530, 1550, 1600, 1700, 2600, 2700, 3500, 3600, and 3700 series access points support DTLS data encryption with hardware-based encryption.
- Cisco Aironet 1552 and 1522 outdoor access points support data DTLS.
- DTLS data encryption is not supported on Cisco Aironet 700 Series Access Points.
- 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.
- In a Cisco unified local wireless network environment, do not enable DTLS on the Cisco 1130 and 1240 access points, as it may result in severe throughput degradation and may render the APs unusable. See the OfficeExtend Access Points section for more information on OfficeExtend access points.
- You can use the controller to enable or disable DTLS data encryption for a specific access point or for all access points.
- The availability of data DTLS is as follows:
  - The Cisco 5500 Series Controller will be available with two license options: One that allows data DTLS without any license requirements and another image that requires a license to use data DTLS. See the Upgrading or Downgrading DTLS Images for Cisco 5508 WLC section. The images for the DTLS and licensed DTLS images are as follows:
    - Licensed DTLS—AS_5500_LDPE_x_x_x_x.aes
    - Non licensed DTLS—AS_5500_x_x_x_x.aes
  - Cisco 2500, Cisco WiSM2, Cisco Virtual Wireless Controller—By default, these platforms do not contain DTLS. To turn on data DTLS, you must install a license. These platforms have a single image with data DTLS turned off. To use data DTLS you must have a license.
    - For Cisco Virtual Wireless Controllers without Data DTLS, the average controller throughput is about 200 Mbps. With all APs using Data DTLS, the average controller throughput is about 100 Mbps.
- 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.
• Non-Russian customers using Cisco 5508 Series Controller do not need data DTLS license. However all customers using Cisco 2500 Series Controllers, Cisco 8500 Series Controllers, WISM2, and Cisco Virtual Wireless Controllers need a data DTLS license to turn on the Data DTLS feature.

Upgrading or Downgrading DTLS Images for Cisco 5508 WLC

Step 1
The upgrade operation fails on the first attempt with a warning indicating that the upgrade to a licensed DTLS image is irreversible.
Note Do not reboot the controller after Step 1.

Step 2
On a subsequent attempt, the license is applied and the image is successfully updated.

Guidelines When Upgrading to or from a DTLS Image

• You cannot install a regular image (nonlicensed data DTLS) once a licensed data DTLS image is installed.
• You can upgrade from one licensed DTLS image to another licensed DTLS image.
• You can upgrade from a regular image (DTLS) to a licensed DTLS image in a two step process.
• You can use the show sysinfo command to verify the LDPE image, before and after the image upgrade.

Configuring Data Encryption (GUI)

Ensure that the base license is installed on the Cisco 5500 Series Controller. Once the license is installed, you can enable data encryption for the access points.

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 enable data encryption.

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

Step 4
Select 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
Click Apply.

Step 6
Click Save 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:

**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}
```

**Step 7**
See the summary of DTLS cipher suite by entering this command:
```
show ap dtls-cipher-suite
```

---

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
```
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.

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:

• Upgrade and downgrade paths from LWAPP to CAPWAP or from CAPWAP to LWAPP are supported. An access point with an LWAPP image starts the discovery process in LWAPP. If it finds an LWAPP controller, it starts the LWAPP discovery process to join the controller. If it does not find a LWAPP controller, it starts the discovery in CAPWAP. If the number of times that the discovery process starts with one discovery type (CAPWAP or LWAPP) exceeds the maximum discovery count and the access point does not receive a discovery response, the discovery type changes to the other type. For example, if the access point does not discover the controller in LWAPP, it starts the discovery process in CAPWAP.
• 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.
• 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.
• 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 than 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. For more information about DHCP option 43, see the “Using DHCP Option 43 and DHCP Option 60” section.

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.

Restrictions for Controller Discovery Process

- During the discovery process, the 1040, 1140, 1260, 3500, and 3600 series access points will only query for Cisco CAPWAP Controllers. It will not query for LWAPP controllers. If you want these access points to query for both LWAPP and CAPWAP controllers then you need to update the DNS.

- 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.

- 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 background. If the discovery with primary is successful, it goes back and joins the primary again.

Verifying that Access Points Join the Controller

When replacing a controller, ensure that access points join the new controller.
Verifying that Access Points Join the Controller (GUI)

**Step 1** Configure the new controller as a master controller as follows:

a) Choose **Controller > Advanced > Master Controller Mode** to open the Master Controller Configuration page.

b) Select the **Master Controller Mode** check box.

c) Click **Apply** to commit your changes.

d) Click **Save Configuration** to save your changes.

**Step 2** (Optional) Flush the ARP and MAC address tables within the network infrastructure.

**Step 3** Restart the access points.

**Step 4** Once all the access points have joined the new controller, configure the controller not to be a master controller by unselecting the **Master Controller Mode** check box on the Master Controller Configuration page.

---

Verifying that Access Points Join the Controller (CLI)

**Step 1** Configure the new controller as a master controller by entering this command:

```
config network master-base enable
```

**Step 2** (Optional) Flush the ARP and MAC address tables within the network infrastructure.

**Step 3** Restart the access points.

**Step 4** Configure the controller not to be a master controller after all the access points have joined the new controller by entering this command:

```
config network master-base disable
```