



CHAPTER 1

概要

この章では、コントローラの構成要素と機能について説明します。この章の内容は、次のとおりです。

- 「Cisco Unified Wireless Network ソリューションの概要」 (P.1-1)
- 「オペレーティング システム ソフトウェア」 (P.1-4)
- 「オペレーティング システムのセキュリティ」 (P.1-4)
- 「レイヤ 2 およびレイヤ 3 の動作」 (P.1-5)
- 「Cisco ワイヤレス LAN コントローラ」 (P.1-6)
- 「コントローラ プラットフォーム」 (P.1-7)
- 「Cisco UWN ソリューションの有線接続」 (P.1-10)
- 「Cisco UWN ソリューション無線 LAN」 (P.1-11)
- 「ファイル転送」 (P.1-11)
- 「Power over Ethernet」 (P.1-11)
- 「Cisco ワイヤレス LAN コントローラ のメモリ」 (P.1-12)
- 「Cisco ワイヤレス LAN コントローラ のフェールオーバーの保護」 (P.1-12)

Cisco Unified Wireless Network ソリューションの概要

Cisco Unified Wireless Network (Cisco UWN) ソリューションは、企業およびサービス プロバイダーに 802.11 無線ネットワーク ソリューションを提供するよう、設計されています。Cisco UWN ソリューションを使用すると、大規模無線 LAN の展開および管理が簡素化され、他に類のないクラス最高のセキュリティ インフラストラクチャを実現できます。オペレーティング システムは、すべてのデータ クライアント、通信、およびシステム管理機能を管理し、Radio Resource Management (RRM) 機能を実行します。また、オペレーティング システム セキュリティ ソリューションを使用してシステム全体のモビリティ ポリシーを管理したり、オペレーティング システムのセキュリティ フレームワークを使用してすべてのセキュリティ機能を調整することもできます。

Cisco UWN ソリューションは、Cisco ワイヤレス LAN コントローラとそれにアソシエートされている Lightweight アクセス ポイントで構成されます。これらはすべてオペレーティング システムによって制御され、次のいずれか、またはすべてのオペレーティング システム ユーザ インターフェイスによって同時に管理されます。

- HTTP、HTTPS、またはこれら両方を備えた Cisco ワイヤレス LAN コントローラの Web ユーザ インターフェイス。個々のコントローラを設定および監視できます。第 2 章「Web ブラウザと CLI インターフェイスの使用法」を参照してください。

- 全機能を備えたコマンドライン インターフェイス (CLI)。個々の Cisco ワイヤレス LAN コントローラの設定と監視に使用できます。第 2 章「Web ブラウザと CLI インターフェイスの使用方法」を参照してください。
- ネットワーク制御システム (NCS)。1 つ以上の Cisco ワイヤレス LAN コントローラと、アソシエートされているアクセス ポイントを設定、監視する場合に使用します。NCS には、大規模システムの監視と制御を容易にするツールが備わっています。WCS は、Windows 2000、Windows 2003、および Red Hat Enterprise Linux ES サーバ上で動作します。



(注) NCS ソフトウェア リリース 1.1 は、コントローラ ソフトウェア リリース 7.2 を実行するコントローラとともに使用する必要があります。

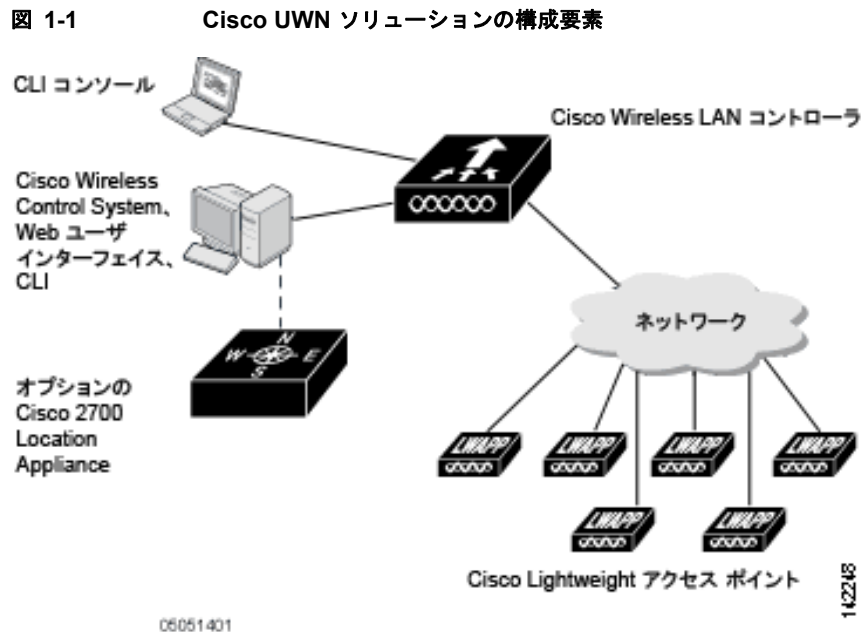
- 業界標準の SNMP V1、V2c、および V3 インターフェイスであれば、SNMP 準拠のサードパーティ製ネットワーク管理システムと併用できます。

Cisco UWN ソリューションは、クライアント データ サービス、クライアントの監視と制御、すべての不正なアクセス ポイントの検出、監視、および阻止機能をサポートします。これによって、Lightweight アクセス ポイント、Cisco ワイヤレス LAN コントローラ、およびオプションの Cisco WCS を使用して、企業やサービス プロバイダーに無線サービスを提供します。



(注) このマニュアル内では、特に記載されていない限り、すべての Cisco ワイヤレス LAN コントローラをコントローラと呼び、すべての Cisco Lightweight アクセス ポイントをアクセス ポイントと呼びます。

図 1-1 は、複数のフロアとビルディングに同時に展開できる Cisco ワイヤレス LAN コントローラの構成要素を示しています。



シングルコントローラ展開

スタンドアロンのコントローラは、複数のフロアとビルディングに配置されている Lightweight アクセス ポイントを同時にサポートすることができます。サポートされている機能は、次のとおりです。

- ネットワークに追加された Lightweight アクセス ポイントの自動検出と自動設定。
- Lightweight アクセス ポイントの完全制御。
- ネットワークを介したコントローラへの Lightweight アクセス ポイントの接続。ネットワーク機器は、アクセス ポイントに Power over Ethernet (PoE) を提供してもしなくてもかまいません。

一部のコントローラでは、1 つのネットワークに障害が発生した場合、冗長ギガビット イーサネット接続を使用してこれを迂回します。

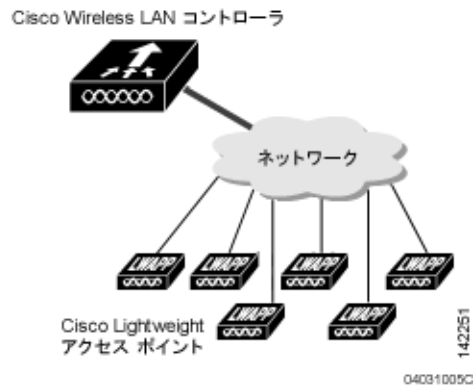


(注)

一部のコントローラは、複数の物理ポートを使用して、ネットワークの複数のサブネットに接続できます。この機能は、複数の VLAN を別々のサブネットに限定する場合に役立ちます。

図 1-2 に、一般的なシングルコントローラ展開を示します。

図 1-2 シングルコントローラ展開



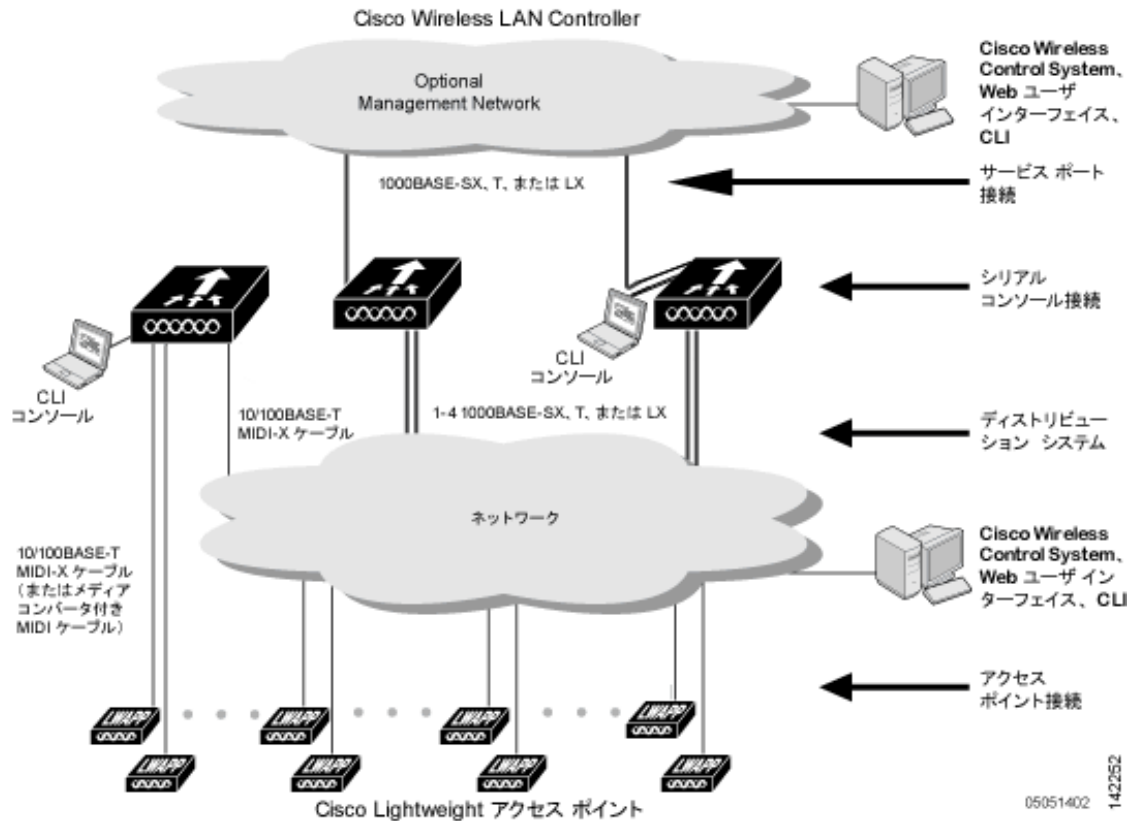
マルチコントローラ展開

すべてのコントローラは、複数のフロアとビルディングに配置されている Lightweight アクセス ポイントを同時にサポートできます。しかし、複数のコントローラを導入すれば、Cisco ワイヤレス LAN ソリューションの機能をフルに利用できます。マルチコントローラ システムには、次の追加の機能があります。

- ネットワークに追加されたコントローラの RF パラメータの自動検出と自動設定。
- 同一サブネット (レイヤ 2) でのローミングとサブネット間 (レイヤ 3) でのローミング。
- アクセス ポイントの負荷を減らす、任意の冗長コントローラへのアクセス ポイントの自動フェールオーバー (「Cisco ワイヤレス LAN コントローラのフェールオーバーの保護」(P.1-12) を参照)。

図 1-3 に、一般的なマルチコントローラ展開を示します。また、この図では、オプションの専用管理ネットワークと、ネットワークとコントローラ間の 3 つの物理接続タイプも示しています。

図 1-3 一般的なマルチコントローラ展開



オペレーティング システム ソフトウェア

オペレーティング システム ソフトウェアは、コントローラと Lightweight アクセス ポイントを制御します。このソフトウェアには、オペレーティング システムのセキュリティ機能と Radio Resource Management (RRM) 機能がすべて組み込まれています。

オペレーティング システムのセキュリティ

オペレーティング システムのセキュリティ機能は、レイヤ 1、レイヤ 2、およびレイヤ 3 のセキュリティ コンポーネントを、Cisco WLAN ソリューション全体を対象とするシンプルなポリシー マネージャに統合したものです。ポリシー マネージャは、最大 16 の無線 LAN それぞれに対して、独立したセキュリティ ポリシーを作成する管理ツールです。「[Cisco UWN ソリューション無線 LAN](#)」(P.1-11)を参照してください。

802.11 Static WEP の脆弱性は、次の強化された業界標準のセキュリティ ソリューションを使用することで克服できます。

- Extensible Authentication Protocol (EAP; 拡張認証プロトコル) を使用した 802.1X ダイナミック キー。
- Wi-Fi Protected Access (WPA) ダイナミック キー。Cisco WLAN ソリューションの WPA 実装は次のとおりです。

- Temporal Key Integrity Protocol (TKIP) と Message Integrity Code Checksum ダイナミックキー
- WEP キー (事前共有キーのパスフレーズの有または無を問わない)
- RSN (事前共有キーの有または無を問わない)
- オプションの MAC フィルタリング

WEP の問題は、次の業界標準のレイヤ 3 セキュリティ ソリューションを使用すると、さらに進んだ解決が可能です。

- パススルー VPN
- ローカルおよび RADIUS による MAC アドレス フィルタリング
- ローカルおよび RADIUS によるユーザ/パスワード認証
- ネットワーク サービスへのアクセスをブロックするための手動および自動による無効化。手動による無効化では、クライアント MAC アドレスを使用してアクセスをブロックします。自動による無効化は常にアクティブであり、クライアントが一定の回数の認証を繰り返し試みて失敗すると、オペレーティング システム ソフトウェアにより、ユーザが設定した時間だけネットワーク サービスへのアクセスが自動的にブロックされます。この機能を使用すると、ブルートフォース ログイン アタックを阻止できます。

これらとその他のセキュリティ機能は、業界標準の認可および認証方式を使用して、ビジネスクリティカルな無線 LAN トラフィックに対する最高のセキュリティを実現します。

Cisco WLAN ソリューションの有線セキュリティ

コントローラと Lightweight アクセス ポイントには、それぞれ固有の署名付き X.509 証明書が添付されます。この署名付き証明書は、ダウンロードしたコードを読み込む前の検証に使用され、悪意のあるコードがハッカーによってコントローラや Lightweight アクセス ポイントにダウンロードされることを防ぎます。

また、コントローラと Lightweight アクセス ポイントでは、ダウンロードしたコードを、署名付き証明書を使用して検証してから読み込むことで、ハッカーが Cisco ワイヤレス コントローラや Lightweight アクセス ポイントに悪意のあるコードをダウンロードできないようにしています。

レイヤ 2 およびレイヤ 3 の動作

コントローラと Lightweight アクセス ポイント間の Lightweight アクセス ポイント プロトコル (LWAPP) 通信は、レイヤ 2 またはレイヤ 3 で実行できます。コントローラと Lightweight アクセス ポイント間の Control and Provisioning of Wireless Access Points プロトコル (CAPWAP) 通信は、レイヤ 3 で実行されます。レイヤ 2 モードでは CAPWAP はサポートしていません。



(注)

コントローラ ソフトウェア リリース 5.2 以降のリリースではレイヤ 3 CAPWAP モードのみ、コントローラ ソフトウェア リリース 5.0 および 5.1 ではレイヤ 3 LWAPP モードのみ、5.0 より前のコントローラ ソフトウェア リリースではレイヤ 2 またはレイヤ 3 LWAPP モードをサポートしています。



(注)

IPv4 ネットワーク層プロトコルは、CAPWAP または LWAPP コントローラ システムでの転送でサポートされています。IPv6 (クライアント用のみ) と Appletalk もサポートされていますが、Cisco 5500 シリーズ コントローラおよび Cisco WiSM でのみのサポートとなります。他のレイヤ 3 プロトコル (IPX、DECnet Phase IV、OSI CLNP など) およびレイヤ 2 (ブリッジ) プロトコル (LAT および NetBeui など) はサポートされていません。

動作上の要件

レイヤ 3 LWAPP 通信を行う場合、コントローラと Lightweight アクセス ポイントが同一サブネットにあるときには、それらをレイヤ 2 デバイスを使用して接続します。異なるサブネットにある場合は、レイヤ 3 デバイスを使用して接続します。また、アクセス ポイントの IP アドレスが外部 DHCP サーバを介して静的または動的に割り当てられていることも必要です。

レイヤ 3 CAPWAP 通信を行う場合、コントローラと Lightweight アクセス ポイントが異なるサブネットにあるときには、レイヤ 3 デバイスを使用して接続します。また、アクセス ポイントの IP アドレスが外部 DHCP サーバを介して静的または動的に割り当てられていることも必要です。

設定要件

レイヤ 2 モードで Cisco ワイヤレス LAN ソリューション を稼働させている場合は、レイヤ 2 通信を制御するよう管理インターフェイスを設定する必要があります。

レイヤ 3 モードで Cisco ワイヤレス LAN ソリューション を稼働させている場合は、Lightweight アクセス ポイントおよびレイヤ 2 モード用に設定された管理インターフェイスを制御するよう AP 管理インターフェイスを設定する必要があります。

Cisco ワイヤレス LAN コントローラ

コントローラが複数展開されたネットワークに Lightweight アクセス ポイントを追加する場合、すべての Lightweight アクセス ポイントを、同一サブネット上の 1 つのマスター コントローラにアソシエートさせると便利です。そうすれば、複数のコントローラにログインして、新たに追加された Lightweight アクセス ポイントがアソシエートされているコントローラを検索する必要はなくなります。

Lightweight アクセス ポイントを追加するとき、各サブネット内の 1 つのコントローラをマスター コントローラとして割り当てることができます。同一サブネット上のマスター コントローラがアクティブである限り、プライマリ、セカンダリ、およびターシャリ コントローラが割り当てられていない新しいアクセス ポイントはすべて、マスター コントローラとのアソシエートを自動的に試みます。このプロセスについては、「[Cisco ワイヤレス LAN コントローラ のフェールオーバーの保護](#)」(P.1-12) で説明します。

WCS Web ユーザ インターフェイスを使用して、マスター コントローラを監視し、アクセス ポイントがマスター コントローラにアソシエートするのを確認できます。その後、アクセス ポイント設定を確認して、プライマリ、セカンダリ、ターシャリ コントローラをアクセス ポイントに割り当てて、プライマリ、セカンダリ、またはターシャリ コントローラに再アソシエートするように、アクセス ポイントをリポートできます。



(注)

Lightweight アクセス ポイントでは、プライマリ、セカンダリ、またはターシャリ コントローラが割り当てられていない場合、リブート時には必ずマスター コントローラが最初に検索されます。マスター コントローラによって Lightweight アクセス ポイントを追加した後、プライマリ、セカンダリ、およびターシャリ コントローラを各アクセス ポイントに割り当てる必要があります。初期設定後は、すべてのコントローラのマスター設定を無効にすることを推奨します。

クライアント ロケーション

Cisco ワイヤレス LAN ソリューションで Cisco WCS を使用する場合、コントローラは、クライアント、不正なアクセス ポイント、不正なアクセス ポイントクライアント、無線周波数 ID (RFID) タグロケーションを定期的にチェックし、そのロケーションを Cisco WCS データベースに保存します。ロケーション ソリューションの詳細については、次のマニュアルを参照してください。

『Cisco Wireless Control System Configuration Guide』

http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html

『Cisco Location Appliance Configuration Guide』

http://www.cisco.com/en/US/products/ps6386/products_installation_and_configuration_guides_list.html

『Cisco 3300 Series Mobility Services Engine Configuration Guide』

http://www.cisco.com/en/US/products/ps9742/products_installation_and_configuration_guides_list.html

コントローラ プラットフォーム

コントローラは、802.11a/n プロトコルおよび 802.11b/g/n プロトコルをサポートする、企業向けの高性能無線スイッチング プラットフォームです。Radio Resource Management (RRM) 機能が搭載されているオペレーティング システムの制御下で稼働することにより、802.11 RF 環境でのリアルタイムの変化に自動対応する Cisco UWN ソリューションを実現します。コントローラは、高性能なネットワークおよびセキュリティ ハードウェアを中心に設計されており、他に例のないセキュリティを備えた信頼性の高い 802.11 企業ネットワークを実現します。

ソフトウェア リリース 7.2 では、次のコントローラがサポートされています。

- Cisco 2500 シリーズ コントローラ
- Cisco 5500 シリーズ コントローラ
- Catalyst 6500 シリーズ スイッチ Wireless Services Module (WiSM2s)
- Cisco Flex 7500 シリーズ コントローラ

Cisco 2500 シリーズ コントローラ

Cisco 2500 シリーズ ワイヤレス コントローラは、Cisco Lightweight アクセス ポイントおよび Cisco Wireless Control System (WCS) と組み合わせて使用することで、システム全体での無線 LAN 機能を実現します。Cisco Unified Wireless Network (CUWN) のコンポーネントとして、Cisco 2500 シリーズ コントローラは、ワイヤレス アクセス ポイントとその他のデバイスとの間のリアルタイム通信を提

供します。それにより、一元化されたセキュリティ ポリシー、ゲスト アクセス、wireless Intrusion Prevention System (wIPS)、Context-Aware (ロケーション)、RF 管理、音声やビデオなどのモビリティ サービス用の QoS、およびテレワーカー ソリューション用の OEAP サポートが実現されます。

Cisco 2500 シリーズ ワイヤレス コントローラは、5 ～ 50 台の Lightweight アクセス ポイントをサポートし、5 および 25 台単位でアクセス ポイントを追加できます。

Cisco 2500 シリーズ コントローラは、802.11 a/b/g により安定したカバレッジを提供します。あるいは、802.11n と Cisco Next-Generation Wireless ソリューションおよび Cisco Enterprise Wireless Mesh を使用して高い信頼性を実現します。

サポートされない機能

- 有線ゲスト アクセス
- 自動アンカー コントローラとして設定できません。ただし、外部コントローラとしては設定できます
- 帯域幅コントラクト
- 直接接続モードのアクセス ポイント
- サービス ポート
- Apple Talk ブリッジ
- LAG

Cisco 5500 シリーズ コントローラ

現在、Cisco 5500 シリーズ Wireless LAN Controller には 1 つのモデル (5508) があります。5508 コントローラは、最大 500 台の Lightweight アクセス ポイントと 7000 台のワイヤレス クライアント (クライアント ロケーション機能を使用する場合は、5000 台のワイヤレス クライアントと 2500 個の RFID タグ) をサポートする、大企業や高密度アプリケーションに最適なコントローラです。

Cisco 5500 シリーズ コントローラには、電源装置を 1 つまたは 2 つ装着できます。コントローラに電源装置を 2 つ装着しておけば、電源装置が冗長構成になり、一方の電源装置に障害が発生しても、もう一方の電源装置から引き続きコントローラに電力を供給できます。

サポートされない機能

- 静的 AP マネージャ インターフェイス



(注) Cisco 5500 シリーズ コントローラでは、AP マネージャ インターフェイスを設定する必要はありません。管理インターフェイスはデフォルトで、AP マネージャ インターフェイスのように動作するので、アクセス ポイントはこのインターフェイスで接続できます。

- アシンメトリック モビリティ トンネリング
- スパニングツリー プロトコル (STP)
- ポートのミラーリング
- レイヤ 2 アクセス コントロール リスト (ACL) のサポート
- VPN 終端 (IPSec や L2TP など)
- VPN パススルー オプション



(注) ACL を使用してオープン WLAN を作成すると、この機能を Cisco 5500 シリーズ コントローラで再現できます。

- 802.3 ブリッジング、AppleTalk、および Point-to-Point Protocol over Ethernet (PPPoE) の設定



(注) Cisco 5500 シリーズ コントローラはデフォルトでこれらのパケットをブリッジ処理します。必要に応じて、ACL を使用してこれらのプロトコルのブリッジングをブロックすることができます。

Cisco Flex 7500 シリーズ コントローラ

Cisco Flex 7500 シリーズ コントローラを使用し、全機能を備えたスケーラブルでセキュアな FlexConnect ネットワーク サービスを、地理的な拠点間に展開できます。Cisco Flex 7500 シリーズ コントローラは、セキュリティ、管理、設定、およびトラブルシューティングの複雑な操作をデータセンター内で仮想化し、それらのサービスを各ストアまで透過的に拡張します。Cisco Flex 7500 シリーズ コントローラを使用した展開は、IT 部門が行うセットアップ、管理、および拡張作業を簡単にします。

Cisco Flex 7500 シリーズ コントローラは、ブランチ ネットワーク内に FlexConnect ソリューションを導入する際の規模要件を満たすように設計されています。Cisco Unified Wireless ソリューションでは、主要な導入モデルとして、FlexConnect と モニタ モードの 2 つがサポートされています。FlexConnect は、アクセス ポイントを中央のコントローラによって制御および管理しながら、データはローカルでスイッチングできるようにすることで、ワイヤレス ブランチ ネットワークをサポートするように設計されています。これは、大規模でもコスト効率の良い FlexConnect ソリューションを実現することを目指しています。

Cisco Flex 7500 シリーズ コントローラがサポートしているアクセス ポイントは、1140、3500、1250、1260、1040、1130、1240、ISR 891、および Cisco Aironet 600 シリーズ OfficeExtend アクセス ポイントです。

Cisco Flex 7500 シリーズ コントローラは、次の機能を提供します。

- 3000 台の AP サポートによる拡張性の向上。
- コントローラの冗長性と FlexConnect の耐障害性による復元力の向上。
- FlexConnect を使用したトラフィック区分けの向上（中央およびローカルのスイッチング）。
- FlexConnect で Enhanced wIPS (ELM) をサポートし、セキュリティを強化 (PCI 準拠)。
- AP グループと FlexConnect グループを使用したストア設計の複製。



(注) Cisco 7500 Flex コントローラは、システム プローブを 10 分間隔で繰り返し実行して、電源装置のステータスを検出します。そのため、Cisco 7500 Flex コントローラ上の実際の電源装置のステータスを検出する際に 10 分の遅延が発生します。

サポートされない機能

次のソフトウェア機能は、Cisco Flex 7500 シリーズ コントローラではサポートされていません。

- L3 ローミング
- VideoStream
- TrustSec SXP

- IPv6
- WGB
- マルチキャスト
- 中央スイッチングされるクライアントのクライアント レート制限

Cisco Wireless Services Module 2

Cisco Wireless Services Module 2 (WiSM2) は、非常に優れたパフォーマンス、セキュリティ、および拡張性を実現し、中規模から大規模の単一拠点の WLAN 展開を提供、ミッションクリティカルなワイヤレス ビジネス コミュニケーションをサポートします。ハードウェア コストの低減に役立つとともに、ワイヤレス ネットワークの総所有コストを削減できる柔軟な設定オプションを提供します。次の機能があります。

- 最大 1,000 台のアクセス ポイントと 15,000 台のクライアントの接続
- 他のワイヤレス LAN コントローラよりもクライアントを高密度でサポート
- 500 台のアクセス ポイントを一度にアップデート可能
- ビデオ、音声、ゲスト、ロケーション、エンタープライズ ワイヤレス メッシュ、およびテレワーキング用のレイヤ 3 モビリティ サービス
- 高度なワイヤレス セキュリティ (レイヤ 1 wireless Intrusion Prevention System (wIPS) 機能など)

サポートされない機能

- 静的 AP マネージャ インターフェイス
- アシメトリック モビリティ トンネリング
- スパニングツリー プロトコル (STP)
- ポートのミラーリング
- レイヤ 2 アクセス コントロール リスト (ACL) のサポート
- VPN 終端 (IPSec や L2TP など)
- VPN パススルー オプション
- 802.3 ブリッジング、AppleTalk、および Point-to-Point Protocol over Ethernet (PPPoE) の設定
- インターフェイス上でのフラグメントされた ping

Cisco UWN ソリューションの有線接続

Cisco UWN ソリューションの構成要素は、業界標準のイーサネット ケーブルとコネクタを使用して相互に通信します。有線接続の詳細は次のとおりです。

- Cisco 5500 シリーズ コントローラは、最大 8 本の光ファイバ ギガビット イーサネット ケーブルを使用し、ネットワークに接続します。
- Cisco Flex 7500 シリーズ コントローラは、2 つの 10 ギガビット イーサネット インターフェイスをサポートします。
- Cisco 2500 シリーズ コントローラは、4 つの 1 Gbps イーサネットをサポートします。

- Cisco Lightweight アクセス ポイントは、10/100BASE-T イーサネット ケーブルを使用してネットワークに接続します。標準の CAT-5 ケーブルを使用して、Power over Ethernet (PoE) 機能が搭載されているネットワーク デバイスから Lightweight アクセス ポイントへ電力を供給することもできます。この電源分配プランを使用すると、個々のアクセス ポイント電源供給と接続用ケーブルにかかるコストを低減できます。

Cisco UWN ソリューション無線 LAN

Cisco UWN ソリューションでは、Lightweight アクセス ポイント全体に対して、最大 512 の WLAN を制御できます。各 WLAN には、それぞれ異なる WLAN ID (1 ~ 512)、それぞれ異なるプロファイル名、および WLAN SSID が割り当てられます。また、一意のセキュリティ ポリシーを割り当てることもできます。Lightweight アクセス ポイントでは、すべてのアクティブな Cisco UWN ソリューション WLAN SSID をブロードキャストし、各 WLAN に定義されているポリシーを適用します。



(注)

コントローラが最適な性能と容易な管理で動作できるよう、WLAN と管理インターフェイスにはそれぞれ別の VLAN を割り当てることをお勧めします。

Cisco UWN ソリューションで無線による管理を有効にすると、CLI と Telnet、http/https、および SNMP を使用して、有効になった WLAN 全体のシステムを管理できるようになります。

WLAN を設定するには、第 7 章「WLAN の使用」を参照してください。

ファイル転送

次のように GUI、CLI、または Cisco WCS を使用して、オペレーティング システムのコード、設定、および証明書ファイルをコントローラにアップロードしたり、コントローラからダウンロードしたりできます。

- コントローラ GUI または CLI を使用する場合は、第 10 章「コントローラ ソフトウェアと設定の管理」を参照してください。
- Cisco WCS を使用してソフトウェアをアップグレードする場合は、『Cisco Wireless Control System Configuration Guide』を参照してください。次の URL をクリックすると、この資料を参照できます。

http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html

Power over Ethernet

Lightweight アクセス ポイントは、イーサネット ケーブルを介して、802.3af 準拠の Power over Ethernet (PoE) デバイスから電力供給を受けることができます。これにより、個々のデバイスへの電力供給や、余分な配線、コンジット、コンセントにかかるコストが低減され、設置時間を短縮できます。PoE 機能を使用すると、AC コンセントの近くに Lightweight アクセス ポイントやその他の電力供給を要する装置を取り付ける必要がなくなるため、アクセス ポイントを、より柔軟に配置して、最大限のカバレッジを得ることができます。

PoE を使用している場合、1 本の CAT-5 ケーブルを各 Lightweight アクセス ポイントから PoE 機能が搭載されているネットワーク機器（PoE 電源ハブや、Cisco WLAN ソリューション シングルライン PoE インジェクタなど）に接続します。PoE 機器で Lightweight アクセス ポイントが PoE 対応であると判断された場合は、使用されていないイーサネット ケーブル ペアを使って、48 VDC の電力が Lightweight アクセス ポイントに供給されます。

PoE ケーブルの長さは、100BASE-T 仕様では 100 m、10BASE-T 仕様では 200 m に制限されています。

Lightweight アクセス ポイントは、802.3af 準拠デバイスまたは外部電源装置から電力供給を受けることができます。

Cisco ワイヤレス LAN コントローラのメモリ

コントローラには 2 種類のメモリが搭載されています。揮発性 RAM には、現在のアクティブなコントローラ設定が保持され、NVRAM（不揮発性 RAM）にはリブート設定が保持されます。コントローラのオペレーティング システムを設定すると、揮発性 RAM の内容が変更されます。したがって、揮発性 RAM の設定を NVRAM に保存し、コントローラが現在の設定でリブートされるようにする必要があります。

次の作業を実行するときは、どちらのメモリを編集しているか理解していることが重要となります。

- 設定ウィザードの使用
- コントローラの設定のクリア
- 設定の保存
- コントローラのリセット
- CLI からのログアウト

Cisco ワイヤレス LAN コントローラのフェールオーバーの保護

インストール時に、すべての Lightweight アクセス ポイントを専用のコントローラに接続して、正式な運用のために各 Lightweight アクセス ポイントを設定することをお勧めします。この手順では、プライマリ、セカンダリ、ターシャリ コントローラについてそれぞれの Lightweight アクセス ポイントを設定し、設定したモビリティ グループ情報を格納できるようにします。

フェールオーバー回復時に、次のタスクが実行されます。

- 設定済みのアクセス ポイントは、プライマリ、セカンダリ、およびターシャリ コントローラとの通信を試み、その後にモビリティ グループ内の他のコントローラの IP アドレスとの通信を試みます。
- DNS は、コントローラ IP アドレスで解決されます。
- DHCP サーバは、コントローラ IP アドレスを取得します（DHCP オファラのベンダー固有オプション 43）。

マルチコントローラ展開では、1 台のコントローラに障害が発生すると、アクセス ポイントによって次のタスクが実行されます。

- Lightweight アクセス ポイントは、プライマリ、セカンダリ、またはターシャリ コントローラが割り当てられている場合、そのコントローラにアソシエイトを試みます。

- アクセス ポイントにプライマリ、セカンダリ、ターシャリ コントローラが割り当てられていない場合、またはプライマリ、セカンダリ、ターシャリ コントローラが使用できない場合には、マスター コントローラにアソシエートを試みます。
- アクセス ポイントがマスター コントローラを検出できなかった場合は、格納されているモビリティ グループ メンバに IP アドレスで接続を試みます。
- モビリティ グループ メンバが使用可能な場合、および Lightweight アクセス ポイントにプライマリ、セカンダリ、ターシャリ コントローラが割り当てられておらず、アクティブなマスター コントローラがない場合、Lightweight アクセス ポイントは、最も負荷の少ないコントローラにアソシエートを試み、その discovery メッセージに応答します。

十分なコントローラが展開されている場合には、1 台のコントローラに障害が発生しても、アクティブなアクセス ポイントのクライアント セッションがただちにドロップする一方で、ドロップしたアクセス ポイントが別のコントローラにアソシエートするため、クライアント デバイスはすぐに再アソシエートと再認証を行うことができます。

ハイアベイラビリティの詳細については、

http://www.cisco.com/en/US/products/ps6366/products_tech_note09186a00809a3f5d.shtml を参照してください。

