# AP Power and Uplink LAN Connections



# Power over Ethernet

This section contains the following subsections:

## Configuring Power over Ethernet (GUI)

**Procedure**

**Step 1** Choose **Wireless** > **Access Points** > **All APs** and then the name of the desired access point.

**Step 2** Choose the **Advanced** tab to open the **All APs > Details for (Advanced)** page.

The **PoE Status** text box shows the power level at which the access point is operating: High (20 W), Medium (16.8 W), or Medium (15.4 W). This text box is not configurable. The controller auto-detects the access point's power source and displays the power level here.

**Note** This text box applies only to 1250 series access points that are powered using PoE. There are two other ways to determine if the access point is operating at a lower power level. First, the "Due to low PoE, radio is transmitting at degraded power" message appears under the Tx Power Level Assignment section on the 802.11a/n/ac (or 802.11b/g/n) **Cisco APs > Configure** page. Second, the "PoE Status: degraded operation" message appears in the controller's trap log on the Trap Logs page.

**Step 3** Perform one of the following:

- Check the **Pre-standard 802.3af switches** check box if the access point is being powered by a high-power 802.3af Cisco switch. This switch provides more than the traditional 6 Watts of power but do not support the intelligent power management (IPM) feature.
- Uncheck the **Pre-standard 802.3af switches** check box if power is being provided by a power injector. This is the default value.

**Step 4** Check the **Power Injector State** check box if the attached switch does not support IPM and a power injector is being used. If the attached switch supports IPM, you do not need to select this check box.

**Step 5** If you selected the Power Injector State check box in the previous step, the Power Injector Selection and Injector Switch MAC Address parameters appear. The Power Injector Selection parameter enables you to protect your switch port from an accidental overload if the power injector is inadvertently bypassed. Choose one of these options from the drop-down list to specify the desired level of protection:

- **Installed**—This option examines and remembers the MAC address of the currently connected switch port and assumes that a power injector is connected. Choose this option if your network contains older Cisco 6-Watt switches and you want to avoid possible overloads by forcing a double-check of any relocated access points.

  If you want to configure the switch MAC address, enter the MAC address in the Injector Switch MAC Address text box. If you want the access point to find the switch MAC address, leave the Injector Switch MAC Address text box blank.

  **Note** Each time an access point is relocated, the MAC address of the new switch port fails to match the remembered MAC address, and the access point remains in low-power mode. You must then physically verify the existence of a power injector and reselect this option to cause the new MAC address to be remembered.

- **Override**—This option allows the access point to operate in high-power mode without first verifying a matching MAC address. You can use this option if your network does not contain any older Cisco 6-W switches that could be overloaded if connected directly to a 12-W access point. The advantage of this option is that if you relocate the access point, it continues to operate in high-power mode without any further configuration. The disadvantage of this option is that if the access point is connected directly to a 6-W switch, an overload occurs.

**Step 6** Click **Apply**.

**Step 7** If you have a dual-radio 1250 series access point and want to disable one of its radios in order to enable the other radio to receive full power, follow these steps:

a) Choose **Wireless** > **Access Points** > **Radios** > **802.11a/n/**/ac or **802.11b/g/n** to open the 802.11a/n/ac (or 802.11b/g/n) Radios page.
b) Hover your cursor over the blue drop-down arrow for the radio that you want to disable and choose **Configure**.
c) On the 802.11a/n/ac (or 802.11b/g/n) Cisco APs > Configure page, choose **Disable** from the **Admin Status** drop-down list.
d) Click **Apply**.
e) Manually reset the access point in order for the change to take effect.

**Step 8** Click **Save Configuration**.

# Configuring Power over Ethernet (CLI)

Use these commands to configure and See PoE settings using the controller CLI:

- If your network contains any older Cisco 6-W switches that could be accidentally overloaded if connected directly to a 12-W access point, enter this command:

  **config ap power injector enable** {*Cisco_AP* | **all**} **installed**

The access point remembers that a power injector is connected to this particular switch port. If you relocate the access point, you must reissue this command after the presence of a new power injector is verified.

**Note** Ensure CDP is enabled before entering this command. Otherwise, this command will fail.

- Remove the safety checks and allow the access point to be connected to any switch port by entering this command:

  **config ap power injector enable** {*Cisco_AP* | **all**} **override**

  You can use this command if your network does not contain any older Cisco 6-W switches that could be overloaded if connected directly to a 12-W access point. The access point assumes that a power injector is always connected. If you relocate the access point, it continues to assume that a power injector is present.

- If you know the MAC address of the connected switch port and do not want to automatically detect it using the installed option, enter this command:

  **config ap power injector enable** {*Cisco_AP* | **all**} *switch_port_mac_address*

- If you have a dual-radio 1250 series access point and want to disable one of its radios in order to enable the other radio to receive full power, enter this command:

  **config** {**802.11a** | **802.11b**} **disable** *Cisco_AP*

**Note** You must manually reset the access point in order for the change to take effect.

- See the PoE settings 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
...
PoE Pre-Standard Switch.......................... Enabled
PoE Power Injector MAC Addr...................... Disabled
Power Type/Mode.................................. PoE/Low Power (degraded mode)
...
```

  The Power Type/Mode text box shows “degraded mode” if the access point is not operating at full power.

- See the controller’s trap log by entering this command:

  **show traplog**

  If the access point is not operating at full power, the trap contains “PoE Status: degraded operation.”

- You can power an access point by a Cisco prestandard 15-W switch with Power over Ethernet (PoE) by entering this command:

**config ap power pre-standard** {**enable** | **disable**} {**all** | *Cisco_AP*}

A Cisco prestandard 15-W switch does not support intelligent power management (IPM) but does have sufficient power for a standard access point. The following Cisco prestandard 15-W switches are available:

- WS-C3550, WS-C3560, WS-C3750
- C1880
- 2600, 2610, 2611, 2621, 2650, 2651
- 2610XM, 2611XM, 2621XM, 2650XM, 2651XM, 2691
- 2811, 2821, 2851
- 3631-telco, 3620, 3640, 3660
- 3725, 3745
- 3825, 3845

The **enable** version of this command is required for full functionality when the access point is powered by a Cisco prestandard 15-W switch. It is safe to use if the access point is powered by either an IPM switch or a power injector or if the access point is not using one of the 15-W switches listed above.

You might need this command if your radio operational status is "Down" when you expect it to be "Up." Enter the **show msglog** command to look for this error message, which indicates a PoE problem:

```
Apr 13 09:08:24.986 spam_lrad.c:2262 LWAPP-3-MSGTAG041: AP 00:14:f1:af:f3:40 is unable
 to
verify sufficient in-line power. Radio slot 0 disabled.
```

# Cisco Discovery Protocol

The Cisco Discovery Protocol (CDP) is a device discovery protocol that runs on all Cisco-manufactured equipment. A device enabled with CDP sends out periodic interface updates to a multicast address in order to make itself known to neighboring devices.

The default value for the frequency of periodic transmissions is 60 seconds, and the default advertised time-to-live value is 180 seconds. The second and latest version of the protocol, CDPv2, introduces new time-length-values (TLVs) and provides a reporting mechanism that allows for more rapid error tracking, which reduces downtime.

**Note** We recommend that you disable Cisco Discovery Protocol on the controller and access point when connected to non-Cisco switches as CDP is unsupported on non-Cisco switches and network elements.

# Restrictions for Cisco Discovery Protocol

- CDPv1 and CDPv2 are supported on the following devices:
  - Cisco 2504 Wireless Controller

- Cisco 5508 Wireless Controller
- Cisco 5520 Wireless Controller
- Cisco 8510 Wireless Controller
- Cisco 8540 Wireless Controller
- CAPWAP-enabled access points
- An access point connected directly to a Cisco 2504 Wireless Controller

**Note** To use the Intelligent Power Management feature, ensure that CDPv2 is enabled on the Cisco 2504 Wireless Controller. CDP v2 is enabled by default.

- The Cisco 600 Series OEAPs do not support CDP.
- The support of CDPv1 and CDPv2 enables network management applications to discover Cisco devices.
- The following TLVs are supported by both the controller and the access point:
  - Device-ID TLV: 0x0001—The hostname of the controller, the access point, or the CDP neighbor.
  - Address TLV: 0x0002—The IP address of the controller, the access point, or the CDP neighbor.
  - Port-ID TLV: 0x0003—The name of the interface on which CDP packets are sent out.
  - Capabilities TLV: 0x0004—The capabilities of the device. The controller sends out this TLV with a value of Host: 0x10, and the access point sends out this TLV with a value of Transparent Bridge: 0x02.
  - Version TLV: 0x0005—The software version of the controller, the access point, or the CDP neighbor.
  - Platform TLV: 0x0006—The hardware platform of the controller, the access point, or the CDP neighbor.
  - Power Available TLV: 0x001a— The amount of power available to be transmitted by power sourcing equipment to permit a device to negotiate and select an appropriate power setting.
  - Full/Half Duplex TLV: 0x000b—The full- or half-duplex mode of the Ethernet link on which CDP packets are sent out.
- These TLVs are supported only by the access point:
  - Power Consumption TLV: 0x0010—The maximum amount of power consumed by the access point.
  - Power Request TLV:0x0019—The amount of power to be transmitted by a powerable device in order to negotiate a suitable power level with the supplier of the network power.
- If the switch has provided power through CDP, it continues to provide only with CDP, and vice-versa with LLDP. (CSCvg86156)
- Changing the CDP configuration on the controller does not change the CDP configuration on the access points that are connected to the controller. You must enable and disable CDP separately for each access point.

- You can enable or disable the CDP state on all or specific interfaces and radios. This configuration can be applied to all access points or a specific access point.
- The following is the behavior assumed for various interfaces and access points:
  - CDP is disabled on radio interfaces on indoor (nonindoor mesh) access points.
  - Nonmesh access points have CDPs disabled on radio interfaces when they join the controller. The persistent CDP configuration is used for the APs that had CDP support in its previous image.
  - CDP is enabled on radio interfaces on indoor-mesh and mesh access points.
  - Mesh access points will have CDP enabled on their radio interfaces when they join the controller. The persistent CDP configuration is used for the access points that had CDP support in a previous image. The CDP configuration for radio interfaces is applicable only for mesh APs.
- CDP over radio backhaul link is not supported in Wave 2 (COS) APs.
- CDP is not supported in radio interfaces of Wave 2 (COS) APs. The GUI configuration of this has no effect.
- LLDP is enabled on the APs by default and cannot be disabled.

# Configuring the Cisco Discovery Protocol

## Configuring the Cisco Discovery Protocol (GUI)

### Procedure

**Step 1** Choose **Controller** > **CDP** > **Global Configuration** to open the CDP > Global Configuration page.

**Step 2** Select the **CDP Protocol Status** check box to enable CDP on the controller or unselect it to disable this feature. The default value is selected.

**Note** Enabling or disabling this feature is applicable to all controller ports.

**Step 3** From the CDP Advertisement Version drop-down list, choose **v1** or **v2** to specify the highest CDP version supported on the controller. The default value is v1.

**Step 4** In the Refresh-time Interval text box, enter the interval at which CDP messages are to be generated. The range is 5 to 254 seconds, and the default value is 60 seconds.

**Step 5** In the Holdtime text box, enter the amount of time to be advertised as the time-to-live value in generated CDP packets. The range is 10 to 255 seconds, and the default value is 180 seconds.

**Step 6** Click **Apply** to commit your changes.

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

**Step 8** Perform one of the following:

- To enable or disable CDP on a specific access point, follow these steps:

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

  Click the link for the desired access point.

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

Select the **Cisco Discovery Protocol** check box to enable CDP on this access point or unselect it to disable this feature. The default value is enabled.

**Note** If CDP is disabled in Step 2, a message indicating that the Controller CDP is disabled appears.

- Enable CDP for a specific Ethernet interface, radio, or slot as follows:

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

  Click the link for the desired access point.

  Choose the **Interfaces** tab and select the corresponding check boxes for the radios or slots from the CDP Configuration section.

  **Note** Configuration for radios is only applicable for mesh access points.

  Click **Apply** to commit your changes.

- To enable or disable CDP on all access points currently associated to the controller, follow these steps:

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

  Select the **CDP State** check box to enable CDP on all access points associated to the controller or unselect it to disable CDP on all access points. The default value is selected. You can enable CDP on a specific Ethernet interface, radio, or slot by selecting the corresponding check box. This configuration will be applied to all access points associated with the controller.

  Click **Apply** to commit your changes.

**Step 9** Click **Save Configuration** to save your changes.

## Configuring the Cisco Discovery Protocol (CLI)

**Procedure**

**Step 1** Enable or disable CDP on the controller by entering this command:

**config cdp** {**enable** | **disable**}

CDP is enabled by default.

**Step 2** Specify the interval at which CDP messages are to be generated by entering this command:

**config cdp timer** *seconds*

The range is 5 to 254 seconds, and the default value is 60 seconds.

**Step 3** Specify the amount of time to be advertised as the time-to-live value in generated CDP packets by entering this command:

**config cdp holdtime** *seconds*

The range is 10 to 255 seconds, and the default value is 180 seconds.

**Step 4** Specify the highest CDP version supported on the controller by entering this command:

**config cdp advertise** {**v1** | **v2**}

The default value is v1.

**Step 5** Enable or disable CDP on all access points that are joined to the controller by entering the **config ap cdp** {**enable** | **disable**} **all** command.

The **config ap cdp disable all** command disables CDP on all access points that are joined to the controller and all access points that join in the future. CDP remains disabled on both current and future access points even after the controller or access point reboots. To enable CDP, enter the **config ap cdp enable all** command.

**Note** After you enable CDP on all access points joined to the controller, you may disable and then reenable CDP on individual access points using the command in Step 6. After you disable CDP on all access points joined to the controller, you may not enable and then disable CDP on individual access points.

**Step 6** Enable or disable CDP on a specific access point by entering this command:

**config ap cdp** {**enable** | **disable**} *Cisco_AP*

**Step 7** Configure CDP on a specific or all access points for a specific interface by entering this command:

**config ap cdp {ethernet | radio}** *interface_number slot_id* **{enable** | **disable} {all |** *Cisco_AP***}**

**Note** When you use the config ap cdp command to configure CDP on radio interfaces, a warning message appears indicating that the configuration is applicable only for mesh access points.

**Step 8** Save your changes by entering this command:

**save config**

# Viewing Cisco Discovery Protocol Information

## Viewing Cisco Discovery Protocol Information (GUI)

**Procedure**

**Step 1** Choose **Monitor** > **CDP** > **Interface Neighbors** to open the CDP > Interface Neighbors page appears.

This page shows the following information:

- The controller port on which the CDP packets were received
- The name of each CDP neighbor
- The IP address of each CDP neighbor
- The port used by each CDP neighbor for transmitting CDP packets
- The time left (in seconds) before each CDP neighbor entry expires

- The functional capability of each CDP neighbor, defined as follows: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP, r - Repeater, or M - Remotely Managed Device
- The hardware platform of each CDP neighbor device

**Step 2** Click the name of the desired interface neighbor to see more detailed information about each interface's CDP neighbor. The CDP > Interface Neighbors > Detail page appears.

This page shows the following information:

- The controller port on which the CDP packets were received
- The name of the CDP neighbor
- The IP address of the CDP neighbor
- The port used by the CDP neighbor for transmitting CDP packets
- The CDP version being advertised (v1 or v2)
- The time left (in seconds) before the CDP neighbor entry expires
- The functional capability of the CDP neighbor, defined as follows: Router, Trans Bridge,?Source Route Bridge, Switch, Host, IGMP, Repeater, or Remotely Managed Device
- The hardware platform of the CDP neighbor device
- The software running on the CDP neighbor

**Step 3** **Note** If your Cisco Aironet 1830 Series or Cisco Aironet 1850 Series AP does not receive an IP address through DHCP, the AP is assigned a default IP address from the 6.x.x.x range. Executing the show cdp neighbor command on a connected switch displays this IP address in the AP's CDP neighbor table.

After DHCP issues, if any, are resolved, the AP is reassigned an IP address from the DHCP pool.

Choose **AP Neighbors** to see a list of CDP neighbors for all access points connected to the controller. The CDP AP Neighbors page appears.

**Step 4** Click the **CDP Neighbors** link for the desired access point to see a list of CDP neighbors for a specific access point. The CDP > AP Neighbors page appears.

This page shows the following information:

- The name of each access point
- The IP address of each access point
- The name of each CDP neighbor
- The IP address of each CDP neighbor
- The port used by each CDP neighbor
- The CDP version being advertised (v1 or v2)

**Step 5** Click the name of the desired access point to see detailed information about an access point's CDP neighbors. The CDP > AP Neighbors > Detail page appears.

This page shows the following information:

- The name of the access point
- The MAC address of the access point's radio
- The IP address of the access point
- The interface on which the CDP packets were received
- The name of the CDP neighbor
- The IP address of the CDP neighbor
- The port used by the CDP neighbor
- The CDP version being advertised (v1 or v2)
- The time left (in seconds) before the CDP neighbor entry expires
- The functional capability of the CDP neighbor, defined as follows: R - Router, T - Trans Bridge,?B - Source Route Bridge, S - Switch, H - Host, I - IGMP, r - Repeater, or M - Remotely Managed Device
- The hardware platform of the CDP neighbor device
- The software running on the CDP neighbor

**Step 6** Choose **Traffic Metrics** to see CDP traffic information. The CDP > Traffic Metrics page appears.

This page shows the following information:

- The number of CDP packets received by the controller
- The number of CDP packets sent from the controller
- The number of packets that experienced a checksum error
- The number of packets dropped due to insufficient memory
- The number of invalid packets

## Viewing Cisco Discovery Protocol Information (CLI)

### Procedure

**Step 1** See the status of CDP and to view CDP protocol information by entering this command:

**show cdp**

**Step 2** See a list of all CDP neighbors on all interfaces by entering this command:

**show cdp neighbors [detail]**

The optional detail command provides detailed information for the controller's CDP neighbors.

**Note** This command shows only the CDP neighbors of the controller. It does not show the CDP neighbors of the controller's associated access points. Additional commands are provided below to show the list of CDP neighbors per access point.

**Step 3** See all CDP entries in the database by entering this command:

**show cdp entry all**

**Step 4** See CDP traffic information on a given port (for example, packets sent and received, CRC errors, and so on) by entering this command:

**show cdp traffic**

**Step 5** See the CDP status for a specific access point by entering this command:

**show ap cdp ap-name** *Cisco_AP*

**Step 6** See the CDP status for all access points that are connected to the controller by entering this command:

**show ap cdp all**

**Step 7** See a list of all CDP neighbors for a specific access point by entering these commands:

- **show ap cdp neighbors ap-name** *Cisco_AP*
- **show ap cdp neighbors detail** *Cisco_AP*

**Note** The access point sends CDP neighbor information to the controller only when the information changes.

**Step 8** See a list of all CDP neighbors for all access points connected to the controller by entering these commands:

- **show ap cdp neighbors all**
- **show ap cdp neighbors detail all**

**Note** The access point sends CDP neighbor information to the controller only when the information changes.

## Getting CDP Debug Information

- Get debug information related to CDP packets by entering by entering this command:

  **debug cdp packets**

- Get debug information related to CDP events by entering this command:

  **debug cdp events**

# Cisco 700 Series Access Points

The Cisco Aironet 700 Series is a compact access point that delivers secure and reliable wireless connections. The main features are:

- Simultaneous dual band, dual radio with support for 2.4GHz and 5GHz.

- Optimized antenna and radio designs: Consistent network transmit and receive for optimized rate versus range.
- Radio resource management (RRM): Automated self-healing optimizes the unpredictability of RF to reduce dead spots and help ensure high-availability client connections.
- Cisco BandSelect improves 5-GHz client connections in mixed-client environments.
- Advanced security features including Rogue Detection, wIPS and Context-Aware.

# Configuring Cisco 700 Series Access Points

The Cisco 700 series access points has four LAN ports. The configuration of these ports is stored in a file on flash. The AP retrieves the configuration when restarted. The AP then shares the information with Controller after joining so that Controller can display the updated information.

**Note** The AP deletes the saved port information and applies the default configuration when the controller clears all the existing configuration on the AP. All LAN ports are disabled by default.

## Enabling the LAN Ports (CLI)

### Procedure

- Enable or disable a LAN port on the access point by entering this command:
  **config ap lan port-id** *port-id* {**enable** | **disable**} *ap-name*
- See the port information by entering this command:
  **showap lan port-id** *port-id ap-name*
- See the port summary information by entering this command:
  **showap lan port-summary** *ap-name*

### Enabling 702W LAN Ports

All ports are mapped to the same access VLAN that the AP's switch port is configured to. Alternatively, the ports are mapped to the native VLAN if port is a trunk. It is possible to enable or disable the ports and map them to specific VLANs if needed. This allows traffic to be separated not only between wireless and wired networks, but also among the four Ethernet ports.

### Procedure

**Step 1** Enable or disable a LAN port on the access point by entering this command:
**config ap lan port-id** *port-id* { **enable** | **disable**} *ap-name*

**Step 2** Configure the port ID by entering this command:
**config ap lan port-id** *port-id ap-name*

**Step 3** Configure VLAN for the AP by entering this command:

**config ap lan enable access vlan** *vlan-id port-id ap-name*