AP 電源および LAN 接続

イーサネット経由の電源供給

Power over Ethernet の設定（GUI）

手順

ステップ 1 **[Wireless]** > **[Access Points]** > **[All APs]** の順に選択して、目的のアクセス ポイントの名前を選択します。

ステップ 2 [Advanced] タブを選択して、[All APs >Details for]（[Advanced]）ページを開きます。

[PoE Status] テキスト ボックスに、アクセス ポイントが動作している電力レベル（[High (20 W)]、[Medium (16.8 W)]、または [Medium (15.4 W)]）が表示されます。このテキスト ボックスは設定できません。コントローラによりアクセスポイントの電源が自動検出され、ここにその電力レベルが表示されます。

（注） このテキスト ボックスは、PoE を使用して電力供給している 1250 シリーズ アクセス ポイントにのみ適用されます。アクセスポイントの電力レベルが低いかどうかを判断する方法は、ほかに 2 つあります。1 つめは、[802.11a/n/ac（または 802.11b/g/n）Cisco APs] > [Configure] ページの [Tx Power Level Assignment] セクションに表示される「Due to low PoE, radio is transmitting at degraded power」というメッセージです。2 つめは、[Trap Logs] ページのコントローラのトラップ ログに表示される「PoE Status: degraded operation」というメッセージです。

ステップ 3 次のいずれかの操作を行います。

- アクセス ポイントが高出力の 802.3af Cisco スイッチによって給電されている場合は、[Pre-standard 802.3af switches] チェックボックスをオンにします。これらのスイッチは従来

の 6 ワットを超える電力を供給しますが、Intelligent Power Management（IPM）機能をサポートしません。

- パワーインジェクタから電力が供給されている場合は、[Pre-standard 802.3af switches] チェックボックスをオフにします。これはデフォルト値です。

ステップ 4 付属のスイッチが IPM をサポートしておらず、パワーインジェクタが使用されている場合は、[Power Injector State] チェックボックスをオンにします。付属のスイッチが IPM をサポートしている場合、このチェックボックスをオンにする必要はありません。

ステップ 5 前の手順で [Power Injector State] チェックボックスをオンにした場合、[Power Injector Selection] パラメータおよび [Injector Switch MAC Address] パラメータが表示されます。Power Injector Selection パラメータは、パワーインジェクタが過失によりバイパスされた場合にスイッチ ポートが突発的に過負荷にならないよう保護します。ドロップダウン リストから次のオプションのいずれかを選択して、必要な保護のレベルを指定します。

- [Installed]：現在接続されているスイッチ ポートの MAC アドレスを点検して記憶し、パワーインジェクタが接続されていることを想定します。ネットワークに従来のシスコ 6 W スイッチが装備されていて、再配置されたアクセス ポイントを強制的にダブルチェックしたときに発生する可能性のある過負荷を避けたい場合に、このオプションを選択します。

  スイッチの MAC アドレスを設定する場合は、[Injector Switch MAC Address] テキスト ボックスに MAC アドレスを入力します。アクセス ポイントにスイッチの MAC アドレスを検知させる場合は、[Injector Switch MAC Address] テキスト ボックスは空白のままにします。

  （注） アクセス ポイントが再配置されるたびに、新しいスイッチ ポートの MAC アドレスは記憶した MAC アドレスとの一致に失敗し、アクセス ポイントは低電力モードのままになります。その場合、パワーインジェクタの存在を物理的に検証し、このオプションを再選択して新しい MAC アドレスを記憶させます。

- [Override]：このオプションにより、アクセス ポイントは最初に MAC アドレスの一致を検証しなくても、高電力モードで稼働できます。ネットワークに、12 W アクセス ポイントへ直接接続すると過負荷を発生する可能性のある、従来のシスコ 6 W スイッチが装備されていない場合には、このオプションを選択できます。このオプションのメリットは、アクセス ポイントを再配置した場合、設定しなおさずに高電力モードで稼働を継続できることです。このオプションのデメリットは、アクセス ポイントが直接 6 W スイッチへ接続されていると、過負荷が発生することです。

ステップ 6 [Apply] をクリックします。

ステップ 7 デュアル無線 1250 シリーズ アクセス ポイントを所有しており、無線のうちの 1 つを無効にして他方の無線に最大電力を供給する場合の手順は次のとおりです。

a) **[Wireless]** > **[Access Points]** > **[Radios]** > **[802.11a/n**//ac] または [802.11b/g/n] を選択して、[802.11a/n/ac（または 802.11b/g/n）Radios] ページを開きます。

b) 無効にする無線の青いドロップダウンの矢印の上にカーソルを置いて、[Configure] を選択します。

c) [802.11a/n/ac（または 802.11b/g/n）Cisco APs > Configure] ページで、[Admin Status] ドロップダウン リストから [Disable] を選択します。

d) [Apply] をクリックします。

e) 手動でアクセス ポイントをリセットして、変更を適用します。

ステップ 8 [Save Configuration] をクリックします。

Power over Ethernet の設定（CLI）

コントローラの CLI を使用して PoE を設定し、設定内容を表示するには、次のコマンドを使用します。

- ネットワークに、12 W アクセス ポイントへ直接接続すると過負荷を発生する可能性のある、従来のシスコ 6 W スイッチが装備されている場合には、次のコマンドを入力します。

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

  アクセス ポイントは、パワー インジェクタがこの特定のスイッチ ポートに接続されていることを記憶します。アクセス ポイントを再配置する場合、新しいパワー インジェクタの存在を検証した後で、このコマンドを再度実行する必要があります。

  （注） このコマンドを入力する前に、CDP が有効化されていることを確認します。有効になっていない場合、このコマンドは失敗します。

- 次のコマンドを入力して、安全確認の必要をなくし、アクセス ポイントをどのスイッチ ポートにも接続できるようにします。

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

  ネットワークに、12 W アクセス ポイントに直接接続すると過負荷を発生する可能性のある従来のシスコ 6 W スイッチが装備されていない場合は、このコマンドを使用できます。アクセス ポイントは、パワー インジェクタが常に接続されていることを前提としています。アクセスポイントを再配置した場合も、パワーインジェクタの存在を前提とします。

- 接続スイッチ ポートの MAC アドレスがわかっていて、[Installed] オプションを使用して自動的に検出しない場合は、次のコマンドを入力します。

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

- デュアル無線 1250 シリーズ アクセス ポイントを所有しており、無線のうちの 1 つを無効にして他方の無線に最大電力を供給する場合は、次のコマンドを入力します。

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

  （注） 手動でアクセスポイントをリセットして、変更を適用する必要があります。

- 次のコマンドを入力して、特定のアクセス ポイントの PoE 設定を表示します。

show ap config general *Cisco_AP*

以下に類似した情報が表示されます。

```
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)
...
```

アクセス ポイントが最大電力で動作していない場合、[Power Type/Mode] テキスト ボックスには、「degraded mode」と表示されます。

- 次のコマンドを入力して、コントローラのトラップ ログを表示します。

  show traplog

  アクセスポイントが最大電力で動作していない場合は、トラップには「PoE Status: degraded operation」が含まれます。

- 次のコマンドを入力して、Power over Ethernet（PoE）を搭載したシスコ準規格 15-W スイッチでアクセス ポイントに電源を投入できます。

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

  シスコ準規格 15-W スイッチは Intelligent Power Management（IPM）をサポートしていませんが、標準アクセス ポイントに十分な電力を供給できます。次のシスコ準規格 15-W スイッチを使用できます。

  - 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

  アクセス ポイントがシスコ準規格 15-W スイッチにより電力供給されている場合、全機能を使用するには、このコマンドの **enable** バージョンが必要です。アクセス ポイントが IPM スイッチまたはパワー インジェクタを使用して電力を供給するか、またはアクセス ポイントが上記 15-W スイッチの 1 つを使用しない場合は使用しても安全です。

  無線の動作ステータスが「Down」になっていて「Up」にする場合、このコマンドが必要になることがあります。**show msglog** コマンドを入力して、PoE 障害を示す次のエラー メッセージを探します。

```
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.
```

AP の有用性の表示（AP CLI）

このセクションには、有用性パラメータを表示するために使用できる、Cisco Wave 2 AP でサポートされている CLI が一覧表示されています。

手順

- 次のコマンドを入力して、アンテナから記録された最後の電力レベル（アンテナ RSSI ごと）を表示します。

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

- 次のコマンドを入力して、クライアントの詳細（レート選択、ストリームなど）を表示します。

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

Cisco Discovery Protocol

Cisco Discovery Protocol の設定について

Cisco Discovery Protocol（CDP）は、すべてのシスコ製の機器で実行されるデバイス ディスカバリ プロトコルです。CDP を使用して有効化されたデバイスは、近隣のデバイスにその存在を認識させるためにインターフェイスの更新をマルチキャスト アドレスに周期的に送信します。

周期的な送信の間隔のデフォルト値は 60 秒で、アドバタイズされた有効期間のデフォルト値は 180 秒です。最新の 2 番目のバージョンのプロトコルである CDPv2 は、新しい Time Length Value（TLV）が導入されるとともに、従来よりも迅速なエラー追跡を可能にするレポート メカニズムを備えており、ダウン タイムが短縮されます。

（注） CDP はシスコ以外のスイッチとネットワーク要素でサポートされていないため、シスコ以外のスイッチに接続するときは、コントローラとアクセス ポイント上で Cisco Discovery Protocol を無効にすることをお勧めします。

Cisco Discovery Protocol の設定の制約事項

- CDPv1 および CDPv2 は次のデバイスでサポートされています。

- Cisco 2504 WLC
- Cisco 3504 WLC
- Cisco 5508 WLC
- Cisco 5520 WLC
- Cisco 8510 WLC
- Cisco 8540 WLC
- CAPWAP が有効化されているアクセス ポイント
- Cisco 2504 WLC に直接接続されたアクセス ポイント

（注） Intelligent Power Management 機能を使用するには、Cisco 2504 ワイヤレス コントローラで CDPv2 を有効にしておく必要があります。CDP v2 は、デフォルトで有効になっています。

- CDPv1 と CDPv2 のサポートにより、ネットワーク管理アプリケーションは、シスコ デバイスを検出できるようになります。
- 次の TLV は、コントローラとアクセス ポイントの両方でサポートされています。
  - Device-ID TLV（0x0001）：コントローラ、アクセス ポイント、または CDP ネイバーのホスト名。
  - Address TLV（0x0002）：コントローラ、アクセス ポイント、または CDP ネイバーの IP アドレス。
  - Port-ID TLV（0x0003）：CDP パケットが送信されるインターフェイス名。
  - Capabilities TLV（0x0004）：デバイスの機能。コントローラから送信されるこの TLV の値は Host: 0x10、アクセス ポイントから送信されるこの TLV の値は Transparent Bridge: 0x02 です。
  - Version TLV（0x0005）：コントローラ、アクセス ポイント、または CDP ネイバーのソフトウェア バージョン。
  - Platform TLV（0x0006）：コントローラ、アクセス ポイント、または CDP ネイバーのハードウェア プラットフォーム。
  - Power Available TLV（0x001a）：使用可能な電力量。デバイスが適切な電力設定をネゴシエートし、選択するために、給電側機器から送信されます。
  - Full/Half Duplex TLV（0x000b）：CDP パケットが送信されるイーサネット リンクの全二重または半二重モード。
- 次の TLV は、アクセス ポイントでのみサポートされます。
  - Power Consumption TLV（0x0010）：アクセス ポイントが消費する電力の最大量。

- Power Request TLV（0x0019）：ネットワーク電力の供給側と適切な電力レベルをネゴシエートするために給電可能デバイスから送信される電力量。

- CDP から供給された電力があるスイッチは、CDP とのみ供給関係を続けます。逆の場合は LLDP とのみ続けます。(CSCvg86156)
- CDP 設定をコントローラで変更しても、コントローラに接続されているアクセス ポイントの CDP 設定は変更されません。各アクセス ポイントに対して個別に CDP を有効または無効にする必要があります。
- すべてまたは特定のインターフェイスおよび無線に対して CDP の状態を有効または無効にできます。この設定は、すべてのアクセス ポイントまたは特定のアクセス ポイントに適用できます。
- 各種インターフェイスおよびアクセス ポイントに対して想定される動作は次のとおりです。
  - 屋内（非屋内メッシュ）アクセス ポイント上の無線インターフェイスでは、CDP は無効になります。
  - 非メッシュ アクセス ポイントでは、それらがコントローラに join している場合、無線インターフェイス上で CDP は無効になります。前のイメージで CDP がサポートされていた AP には、永続的な CDP 設定が使用されます。
  - 屋内メッシュ アクセス ポイント上とメッシュ アクセス ポイント上の無線インターフェイスでは、CDP は有効になります。
  - メッシュ アクセス ポイントでは、それらがコントローラに join している場合、無線インターフェイス上で CDP が有効になります。前のイメージで CDP がサポートされていたアクセスポイントには、永続的なCDP設定が使用されます。無線インターフェイスの CDP 設定は、メッシュ AP に対してだけ適用されます。

Cisco Discovery Protocol の設定

Cisco Discovery Protocol の設定（GUI）

手順

ステップ 1 [Controller] > [CDP] > [Global Configuration] の順に選択して [CDP > Global Configuration] ページを開きます。

ステップ 2 コントローラ上で CDP を有効にする場合は [CDP Protocol Status] チェックボックスをオンにします。この機能を無効にする場合は、オフにします。デフォルト値はオンです。

（注） この機能の有効化と無効化は、すべてのコントローラ ポートに適用されます。

ステップ 3 [CDP Advertisement Version] ドロップダウン リストから、コントローラでサポートされている CDP の最新バージョン（[v1] または [v2]）を選択します。デフォルト値は [v1] です。

ステップ 4 [Refresh-time Interval] テキスト ボックスに、CDP メッセージが生成される間隔を入力します。範囲は 5 ～ 254 秒で、デフォルト値は 60 秒です。

ステップ 5 [Holdtime] テキスト ボックスに、生成された CDP パケットの中の存続可能時間値としてアドバタイズされる時間の長さを入力します。範囲は 10 ～ 255 秒で、デフォルト値は 180 秒です。

ステップ 6 [Apply] をクリックして、変更を確定します。

ステップ 7 [Save Configuration] をクリックして、変更を保存します。

ステップ 8 次のいずれかの操作を行います。

- 特定のアクセス ポイントで CDP を有効または無効にする手順は、次のとおりです。

  [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

  目的のアクセス ポイントのリンクをクリックします。

  [Advanced] タブを選択して、[All APs > Details for]（[Advanced]）ページを開きます。

  このアクセス ポイントで CDP を有効にする場合は [Cisco Discovery Protocol] チェックボックスをオンにします。この機能を無効にする場合は、オフにします。デフォルト値はイネーブルです。

  （注） ステップ 2 で CDP を無効していた場合、コントローラ CDP が無効になっていることを示すメッセージが表示されます。

- 次の手順に従って、特定のイーサネットインターフェイス、無線、またはスロットに対して CDP を有効にします。

  [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

  目的のアクセス ポイントのリンクをクリックします。

  [Interfaces] タブを選択し、[CDP Configuration] セクションで無線またはスロットの対応するチェックボックスをオンにします。

  （注） 無線に対する設定は、メッシュ アクセス ポイントにだけ適用されます。

  [Apply] をクリックして、変更を確定します。

- このコントローラに現在アソシエートされているすべてのアクセス ポイントで CDP を有効または無効にする手順は、次のとおりです。

  [Wireless] > [Access Points] > [Global Configuration] の順に選択して [Global Configuration] ページを開きます。

  コントローラにアソシエートされているすべてのアクセス ポイントで CDP を有効にするには、[CDP State] チェックボックスをオンにします。すべてのアクセス ポイントで CDP を無効にするには、オフにします。デフォルト値はオンです。特定のイーサネット インターフェイス、無線、またはスロットのチェックボックスをオンにすることで、それらに対する CDP を有効にできます。この設定は、コントローラにアソシエートされているすべてのアクセス ポイントに適用されます。

[Apply] をクリックして、変更を確定します。

ステップ 9 [Save Configuration] をクリックして、変更を保存します。

Cisco Discovery Protocol の設定（CLI）

手順

ステップ 1 次のコマンドを入力して、コントローラ上で CDP を有効または無効にします。

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

CDP はデフォルトで有効になっています。

ステップ 2 次のコマンドを入力して、CDP メッセージが生成される間隔を指定します。

config cdp timer *seconds*

範囲は 5 ～ 254 秒で、デフォルト値は 60 秒です。

ステップ 3 次のコマンドを入力して、生成された CDP パケットの中の存続可能時間値としてアドバタイズされる時間の長さを指定します。

config cdp holdtime *seconds*

範囲は 10 ～ 255 秒で、デフォルト値は 180 秒です。

ステップ 4 次のコマンドを入力して、コントローラでサポートされる最高の CDP バージョンを指定します。

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

デフォルト値は [v1] です。

ステップ 5 **config ap cdp** {**enable** | **disable**} **all** コマンドを入力して、コントローラに join しているすべてのアクセス ポイント上で CDP を有効または無効にします。

config ap cdp disable all コマンドは、コントローラに join しているすべてのアクセス ポイントおよび今後 join するすべてのアクセス ポイントの CDP を無効にします。CDP は、コントローラまたはアクセス ポイントのリブート後も現在と将来のアクセス ポイントで無効のままになります。CDP を有効にするには、**config ap cdp enable all** コマンドを入力します。

（注） コントローラに join しているすべてのアクセス ポイントで CDP を有効にした後、ステップ 6 のコマンドを使用して個々のアクセス ポイントで CDP を無効にした後再び有効にできます。コントローラに join されたすべてのアクセス ポイントで CDP を無効にした後は、個々のアクセス ポイントで CDP を有効にし、無効にすることはできません。

ステップ 6 次のコマンドを入力して、特定のアクセス ポイントで CDP を有効または無効にします。

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

ステップ 7 次のコマンドを入力して、特定またはすべてのアクセス ポイントで特定のインターフェイスに CDP を設定します。

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

（注） config ap cdp コマンドを使用して無線インターフェイスに CDP を設定した場合、その設定はメッシュ アクセス ポイントにしか適用されないことを示す警告メッセージが表示されます。

ステップ 8 次のコマンドを入力して、変更を保存します。

save config

Cisco Discovery Protocol 情報の表示

Cisco Discovery Protocol 情報の表示（GUI）

手順

ステップ 1 [Monitor] > [CDP] > [Interface Neighbors] の順に選択して、[CDP > Interface Neighbors] ページを開きます。

このページには、次の情報が表示されます。

- CDP パケットが受信されたコントローラ ポート
- 各 CDP ネイバーの名前
- 各 CDP ネイバーの IP アドレス
- CDP パケットの送信に各 CDP ネイバーが使用するポート
- 各 CDP ネイバー エントリの有効期限までの残り時間（秒）
- 各 CDP ネイバーの機能は、R：ルータ、T：転送ブリッジ、B：ソース ルート ブリッジ、S：スイッチ、H：ホスト、I：IGMP、r：リピータ、M：リモート管理デバイスとして表示されます。
- 各 CDP ネイバー デバイスのハードウェア プラットフォーム

ステップ 2 目的のインターフェイス ネイバーの名前をクリックして、各インターフェイスの CDP ネイバーの詳細情報を表示します。[CDP > Interface Neighbors > Detail] ページが表示されます。

このページには、次の情報が表示されます。

- CDP パケットが受信されたコントローラ ポート
- CDP ネイバーの名前

- CDP ネイバーの IP アドレス
- CDP パケットの送信に CDP ネイバーが使用するポート
- アドバタイズされている CDP バージョン（v1 または v2）
- CDP ネイバー エントリの有効期限までの残り時間（秒）
- CDP ネイバーの機能（[Router]、[Trans Bridge]、[Source Route Bridge]、[Switch, Host]、[IGMP]、[Repeater]、または [Remotely Managed Device]）
- CDP ネイバー デバイスのハードウェア プラットフォーム
- CDP ネイバーで実行されているソフトウェア

ステップ 3 （注） Cisco Aironet 1830 シリーズまたは Cisco Aironet 1850 シリーズの AP が DHCP 経由で IP アドレスを受信しない場合、6.x.x.x の範囲のデフォルト IP アドレスが AP に割り当てられます。接続されているスイッチで show cdp neighbor コマンドを実行すると、AP の CDP ネイバー テーブル内のこの IP アドレスが表示されます。

DHCP の問題が解決された後（問題があった場合）、AP に DHCP プールから IP アドレスが再度割り当てられます。

[AP Neighbors] を選択して、コントローラに接続されているすべてのアクセス ポイントの CDP ネイバーのリストを表示します。[CDP AP Neighbors] ページが表示されます。

ステップ 4 目的のアクセス ポイントの [CDP Neighbors] リンクをクリックして、特定のアクセス ポイントの CDP ネイバーのリストを表示します。[CDP > AP Neighbors] ページが表示されます。

このページには、次の情報が表示されます。

- 各アクセス ポイントの名前
- 各アクセス ポイントの IP アドレス
- 各 CDP ネイバーの名前
- 各 CDP ネイバーの IP アドレス
- 各 CDP ネイバーが使用するポート
- アドバタイズされている CDP バージョン（v1 または v2）

ステップ 5 目的のアクセス ポイントの名前をクリックして、アクセス ポイントの CDP ネイバーの詳細情報を表示します。[CDP > AP Neighbors > Detail] ページが表示されます。

このページには、次の情報が表示されます。

- アクセス ポイントの名前
- アクセス ポイントの無線の MAC アドレス
- アクセス ポイントの IP アドレス
- CDP パケットが受信されたインターフェイス

- CDP ネイバーの名前
- CDP ネイバーの IP アドレス
- CDP ネイバーが使用するポート
- アドバタイズされている CDP バージョン（v1 または v2）
- CDP ネイバー エントリの有効期限までの残り時間（秒）
- CDP ネイバーの機能（R：ルータ、T：転送ブリッジ、B：ソースルートブリッジ、S：スイッチ、H：ホスト、I：IGMP、r：リピータ、M：リモート管理デバイス）
- CDP ネイバー デバイスのハードウェア プラットフォーム
- CDP ネイバーで実行されているソフトウェア

ステップ 6 [Traffic Metrics] を選択して、CDP トラフィック情報を表示します。[CDP > Traffic Metrics] ページが表示されます。

このページには、次の情報が表示されます。

- コントローラで受信した CDP パケット数
- コントローラから送信した CDP パケット数
- チェックサム エラーが発生したパケット数
- メモリ不足のためにドロップされたパケット数
- 無効なパケット数

Cisco Discovery Protocol 情報の表示（CLI）

手順

ステップ 1 次のコマンドを入力して、CDP のステータスを確認し、CDP プロトコル情報を表示します。

show cdp

ステップ 2 次のコマンドを入力して、すべてのインターフェイスのすべての CDP ネイバーのリストを確認します。

show cdp neighbors [detail]

オプションの detail コマンドを指定すると、コントローラの CDP ネイバーの詳細な情報が表示されます。

（注） このコマンドは、コントローラの CDP ネイバーのみを表示します。コントローラにアソシエートしているアクセス ポイントの CDP ネイバーは表示されません。アクセス ポイントごとの CDP ネイバーのリストを表示するコマンドは、この後で説明します。

ステップ 3 次のコマンドを入力して、データベース内のすべての CDP エントリを表示します。

show cdp entry all

ステップ 4 次のコマンドを入力して、指定されたポートの CDP トラフィック情報（送受信されるパケット、CRC エラーなど）を表示します。

show cdp traffic

ステップ 5 次のコマンドを入力して、特定のアクセス ポイントの CDP ステータスを表示します。

show ap cdp ap-name *Cisco_AP*

ステップ 6 次のコマンドを入力して、このコントローラに接続されたすべてのアクセス ポイントの CDP ステータスを表示します。

show ap cdp all

ステップ 7 次のコマンドを入力して、特定のアクセス ポイントのすべての CDP ネイバーのリストを表示します。

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

（注） アクセス ポイントからコントローラに CDP ネイバー情報が送信されるのは、情報が変更されたときだけです。

ステップ 8 次のコマンドを入力して、コントローラに接続されているすべてのアクセスポイントのすべての CDP ネイバーのリストを表示します。

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

（注） アクセス ポイントからコントローラに CDP ネイバー情報が送信されるのは、情報が変更されたときだけです。

CDP デバッグ情報の取得

- 次のコマンドを入力して、CDP パケットに関連したデバッグ情報を取得します。

  debug cdp packets

- 次のコマンドを入力して、CDP イベントに関連したデバッグ情報を取得します。

debug cdp events

Cisco Aironet 700 シリーズ アクセス ポイント

Cisco 700 シリーズ アクセス ポイントに関する情報

The Cisco Aironet 700 シリーズは、コンパクトなアクセス ポイントで、安全で信頼性の高いワイヤレス接続を提供します。主な特徴：

- 2.4 GHz と 5 GHz に対応した同時デュアル バンド、デュアル無線。
- 最適化されたアンテナおよび無線設計：レート対範囲を最適化するための一貫性のあるネットワーク送受信。
- 無線リソース管理（RRM）：自動自己回復機能により、RF の予測不可能性が最適化され、デッド スポットが減少し、ハイ アベイラビリティ クライアントの接続が保護されます。
- Cisco BandSelect が混合クライアント環境における 5 GHz クライアント接続を強化します。
- 不正検出、wIPS、コンテキスト認識などの高度なセキュリティ機能。

設定の Cisco 700 シリーズ アクセス ポイント

Cisco 700 シリーズ アクセス ポイントには 4 つの LAN ポートがあります。これらのポートの設定はフラッシュ上のファイルに保存されます。AP は再起動時にこの設定を取得します。AP は join 後にこの情報をコントローラと共有し、コントローラに最新情報が表示されるようにします。

（注） コントローラが AP 上の既存の設定をすべて消去すると、AP は保存されたポート情報を削除して、デフォルト設定を適用します。すべての LAN ポートがデフォルトで無効になっています。

LAN ポートの有効化（CLI）

手順

- 次のコマンドを入力して、アクセス ポイントの LAN ポートを有効または無効にします。
  config ap lan port-id *port-id* {**enable** | **disable**} *AP-NAME*
- 次のコマンドを入力して、ポート情報を表示します。
  showap lan port-id *port-id AP-NAME*
- 次のコマンドを入力して、ポートの要約情報を表示します。
  showap lan port-summary *AP-NAME*

702W LAN ポートの有効化

リリース 7.6 では、イーサネット ポートの管理またはそれらの別々の VLAN への割り当てはサポートされません。すべてのポートが、AP のスイッチ ポートが設定されている同じアクセス VLAN にマッピングされます。または、ポートがトランクの場合は、ネイティブ VLAN にマッピングされます。リリース 8.0 以降は、ポートを有効または無効にして、必要に応じてそれらを特定の VLAN にマッピングできます。これにより、トラフィックを無線ネットワークと有線ネットワーク間だけでなく、4 つのイーサネット ポート間でも分離することができます。

手順

ステップ 1 次のコマンドを入力して、アクセス ポイントの LAN ポートを有効または無効にします。
config ap lan port-id *port-id* ｛ **enable**｜**disable**｝*AP-NAME*

ステップ 2 次のコマンドを入力して、ポート ID を設定します。
Configap lan port-id *port-id AP-NAME*

ステップ 3 次のコマンドを入力して、アクセス VLAN を有効にします。
Configap lan enable accessvlan*vlan-id*

ステップ 4 次のコマンドを入力して、VLAN のポート ID を有効にします。
Configap lan enable accessvlan*port-id*

ステップ 5 次のコマンドを入力して、AP の VLAN を設定します。
Configap lan enable accessvlan*vlan-id port-id Cisco AP*

Cisco Aironet 702W AP 上の有線ポートの RLAN サポート

Cisco Aironet 702W AP 上の有線ポートのリモート LAN サポートについて

Cisco Aironet 702W アクセス ポイント（AP）のリモート LAN（RLAN）は、シスコ ワイヤレス LAN コントローラを使用した有線クライアントの認証に使用されます。Cisco 702W AP の LAN ポートには、RLAN で設定することで、さまざまな IEEE 802.1 X 認証モードを設定できます。

クライアントと認証サーバ間の IEEE 802.1 X 認証メッセージ交換は、AP でローカルに行われます。IEEE 802.1 X の設定はすべて Cisco WLC を介して行われます。両方のポートの制御と制約事項は、AP でローカルに考慮されます。

Cisco WLC の役割

Cisco WLC はオーセンティケータとして機能し、有線クライアントからの Extensible Authentication Protocol（EAP）over LAN（EAPOL）メッセージは AP を経由して Cisco WLC に届きます。そして、Cisco WLC は設定されている認証、認可、およびアカウンティング（AAA）サーバと通信します。

AP の役割

AP は、Control and Provisioning of Wireless Access Points（CAPWAP）トンネルを使用した、有線クライアントからCisco WLCへの認証パケットのトンネリングにおけるリレーとして機能します。ポートが認証されると、AP はポートの制御と監視を担当します。

AP の LAN ポートは Cisco WLC で設定されて、対応する AP にプッシュされます。

最初に、AP を結合するクライアントが Cisco WLC に EAPOL パケットを渡すと、その AP が IEEE 802.1 X ポートを設定します。

IEEE 802.1X 認証モードについて

このトピックでは、さまざまな IEEE 802.1 X 認証モードについて説明します。

シングルホスト モード

AP でシングルホスト認証モードが設定されていて、ポート リンク ステートがアップになっている場合、AP はEAPoLフレームを送信してクライアントを検出します。クライアントがログオフした場合、または別のクライアントと置き換わった場合、AP はそのポート リンク ステートをダウンに変更し、ポートを無許可ステートにします。

シングルホスト設定モードは、コントローラの既存のRLANの設定を使用して設定されます。

マルチホスト モード

マルチホスト認証モードが設定されている場合、そのポートでネットワーク アクセスを取得するすべてのクライアントのうち1つのクライアントのみ認証できます。ポートが無許可ステートになると、スイッチは接続しているすべてのクライアントへのアクセスを拒否します。

違反モード

セキュリティ違反が発生すると、ポートは、次のような設定済みの違反アクションに基づいて保護されます。

- [Shutdown]：ポートを無効にします。
- [Replace]：現在のセッションを削除し、新しいホストの認証を開始します。これはデフォルトの動作です。
- [Protect]：システム メッセージを生成せずに、予期しないMACアドレスを使用するパケットをドロップします。

シングルホスト認証モードでは、データ VLAN で複数のデバイスが検出された場合に違反がトリガーされます。マルチホスト認証モードでは、データ VLAN または音声 VLAN で複数のデバイスが検出された場合に違反がトリガーされます。

（注） セキュリティ違反はマルチホスト認証モードではトリガーできません。

事前認証オープンの設定（CLI）

- 事前認証オープン オプションを使用すると、当初はAP LANポートで無制限のトラフィックが許可され、その他のアクセス制限によってのみ制限されます。
- 事前認証オープン機能は、Cisco Aironet 1810 OEAP ではサポートされていません。

手順

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

例：

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

VLAN で事前認証オープンを設定します。

IEEE 802.1x 認証モードの設定（CLI）

次の 3 つの異なる認証モードを設定できます。

- シングルホスト
- マルチホスト
- 違反モード

手順

認証を設定するには、次のいずれかのタスクを実行します。

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

  例：

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

  リモート LAN シングルホスト モードを設定します。シングルホスト モードでは、データ VLAN で複数のデバイスが検出された場合に違反がトリガーされます。

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

  例：

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

  リモート LAN マルチホスト モードを設定します。マルチホスト モードでは、データまたは音声 VLAN で複数のデバイスが検出された場合に違反がトリガーされます。マルチホスト モードではセキュリティ違反をトリガーできません。

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

  例：

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

  リモート LAN の違反モードを設定します。

Cisco WLC での IEEE 802.1x 認証の有効化（GUI）

手順

ステップ 1 [WLANs] を選択します。

[WLANs] ウィンドウが表示されます。

ステップ 2 対応する WLAN の ID 番号をクリックします。

[WLANs > Edit] ウィンドウが表示されます。

ステップ 3 [Security] > [Layer 2] タブをクリックします。

ステップ 4 [Layer 2 Security] ドロップダウン リストから [802.1x] を選択します。

IEEE 802.1x パラメータが表示されます。

a) ドロップダウン リストで [Host Mode] を選択します。
b) ドロップダウン リストで [Violation Mode] を選択します。
c) [Pre Authentication] チェックボックスをオンにし、[Pre Auth Vlan] フィールドに事前認証 VLAN ID を入力します。

ステップ 5 [Apply] をクリックします。

IEEE 802.1x 認証の有効化（CLI）

既存のリモート LAN の設定を使用して IEEE 802.1x 認証を有効にします。Cisco WLC でリモート LAN を設定後、その設定を AP グループに適用し、その AP グループ内の個々の AP にプッシュします。

手順

ステップ 1 **config remote-lan security 802.1x** {**enable** | **disable**} *remote-lan-id*

例：

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

リモート LAN のセキュリティ ポリシーを設定します。

ステップ 2 **config remote-lan apgroup add** *ap-group*

例：

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

リモート LAN の WLAN AP グループを追加します。

Cisco WLC 内の AP ポートへの RLAN のマッピング（GUI）

AP ポートに RLAN をマッピングするには、次の手順を実行します。このタスクは、AP 単位または AP グループ単位で実行できます。

手順

ステップ 1 [WLANs] > [Advanced] > [AP Groups] を選択します。

[AP Groups] ウィンドウが表示されます。

ステップ 2 対応する AP グループ名をクリックします。

[AP Group] > [Edit] ウィンドウが表示されます。

ステップ 3 [WLANs] タブをクリックして、[Add New] をクリックします。

[Add New] エリアが表示されます。

ステップ 4 WLAN SSID のドロップダウン リストを使用して、追加する RLAN を選択します。

ステップ 5 [Interface/Interface Group] ドロップダウン リストから、所属先のグループを選択します。デフォルトの選択肢は [management] です。

ステップ 6 [Add] をクリックします。

ステップ 7 [Ports/Module] タブをクリックします。

ステップ 8 [LAN Ports] エリアでドロップダウンを使用して、LAN ポートに RLAN を追加します。

ステップ 9 [Apply] をクリックします。

Cisco WLC 内の AP ポートへの RLAN のマッピング（CLI）

認証を行うために設定されているリモート LAN に、AP 内の LAN ポートをマッピングします。AP グループ レベルでは、LAN ポート設定を使用してポート レベルの設定を行います。

手順

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

例：

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

リモート LAN を AP グループ内の LAN ポートに割り当てます。

AP ごとの Cisco WLC 内の AP ポートへの RLAN のマッピング（GUI）

AP ポートに RLAN をマッピングするには、次の手順を実行します。このタスクは、AP 単位または AP グループ単位で実行できます。

手順

ステップ 1 [Wireless] > [Access Points] > [All APs] の順に選択します。

[All APs] ウィンドウが表示されます。

ステップ 2 対応する AP をクリックします。

[All Details] ウィンドウが表示されます。

ステップ 3 [Interfaces] タブをクリックします。

ステップ 4 [LAN Ports] エリアで、ポートの状態を [Enable] に設定し、[VLAN] チェックボックスをオンにして、[VLAN ID] フィールドに RLAN WLAN ID を入力します。

ステップ 5 [Layer 2 Security] ドロップダウン リストから [802.1x] を選択します。

IEEE 802.1x のパラメータが表示されます。

ステップ 6 [Key Size] ドロップダウンリストから、IEEE 802.1x データ暗号化のキーサイズを選択します。

（注） 事前認証 VLAN が必要な場合は、[Pre Authentication] を有効にして、事前認証 VLAN ID を入力します。

Cisco Aironet 702w アクセス ポイントの AP ポート LAN クライアントに対する MAB 認証のサポート

Cisco Aironet 702w アクセス ポイントの AP ポート LAN クライアントに対する MAB 認証のサポート

MAC 認証バイパス（MAB）機能を使用すると、エンドポイントの MAC アドレスを使用してポートベースのアクセス コントロールができます。MAB 対応ポートは、接続するデバイスの MAC アドレスに基づいて有効または無効にできます。MAB は、クライアントが EAP パケットを認識しない場合、主に、非-802.1 x クライアントの場合に役立ちます。

この機能は、リモート LAN（RLAN）の Cisco Aironet 702w アクセス ポイントでサポートされています。

AP ポート LAN クライアントでの MAB のサポートの設定（GUI）

始める前に

この機能は、RLAN 機能をサポートする Cisco Aironet 702w アクセス ポイントでのみサポートされています。

手順

ステップ 1 [WLANs] を選択して、[WLANs] ウィンドウを開きます。

ステップ 2 目的の WLAN の ID 番号をクリックして、[WLANs] > [Edit] ウィンドウを開きます。

ステップ 3 [Security] > [Layer 2] タブを選択します。

ステップ 4 [MAB Mode] チェックボックスをオンにします。

エンドポイントの MAC アドレスを使用してポートベースのアクセス コントロールを有効にします。

AP ポート LAN クライアントでの MAB のサポートの設定（CLI）

手順

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

例：

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

エンドポイントの MAC アドレスを使用してポートベースのアクセス コントロールを有効にします。