



ポートとインターフェイスの設定

この章では、コントローラの物理ポートとインターフェイスの概要、およびこれらを設定する手順について説明します。この章の内容は、次のとおりです。

- [ポートとインターフェイスの概要 \(P. 3-2\)](#)
- [管理、AP マネージャ、仮想、およびサービス ポートの各インターフェイスの設定 \(P. 3-12\)](#)
- [動的インターフェイスの設定 \(P. 3-18\)](#)
- [ポートの設定 \(P. 3-22\)](#)
- [リンク集約の有効化 \(P. 3-34\)](#)
- [49 個以上のアクセス ポイントをサポートするように 4400 シリーズ コントローラを設定 \(P. 3-39\)](#)

ポートとインターフェイスの概要

コントローラと無線ネットワーク ポートの接続方法を理解するカギとなるのは、ポート、インターフェイス、および WLAN の3つの概念です。

ポート

ポートは、コントローラ プラットフォーム上に存在し、接続に使用される物理的実体です。コントローラには、ディストリビューション システム ポートと、サービス ポートの2種類があります。各コントローラに用意されているポートは以下の図のとおりです。



(注)

Cisco Integrated Services Router のコントローラ、および Cisco WiSM のコントローラには外部物理ポートはありません。これらをネットワークに接続する場合、ルータ上またはスイッチ上のポートを使用します。

図 3-1 Cisco 2000 シリーズ Wireless LAN Controller のポート

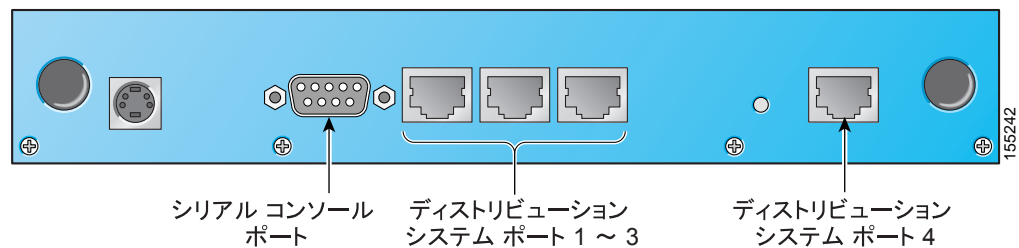


図 3-2 Cisco 2100 シリーズ Wireless LAN Controller のポート

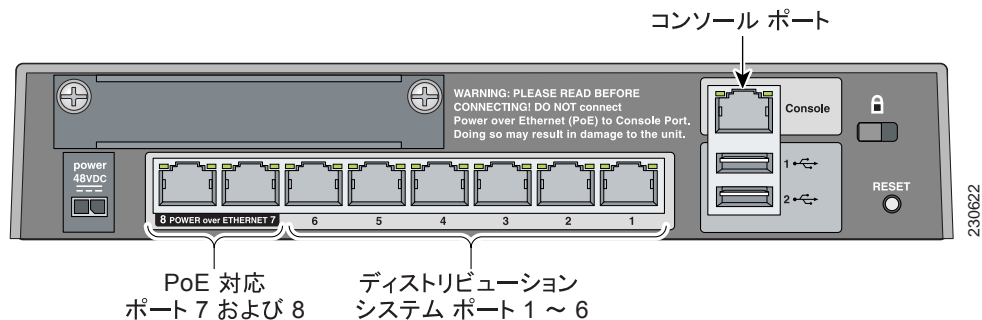
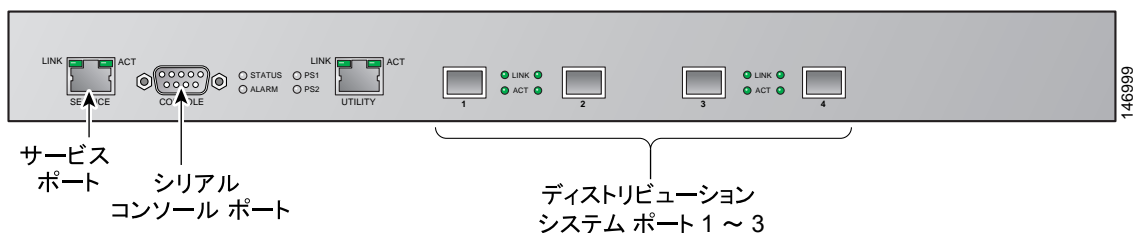


図 3-3 Cisco 4400 シリーズ Wireless LAN Controller のポート





(注) 図 3-3 は Cisco 4404 コントローラです。Cisco 4402 コントローラもこれに類似していますが、ディストリビューションシステム ポートの数は2つです。

図 3-4 Catalyst 3750G 統合型無線 LAN コントローラ スイッチのポート

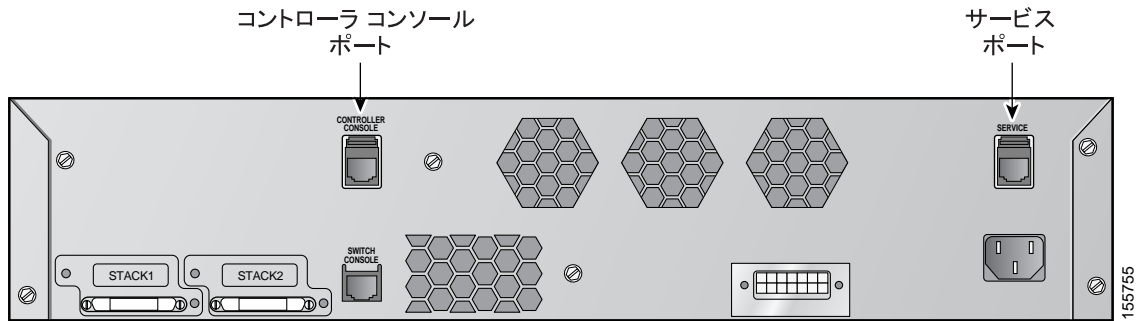


表 3-1 は、1 コントローラあたりのポート数の一覧です。

表 3-1 コントローラ ポート

コントローラ	サービス ポート	ディストリビューションシステムイーサネット ポート	シリアルコンソールポート
2000 シリーズ	なし	4	1
2100 シリーズ	なし	8 (6 + PoE ポート 2 個)	1
4402	1	2	1
4404	1	4	1
Cisco WiSM	2 (ポート 9 および 10)	8 (ポート 1 ~ 8)	2
Cisco 28/37/38xx シリーズ サービス統合型ルータに内蔵されたコントローラネットワーク モジュール	なし	1	1 ¹
Catalyst 3750G 統合型無線 LAN コントローラ スイッチ	1	2 (ポート 27 および 28)	1

1. ギガビットイーサネットバージョンのコントローラ ネットワーク モジュールのポートレートは最高 9600bps ですが、ファストイーサネットバージョンでは 57600bps までサポートされます。



(注) 付録 E には、統合型コントローラの論理接続図および関連するソフトウェア コマンドが記載されています。

ディストリビューション システム ポート

ディストリビューション システム ポートは近接スイッチにコントローラを接続し、これら 2 つのデバイス間のデータ パスとして働きます。

- Cisco 2000 シリーズ コントローラは、4 個の 10/100 銅線イーサネット ディストリビューション システム ポートを持ち、これらのポートを通じて最大 6 個のアクセス ポイントをサポートします。
- Cisco 2100 シリーズ コントローラは、8 個の 10/100 銅線イーサネット ディストリビューション システム ポートを持ち、これらのポートを通じて最大 6 個のアクセス ポイントをサポートします。ポート 7 と 8 の 2 つは Power-over-Ethernet (PoE) に対応しており、ポートに接続されたアクセス ポイントに直接電力を供給することができます。
- Cisco 4402 コントローラは、2 つのギガビット イーサネット ディストリビューション システム ポートを持ち、これらはそれぞれ、最大 48 個のアクセス ポイントを管理できます。ただし、帯域幅の制約により、アクセス ポイントの数は、1 ポートあたり最大 25 個にしておくことをお勧めします。4402-25 モデルおよび 4402-50 モデルでは、合計 25 個または 50 個のアクセス ポイントをコントローラに接続できます。
- Cisco 4404 コントローラは、4 つのギガビット イーサネット ディストリビューション システム ポートを持ち、これらはそれぞれ、最大 48 個のアクセス ポイントを管理できます。ただし、帯域幅の制約により、アクセス ポイントの数は、1 ポートあたり最大 25 個にしておくことをお勧めします。4404-25 モデル、4404-50 モデル、および 4404-100 モデルでは、合計 25 個、50 個、または 100 個のアクセス ポイントをコントローラに接続できます。



- (注) 4402 および 4404 コントローラのギガビット イーサネット ポートは、次の SX/LC/T 小型フォーム ファクタ プラグイン (SFP) モジュールを受け付けます。
- 1000BASE-SX SFP モジュール。LC 物理コネクタを使用した 850nm (SX) 光ファイバリンクで 1000Mbps の有線接続をネットワークに提供します。
 - 1000BASE-LX SFP モジュール。LC 物理コネクタを使用した 1300nm (LX/LH) 光ファイバリンクで 1000Mbps の有線接続をネットワークに提供します。
 - 1000BASE-T SFP モジュール。RJ-45 物理コネクタを使用した銅線リンクで 1000Mbps の有線接続をネットワークに提供します。

- Cisco Catalyst 6500 シリーズ スイッチ Wireless Services Module (WiSM; ワイヤレス サービス モジュール) および Cisco 7600 シリーズ ルータ Wireless Services Module (WiSM) には、スイッチまたはルータと統合コントローラを接続する内部ギガビット イーサネット ディストリビューション システム ポートが 8 つあります (ポート 1 ~ 8)。これらの内部ポートは、スイッチまたはルータのバックプレーン上にあり、フロントパネルからは見えません。これらのポートを通じて、最大 300 個のアクセス ポイントをサポートできます。
- Cisco 28/37/38xx シリーズ サービス統合型ルータの内蔵コントローラ ネットワーク モジュールがサポートするアクセス ポイント数は、ネットワーク モジュールのバージョンに応じて最大 6 個、8 個、または 12 個 (最大クライアント数はそれぞれ 256、256、350) となります。ネットワーク モジュールは、ルータと統合コントローラを接続するファスト イーサネット ディストリビューション システム ポート (6 アクセス ポイントバージョンの場合) またはギガビット イーサネット ディストリビューション システム ポート (8 アクセス ポイントバージョンまたは 12 アクセス ポイントバージョンの場合) を通じてこれらのアクセス ポイントをサポートします。このポートは、ルータのバックプレーン上にあり、フロントパネルからは見えません。ファスト イーサネット ポートの動作速度は最大 100Mbps、ギガビット イーサネット ポートの動作速度は最大 1Gbps です。

- Catalyst 3750G 統合型無線 LAN コントローラ スイッチには、スイッチと統合コントローラを接続する内部ギガビットイーサネット ディストリビューション システム ポートが2つあります (ポート 27 と 28)。これらの内部ポートは、スイッチ バックプレーン上にあり、フロント パネルからは見えません。各ポートでは、最大 48 個のアクセス ポイントを管理できます。ただし、帯域幅の制約により、アクセス ポイントの数は、1 ポートあたり最大 25 個にしておくことをお勧めします。-S25 モデル、および -S50 モデルでは、コントローラの接続に、合計 25 または 50 個のアクセス ポイントが利用できます。



(注) 49 個以上のアクセス ポイントをサポートするように Cisco 4400 シリーズ コントローラを設定するには、「[49 個以上のアクセス ポイントをサポートするように 4400 シリーズ コントローラを設定](#)」の項 (P. 3-39) を参照してください。

デフォルトでは、各ディストリビューション システム ポートは 802.1Q VLAN トランク ポートです。ポートの VLAN トランク特性は設定できません。



(注) 一部のコントローラは、コントローラのディストリビューション システム ポートすべてを 1 つの 802.3ad ポート チャネルにまとめる Link Aggregation (LAG; リンク集約) をサポートしています。Cisco 4400 シリーズ コントローラは、ソフトウェア リリース 3.2 以降で LAG をサポートし、LAG は Cisco WiSM コントローラ上で自動的に有効になります。詳細は、「[リンク集約の有効化](#)」の項 (P. 3-34) を参照してください。

サービス ポート

Cisco 4100 および 4400 シリーズ コントローラには、10/100 銅線イーサネット サービス ポートもあります。このサービス ポートは、サービス ポート インターフェイスにより制御され、コントローラのアウトオブバンド管理と、ネットワーク障害時のシステム復旧とメンテナンスのために割り当てられています。また、これは、コントローラがブート モードのときにアクティブな唯一のポートです。このサービス ポートは 802.1Q タグを持つことはできないので、近接スイッチ上のアクセス ポートに接続する必要があります。サービス ポートの使用は任意です。



(注) このサービス ポートは、Cisco WiSM の 4404 コントローラと Supervisor 720 の間の内部プロトコル通信に使用されます。



(注) Cisco 2000 および 2100 シリーズ コントローラ、および Cisco サービス統合型ルータのコントローラには、サービス ポートはありません。



(注) サービス ポートには自動認識機能が備わっていません。サービス ポートと通信するには、適切なストレートまたはクロス イーサネット ケーブルを使用する必要があります。

インターフェイス

インターフェイスはコントローラ上の論理実体です。インターフェイスには、IP アドレス、デフォルト ゲートウェイ (IP サブネット用)、プライマリ物理ポート、セカンダリ物理ポート、VLAN 識別子、DHCP サーバなど、複数のパラメータが関連付けられています。

以下の 5 種類のインターフェイスはコントローラで使用できます。これらのうち 4 種類は固定で、セットアップ時に設定されます。

- 管理インターフェイス (固定でセットアップ時に設定。必須)
- AP マネージャ インターフェイス (レイヤ 3 LWAPP を使用する場合。固定でセットアップ時に設定。必須)
- 仮想インターフェイス (固定でセットアップ時に設定。必須)
- サービスポート インターフェイス (固定でセットアップ時に設定。任意)
- 動的インターフェイス (ユーザ定義)

各インターフェイスは少なくとも 1 つのプライマリ ポートにマップされます。一部のインターフェイス (管理および動的) は、オプションのセカンダリ (または、バックアップ) ポートにマップできます。あるインターフェイスのプライマリ ポートに障害が発生すると、このインターフェイスは自動的にバックアップ ポートに移動します。また、複数のインターフェイスを 1 つのコントローラ ポートにマップできます。



(注)

各インターフェイスに対してプライマリ ポートとセカンダリ ポートを個別に設定するのではなく、複数のインターフェイスが 1 つのポート チャネルに動的にマップされるようにコントローラを設定する方法については、「[リンク集約の有効化](#)」の項 (P. 3-34) を参照してください。

管理インターフェイス

管理インターフェイスは、コントローラのインバンド管理や、AAA サーバなどのエンタープライズ サービスへの接続に使用されるデフォルト インターフェイスです。管理インターフェイスは、唯一常時「ping 可能」な、コントローラのインバンド インターフェイス IP アドレスを持ちます。コントローラの GUI にアクセスするには、Internet Explorer の Address フィールドに、コントローラの管理インターフェイスの IP アドレスを入力します。

管理インターフェイスは、コントローラと Cisco 1000 シリーズ Lightweight アクセス ポイントの間のレイヤ 2 通信にも使用されます。このインターフェイスはディストリビューション システム ポート 1 に割り当てる必要がありますが、必要に応じて、バックアップ ポートにマップしたり、WLAN に割り当てることもできます。これは、AP マネージャ インターフェイスと同じ VLAN または IP サブネットに設定できます。ただし、管理インターフェイスは、次のように、他のディストリビューション システム ポートを通じて通信することも可能です。

- レイヤ 2 ネットワークでメッセージを送信し、すべてのディストリビューション システム ポートを通じて、他のコントローラを自動検出し、通信します。
- レイヤ 2 ネットワーク全体で、Cisco 1000 シリーズ Lightweight アクセス ポイント LWAPP ポーリング メッセージを受信し、可能な限り多くの Cisco 1000 シリーズ Lightweight アクセス ポイントを自動検出して、アソシエートし、通信を行います。

LWAPP 通信がレイヤ 2 (同一サブネット) モードに設定されている場合、ポートの数に関係なく、このコントローラには、コントローラ間の全通信と、コントローラとアクセス ポイント間の全通信を制御する管理インターフェイスが 1 つ必要です。LWAPP 通信がレイヤ 3 (異なるサブネット) モードに設定されている場合、ポートの数に関係なく、このコントローラには、コントローラ間の全通信を制御する管理インターフェイスが 1 つと、コントローラとアクセス ポイント間の全通信を制御する AP マネージャ インターフェイスが 1 つ必要です。



- (注) サービスポートが使用中の場合は、サービスポートインターフェイスとは異なるスーパーネット上に管理インターフェイスが存在する必要があります。

AP マネージャ インターフェイス

1つのコントローラに1つ以上の AP マネージャ インターフェイスがあります。このインターフェイスは、Lightweight アクセス ポイントがコントローラに接続した後でコントローラとアクセス ポイントの間で行われるすべてのレイヤ 3 通信に使用されます。AP マネージャの IP アドレスは、コントローラからアクセス ポイントへの LWAPP パケットのトンネル発信元、およびアクセス ポイントからコントローラへの LWAPP パケットの宛先として使用されます。

Cisco 4404 および WiSM コントローラの場合は、すべてのディストリビューション システム ポート (1、2、3、および4) に対して AP マネージャ インターフェイスを設定します。Cisco 4402 コントローラの場合は、ディストリビューション システム ポート 1 および 2 に対して AP マネージャ インターフェイスを設定します。どちらの場合も、静的 (または固定) AP マネージャ インターフェイスは必ずディストリビューション システム ポート 1 に割り当てられ、固有の IP アドレスが与えられます。管理インターフェイスと同じ VLAN または IP サブネット上で AP マネージャ インターフェイスを設定すると、アクセス ポイントのアソシエートにおいて最良の結果が得られますが、このような設定は必須ではありません。



- (注) LAG が有効化されているときは、AP マネージャ インターフェイスは1つだけ存在することができます。LAG が無効の場合は、コントローラの各ポートに対して AP マネージャ インターフェイスを割り当てる必要があります。



- (注) 使用可能なディストリビューション システム ポートが1つだけの場合は、ディストリビューション システム ポート 1 を使用してください。

AP マネージャ インターフェイスは、どのディストリビューション システム ポートを介して通信するときも、できる限り多くの Lightweight アクセス ポイントのアソシエートおよび通信を行うために、レイヤ 3 またはレイヤ 2 ネットワーク全体をリッスンして Lightweight アクセス ポイント (LWAPP) の参加メッセージを検出します。



- (注) AP マネージャ インターフェイスに対するポート冗長化はサポートされません。AP マネージャ インターフェイスをバックアップ ポートにマッピングすることはできません。



- (注) 複数の AP マネージャ インターフェイスの作成と使用については、「[複数の AP マネージャ インターフェイスの使用](#)」の項 (P. 3-39) を参照してください。

仮想インターフェイス

仮想インターフェイスは、モビリティ管理、Dynamic Host Configuration Protocol (DHCP) リレー、およびゲスト Web 認証などのレイヤ 3 の組み込みセキュリティをサポートするために使用されます。また、レイヤ 3 Web 認証が有効な場合に証明書のソースを確認するために、レイヤ 3 Security Manager と Mobility Manager で使用される Domain Name System (DNS; ドメイン ネーム システム) ゲートウェイのホスト名も管理します。

具体的には、仮想インターフェイスは主に次の 2 つの役割を果たします。

- その IP アドレスを DHCP サーバから取得する無線クライアントの DHCP サーバプレースホルダの役割。
- Web Authentication Login ウィンドウのリダイレクトアドレスの役割。



(注) Web 認証の詳細は、第 5 章を参照してください。

仮想インターフェイスの IP アドレスは、コントローラと無線クライアントの間の通信でのみ使用されます。ディストリビューション システム ポートから出て、スイッチド ネットワークに入るパケットの発信元アドレスや、宛先アドレスとなることは決してありません。システムを正常に動作させるには、仮想インターフェイスの IP アドレスを設定する必要がありますが (0.0.0.0 は設定できません)、ネットワーク上の他のデバイスは、この仮想インターフェイスと同じアドレスを使用できません。したがって、仮想インターフェイスは、1.1.1.1 など、割り当てられず、使用もされないゲートウェイ IP アドレスを使って設定する必要があります。仮想インターフェイスの IP アドレスは ping できませんし、ネットワーク上のいかなるルーティング テーブルにも存在してはいけません。また、仮想インターフェイスをバックアップ ポートにマップすることもできません。



(注) 同一のモビリティ グループに属するコントローラはすべて、同じ仮想インターフェイス IP アドレスを使用して設定する必要があります。設定しなかった場合、コントローラ間ローミングが動作しているように見えても、ハンドオフが完了せず、クライアントの接続はしばらくの間切断されます。

サービス ポート インターフェイス

サービス ポート インターフェイスはサービス ポートを介した通信を制御し、サービス ポートに対して静的にマップされます。このインターフェイスは、管理インターフェイス、AP マネージャ インターフェイス、およびその他の動的インターフェイスとは異なるスーパーネット上の IP アドレスを必要とします。また、バックアップ ポートにマップすることはできません。この設定により、コントローラを直接管理したり、10.1.2.x などの専用オペレーティング システム ネットワーク経由で管理したりできるようになり、ネットワーク ダウンタイム時のサービスのアクセスが保証されます。

サービス ポートは DHCP を使用して IP アドレスを取得したり、このポートに固定 IP アドレスを割り当てたりすることはできませんが、サービス ポート インターフェイスにデフォルト ゲートウェイを割り当てることはできません。サービス ポートへのリモート ネットワーク アクセスに使用される静的なルートはコントローラを通じて定義できます。



(注) サービス ポート インターフェイスを持つのは Cisco 4400 シリーズのコントローラのみです。



(注) Cisco WiSM コントローラの両方のサービス ポート インターフェイス上に IP アドレスを設定する必要があります。設定しないと、近接スイッチは各コントローラの状態をチェックできません。

動的インターフェイス

動的インターフェイスは VLAN インターフェイスとも呼ばれ、ユーザによって作成され、無線 LAN クライアントの VLAN に相当する設計になっています。1つのコントローラで最大 512 個の動的インターフェイス (VLAN) をサポートできます。動的インターフェイスはそれぞれ、個別に設定され、コントローラの任意またはすべてのディストリビューション システム ポートに独立した通信ストリームを設定できます。動的インターフェイスはそれぞれ、コントローラとその他のネットワーク デバイスの間の VLAN などの通信を制御し、このインターフェイスにマップされている WLAN に関連付けられた無線クライアントの DHCP リレーとして働きます。動的インターフェイスは、WLAN、レイヤ 2 管理インターフェイス、およびレイヤ 3 AP マネージャ インターフェイスに割り当てることができます。また、動的インターフェイスをバックアップ ポートにマップすることもできます。

1つ、または複数の動的インターフェイスをディストリビューション システム ポートに設定できます。また、1つも設定しなくても問題ありません。ただし、動的インターフェイスはすべて、このポートに設定された他のインターフェイスとは異なる VLAN または IP サブネットに設定する必要があります。ポートにタグが付いていない場合は、動的インターフェイスはすべて、このポートに設定されている他のインターフェイスとは異なる IP サブネットに設定する必要があります。



(注) 動的インターフェイスでは、タグ付きの VLAN を使用する必要があります。

WLAN

WLAN は、Service Set Identifier (SSID; サービス セット ID) をインターフェイスにアソシエートします。これは、セキュリティ、Quality of Service (QoS)、無線ポリシーなどその他の無線ネットワーク パラメータを使って設定されます。WLAN は、コントローラ 1つあたり、最大 16 個のアクセス ポイントを設定できます。



(注) WLAN を設定する手順については、第 6 章を参照してください。

図 3-5 は、ポート、インターフェイス、および WLAN の関係を表しています。

図 3-5 ポート、インターフェイス、および WLAN

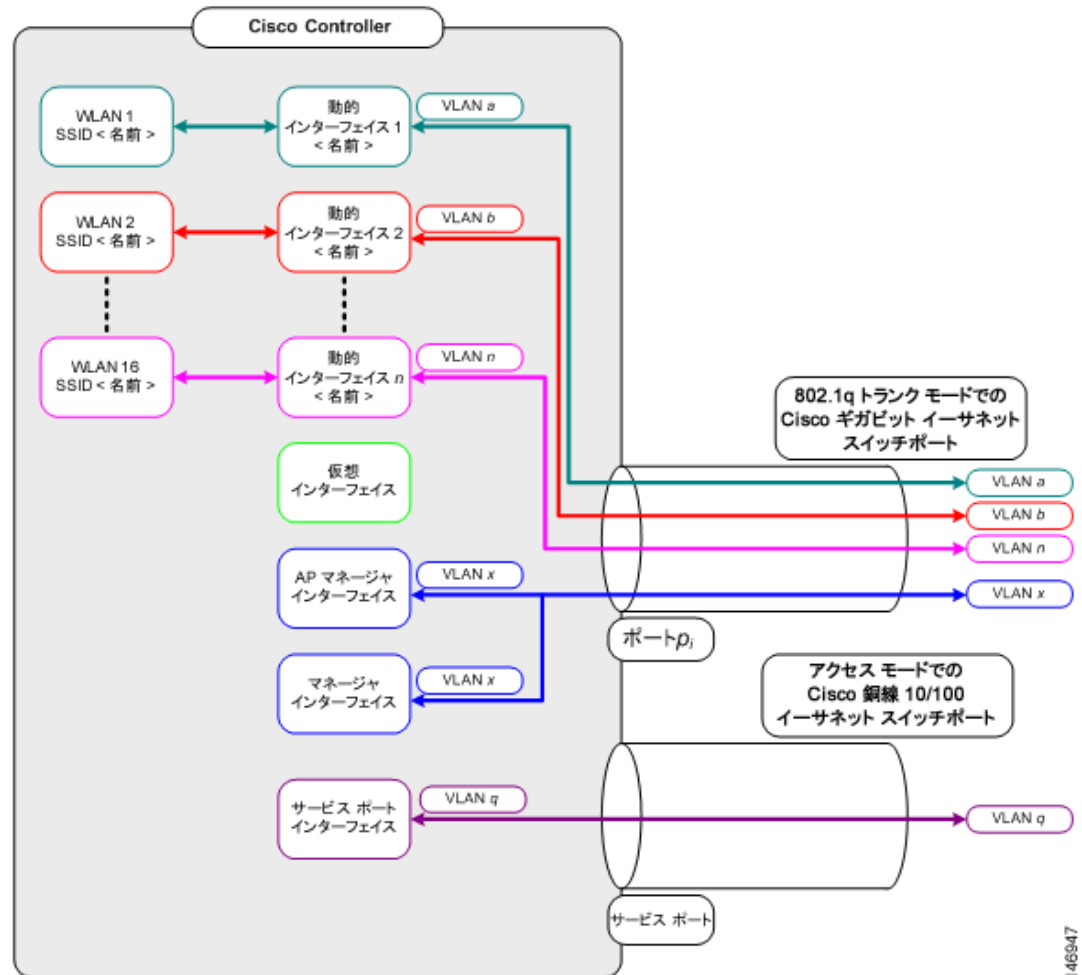


図 3-5 に示すとおり、個々のコントローラ ポート接続は 802.1Q トランクなので、近接スイッチ上ではそのように設定する必要があります。Cisco スイッチでは、802.1Q トランクのネイティブ VLAN にはタグはついていません。したがって、隣接する Cisco スイッチでネイティブ VLAN を使用するためにインターフェイスを設定するには、タグなしになるように、コントローラのインターフェイスを設定する必要があります。



(注) VLAN 識別子の値 0 (Controller > Interfaces ページ) は、インターフェイスにタグがつけられていないことを表します。

Cisco スイッチにおいて、デフォルト (タグなし) のネイティブ VLAN は VLAN 1 です。コントローラ インターフェイスがタグ付きとして設定されている (つまり、VLAN 識別子に 0 以外の値が設定されている) 場合、ネイティブのタグなし VLAN ではなく、近接スイッチの 802.1Q トランク設定で VLAN を可能にする必要があります。

コントローラでは、タグ付き VLAN のみを使用することをお勧めします。また、近接スイッチからコントローラポートへの 802.1Q トランク接続では、関連する VLAN のみを許可するようにしてください。その他の VLAN はすべて無効にするか、スイッチポート トランク設定にプルニングする必要があります。コントローラのパフォーマンスを最適化するには、この慣例は極めて重要です。

**(注)**

コントローラが VLAN トラフィックを正常にルーティングできるよう、WLAN と管理インターフェイスにはそれぞれ別の VLAN セットを割り当てることをお勧めします。

以下のページに記載された手順に従って、コントローラのインターフェイスやポートを設定してください。

- [管理、AP マネージャ、仮想、およびサービス ポートの各インターフェイスの設定 \(P. 3-12\)](#)
- [動的インターフェイスの設定 \(P. 3-18\)](#)
- [ポートの設定 \(P. 3-22\)](#)
- [リンク集約の有効化 \(P. 3-34\)](#)
- [49 個以上のアクセス ポイントをサポートするように 4400 シリーズ コントローラを設定 \(P. 3-39\)](#)

管理、AP マネージャ、仮想、およびサービス ポートの各インターフェイスの設定

通常、管理、AP マネージャ、仮想、およびサービス ポートの各インターフェイス パラメータを定義するには、スタートアップ ウィザードを使用します。ただし、コントローラが実行されていれば、GUI または CLI のどちらかを介して、インターフェイス パラメータを表示し、設定できます。



(注) WLAN を DHCP サーバに割り当てるときは、両方が同じサブネット上に存在するようにしてください。同じサブネット上にない場合は、ルータを使用して WLAN と DHCP サーバの間のトラフィックをルーティングする必要があります。

GUI を使用した、管理、AP マネージャ、仮想、およびサービス ポートの各インターフェイスの設定

GUI を使用して、管理、AP マネージャ、仮想、およびサービス ポートの各インターフェイス パラメータを表示し、設定する手順は、次のとおりです。

ステップ 1 **Controller > Interfaces** の順にクリックして、Interfaces ページを開きます (図 3-6 を参照)。

図 3-6 Interfaces ページ

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
ap-manager	untagged	1.100.163.25	Static	Enabled
management	untagged	1.100.163.24	Static	Not Supported
service-port	N/A	172.19.35.31	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported

このページには、現在のコントローラ インターフェイスの設定が表示されます。

ステップ 2 特定のインターフェイスの設定を変更するには、そのインターフェイスの名前をクリックします。このインターフェイスの **Interfaces > Edit** ページが表示されます。

ステップ 3 各インターフェイス タイプについて、次のパラメータを設定します。

管理インターフェイス



(注) 管理インターフェイスでは、工場出荷時にコントローラに設定されたディストリビューション システムの MAC アドレスが使用されます。

- VLAN 識別子



(注) タグなし VLAN については **0**、タグ付き VLAN についてはゼロ以外の値を指定します。コントローラでは、タグ付き VLAN のみを使用することをお勧めします。

- 固定 IP アドレス、IP ネットマスク、およびデフォルト ゲートウェイ
- 物理ポート割り当て
- プライマリ DHCP サーバとセカンダリ DHCP サーバ
- 必要に応じて、アクセス コントロール リスト (ACL) の設定



(注) ACL を作成するには、[第 5 章](#)にある手順に従ってください。

AP マネージャ インターフェイス

- VLAN 識別子



(注) タグなし VLAN については **0**、タグ付き VLAN についてはゼロ以外の値を指定します。コントローラでは、タグ付き VLAN のみを使用することをお勧めします。

- 固定 IP アドレス、IP ネットマスク、およびデフォルト ゲートウェイ



(注) AP マネージャ インターフェイスの IP アドレスは、管理インターフェイスの IP アドレスと異なるものであることが必要です。サブネットは、管理インターフェイスと同じでも同じでなくてもかまいません。ただし、アクセス ポイントのアソシエートにおいて最良の結果を得るには、両方のインターフェイスを同じサブネット上に置くことをお勧めします。

- 物理ポート割り当て
- プライマリ DHCP サーバとセカンダリ DHCP サーバ
- 必要に応じて、アクセス コントロール リスト (ACL) の名前



(注) ACL を作成するには、[第 5 章](#)にある手順に従ってください。

仮想インターフェイス

- 1.1.1.1 のような、架空、未割り当て、または未使用のゲートウェイ IP アドレス。
- DNS ゲートウェイ ホスト名



(注) 確実に接続と Web 認証が行われるためには、DNS サーバは常に仮想インターフェイスをポイントしている必要があります。仮想インターフェイスの DNS ホスト名が設定されている場合は、クライアントが使用する DNS サーバ上で同じ DNS ホスト名が設定されている必要があります。

サービス ポート インターフェイス



(注) サービス ポート インターフェイスでは、工場出荷時にコントローラに設定されたサービス ポートの MAC アドレスが使用されます。

- DHCP プロトコル (有効) または
- DHCP プロトコル (無効) および IP アドレスと IP ネットマスク

ステップ 4 **Save Configuration** をクリックして、変更内容を保存します。

ステップ 5 仮想インターフェイスに何らかの変更を行ったときに変更を有効にするには、コントローラをリブートします。

CLI を使用した、管理、AP マネージャ、仮想、およびサービス ポートの各インターフェイスの設定

この項では、CLI を使用して、管理、AP マネージャ、仮想、およびサービス ポートの各インターフェイス パラメータを表示し、設定する手順について説明します。

CLI を使用した、管理インターフェイスの設定

CLI を使用して、管理インターフェイス パラメータを表示し、設定する手順は、次のとおりです。

ステップ 1 **show interface detailed management** と入力し、現在の管理インターフェイスの設定を表示します。



(注) 管理インターフェイスでは、工場出荷時にコントローラに設定されたディストリビューションシステムの MAC アドレスが使用されます。

ステップ 2 ディストリビューションシステム通信で管理インターフェイスを使用する WLAN を無効にするには、**config wlan disable wlan-number** と入力します。

ステップ 3 次のコマンドを入力し、管理インターフェイスを定義します。

- **config interface address management** *ip-addr ip-netmask gateway*
- **config interface vlan management** {*vlan-id* | 0}



(注) タグなし VLAN については 0、タグ付き VLAN についてはゼロ以外の値を指定します。コントローラでは、タグ付き VLAN のみを使用することをお勧めします。

- **config interface port management** *physical-ds-port-number*
- **config interface dhcp management** *ip-address-of-primary-dhcp-server*
[*ip-address-of-secondary-dhcp-server*]

- **config interface acl management** *access-control-list-name*



(注) ACLの詳細は、第5章を参照してください。

ステップ4 **save config** と入力して、変更内容を保存します。

ステップ5 **show interface detailed management** と入力し、変更内容が保存されたかどうか確認します。

CLI を使用した、AP マネージャ インターフェイスの設定

CLI を使用して、AP マネージャ インターフェイス パラメータを表示し、設定する手順は、次のとおりです。

ステップ1 **show interface summary** と入力し、現在のインターフェイスを表示します。



(注) システムがレイヤ 2 モードで動作している場合は、AP マネージャ インターフェイスは出力に表示されません。

ステップ2 **show interface detailed ap-manager** と入力し、現在の AP マネージャ インターフェイスの設定を表示します。

ステップ3 ディストリビューション システム通信で AP マネージャ インターフェイスを使用する WLAN を無効にするには、**config wlan disable wlan-number** と入力します。

ステップ4 次のコマンドを入力し、AP マネージャ インターフェイスを定義します。

- **config interface address ap-manager** *ip-addr ip-netmask gateway*
- **config interface vlan ap-manager** {*vlan-id* | 0}



(注) タグなし VLAN については 0、タグ付き VLAN についてはゼロ以外の値を指定します。コントローラでは、タグ付き VLAN のみを使用することをお勧めします。

- **config interface port ap-manager** *physical-ds-port-number*
- **config interface dhcp ap-manager** *ip-address-of-primary-dhcp-server*
[*ip-address-of-secondary-dhcp-server*]
- **config interface acl ap-manager** *access-control-list-name*



(注) ACLの詳細は、第5章を参照してください。

ステップ5 **save config** と入力して、変更内容を保存します。

ステップ 6 `show interface detailed ap-manager` と入力し、変更内容が保存されたことを確認します。

CLI を使用した、仮想インターフェイスの設定

CLI を使用して、仮想インターフェイス パラメータを表示し、設定する手順は、次のとおりです。

ステップ 1 `show interface detailed virtual` と入力し、現在の仮想インターフェイスの設定を表示します。

ステップ 2 ディストリビューション システム通信で仮想インターフェイスを使用する WLAN を無効にするには、`config wlan disable wlan-number` と入力します。

ステップ 3 次のコマンドを入力し、仮想インターフェイスを定義します。

- `config interface address virtual ip-address`



(注) `ip-address` には、1.1.1.1 など、架空で、割り当てられていない、未使用のゲートウェイ IP アドレスを入力します。

- `config interface hostname virtual dns-host-name`

ステップ 4 `reset system` と入力します。NVRAM に設定変更を保存するには、確認のプロンプトで **Y** と入力します。コントローラがリブートします。

ステップ 5 `show interface detailed virtual` と入力し、変更内容が保存されたかどうか確認します。

CLI を使用した、サービス ポート インターフェイスの設定

CLI を使用して、サービス ポート インターフェイス パラメータを表示し、設定する手順は、次のとおりです。

ステップ 1 `show interface detailed service-port` と入力し、現在のサービス ポート インターフェイスの設定を表示します。



(注) サービス ポート インターフェイスでは、工場出荷時にコントローラに設定されたサービス ポートの MAC アドレスが使用されます。

ステップ 2 次のコマンドを入力し、サービス ポート インターフェイスを定義します。

- DHCP サーバを設定する場合：`config interface dhcp service-port ip-address-of-primary-dhcp-server [ip-address-of-secondary-dhcp-server]`
- DHCP サーバを無効にする場合：`config interface dhcp service-port none`

- IP アドレスを設定する場合：**config interface address service-port ip-addr ip-netmask gateway**



(注) サービス ポート インターフェイスの最初のオクテットが、内部ネットワーク上の他のインターフェイスのものとは異なるようにしてください。たとえば、次のようなアドレスはサービス ポートに使用しないでください。

- management:10.1.1.1/24

- AP マネージャ：10.1.2.1/24

- サービス ポート：10.10.10.1/24

この例では、他のプライベート ネットワーク、たとえば 192.x、172.x、あるいは 11.x などの範囲内ならばサービス ポートのアドレスとして使用できます。

ステップ 3 このサービス ポートは、コントローラの帯域外管理に使用されます。管理ワークステーションがリモート サブネットにある場合、このリモート ワークステーションからコントローラを管理するには、コントローラにルートを追加する必要があります。そのためには、次のコマンドを入力します。

```
config route network-ip-addr ip-netmask gateway
```

ステップ 4 **save config** と入力して、変更内容を保存します。

ステップ 5 **show interface detailed service-port** と入力し、変更内容が保存されたことを確認します。

動的インターフェイスの設定

この項では、GUI または CLI を使用して動的インターフェイスを設定する手順について説明します。

GUI を使用した動的インターフェイスの設定

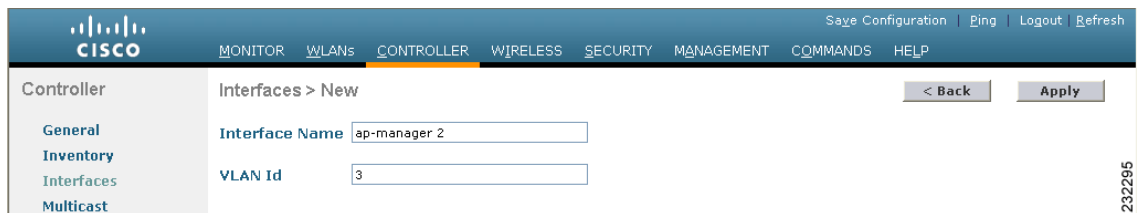
GUI を使用して、動的インターフェイスの新規作成や編集を行う手順は、次のとおりです。

ステップ 1 **Controller > Interfaces** の順にクリックして、**Interfaces** ページを開きます (図 3-6 を参照)。

ステップ 2 次のいずれかの操作を行います。

- 新たに動的インターフェイスを作成するには、**New** をクリックします。**Interfaces > New** ページが表示されます (図 3-7 を参照)。ステップ 3 に進みます。
- 既存の動的インターフェイスの設定を変更するには、インターフェイスの名前をクリックします。そのインターフェイスの **Interfaces > Edit** ページが表示されます (図 3-8 を参照)。ステップ 5 に進みます。
- 既存の動的インターフェイスを削除するには、そのインターフェイスの青いドロップダウン矢印にカーソルを置いて **Remove** を選択します。

図 3-7 Interfaces > New ページ



ステップ 3 図 3-7 のようにインターフェイス名と VLAN 識別子を入力します。



(注) VLAN 識別子に対して 0 以外の値を入力します。動的インターフェイスでは、タグ付きの VLAN を使用する必要があります。

ステップ 4 **Apply** をクリックして、変更を適用します。**Interfaces > New** ページが表示されます (図 3-8 を参照)。

図 3-8 Interfaces > Edit ページ

The screenshot shows the Cisco Wireless LAN Controller configuration page for an interface. The page is titled "Interfaces > Edit" and includes a navigation menu with options like "MONITOR", "WLANs", "CONTROLLER", "WIRELESS", "SECURITY", "MANAGEMENT", "COMMANDS", and "HELP". The left sidebar shows a navigation tree with categories like "General", "Inventory", "Interfaces", "Multicast", "Network Routes", "Internal DHCP Server", "Mobility Management", "Ports", "NTP", "CDP", and "Advanced". The main content area is divided into several sections:

- General Information:** Interface Name (vlan 101), MAC Address (00:0b:85:32:42:c0).
- Interface Address:** VLAN Identifier (101), IP Address (0.0.0.0), Netmask, Gateway.
- Physical Information:** Port Number (0), Backup Port (0), Active Port (0), Enable Dynamic AP Management (checkbox).
- Configuration:** Quarantine (checkbox), Guest Lan (checkbox).
- DHCP Information:** Primary DHCP Server, Secondary DHCP Server.
- Access Control List:** ACL Name (none).

A note at the bottom of the page states: "Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients."

ステップ 5 以下のパラメータを設定します。

- VLAN 識別子
- 固定 IP アドレス、IP ネットマスク、およびデフォルト ゲートウェイ
- 物理ポート割り当て
- 検疫



(注) **Quarantine** チェックボックスは、この VLAN を正常に動作していない VLAN として設定する場合にオンにします。そうすることにより、WLAN がローカル スイッチングに設定されている場合でも、この VLAN に割り当てられた任意のクライアントのデータトラフィックがコントローラを経由するようにします。このコマンドを使用するのは一般に、クライアントがアソシエートされるアクセス ポイントが hybrid-REAP アクセス ポイントであり、ネットワーク アクセス コントロール (NAC) を行うようにアクセス ポイントのコントローラが設定されている場合です。hybrid REAP の詳細は、第 12 章を参照してください。

- プライマリ DHCP サーバとセカンダリ DHCP サーバ
- 必要に応じて、アクセス コントロール リスト (ACL) の名前



(注) ACLの詳細は、第5章を参照してください。



(注) 適切な動作を保証するには、Port Number パラメータと Primary DHCP Server パラメータを設定する必要があります。

ステップ6 **Save Configuration** をクリックして、変更内容を保存します。

ステップ7 作成または編集する動的インターフェイスそれぞれについて、この手順を繰り返します。

CLI を使用した動的インターフェイスの設定

CLI を使用して動的インターフェイスを設定する手順は、次のとおりです。

ステップ1 **show interface summary** と入力し、現在の動的インターフェイスを表示します。

ステップ2 特定の動的インターフェイスの詳細を表示するには、**show interface detailed operator-defined-interface-name** と入力します。

ステップ3 ディストリビューション システム通信に動的インターフェイスを使用する WLAN を無効にするには、**config wlan disable WLAN ID** と入力します。

ステップ4 次のコマンドを入力し、動的インターフェイスを設定します。

- **config interface create operator-defined-interface-name {vlan-id | x}**



(注) VLAN 識別子に対して 0 以外の値を入力します。動的インターフェイスでは、タグ付きの VLAN を使用する必要があります。

- **config interface address operator-defined-interface-name ip-addr ip-netmask [gateway]**
- **config interface vlan operator-defined-interface-name {vlan-id | 0}**
- **config interface port operator-defined-interface-name physical-ds-port-number**
- **config interface dhcp operator-defined-interface-name ip-address-of-primary-dhcp-server [ip-address-of-secondary-dhcp-server]**
- **config interface operator-defined-interface-name quarantine enable**



(注) この VLAN を正常に動作していない VLAN として設定する場合には、このコマンドを使用します。そうすることにより、WLAN がローカル スイッチングに設定されている場合でも、この VLAN に割り当てられた任意のクライアントのデータ トラフィックがコントローラを経由するようにします。このコマンドを使用するのは一般に、クライアントがアソシエートされるアクセス ポイントが hybrid-REAP アクセス ポイントであり、ネットワーク アクセス コントロール (NAC) を行うようにアクセス ポイントのコントローラが設定されている場合です。hybrid REAP の詳細は、第 12 章を参照してください。

- `config interface acl operator-defined-interface-name access-control-list-name`



(注) ACL の詳細は、第 5 章を参照してください。

ステップ 5 ディストリビューション システム通信に動的インターフェイスを使用する WLAN を再度有効にするには、`config wlan enable WLAN ID` と入力します。

ステップ 6 `save config` と入力して、変更内容を保存します。

ステップ 7 `show interface detailed operator-defined-interface-name` および `show interface summary` と入力し、変更内容が保存されたかどうか確認します。



(注) 動的インターフェイスを削除するには、`config interface delete operator-defined-interface-name` と入力します。

ポートの設定

コントローラのポートは、工場出荷時にあらかじめデフォルト設定が行われていて、追加設定しなくても動作する設計になっています。しかし、必要に応じて、コントローラのポートのステータスを表示し、設定パラメータを編集できます。

GUI を使用してコントローラのポートのステータスを表示し、必要に応じて設定を変更する手順は、次のとおりです。

ステップ 1 **Controller > Ports** をクリックして、Ports ページを開きます (図 3-9 を参照)。

図 3-9 Ports ページ

Port No	STP Status	Admin Status	Physical Mode	Physical Status	Link Status	Link Trap	POE	Mcast Appliance
1	Forwarding	Enable	Auto	1000 Mbps Full Duplex	Link Up	Enable	N/A	Enable
2	Disabled	Enable	Auto	Auto	Link Down	Enable	N/A	Enable
3	Disabled	Enable	Auto	Auto	Link Down	Enable	N/A	Enable
4	Disabled	Enable	Auto	Auto	Link Down	Enable	N/A	Enable

このページには、コントローラのポート別に現在の設定が表示されます。

ステップ 2 特定のポートの設定を変更するには、そのポートの番号をクリックします。Port > Configure ページが表示されます (図 3-10 を参照)。



(注) 管理インターフェイスと AP マネージャ インターフェイスが同じポートにマッピングされており、同じ VLAN のメンバである場合は、これらのインターフェイスのポートマッピングを変更する前に WLAN を無効にする必要があります。管理インターフェイスと AP マネージャ インターフェイスがそれぞれ別の VLAN に割り当てられている場合は、WLAN を無効にする必要はありません。



(注) Port > Configure ページで使用できるパラメータの数は、使用しているコントローラの種類によって異なります。たとえば、図 3-10 は Cisco 4400 シリーズのコントローラの例ですが、Cisco 2000 および 2100 シリーズ コントローラや Cisco サービス統合型ルータのコントローラで設定可能なパラメータはこれよりも少なくなっています。

図 3-10 Ports > Configure ページ

The screenshot displays the Cisco Wireless LAN Controller configuration interface for a port. The left sidebar shows the navigation menu with 'Ports' selected. The main content area is titled 'Port > Configure' and includes a 'Back' and 'Apply' button. The configuration is divided into two sections: 'General' and 'Spanning Tree Protocol Configuration'.



General	
Port No	1
Admin Status	Enable
Mirror Mode	Disable
Physical Mode	Auto
Physical Status	1000 Mbps Full Duplex
Link Status	Link Up
Link Trap	Enable
Power Over Ethernet	N/A
Multicast Appliance Mode	Enable

Spanning Tree Protocol Configuration	
STP Port ID	8001
STP Mode	Off
STP State	Forwarding
STP Port Designated Root	0000 00:00:00:00:00:00
STP Port Designated Cost	0
STP Port Designated Bridge	0000 00:00:00:00:00:00
STP Port Designated Port	0000
STP Port Forward Transitions Count	0
STP Port Priority	128
STP Port Path Cost Mode	Auto
STP Port Path Cost	4

232328


表 3-2 は、現在のポートのステータスを示しています。

表 3-2 ポートのステータス

パラメータ	説明	
Port Number	現在のポートの番号。	
Physical Status	このポートにより使用されているデータ レート。使用可能なデータ レートは、コントローラの種類によって異なります。	
	コントローラ	使用可能なデータ レート
	4400 シリーズ	1000 Mbps 全二重
	2000 および 2100 シリーズ	10 または 100 Mbps、半または全二重
	WiSM	1000 Mbps 全二重
	コントローラ ネットワーク モジュール	100 Mbps 全二重
	Catalyst 3750G 統合型無線 LAN コントローラ スイッチ	1000 Mbps 全二重
Link Status	ポートのリンク ステータス。 値： Link Up、または Link Down	
Power Over Ethernet (PoE)	接続デバイスにイーサネット ケーブル経由で電力を受け取る機能があるかどうかを判断し、受け取ることができる場合は、-48VDC を供給します。 値： Enable または Disable  (注) 古い Cisco アクセス ポイントの中には、コントローラ ポートで有効になっていても、PoE を受け付けられないものがあります。このような場合は、Cisco Technical Assistance Center (TAC) にお問い合わせください。  (注) Catalyst 3750G 統合型無線 LAN コントローラ スイッチのコントローラでは、すべてのポートで PoE がサポートされます。	

ステップ 3 表 3-3 は、ポートで設定可能なパラメータとその説明をまとめたものです。表の指示に従って、必要な変更を行います。

表 3-3 ポート パラメータ

パラメータ	説明												
Admin Status	<p>ポートを経由するトラフィックのフローを有効、または無効にします。</p> <p>オプション : Enable または Disable</p> <p>デフォルト : Enable</p> <p> (注) 管理者がコントローラのポートを無効にしても、ポートのリンクステータスには影響しません。リンクがダウン状態になるのは、他のシスコ製デバイスによってのみです。ただし、他のシスコ製品では、管理者がポートを無効にするとリンクがダウンします。</p>												
Physical Mode	<p>ポートのデータレートが自動的に設定されるか、ユーザによって指定されるかを表します。サポートされているデータレートは、コントローラの種類によって異なります。</p> <p>デフォルト : Auto</p> <table border="1" data-bbox="654 974 1476 1332"> <thead> <tr> <th>コントローラ</th> <th>サポートされているデータレート</th> </tr> </thead> <tbody> <tr> <td>4400 シリーズ</td> <td>自動、または 1000 Mbps 全二重</td> </tr> <tr> <td>2000 および 2100 シリーズ</td> <td>自動、または 10 または 100 Mbps、半または全二重</td> </tr> <tr> <td>WiSM</td> <td>自動、または 1000 Mbps 全二重</td> </tr> <tr> <td>コントローラ ネットワーク モジュール</td> <td>自動、または 100 Mbps 全二重</td> </tr> <tr> <td>Catalyst 3750G 統合型無線 LAN コントローラ スイッチ</td> <td>自動、または 1000 Mbps 全二重</td> </tr> </tbody> </table>	コントローラ	サポートされているデータレート	4400 シリーズ	自動、または 1000 Mbps 全二重	2000 および 2100 シリーズ	自動、または 10 または 100 Mbps、半または全二重	WiSM	自動、または 1000 Mbps 全二重	コントローラ ネットワーク モジュール	自動、または 100 Mbps 全二重	Catalyst 3750G 統合型無線 LAN コントローラ スイッチ	自動、または 1000 Mbps 全二重
コントローラ	サポートされているデータレート												
4400 シリーズ	自動、または 1000 Mbps 全二重												
2000 および 2100 シリーズ	自動、または 10 または 100 Mbps、半または全二重												
WiSM	自動、または 1000 Mbps 全二重												
コントローラ ネットワーク モジュール	自動、または 100 Mbps 全二重												
Catalyst 3750G 統合型無線 LAN コントローラ スイッチ	自動、または 1000 Mbps 全二重												
Link Trap	<p>ポートのリンクステータスが変化したときにポートからトラップが送信されるようにします。</p> <p>オプション : Enable または Disable</p> <p>デフォルト : Enable</p>												
Multicast Appliance Mode	<p>このポートでマルチキャスト アプライアンス サービスを有効、または無効にします。</p> <p>オプション : Enable または Disable</p> <p>デフォルト : Enable</p>												

ステップ 4 **Apply** をクリックして、変更を適用します。

ステップ 5 **Save Configuration** をクリックして、変更内容を保存します。

ステップ 6 Ports ページに戻り、変更内容を確認するには、**Back** をクリックします。

ステップ 7 設定するポートそれぞれについて、この手順を繰り返します。

ステップ 8 次の拡張機能を使用できるようにコントローラのポートを設定する必要がある場合は、指定された項を参照してください。

- ポートのミラーリング。次の項を参照してください。
- Spanning Tree Protocol (STP; スパニング ツリー プロトコル)、(P. 3-27)

ポートのミラーリングの設定

ミラー モードでは、特定のクライアント デバイスまたはアクセス ポイントが起点または終点であるトラフィックをすべて別のポートに複製することができます。このモードは、ネットワークで発生している特定の問題を診断するには便利です。このポートは接続にいつさい応答しなくなりますので、ミラー モードは使用されていないポートでのみ有効にしてください。



(注)

WiSM コントローラは、ミラー モードをサポートしません。また、コントローラのサービス ポートをミラーリングされたポートとして使用することもできません。



(注)

コントローラでリンク集約 (LAG) が有効になっている場合、ポートのミラーリングはサポートされません。



(注)

ネットワークに問題が発生することがあるので、あるコントローラ ポートから別のコントローラ ポートへのトラフィックのミラーリングはしないでください。

ポートのミラーリングを有効にする手順は、次のとおりです。

ステップ 1 **Controller > Ports** の順にクリックして、Ports ページを開きます (図 3-9 を参照)。

ステップ 2 ミラー モードを有効にする未使用ポートの番号をクリックします。Port > Configure ページが表示されます (図 3-10 を参照)。

ステップ 3 Mirror Mode パラメータを **Enable** に設定します。

ステップ 4 **Apply** をクリックして、変更を適用します。

ステップ 5 次のいずれかの操作を行います。

- コントローラで選択したポートにトラフィックをミラーリングするクライアント デバイスを選択する手順は、次のとおりです。
 - Wireless > Clients** の順にクリックして、Clients ページを開きます。
 - ミラー モードを有効にするクライアントの MAC アドレスをクリックします。Clients > Detail ページが表示されます。
 - Client Details で、Mirror Mode パラメータを **Enable** に設定します。

- コントローラで選択したポートにトラフィックをミラーリングするアクセス ポイントを選択する手順は、次のとおりです。
 - a. **Wireless > All APs** の順にクリックして、**All APs** ページを開きます。
 - b. ミラー モードを有効にするアクセス ポイントの名前をクリックします。**All APs > Details** ページが表示されます。
 - c. **General** で、**Mirror Mode** パラメータを **Enable** に設定します。

ステップ 6 **Save Configuration** をクリックして、変更を保存します。

スパンニング ツリー プロトコルの設定

スパンニング ツリー プロトコル (STP) は、ネットワーク内のループを回避しながらパスを冗長化するためのレイヤ 2 リンク管理プロトコルです。レイヤ 2 イーサネット ネットワークが正しく動作するには、任意の 2 つのネットワーク デバイス間に存在するアクティブ パスの数は 1 つのみです。STP は、ネットワーク デバイス間のアクティブ パスを一度に 1 つのみ許可しますが、最初のリンクが機能しなくなった場合のバックアップとして冗長リンクを確立します。

スパンニング ツリー アルゴリズムによって、レイヤ 2 ネットワークにおける、ループのない最善のパスが計算されます。コントローラやスイッチなどのインフラストラクチャ デバイスは、**Bridge Protocol Data Unit (BPDU; ブリッジプロトコルデータ ユニット)** と呼ばれるスパンニング ツリー フレームを一定の間隔で送受信します。これらのデバイスは、こうしたフレームを転送せず、ループ フリーパスの構築に使用します。

エンドステーション間に複数のアクティブ パスが存在すると、ネットワーク内でループが発生します。ネットワークにループが存在する場合、エンドステーションは重複してメッセージを受信する場合があります。また、インフラストラクチャ デバイスが複数のレイヤ 2 インターフェイスにある複数のエンドステーション MAC アドレスを認識することがあります。これらの条件が重なった結果、ネットワークが不安定になります。

STP は、ルートブリッジと、レイヤ 2 ネットワークのルートから、すべてのインフラストラクチャ デバイスに向かうループフリーパスを使用してツリーを定義します。



(注)

STP の説明では、**ルート** という用語を、次の 2 つの概念を表す用語として使用しています。1 つは、ネットワーク上でスパンニング ツリーの中心点の役割を果たすコントローラで、**ルートブリッジ** と呼ばれます。もう 1 つは、各コントローラ上にあり、ルートブリッジに最も効率的なパスを提供するポートで、**ルートポート** と呼ばれます。スパンニング ツリーのルートブリッジは、スパンニング ツリールートと呼ばれます。

STP によって、冗長データパスは強制的にスタンバイ (ブロックされた) 状態になります。スパンニング ツリーのネットワーク セグメントに不具合が発生したときに冗長パスが存在すれば、スパンニング ツリー アルゴリズムにより、スパンニング ツリー トポロジが再計算され、スタンバイパスがアクティブ化されます。

コントローラの 2 つのポートがループの一部である場合に、どちらのポートが **Forwarding** 状態になり、どちらのポートが **Blocking** 状態になるかは、スパンニング ツリー ポートの優先順位とパスコストの設定によって決まります。ポートの優先順位の値は、ネットワーク トポロジ内でのポートの位置と、このポートがどの程度、トラフィックを渡しやすい場所にあるかを表します。パスコストの値は、メディア速度を表します。

コントローラで設定されているアクティブ VLAN ごとに、別のスパンニング ツリー インスタンスが保持されます。ブリッジの優先順位とコントローラの MAC アドレスから構成されるブリッジ ID が、各インスタンスに関連付けられます。個々の VLAN については、最も小さなコントローラ ID を持つコントローラが、その VLAN のスパンニング ツリー ルートになります。

デフォルトでは、コントローラのディストリビューション システム ポートに対する STP は無効になります。これ以降の項では、GUI、または CLI を使用して、コントローラの STP を設定する手順について説明します。



(注) Catalyst 3750G 統合型無線 LAN コントローラ スイッチのコントローラに対する STP は設定できません。

GUI を使用したスパンニング ツリー プロトコルの設定

GUI を使用して STP を設定する手順は、次のとおりです。

- ステップ 1** **Controller > Ports** の順にクリックして、Ports ページを開きます (図 3-9 を参照)。
- ステップ 2** STP を設定するポートの番号をクリックします。Port > Configure ページが表示されます (図 3-10 を参照)。このページには、ポートの STP ステータスが表示されます。ここから、STP パラメータを設定できます。

表 3-4 は、現在のポートの STP ステータスを示しています。

表 3-4 ポートのスパンニング ツリーのステータス

パラメータ	説明														
STP Port ID	STP が有効、または無効になっているポートの番号。														
STP State	<p>ポートの現在の STP 状態。これにより、フレームを受信したときのポートのアクションが決まります。</p> <p>値: Disabled、Blocking、Listening、Learning、Forwarding、および Broken</p> <table border="1"> <thead> <tr> <th>STP State</th> <th>説明</th> </tr> </thead> <tbody> <tr> <td>Disabled</td> <td>ポートがシャットダウンされている、リンクがダウンしている、またはこのポートでは STP が有効になっていないため、このポートはスパンニング ツリーに参加していません。</td> </tr> <tr> <td>Blocking</td> <td>このポートはフレーム転送に参加していません。</td> </tr> <tr> <td>Listening</td> <td>ポートはフレーム転送に参加すべきであると STP が判断したときに、Blocking 状態後に来る最初の変遷状態です。</td> </tr> <tr> <td>Learning</td> <td>このポートはフレーム転送に参加する準備をしています。</td> </tr> <tr> <td>Forwarding</td> <td>ポートはフレームを転送します。</td> </tr> <tr> <td>Broken</td> <td>ポートは正常に機能していません。</td> </tr> </tbody> </table>	STP State	説明	Disabled	ポートがシャットダウンされている、リンクがダウンしている、またはこのポートでは STP が有効になっていないため、このポートはスパンニング ツリーに参加していません。	Blocking	このポートはフレーム転送に参加していません。	Listening	ポートはフレーム転送に参加すべきであると STP が判断したときに、Blocking 状態後に来る最初の変遷状態です。	Learning	このポートはフレーム転送に参加する準備をしています。	Forwarding	ポートはフレームを転送します。	Broken	ポートは正常に機能していません。
STP State	説明														
Disabled	ポートがシャットダウンされている、リンクがダウンしている、またはこのポートでは STP が有効になっていないため、このポートはスパンニング ツリーに参加していません。														
Blocking	このポートはフレーム転送に参加していません。														
Listening	ポートはフレーム転送に参加すべきであると STP が判断したときに、Blocking 状態後に来る最初の変遷状態です。														
Learning	このポートはフレーム転送に参加する準備をしています。														
Forwarding	ポートはフレームを転送します。														
Broken	ポートは正常に機能していません。														
STP Port Designated Root	設定 BPDU 内のルートブリッジを表す一意の ID。														

表 3-4 ポートのスパンニング ツリーのステータス (続き)


パラメータ	説明
STP Port Designated Cost	指定されたポートのパス コスト。
STP Port Designated Bridge	このポートに対して指定されたブリッジであるとポートがみなしているブリッジの ID。
STP Port Designated Port	このポートに対して指定されたブリッジのポート ID。
STP Port Forward Transitions Count	ポートが Learning 状態から Forwarding 状態に遷移した回数。

ステップ 3 表 3-5 は、ポートで設定可能な STP のパラメータとその説明をまとめたものです。表の指示に従って、必要な変更を行います。

表 3-5 ポートのスパンニング ツリーのパラメータ

パラメータ	説明								
STP Mode	このポートに関連付けられている STP 管理モード。 オプション : Off、802.1D、または Fast デフォルト : Off								
	<table border="1"> <thead> <tr> <th>STP Mode</th> <th>説明</th> </tr> </thead> <tbody> <tr> <td>Off</td> <td>このポートでは STP を無効にします。</td> </tr> <tr> <td>802.1D</td> <td>このポートがスパンニング ツリーに参加できるようにし、リンク状態が Down から Up に変化したときに、すべてのスパンニング ツリー状態を確認します。</td> </tr> <tr> <td>Fast</td> <td>このポートがスパンニング ツリーに参加できるようにし、STP モードが 802.1D に設定されているときよりも早くリンク状態が Down から Up に遷移したときに、このポートを Forwarding 状態にします。</td> </tr> </tbody> </table>	STP Mode	説明	Off	このポートでは STP を無効にします。	802.1D	このポートがスパンニング ツリーに参加できるようにし、リンク状態が Down から Up に変化したときに、すべてのスパンニング ツリー状態を確認します。	Fast	このポートがスパンニング ツリーに参加できるようにし、STP モードが 802.1D に設定されているときよりも早くリンク状態が Down から Up に遷移したときに、このポートを Forwarding 状態にします。
STP Mode	説明								
Off	このポートでは STP を無効にします。								
802.1D	このポートがスパンニング ツリーに参加できるようにし、リンク状態が Down から Up に変化したときに、すべてのスパンニング ツリー状態を確認します。								
Fast	このポートがスパンニング ツリーに参加できるようにし、STP モードが 802.1D に設定されているときよりも早くリンク状態が Down から Up に遷移したときに、このポートを Forwarding 状態にします。								
	 (注) この状態では、リンクのアップ時に、転送遅延タイマーは無視されます。								
STP Port Priority	ネットワーク トポロジ内でのポートの位置と、このポートがどの程度、トラフィックを渡しやすい場所にあるかを表します。 範囲 : 0 ~ 255 デフォルト : 128								
STP Port Path Cost Mode	STP ポート パス コストは自動的に設定されるか、ユーザにより指定されるかを表します。User Configured を選択する場合、STP Port Path Cost パラメータの値も設定する必要があります。 範囲 : Auto、または User Configured デフォルト : Auto								

表 3-5 ポートのスパンニング ツリーのパラメータ (続き)

パラメータ	説明
STP Port Path Cost	<p>トラフィックがポートを通り抜ける速度。このパラメータは、STP Port Path Cost Mode パラメータを User Configured に設定した場合には、必ず設定します。</p> <p>オプション : 0 ~ 65535</p> <p>デフォルト : 0。リンクがアップしたときに、ポートの速度に合わせてコストが調整されるようになります。</p> <p> (注) 通常、10Mbps のポートには 100 を、100Mbps のポートには 19 を使用します。</p>

ステップ 4 Apply をクリックして、変更を適用します。

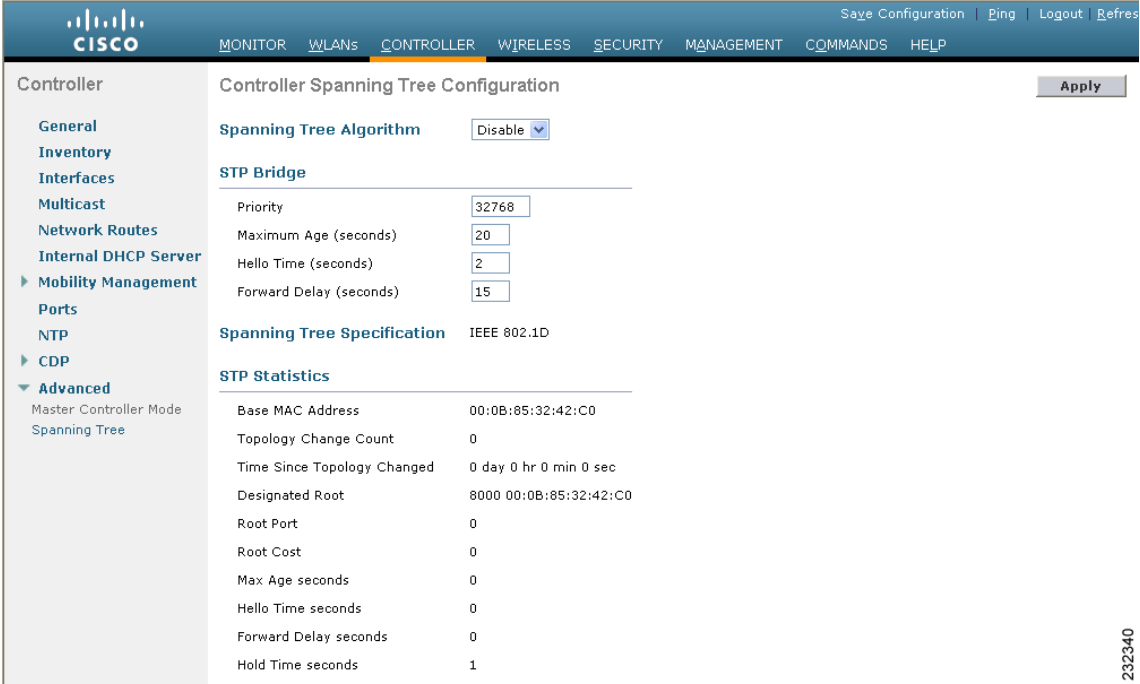
ステップ 5 Save Configuration をクリックして、変更内容を保存します。

ステップ 6 Ports ページに戻るには、Back をクリックします。

ステップ 7 STP を有効にするポートそれぞれについて、ステップ 2 ~ ステップ 6 を繰り返します。

ステップ 8 Controller > Advanced > Spanning Tree の順にクリックして、Controller Spanning Tree Configuration ページを開きます (図 3-11 を参照)。

図 3-11 Controller Spanning Tree Configuration ページ





The screenshot shows the Cisco Wireless LAN Controller configuration interface. The main content area is titled "Controller Spanning Tree Configuration" and includes an "Apply" button. The configuration is divided into several sections:

- Spanning Tree Algorithm:** Set to "Disable".
- STP Bridge:**
 - Priority: 32768
 - Maximum Age (seconds): 20
 - Hello Time (seconds): 2
 - Forward Delay (seconds): 15
- Spanning Tree Specification:** Set to "IEEE 802.1D".
- STP Statistics:**
 - Base MAC Address: 00:0B:85:32:42:C0
 - Topology Change Count: 0
 - Time Since Topology Changed: 0 day 0 hr 0 min 0 sec
 - Designated Root: 8000 00:0B:85:32:42:C0
 - Root Port: 0
 - Root Cost: 0
 - Max Age seconds: 0
 - Hello Time seconds: 0
 - Forward Delay seconds: 0
 - Hold Time seconds: 1

The left sidebar shows the navigation menu with "Advanced" expanded to "Spanning Tree". The top navigation bar includes "MONITOR", "WLANs", "CONTROLLER", "WIRELESS", "SECURITY", "MANAGEMENT", "COMMANDS", and "HELP".

このページでは、コントローラのスパンニング ツリー アルゴリズムの有効化または無効化、その特性の変更、および STP ステータスの表示を行うことができます。表 3-6 は、現在のコントローラの STP ステータスを示しています。

表 3-6 コントローラのスパンニング ツリーのステータス

パラメータ	説明
Spanning Tree Specification	このコントローラにより使用されている STP のバージョン。現在、IEEE 802.1D 実装のみ使用可能です。
Base MAC Address	ブリッジを一意に参照する必要がある場合に、このブリッジにより使用される MAC アドレス。このアドレスと dot1dStpPriority を連結することにより、STP で使用される一意のブリッジ識別子が作成されます。
Topology Change Count	管理実体が最後にリセット、または初期化されてから、このブリッジによって検知されたトポロジに対する変更の総数。
Time Since Topology Changed	ブリッジによりトポロジーの変更が検知されてから経過した時間 (単位は日、時、分、秒)。
Designated Root	スパンニング ツリー ルートのブリッジ識別子。この値は、このノードを起点とする設定 BPDU すべての Root Identifier パラメータとして使用されます。
Root Port	このブリッジからルートブリッジへの最も低いコスト パスを提供するポートの番号。
Root Cost	このブリッジから見た、ルートへのパスのコスト。
Max Age (seconds)	任意のポートについて、ネットワークから得られた STP 情報が破棄されるまでの最大経過時間。
Hello Time (seconds)	任意のポートについて、ノードがスパンニング ツリーのルートである、またはルートになろうとしているときに、このノードによって行われる設定 BPDU の転送の間隔。これは、このブリッジが現在、実際に使用している値です。
Forward Delay (seconds)	この値は、ポートがスパンニング ツリー状態を Forwarding 状態に向かって変化させる速度をコントロールします。この値により、ポートが Forwarding 状態の前に、どのくらい Listening 状態や Learning 状態であるかが決定されます。また、検知されたトポロジの変化が進行中であるときに、フォワーディング データベースの動的エントリすべての時間を経過させるためにも使用されます。  (注) これはこのブリッジによって現在、実際に使用されている値です。対照的に、 <i>Stp Bridge Forward Delay</i> は、このブリッジがルートとなったときに、これを含むその他すべてのブリッジが使用を開始する値です。
Hold Time (seconds)	指定された LAN ポートを通じて行われる設定 BPDU の転送間隔の最小値。  (注) Hold Time 期間に転送される設定 BPDU の数は多くても 1 つです。

ステップ 9 表 3-7 は、コントローラで設定可能な STP のパラメータとその説明をまとめたものです。表の指示に従って、必要な変更を行います。

表 3-7 コントローラのスパンニング ツリーのパラメータ

パラメータ	説明
Spanning Tree Algorithm	コントローラに対して STP を有効、または無効にします。 オプション : Enable または Disable デフォルト : Disable
Priority	ネットワーク トポロジ内でのコントローラの位置と、このコントローラがどの程度、トラフィックを渡しやすい場所にあるかを表します。 範囲 : 0 ~ 65535 デフォルト : 32768
Maximum Age (seconds)	コントローラが、ポートで受信したプロトコル情報を保管する期間。 範囲 : 6 ~ 40 秒 デフォルト : 20 秒
Hello Time (seconds)	コントローラが他のコントローラに Hello メッセージをブロードキャストする期間。 オプション : 1 ~ 10 秒 デフォルト : 2 秒
Forward Delay (seconds)	ポートがフォワーディングを開始する前に、Listening 状態、および Learning 状態である期間。 オプション : 4 ~ 30 秒 デフォルト : 15 秒

ステップ 10 **Apply** をクリックして、変更を適用します。

ステップ 11 **Save Configuration** をクリックして、変更を保存します。

CLI を使用したスパンニング ツリー プロトコルの設定

CLI を使用して STP を設定する手順は、次のとおりです。

-
- ステップ 1** `show spanningtree port` および `show spanningtree switch` と入力し、現在の STP ステータスを表示します。
- ステップ 2** STP が有効な場合は、STP 設定を変更する前に無効にしておく必要があります。`config spanningtree switch mode disable` と入力し、すべてのポートの STP を無効にします。
- ステップ 3** 次のコマンドのいずれか 1 つを使用して、STP ポートの管理モードを設定します。
- `config spanningtree port mode 802.1d {port-number | all}`
 - `config spanningtree port mode fast {port-number | all}`
 - `config spanningtree port mode off {port-number | all}`
- ステップ 4** 次のコマンドのいずれか 1 つを入力し、STP ポートの STP ポート パス コストを設定します。
- `config spanningtree port pathcost 1-65535 {port-number | all}` : ポートのパス コストを 1 ~ 65535 の範囲で指定します。
 - `config spanningtree port mode pathcost auto {port-number | all}` : STP アルゴリズムによるパス コストの自動割り当てを有効にします。これはデフォルト設定です。
- ステップ 5** `config spanningtree port priority 0-255 port-number` と入力し、STP ポートの優先順位を設定します。デフォルトの優先順位は 128 です。
- ステップ 6** 必要であれば、`config spanningtree switch bridgepriority 0-65535` と入力して、コントローラの STP ブリッジ優先順位を設定します。デフォルトのブリッジ優先順位は 32768 です。
- ステップ 7** 必要であれば、`config spanningtree switch forwarddelay 4-30` と入力して、コントローラの STP 転送遅延時間 (秒) を設定します。デフォルトの転送遅延時間は 15 秒です。
- ステップ 8** 必要であれば、`config spanningtree switch hellotime 1-10` と入力して、コントローラの STP ハロー タイム (秒) を設定します。デフォルトのハロー タイムは 2 秒です。
- ステップ 9** 必要であれば、`config spanningtree switch maxage 6-40` と入力して、コントローラの STP 最大経過時間を設定します。デフォルトの最大経過時間は 20 秒です。
- ステップ 10** ポートの STP 設定を完了したら、`config spanningtree switch mode enable` と入力して、コントローラの STP を有効にします。コントローラによって自動的に論理ネットワーク ループが検出され、冗長ポートが待機状態に設定され、最も効率的なパスウェイでネットワークが構築されます。
- ステップ 11** `save config` と入力して、設定を保存します。
- ステップ 12** `show spanningtree port` および `show spanningtree switch` と入力し、変更内容が保存されたことを確認します。
-

リンク集約の有効化

リンク集約 (LAG) は、802.3ad ポート集約標準の部分的な実装です。LAG によって、コントローラのすべてのディストリビューション システム ポートが 1 つの 802.3ad ポート チャンネルにまとめられるので、コントローラのポートの設定に必要な IP アドレスの数を減らすことができます。LAG が有効である場合、ポートの冗長性は動的に管理され、アクセス ポイントはユーザからは透過的にロード バランシングされます。

Cisco 4400 シリーズ コントローラは、ソフトウェア リリース 3.2 以降で LAG をサポートし、LAG は、Cisco WiSM および Catalyst 3750G 統合型無線 LAN コントローラ スイッチのコントローラ上で自動的に有効になります。LAG を使用していない場合、コントローラ上のディストリビューション システム ポート 1 つにつき、最大 48 個のアクセス ポイントがサポートされます。LAG が有効である場合、4402 コントローラの論理ポートは最大 50 個、4404 コントローラの論理ポートは最大 100 個、各 Cisco WiSM コントローラの論理ポートは最大 150 個のアクセス ポイントをサポートします。

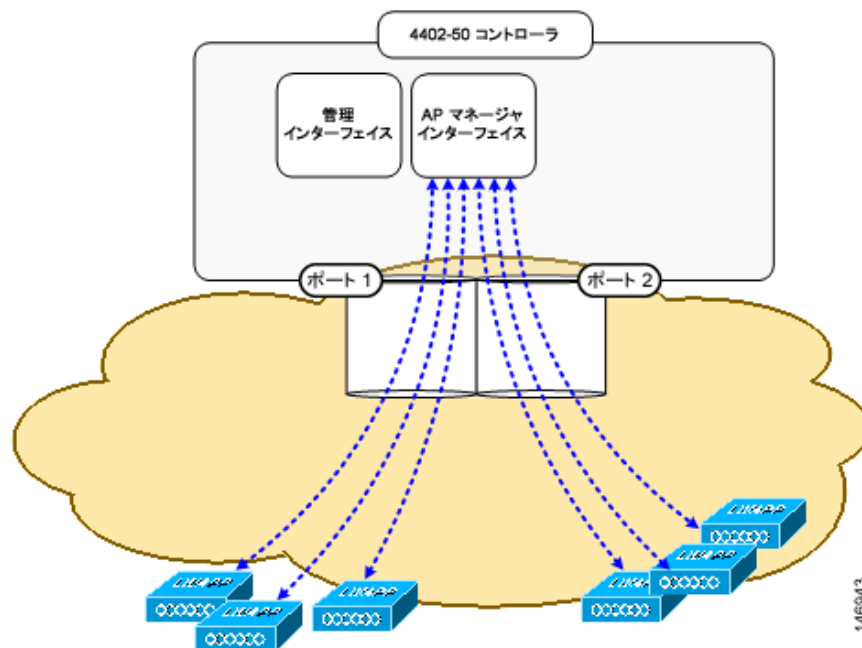


(注)

4404 コントローラの 4 つのポート (または 4402 コントローラの 2 つのポート) をすべて 1 つのリンクにまとめることができます。

図 3-12 は LAG を図示したものです。

図 3-12 リンク集約



LAG を使用すれば、インターフェイスごとにプライマリ ポートとセカンダリ ポートを設定する必要がないので、コントローラ設定も簡単に行えるようになります。いずれかのコントローラ ポートに障害が発生した場合は、他のポートへトラフィックが自動的に移行します。少なくとも 1 つのコントローラ ポートが機能している限り、システムは継続して動作し、アクセス ポイントはネットワークに接続されたままとなります。また、無線クライアントは引き続きデータを送受信します。

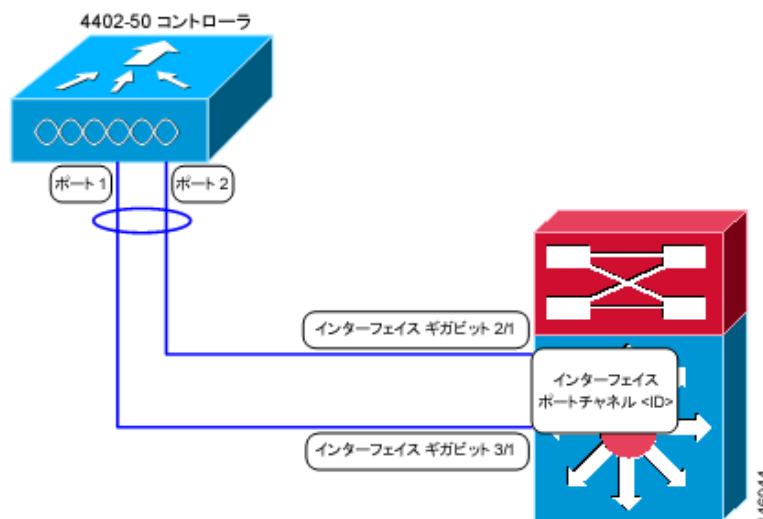
コントローラのポートをまとめるように設定するとき、Catalyst 6500 などのモジュラ スイッチ内の 2 つのモジュールを終端とすることを検討してください。ただし、4400 コントローラの LAG ポートを複数の Catalyst 6500 または 3750G スイッチに接続することはお勧めしません。

単一の Catalyst 6500 スイッチの中の 2 つのモジュールを終端とすることによって冗長化されるので、一方のモジュールに障害が発生してもスイッチとコントローラ間の接続は維持されます。図 3-13 は、この冗長モジュールの使い方を示しています。4402-50 コントローラが Catalyst 6500 内の 2 つのギガビット モジュール (スロット 2 および 3) に接続されています。コントローラのポート 1 は Catalyst 6500 のギガビット インターフェイス 3/1 に接続されており、コントローラのポート 2 はギガビット インターフェイス 2/1 に接続されています。どちらのスイッチ ポートも、同じチャンネル グループに割り当てられています。

4404 コントローラまたは WiSM コントローラ モジュールの LAG ポートの接続先である Catalyst 3750G または 6500 のチャンネル グループまたは 7600 のチャンネル グループで負荷分散が行われているときは、次の点に注意してください。

- LAG を行うには、コントローラと Catalyst スイッチの両方で EtherChannel が「on」モードに設定されている必要があります。
- リンクの両端で EtherChannel が「on」に設定されると、Catalyst スイッチが Link Aggregation Control Protocol (LACP) と Cisco 独自の Port Aggregation Protocol (PAgP) のどちらを使用するように設定されているかは無視されます。コントローラとスイッチ間のチャンネル ネゴシエーションは行われなからです。また、LACP と PAgP はコントローラではサポートされません。
- Catalyst スイッチでのロード バランシングは、すべての IP データグラム フラグメントの終点が単一のコントローラ ポートとなるように設定されている必要があります。この推奨事項に従わない場合は、アクセス ポイントのアソシエートの問題が発生することがあります。
- Catalyst スイッチのロード バランシングには、送信元および宛先 IP アドレスに基づく方法 (CLI コマンド: `port-channel load-balance src_dest_ip`) を使用することをお勧めします。
- 推奨されるロード バランシング方法を Catalyst スイッチ上で設定できない場合は、LAG 接続を単一メンバリンクとして設定するか、コントローラで LAG を行わないように設定します。

図 3-13 Catalyst 6500 近接スイッチを使ったリンク集約



リンク集約に関するガイドライン

LAG を使用するときには、次の点に留意してください。

- 1つのコントローラの複数のポートを別々の LAG グループに設定することはできません。1つのコントローラがサポートする LAG グループは1つのみです。したがって、LAG モードのコントローラ1つを接続できる隣接デバイスは1つのみです。



(注) Catalyst 3750G 統合型無線 LAN コントローラ スイッチのコントローラに装備された2つの内部ギガビットポートは、必ず同じ LAG グループに割り当てられます。

- LAG を有効化したときや、LAG の設定に変更を加えたときは、ただちにコントローラをリブートしてください。
- LAG を有効にした場合、必要な論理ポートは1つのみであるため、AP マネージャ インターフェイスを1つだけ設定できます。LAG を使用する場合は、複数の AP マネージャ インターフェイスのサポートに関する要件はなくなります。
- LAG を有効にした場合、動的 AP マネージャ インターフェイス、およびタグの付いていないインターフェイスはすべて削除されます。同時に、WLAN がすべて無効になり、管理インターフェイスにマップされます。また、管理インターフェイス、静的 AP マネージャ インターフェイス、および VLAN タグ付き動的インターフェイスは、LAG ポートに移されます。
- 複数のタグなしインターフェイスを同じポートに割り当てることはできません。
- LAG を有効にした場合、29 以外のプライマリ ポートを使用してインターフェイスを作成することはできません。
- LAG を有効にした場合、デフォルトでは、すべてのポートが LAG に参加します。したがって、近接スイッチにある接続されたポートすべてについて、LAG を設定する必要があります。
- Cisco WiSM 上で LAG を有効化した場合は、スイッチ上で、コントローラのすべてのポートに対してポート チャネリング/イーサネット チャネリングを有効にする必要があります。
- LAG を有効にした場合、ポートのミラーリングはサポートされません。
- LAG が有効化されているときは、リンクのいずれかがダウンした場合にトラフィックは別のリンクに移されます。
- LAG が有効化されているときは、物理ポートが1つでも機能していればコントローラはクライアントトラフィックを通過させることができます。
- LAG が有効化されているときは、アクセス ポイントはスイッチに接続されたままになります。また、ユーザに対するデータ サービスが中断されることはありません。
- LAG が有効化されているときは、各インターフェイスに対してプライマリとセカンダリのポートを設定する必要はなくなります。
- LAG が有効化されているときは、コントローラがパケットを受信したポートと同じポートからパケットが送信されます。アクセス ポイントからの LWAPP パケットがコントローラの物理ポート1に入ると、コントローラによって LWAPP ラッパーが除去され、パケットが処理され、物理ポート1からネットワークに転送されます。LAG が無効化されている場合は、このようにはならないことがあります。
- LAG を無効化すると、管理、静的 AP マネージャ、および動的の各インターフェイスはポート1に移されます。
- LAG を無効にする場合、すべてのインターフェイスについて、プライマリ ポートとセカンダリ ポートを設定する必要があります。
- LAG を無効にする場合、コントローラ上の各ポートについて、AP マネージャ インターフェイスを割り当てる必要があります。
- Cisco 4400 シリーズ コントローラでは、静的リンク集約バンドルが1つだけサポートされます。
- 通常、LAG はスタートアップ ウィザードを使って設定されますが、GUI または CLI を使用して、必要なときに有効または無効にすることができます。



(注) WiSM コントローラおよび Catalyst 3750G 統合型無線 LAN コントローラ スイッチのコントローラでは、LAG はデフォルトで有効化されており、これが唯一のオプションです。

GUI を使用したリンク集約の有効化

GUI を使用して、コントローラで LAG を有効にする手順は、次のとおりです。

ステップ 1 **Controller > General** の順にクリックして、General ページを開きます (図 3-14 を参照)。

図 3-14 General ページ

The screenshot shows the Cisco Controller GUI for interface 4404. The 'General' tab is selected. The 'LAG Mode on next reboot' parameter is set to 'Enabled'. Other parameters include Name (4404), 802.3x Flow Control Mode (Disabled), LWAPP Transport Mode (Layer 3), Ethernet Multicast Mode (Multicast), Broadcast Forwarding (Disabled), Aggressive Load Balancing (Disabled), Over The Air Provisioning of AP (Disabled), AP Fallback (Enabled), Apple Talk Bridging (Disabled), Fast SSID change (Disabled), Default Mobility Domain Name (snmp_gui), RF-Network Name (snmp_gui), User Idle Timeout (300), ARP Timeout (300), Web Radius Authentication (PAP), 802.3 Bridging (Disabled), Operating Environment (Commercial), and Internal Temp Alarm Limits (0 to 65 C). An 'Apply' button is visible in the top right corner.

ステップ 2 LAG Mode on Next Reboot パラメータを **Enabled** に設定します。



(注) LAG を無効にするには、**Disabled** を選択します。Cisco 4400 シリーズ コントローラでは LAG はデフォルトで無効化されていますが、Cisco WiSM ではデフォルトで有効化されます。

ステップ 3 **Apply** をクリックして、変更を適用します。

ステップ 4 **Save Configuration** をクリックして、変更内容を保存します。

ステップ 5 コントローラをリブートします。

ステップ 6 WLAN を VLAN に割り当てます。

CLI を使ったリンク集約の有効化

CLI を使用して、コントローラで LAG を有効にする手順は、次のとおりです。

ステップ 1 `config lag enable` と入力して、LAG を有効にします。



(注) LAG を無効にするには、`config lag disable` と入力します。

ステップ 2 `save config` と入力して、設定を保存します。

ステップ 3 コントローラをリブートします。

CLI を使ったリンク集約の確認

LAG の設定を確認するには、次のコマンドを入力します。

```
show lag summary
```

次のような情報が表示されます。

```
LAG Enabled
```

LAG をサポートするための隣接デバイスの設定

コントローラの隣接デバイスも、LAG をサポートするように適切に設定する必要があります。

- コントローラが接続されている隣接ポートはそれぞれ、次のように設定します。

```
interface GigabitEthernet <interface id>
switchport
channel-group <id> mode on
no shutdown
```

- 近接スイッチのポート チャンネルは、次のように設定します。

```
interface port-channel <id>
switchport
switchport trunk encapsulation dot1q
switchport trunk native vlan <native vlan id>
switchport trunk allowed vlan <allowed vlans>
switchport mode trunk
no shutdown
```

49 個以上のアクセス ポイントをサポートするように 4400 シリーズコントローラを設定

前述のように、4400 シリーズのコントローラは、ポート1つにつき、最大 48 個のアクセス ポイントをサポートします。しかし、次のいずれかの方法を使用して、さらに多くのアクセス ポイントをサポートするように 4400 シリーズのコントローラを設定することもできます。

- リンク集約（レイヤ3 モードのコントローラ向け）、(P. 3-39)
- 複数の AP マネージャ インターフェイス（レイヤ3 モードのコントローラ向け）、(P. 3-39)
- 追加ポートの接続（レイヤ2 モードのコントローラ向け）、(P. 3-44)

使用方法が記されているページの手順に従って操作してください。

コントローラがレイヤ3 での操作用に設定されている場合、どちらの方法を使用すべきかを判断するポイントは次のとおりです。

- リンク集約では、コントローラのポートはすべて、同一の近接スイッチに接続されている必要があります。近接スイッチがダウンすると、コントローラは接続性を失います。
- 複数の AP マネージャ インターフェイスを使用する場合、ポートをさまざまな隣接デバイスへ接続できます。近接スイッチの1つがダウンしても、コントローラの接続性は失われません。ただし、ポートの冗長性に不安がある場合、複数の AP マネージャ インターフェイスの使用には、多少の問題があります（詳細は、後述の「複数の AP マネージャ インターフェイスの使用」を参照）。

リンク集約の使用

リンク集約の有効化の詳細と手順は、「リンク集約の有効化」の項 (P. 3-34) を参照してください。



(注)

リンク集約は、Cisco WiSM および Catalyst 3750G 統合型無線 LAN コントローラ スイッチのコントローラに対して使用可能な唯一の方法です。

複数の AP マネージャ インターフェイスの使用



(注)

この方法は、Cisco 4400 シリーズのスタンドアロン コントローラでのみ使用できます。

複数の AP マネージャ インターフェイスを作成すると、インターフェイスはそれぞれ異なるポートにマップされます (図 3-15 を参照) AP マネージャ インターフェイス 2 がポート 2、AP マネージャ インターフェイス 3 がポート 3、AP マネージャ インターフェイス 4 がポート 4 となるように、ポートが順番に設定されている必要があります。



(注)

すべての AP マネージャ インターフェイスが同じ VLAN または同じ IP サブネット上になくてもかまいません。また、管理インターフェイスと同じ VLAN または IP サブネットになくても問題はありません。ただし、すべての AP マネージャ インターフェイスが同一の VLAN または IP サブネット上に存在するように設定することをお勧めします。

49 個以上のアクセス ポイントをサポートするように 4400 シリーズ コントローラを設定



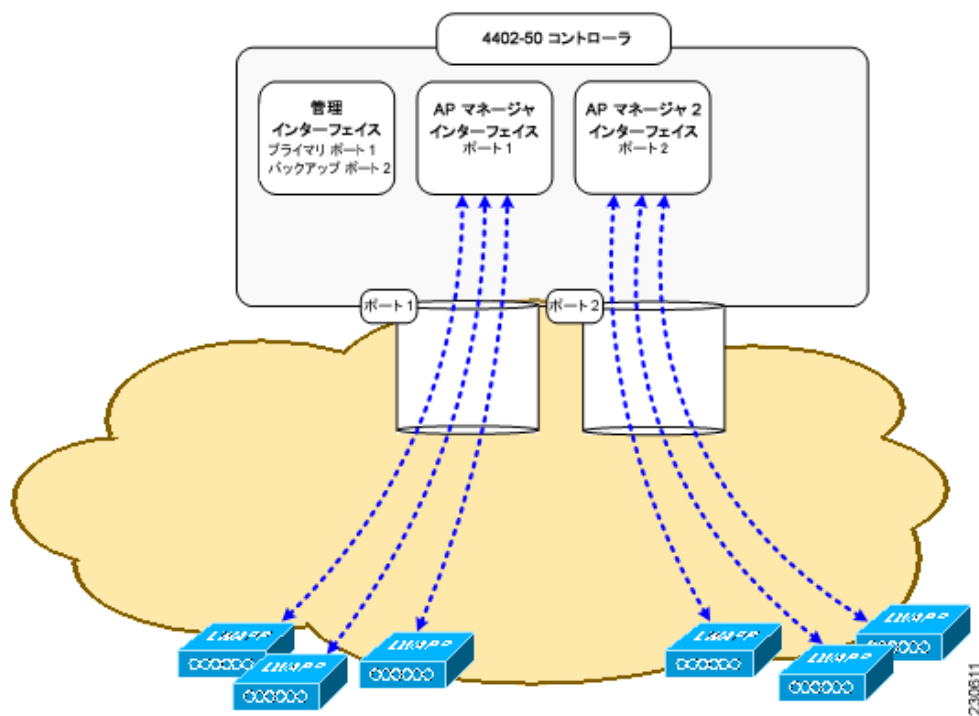
(注) コントローラ上の各ポートについて、AP マネージャ インターフェイスを割り当てる必要があります。

アクセス ポイントはコントローラに接続する前に、ディスカバリ要求を送信します。アクセス ポイントは、受信したディスカバリ応答から、コントローラにある AP マネージャ インターフェイスの数と、各 AP マネージャ インターフェイスにあるアクセス ポイントの数を判断します。アクセス ポイントは、通常、最もアクセス ポイント数の少ない AP マネージャに接続します。この方法により、アクセス ポイントの負荷は、複数の AP マネージャ インターフェイスに対して動的に分散されます。



(注) アクセス ポイントは AP マネージャ インターフェイス全体に、均等に分散されるわけではありませんが、ある程度のロード バランシングは行われます。

図 3-15 2つの AP マネージャ インターフェイス



複数の AP マネージャ インターフェイスを実装する前に、このことがコントローラのポート冗長性に与える影響を考慮する必要があります。

例：

1. 4402-50 コントローラは最大 50 個のアクセス ポイントをサポートし、ポートを 2 つ持っています。最大数のアクセス ポイントをサポートするには、AP マネージャ インターフェイスを 2 つ作成する必要があります (図 3-15 を参照)。コントローラのポート 1 つあたり 48 個しかアクセス ポイントがサポートされないからです。

2. 4404-100 コントローラは最大 100 個のアクセス ポイントをサポートし、ポートを 4 つ持っています。最大数のアクセス ポイントをサポートするには、AP マネージャ インターフェイスを 3 つまたはそれ以上作成する必要があります (図 3-16 を参照)。いずれかの AP マネージャ インターフェイスのポートで障害が発生した場合は、コントローラによってアクセス ポイントの状態がクリアされるので、通常のコントローラ接続プロセスを使用してコントローラとの通信を再確立するために、アクセス ポイントのリブートが必要になります。この後、コントローラからの LWAPP ディスカバリ応答には、障害を起こした AP マネージャ インターフェイスは含まれなくなります。アクセス ポイントは再度コントローラに接続し、アクセス ポイントの負荷は使用可能な AP マネージャ インターフェイス間に分散されます。

図 3-16 3 つの AP マネージャ インターフェイス

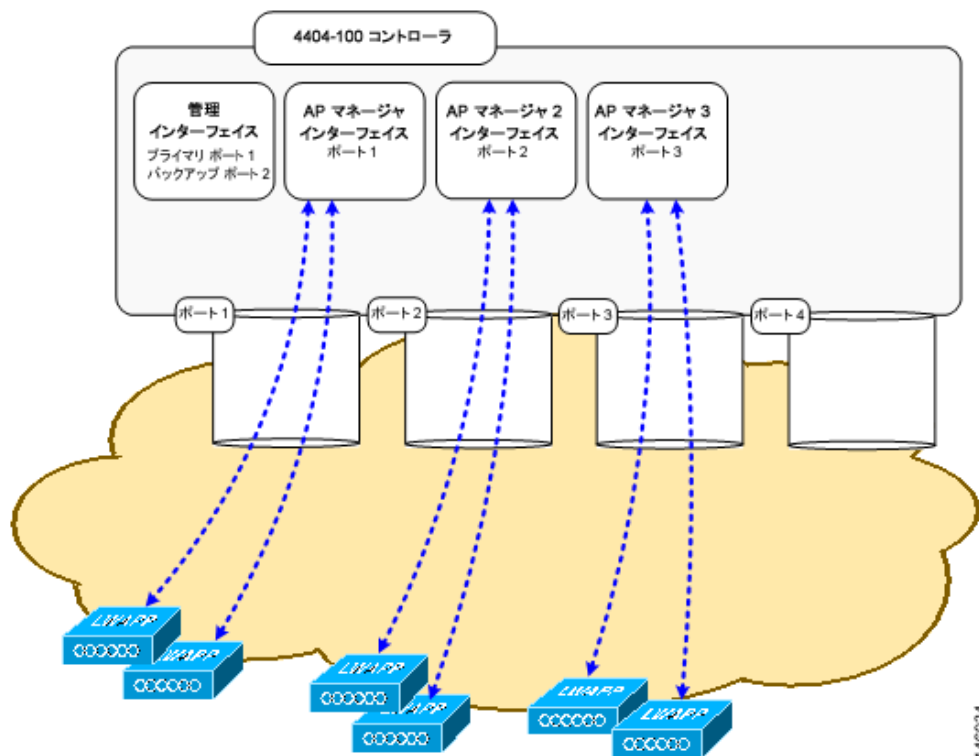
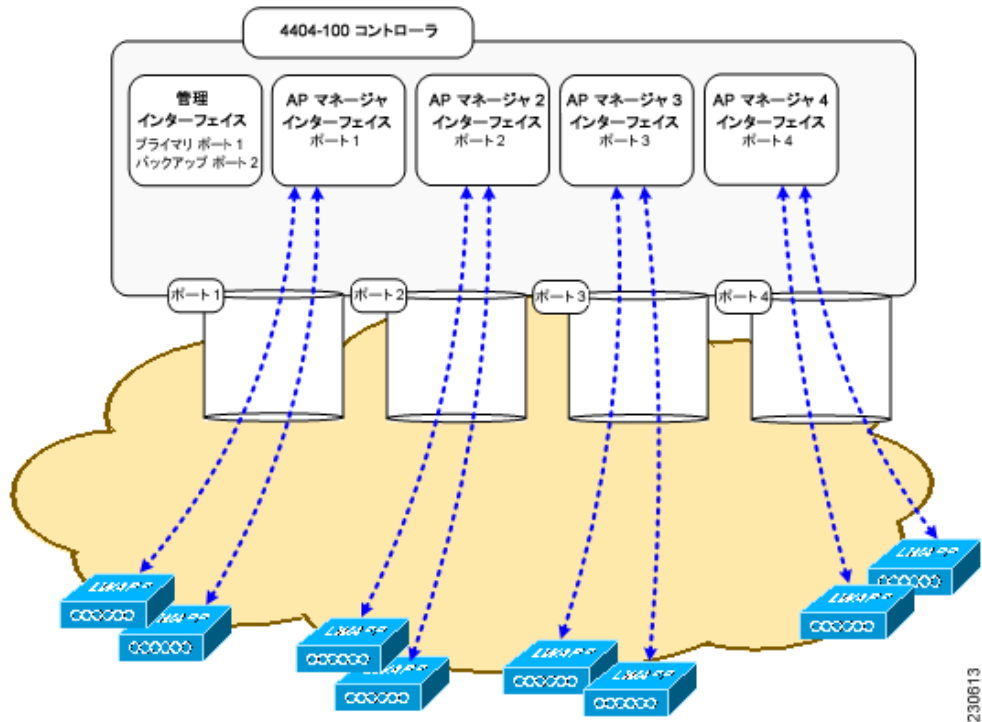


図 3-17 は、4 つの AP マネージャ インターフェイスを使用して、100 個のアクセス ポイントをサポートしている様子を図示したものです。

図 3-17 4 つの AP マネージャ インターフェイス

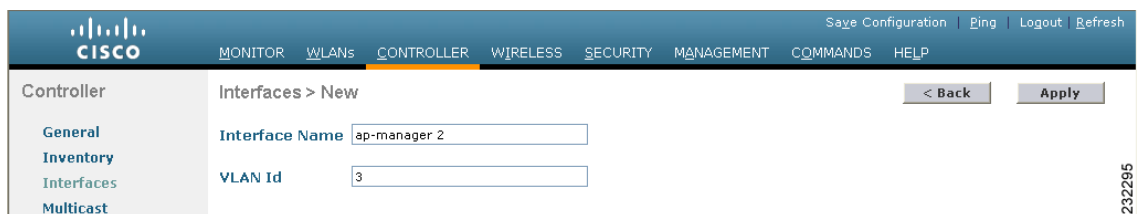


この設定には、4 つの AP マネージャ インターフェイスすべてにわたって、均等に 100 個のアクセス ポイントをすべてロード バランシングできるという利点があります。AP マネージャ インターフェイスの 1 つで障害が発生しても、このコントローラに接続されているアクセス ポイントはすべて、残り 3 つの使用可能な AP マネージャ インターフェイス間で均等に分散されます。たとえば、AP マネージャ インターフェイス 2 で障害が発生した場合、残りの AP マネージャ インターフェイス (1、3、および 4) はそれぞれ約 33 個のアクセス ポイントを管理します。

複数の AP マネージャ インターフェイスを作成する手順は、次のとおりです。

- ステップ 1 **Controller > Interfaces** の順にクリックして、Interfaces ページを開きます。
- ステップ 2 **New** をクリックします。Interfaces > New ページが表示されます (図 3-18 を参照)。

図 3-18 Interfaces > New ページ



- ステップ 3 前述のとおり、AP マネージャ インターフェイスの名前と VLAN 識別子を入力します。

ステップ 4 **Apply** をクリックして、変更を適用します。Interfaces > Edit ページが表示されます (図 3-19 を参照)。

図 3-19 Interfaces > Edit ページ

The screenshot shows the Cisco Wireless LAN Controller configuration interface for editing an interface named 'ap-manager 2'. The left sidebar contains navigation options like General, Inventory, Interfaces, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, and Advanced. The main content area is divided into several sections:

- General Information:** Interface Name (ap-manager 2), MAC Address (00:0b:85:32:42:c0).
- Interface Address:** VLAN Identifier (3), IP Address (10.3.3.2), Netmask (255.255.255.0), Gateway (10.3.3.1).
- Physical Information:** Port Number (1), Backup Port (2), Active Port (0), Enable Dynamic AP Management (checkbox).
- Configuration:** Quarantine (checkbox), Guest Lan (checkbox).
- DHCP Information:** Primary DHCP Server (192.168.50.3), Secondary DHCP Server (0.0.0.0).
- Access Control List:** ACL Name (none).

At the bottom of the page, there is a note: "Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients." The page number 232291 is visible on the right side.

ステップ 5 適切なインターフェイス パラメータを入力します。



(注) AP マネージャ インターフェイスのバックアップ ポートは定義しないでください。AP マネージャ インターフェイスに対するポート冗長化はサポートされません。AP マネージャ インターフェイスで障害が発生した場合は、そのインターフェイスを通してコントローラに接続しているすべてのアクセス ポイントが、他の設定済み AP マネージャ インターフェイスに均等に分散されます。

ステップ 6 このインターフェイスを AP マネージャ インターフェイスにするには、**Enable Dynamic AP Management** チェックボックスをオンにします。

ステップ 7 **Save Configuration** をクリックして、設定内容を保存します。

ステップ 8 作成する AP マネージャ インターフェイスそれぞれについて、この手順を繰り返します。

追加ポートの接続

レイヤ 2 モードの 4400 シリーズ コントローラで 49 個以上のアクセス ポイントをサポートするには、それぞれ完全に分離している複数のブロードキャスト ドメインへ追加のコントローラ ポートを接続する必要があります。表 3-8 は、各コントローラ ポートを別々のスイッチに接続した例です。

表 3-8 レイヤ 2 モードの 4404 コントローラにおけるポート設定の例

[Distribution Switch 1]=Trunk=[Distribution Switch 2]			
dot1q	access	access	access
VLAN 250	VLAN 992	VLAN 993	VLAN 994
ポート 1	ポート 2	ポート 3	ポート 4

VLAN 992、993、および 994（ここで VLAN の例として使用）は access VLAN であり、任意の VLAN ID を割り当てることができます。これらの VLAN には IP アドレスは割り当てられません。これらのポートはアクセス専用です。追加のアクセス ポイントに接続するには、対象のアクセス ポイントに接続するアクセス ポートを VLAN 992、993、または 994 に割り当てます。次に、そのアクセス ポイントにより、隔離 VLAN を使用するコントローラがレイヤ 2 LWAPP に結合されます。ポート 2、3、4 で受信したすべてのレイヤ 2 LWAPP トラフィックは、dot1q タグ 250 の VLAN 250 にある管理ポート（ポート 1 として設定）に渡されます。

レイヤ 2 LWAPP 設定では、VLAN 250、992、993、および 994 にアクセス ポイントを手動で分散する必要があります。できれば、ポートごとに 25 個のアクセス ポイントを割り当て、合計 100 個のアクセス ポイントを均等に分散してください。アクセス ポイント数が 100 未満の場合は、使用するアクセス ポイントの数を 4 で除算し、その個数のアクセス ポイントを各ポートに割り当ててください。たとえば、アクセス ポイントの合計数が 48 の場合、48 を 4 で除算した数（12）のアクセス ポイントを各 4404 ポートに割り当てます。ポート 1 とポート 2 にはそれぞれ 48 個のアクセス ポイントを接続し、ポート 3 には 2 つだけ接続することも可能です。ただし、このようにアクセス ポイントの割り当てが不均衡な場合、最適なスループットが得られません。したがって、このような方法はお勧めできません。

隔離 VLAN のアクセス ポイント設定と通信できるのであれば、ポート 2、3、および 4 をどこに接続してもかまいません。VLAN 250 がネットワーク内で広く使用されているインフラストラクチャ VLAN であり、ネットワーク輻輳が認められる場合は、VLAN 250 に接続されているすべてのアクセス ポイントをポート 2、3、および 4 に割り当て直してください。ポート 1 は、管理ネットワーク インターフェイスとして VLAN 250 に接続されたままですが、コントローラを経由する無線クライアントからのデータのみを転送します。