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.

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 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*

- 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 3504 Wireless Controller
  - Cisco 5520 Wireless Controller
  - Cisco 8540 Wireless Controller
  - CAPWAP-enabled access points
- 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 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 Wave 2 AP's USB Port as Power Source

Cisco Aironet 2800 and 3800 Series APs have a USB port that can act as a source of power for some USB devices. The power can be up to 2.5W; if a USB device draws more than 2.5W of power, the USB port shuts down automatically. The port is enabled when the power draw is 2.5W and lower.

Note The controller records the last five power-overdrawn incidents in its logs.

Caution When unsupported USB device is connected to the Cisco AP, the following message is displayed:

```
The inserted USB module is not a supported device. The behavior of this
USB device and the impact to the Access Point is not guaranteed. If Cisco
determines that a fault or defect can be isolated due to the use of
third-party USB modules installed by a customer or reseller, Cisco may
withhold support under warranty or support program under contract. In the
course of providing support for Cisco networking products, the end user
may be required to install Cisco-supported USB modules in the event Cisco
determines that removing third-party parts will assist Cisco in diagnosing
root cause for troubleshooting purposes. Cisco also reserves the right
to charge the customer per then-current time and material rates for
services provided to the customer when Cisco determines, after having
provided such services, that an unsupported device caused the root cause
of the defective product
```

Configuring Cisco Aironet AP's USB Port as Power Source (GUI)

Procedure

Step 1 Choose **Wireless** > **Access Points** > **All APs** > **access point name** > **Advanced** tab to open the **Advanced** page.

Step 2 Check the **USB Module Status** check box to enable the USB port.

Note When the USB device draws power exceeding 2.5W, the USB port is disabled. The status shows the status as Disabled due to over current.

Note Custom configurations on the *default-group* are not saved and are valid till the next controller reboot only.

Step 3 [Optional] Check the **Override** check box to enable the USB Module on the particular AP or uncheck to apply the AP group setting to the AP.

Step 4 Click **Apply**.

Step 5 Choose the **Inventory** tab to open the **All APs** > **Details** for (Inventory) page.

This page shows the connected USB Module details.

Configuring a Cisco AP Group to Use the Cisco AP's USB Port as Power Source (GUI)

Procedure

Step 1 Choose **WLANs** > **Advanced** > **AP Groups** > **AP_group_name** > **Ports/Module** tab.

Step 2 Check the **USB Module** check box in the **External Module** section to enable on all the APs in this Cisco AP group.

Step 3 Choose **Wireless** > **Access Points** > **All APs** > **Access Point name** > **Advanced** tab to open the **Advanced** page.

Step 4 [Optional] Check the **Override** check box to toggle the override state of USB Module setting on a particular AP or uncheck to apply the AP group setting to the AP.

Step 5 Check the **USB Module Status** to view the **USB Module Operations State** of the port.

Note When the USB device draws power exceeding 2.5W, the USB port is disabled. The status shows the status as Disabled due to over current.

Step 6 Choose the **Inventory** tab to open the **All APs** > **Details** for (Inventory) page.

This page shows the connected USB Module details.

Configuring Cisco Aironet APs USB Port as Power Source (WLC-CLI)

Procedure

- Enable or disable the USB port on an AP by entering this command:

  config ap usb-module {**enable | disable**} *ap-name*

- Enable or disable the USB port, overriding the AP group setting by entering this command:

  config ap usb-module over-ride {**enable | disable**} *ap-name*

- Enable or disable the USB port on all the APs belonging to a specific AP group by entering this command:

  config wlan apgroup port usb-module *ap-group-name* {**enable | disable**}

Note Custom configurations on the *default-group* are not saved and are valid till the next controller reboot only.

- View the inventory details on all APs or a specific AP by entering this command:

  show ap inventory {**all | ap_name**}

Viewing Cisco Aironet APs USB Port as Power Source (AP-CLI)

Procedure

- View the USB Inventory by entering this command:

  show inventory

- View the USB port status by entering this command:

  show interfaces usb

Viewing AP Serviceability (AP CLI)

This section lists the Cisco Wave 2 AP supported CLIs you can use to view the serviceability parameters.

Procedure

- View the last recorded power level (per antenna RSSI) from the antenna by entering this command:

  show controllers dot11Radio *radio(0-1)* **antenna**

- View the details of the client such as rate selection, streams by entering this command:

  show controllers dot11Radio *radio(0-1)* **client** *MAC-address*

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*

Remote LAN Support for Wired Ports on Cisco Aironet 702W APs

A remote LAN (RLAN) in Cisco Aironet 702W access points (APs) are used for authenticating wired clients using Cisco Wireless LAN Controller. You can set the various IEEE 802.1X authentication modes for the LAN ports in Cisco 702W APs by configuring them in RLAN.

The IEEE 802.1X authentication message exchange between a client and an authentication server is carried out locally in APs. All IEEE 802.1X configurations are carried out through controller. Both port control and restrictions are considered locally in APs.

Role of Controller

Controller acts as an authenticator, and Extensible Authentication Protocol (EAP) over LAN (EAPOL) messages from the wired client reaches controller through an AP, and controller communicates with the configured authentication, authorization, and accounting (AAA) server.

Role of an AP

An AP acts as a relay in tunneling the authentication packets from a wired client to controller using the Control and Provisioning of Wireless Access Points (CAPWAP) tunnel. After a port is authenticated, the AP is responsible for port control and monitoring.

LAN ports for an AP are configured in controller and then pushed to the corresponding AP.

Initially, the AP configures the IEEE 802.1X port if the client that joins the AP passes the EAPOL packets to the controller.

IEEE 802.1X Authentication Modes

This topic describes the different IEEE 802.1X authentication modes.

Single-Host Mode

If the single-host authentication mode is configured in an AP and the port link state is up, the AP detects the client by sending the EAPoL frame. If the client leaves or is replaced with another client, the AP changes its port link state to down, making the port unauthorized.

The single-host configuration mode is configured using the existing RLAN configurations in the controller.

Multi-Host Mode

If the multi-host authentication mode is configured, only one client can be authenticated for all the clients to gain network access in that port. If the port becomes unauthorized, the switch denies access to all the attached clients.

Violation Mode

When a security violation occurs, a port is protected based on the following configured violation actions:

- Shutdown—Disables the port.
- Replace—Removes the current session and initiates authentication for the new host. This is the default behavior.
- Protect—Drops packets with unexpected MAC addresses without generating a system message.

In the single-host authentication mode, a violation is triggered when more than one device is detected in data VLAN. In a multi-host authentication mode, a violation is triggered when more than one device is detected in data VLAN or voice VLAN.

Note Security violation cannot be triggered in the multi-host authentication mode.

Configuring Preauthentication Open (CLI)

- The preauthentication open option allows unrestricted traffic on an AP LAN port initially, and is restricted only by other access restrictions.
- The preauthentication open feature is not supported in Cisco Aironet 1810 OEAPs.

Procedure

config remote-lan pre-auth {**enable | disable**} *remote-lan-id* **vlan** *vlan-id*

Example:

```
config remote-lan pre-auth enable 8 vlan vlan2
```

Configures preauthentication open on a VLAN.

Configuring IEEE 802.1X Authentication Modes (CLI)

You can configure three different authentications modes:

- **Single-host**
- **Multi-host**
- **Violation-mode**

Procedure

Perform one of the following tasks to configure authentication:

- **config remote-lan host-mode singlehost** *remote-lan-id*

  Example:

  ```
  (Cisco Controller) > config remote-lan host-mode singlehost 7
  ```

  Configures a remote LAN single-host mode. In single-host mode, violation is triggered when more than one device is detected in data VLAN.

- **config remote-lan host-mode multihost** *remote-lan-id*

  Example:

  ```
  (Cisco Controller) > config remote-lan host-mode multihost 8
  ```

Configuresa remote LAN multi-host mode. In multi-host mode, a violation is triggered when more than one device is detected in data or voice VLAN. Note that security violation cannot be triggered in multi-host mode.

- **config remote-lan violation-mode** {**protect** | **replace** | **shutdown**}*remote-lan-id*

  Example:

  ```
  (Cisco Controller) > config remote-lan violation-mode protect 7
  ```

  Configures violation mode for remote LAN.

Enabling IEEE 802.1X Authentication in Cisco WLC (GUI)

Procedure

Step 1 Choose **WLANs**.

The **WLANs** window is displayed.

Step 2 Click the ID number of the corresponding WLAN.

The **WLANs > Edit** window is displayed.

Step 3 Click the **Security** > **Layer 2** tab.

Step 4 From the **Layer 2 Security** drop-down list, choose **802.1X**.

The IEEE 802.1X parameters are displayed.

a) Select **Host Mode** from the drop-down list.
b) Select **Violation Mode** from the drop-down list.
c) Select the **Pre Authentication** check box and enter pre-authentication VLAN identifier in the Pre Auth Vlan field.

Step 5 Click **Apply**.

Enabling IEEE 802.1X Authentication (CLI)

Enable IEEE 802.1X authentication using the existing remote LAN configuration. After configuring the remote LAN in Cisco WLC, apply the configuration to the AP group and then push to the individual APs present in that AP group.

Procedure

Step 1 **config remote-lan security 802.1x** {**enable** | **disable**} *remote-lan-id*

Example:

```
(Cisco Controller) > config remote-lan security 802.1X enable 7
```

Configures the security policy for a remote LAN.

Step 2 **config remote-lan apgroup add** *ap-group*

Example:

```
(Cisco Controller) > config remote-lan apgroup add apgroup1
```

Adds a WLAN AP group for a remote LAN.

Mapping an RLAN to an AP Port in Controller (GUI)

Perform this procedure to map an RLAN to an AP port. This task can be performed either per AP or per AP group.

Procedure

Step 1 Choose **WLANs > Advanced > AP Groups**.

The AP Groups window is displayed.

Step 2 Click the corresponding AP Group Name.

The **AP Group > Edit** window is displayed.

Step 3 Click on **WLANs** tab, and then click **Add New**.

The **Add New** area is displayed.

Step 4 Use the drop-down list from WLAN SSID to select the RLAN to be added.

Step 5 From the **Interface/Interface Group** drop-down list, to choose the group it belongs to.The default choice is **management**.

Step 6 Click **Add**.

Step 7 Click the **Ports/Module** tab.

Step 8 In the **LAN Ports** area, use the drop-down to add the RLAN to the LAN port.

Step 9 Click **Apply**.

Mapping an RLAN to an AP Port in Controller (CLI)

Map the LAN ports in an AP to the remote LAN that is configured, for authentication to take place. Perform the port-level configurations through the LAN port configuration in the AP group level.

Procedure

config remote-lan apgroup port port-sardinia *port-id*

Example:

```
(Cisco Controller) > config remote-lan apgroup port port-sardinia 1 apgroup1 remote-lan
```

Assigns a remote LAN to a LAN port in an AP group.

Mapping an RLAN to an AP Port in Cisco WLC per AP (GUI)

Perform this procedure to map a RLAN to an AP port. This task can be performed either per AP or per AP group.

Procedure

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

The **All APs** window is displayed.

Step 2 Click the corresponding AP.

The **AP Details** window is displayed.

Step 3 Click the **Interfaces** tab.

Step 4 In the **LAN Ports** area, set the port state to Enable, and check the **VLAN** check box, and enter the RLAN WLAN ID in the **VLAN ID** field.

Step 5 From the **Layer 2 Security** drop-down list, choose **802.1X**.

The IEEE 802.1X parameters are disaplyed.

Step 6 From the **Key Size** drop-down list, choose the key size for IEEE 802.1X data encryption.

Note If a preauthentication VLAN is required, enable **Pre Authentication** and enter the Pre Auth VLAN identifier.

Mapping a RLAN to an AP External Port in Controller (GUI)

Perform this procedure to map an RLAN to an AP port. This task can be performed either per AP or per AP group.

Procedure

Step 1 Choose **WLANs** > **Advanced** > **AP Groups**.

The AP Groups window is displayed.

Step 2 Click the corresponding AP Group Name.

The **AP Group** > **Edit** window is displayed.

Step 3 Click on **Ports/Module** tab.

Step 4 Use the RLAN drop-down list to select the RLAN to be mapped.

Step 5 Check the **External Module** check box.

Note Custom configurations on the *default-group* are not saved and are valid till the next controller reboot only.

Step 6 Click **Apply**.

Mapping a RLAN to an AP External Port in Controller (CLI)

Map the external module in an AP to the remote LAN at the AP group level.

Procedure

config remote-lan apgroup port ext-module *default-group* {**enable** | **disable**}

Example:

```
(Cisco Controller) > config remote-lan apgroup port ext-module default-group enable
```

Enables the external module of the AP in an ap group in the remote LAN .

Note Custom configurations on the *default-group* are not saved and are valid till the next controller reboot only.

MAB Authentication Support for AP Port LAN Client in Cisco Aironet 702w Access Points

MAC Authentication Bypass (MAB) feature enables port-based access control using the MAC address of an endpoint. An MAB-enabled port can be enabled or disabled based on the MAC address of the device it connects to. MAB is useful when the clients does not recognize EAP packets and is mainly for non-802.1x clients.

This feature is supported in Cisco Aironet 702w access points on the Remote LAN (RLAN).

Configuring MAB Support on AP Port LAN Clients (GUI)

Before you begin

This feature is supported only on Cisco Aironet 702w access points that supports RLAN feature.

Procedure

Step 1 Choose **WLANs** to open the WLANs window.

Step 2 Click the ID number of the desired WLAN to open the **WLANs > Edit** window.

Step 3 Choose the **Security** > **Layer 2** tab.

Step 4 Check the **MAB Mode** check box.

Enables port-based access control using the MAC address of an endpoint.

Configuring MAB Support for AP Port LAN Clients (CLI)

Procedure

config remote-lan mab {**enable** | **disable**} *remote-lan-id*

Example:

```
config remote-lan mab enable 8
```

Enables port-based access control using the MAC address of an endpoint.

Converting Cisco Wave 2 AP AUX Port to Downlink LAN (RLAN) Port (CLI)

Some Wave 2 APs' second Ethernet port, also called the AUX port, is used as a link aggregation (LAG) port, by default. It is possible to use this LAG port as a LAN port when LAG is disabled. When the AUX port is configured as a Downlink LAN (RLAN) Port, you can either use the AP group setting to configure the Downlink LAN (RLAN) Port for a group of APs, or use the LAN override functionality to configure the Downlink LAN (RLAN) Port for each AP separately. This Cisco Wave 2 AP AUX port to Downlink LAN (RLAN) Port conversion feature is supported only in the following APs:

- Cisco Aironet 1850 Series AP
- Cisco Aironet 2800 Series AP
- Cisco Aironet 3800 Series AP
- Cisco Aironet 4800 Series AP

Note After global AP LAG is enabled, the CAPWAP connection with the AP is deleted; that is, the connection is deleted from the database in the controller. This results in AP disjoining and then rejoining the controller. The connection is explicitly deleted from the database in the controller.

After global AP LAG is disabled, for the APs that do not have LAG enabled, their connection is deleted from the database in the controller. This results in APs to disjoin and rejoin the controller.

After global AP LAG is disabled, the APs that have LAG enabled are rebooted.

Procedure

Step 1 By default, the APs are in LAG mode. Check the status of an AP by entering this command:

show ap config general *ap-name*

Note The `AP LAG Configuration Status` line in the output shows the current LAG status.

Step 2 If LAG mode in the AP is enabled, disable LAG mode by entering this command:

config ap lag-mode support disable *ap-name*

Step 3 Create a remote LAN (RLAN) and enable it by entering these commands:

a) **config remote-lan create** *rlan-id rlan-name*
b) **config remote-lan enable** *rlan-id*

Step 4 Create an AP group for the RLAN that you created by entering this command:

config wlan apgroup add *apgroup-name description*

Step 5 Add the RLAN and the AP to the AP group by entering these commands:

a) **config wlan apgroup interface-mapping add** *apgroup-name rlan-id interface-name*
b) **config ap group-name** *group_name Cisco_AP*

The AP is rebooted after these commands are entered.

Step 6 After the AP is rebooted, assign the RLAN to the Downlink LAN (RLAN) Port (LAN 1) in the AP group by entering this command:

config wlan apgroup port lan *1 apgroup-name* **remote-lan** *rlan-id*

Note In the supported APs, only LAN 1 can be used.

Step 7 Enable the Downlink LAN (RLAN) Port (LAN 1) for a group of APs in the AP group or for an individual AP by entering these commands:

- For a group of APs in the AP group:

  config wlan apgroup port lan *1 apgroup-name* **enable**

- For an individual AP:

  a. config ap lan over-ride enable *ap-name*

  b. config ap lan port-id *1* **enable**

Step 8 Connect a client to the AP through the AUX port.

Re-enabling LAG Mode on Cisco Wave 2 APs (CLI)

Procedure

Step 1 Disable the Downlink LAN (RLAN) Port (LAN 1) in the AP group by entering this command:

config wlan apgroup port lan *1 apgroup-name* **disable**

Step 2 Disable the RLAN on the Downlink LAN (RLAN) Port (LAN 1) in the AP group by entering this command:

config wlan apgroup port lan *1 apgroup-name* **remote-lan none**

Step 3 If LAN is enabled for an individual AP, disable the LAN override for the AP by entering this command:

config ap lan over-ride disable *ap-name*

Step 4 Enable LAG mode on the AP by entering this command:

config ap lag-mode support enable *ap-name*