CT5760 コントローラ導入ガイド

シスコ次世代 WLAN コントローラ
2013 年 4 月 4 日

Text Part Number: 78-xxxxx-xx-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

FCC クラス A 準拠装置に関する記述：この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス A デジタル装置の制限に準拠していることが確認済みです。これらの制限は、商業環境で装置を使用したときに、干渉を防止する適切な保護を規定しています。この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、この装置のマニュアルに記載された指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。住宅地でこの装置を使用すると、干渉を引き起こす可能性があります。その場合には、ユーザ側の負担で干渉防止措置を講じる必要があります。

FCC クラス B 準拠装置に関する記述：この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス B デジタル装置の制限に準拠していることが確認済みです。これらの制限は、住宅地で使用したときに、干渉を防止する適切な保護を規定しています。この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。ただし、特定の設置条件において干渉が起きないことを保証するものではありません。装置がラジオまたはテレビ受信に干渉する場合には、次の方法で干渉が起きないようにしてください。干渉しているかどうかは、装置の電源のオン / オフによって判断できます。

- 受信アンテナの向きを変えるか、場所を移動します。
- 装置と受信機との距離を離します。
- 受信機と別の回路にあるコンセントに装置を接続します。
- 販売業者またはラジオやテレビに詳しい技術者に連絡します。

シスコでは、この製品の変更または改造を認めていません。変更または改造した場合には、FCC 認定が無効になり、さらに製品を操作する権限を失うことになります。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

CT5760 コントローラ導入ガイド
© 2013 Cisco Systems, Inc. All rights reserved.

CONTENTS

はじめに ix

目標 ix

対象読者 ix

Cisco IOS ソフトウェアに関するマニュアル x

マニュアルの構成 x

コマンド構文の表記法 x

CHAPTER 1 製品概要 1-1

統合アクセス CT5760 ワイヤレス コントローラ 1-1

統合アクセス Catalyst 3850 スイッチ 1-2

CHAPTER 2 サポートされる機能 2-1

シスコのコントローラの比較 2-3

Cisco IOS® ソフトウェア CLI コマンドを使用する新しいオペレーティング システム 2-5

ライセンス 2-5

ソフトウェア リリース番号 2-5

サポートされるプラットフォーム 2-6

統合アクセス導入モード 2-6

一元化モード 2-7

統合アクセス モード 2-7

統合アクセス コンポーネント 2-8

導入の基礎：ポート、インターフェイス、WLAN 2-9

ポートについて 2-9

管理ポート（サービス ポート）（RJ-45） 2-10

コンソール ポート（RJ-45）およびミニ USB タイプ B ポート 2-10

USB ポート 0（タイプ A）： 2-10

SFP ディストリビューション システム ポート 1 ～ 6： 2-10

インターフェイスについて 2-11

WLAN について 2-12

コントローラ検出プロセスに接続する AP 2-12

リンク集約 / ロード バランシング / ポート冗長性 2-12

リンク集約について 2-13

複数 LAG 2-13

コントローラおよびネイバー デバイスの LAG サポートの設定 2-14
CT5760 の一元化設定の例 2-15
ネットワーク トポロジ 2-15
VLAN および IP アドレス 2-15
CLI を使用した CT5760 コントローラ設定の例 2-16
コンソールの接続 2-16
スタートアップ ウィザード 2-16
バージョン 2-18
日付と時刻の設定 2-19
CT5760 コントローラ Web グラフィカル ユーザ インターフェイスのイネーブル化 2-19
基本設定 2-19
CT5760 での DHCP スヌーピングおよび信頼状態の設定 2-20
管理およびクライアント インターフェイスの追加 2-20
WLAN の設定 2-20
AP の接続 2-21
セキュリティ設定 2-21
ワイヤレス WebAuth および Guest Anchor ソリューション 2-22
グローバル コンフィギュレーションの [Parameter Map] セクションの設定 2-22
カスタマイズされた WebAuth の TAR 形式パッケージの設定 2-22
カスタム ページを使用したパラメータ マップの設定 2-23
タイプ同意と電子メール オプションを使用したパラメータ マップの設定 2-23
ローカル WebAuth 認証の設定 2-23
webauth の外部 RADIUS の設定 2-23
WebAuth を使用した WLAN の設定 2-24
グローバル コンフィギュレーションでの HTTP サーバの設定 2-24
チェックを入れたりイネーブルにするその他の設定 2-24
SNMP の設定 2-24
IPv6 Configuration 2-24
IPv6 スヌーピングのイネーブル：CT5760 2-25
インターフェイスでの IPv6 のイネーブル：CT5760 2-25

CHAPTER 3 **CT5760 の一元化設定の例 3-1**
ネットワーク トポロジ 3-1
VLAN および IP アドレス 3-2
CLI を使用した CT5760 コントローラ設定の例 3-2
コンソールの接続 3-2
スタートアップ ウィザード 3-3
バージョン 3-5
日付と時刻の設定 3-5

CT5760 コントローラ Web グラフィカル ユーザ インターフェイスのイネーブル化 3-5
基本設定 3-6
CT5760 での DHCP スヌーピングおよび信頼状態の設定 3-7
管理およびクライアント インターフェイスの追加 3-7
WLAN の設定 3-7
AP の接続 3-8
セキュリティ設定 3-8
ワイヤレス WebAuth および Guest Anchor ソリューション 3-9
グローバル コンフィギュレーションの [Parameter Map] セクションの設定 3-9
カスタマイズされた WebAuth の TAR 形式パッケージの設定 3-9
カスタム ページを使用したパラメータ マップの設定 3-10
タイプ同意と電子メール オプションを使用したパラメータ マップの設定 3-10
ローカル WebAuth 認証の設定 3-10
webauth の外部 RADIUS の設定 3-10
WebAuth を使用した WLAN の設定 3-11
グローバル コンフィギュレーションでの HTTP サーバの設定 3-11
チェックを入れたりイネーブルにするその他の設定 3-11
SNMP の設定 3-11
IPv6 Configuration 3-11
IPv6 スヌーピングのイネーブル：CT5760 3-12
インターフェイスでの IPv6 のイネーブル：CT5760 3-12

CHAPTER 4 **モビリティのアーキテクチャ 4-1**

WLC5760 でのモビリティ設定：モビリティ コントローラ：モビリティ エージェント 4-3
WLC5760 でのモビリティ設定：モビリティ コントローラ：モビリティ オラクル 4-3
WLC5508 でのモビリティ設定：モビリティ コントローラ：モビリティ エージェント： 4-4
モビリティ設計と設定：WLC5760（モビリティ コントローラ）および統合アクセス モードの Catalyst 3850（モビリティ エージェント） 4-4
WLC5760 でのモビリティ設定：モビリティ コントローラ：モビリティ エージェント 4-4
WLC5760 でのモビリティ設定：モビリティ コントローラ：モビリティ オラクル 4-5
WLC5508 でのモビリティ設定：モビリティ コントローラ：モビリティ エージェント 4-5
Catalyst 3850 でのモビリティ設定：モビリティ エージェント 1 4-5
Catalyst 3850 でのモビリティ設定：モビリティ エージェント 2 4-5
Catalyst 3850 でのモビリティ設定：モビリティ エージェント 3 4-6
Catalyst 3850 でのモビリティ設定：モビリティ エージェント 4 4-6
Catalyst 3850 でのモビリティ設定：モビリティ エージェント 5 4-6

Catalyst 3850 でのモビリティ設定：モビリティ エージェント 6 4-6
Catalyst 3850 でのモビリティ設定：モビリティ エージェント 7 4-6
Catalyst 3850 でのモビリティ設定：モビリティ エージェント 8 4-6

CHAPTER 5 モビリティ設計と設定 5-1
モビリティ設計と設定：ハイブリッド モードでの WLC5760、WLC5508、および Catalyst 3850 5-1
WLC5760 でのモビリティ設定：モビリティ コントローラ：モビリティ エージェント 5-2
WLC5760 でのモビリティ設定：モビリティ コントローラ：モビリティ オラクル 5-2
WLC5508 でのモビリティ設定：モビリティ コントローラ：モビリティ エージェント 5-2
Catalyst 3850 でのモビリティ設定：モビリティ エージェント 1 5-2
Catalyst 3850 でのモビリティ設定：モビリティ エージェント 2 5-3
Catalyst 3850 でのモビリティ設定：モビリティ エージェント 3 5-3
Catalyst 3850 でのモビリティ設定：モビリティ エージェント 4 5-3
Catalyst 3850 でのモビリティ設定：モビリティ エージェント 5 5-3
ClientLink（ビーム形成）の設定 5-3

CHAPTER 6 個人所有デバイスの持ち込みのセキュリティ設定 6-1
Apple デバイスの SSID BYOD の単一認証の使用例 6-1
Apple デバイスの SSID BYOD の二重認証の使用例 6-1
トポロジ 6-2
コンポーネント 6-3

CHAPTER 7 セキュアな WLAN の設定 7-1
Catalyst 3850/WLC5508 の Secure WLAN の設定 7-1
ワイヤレス Dot1x 設定 7-1
動的認可の設定 7-1
RADIUS サーバの設定 7-1
URL リダイレクト アクセス リストの設定 7-2
HTTP の設定 7-2
WLAN の設定 7-2
ワイヤレス Dot1x セッションの確認 7-3
クライアントの認証解除 7-3

CHAPTER 8 無線リソース管理の設定 8-1
無線リソース管理の設定 8-1
無線リソース管理について 8-1
RF Group Name 8-2

RRM RF グループ化と次世代のコントローラ 8-3
RF グループ化モードの設定 8-3
RRM TPC の送信電力制御の設定 8-4
RRM DCA 設定 8-4
RRM カバレッジ ホールの検出および軽減 8-5
ネイバー探索プロトコル 8-6

CHAPTER 9 CleanAir 9-1
CleanAir について 9-1
CleanAir の設定 9-1

CHAPTER 10 ハイ アベイラビリティ 10-1
N+1 冗長性 10-2
ハイ アベイラビリティ設定 10-2

CHAPTER 11 インターフェイス グループ 11-1
インターフェイス グループの設定 11-1
AP グループを設定 11-2
AP グループについて 11-2

CHAPTER 12 マルチキャストの設定 12-1
WLC から AP への転送モード 12-1
マルチキャスト VLAN 機能 12-2
ブロードキャスト転送 12-2
設定の確認 12-3
CT5760 へのソフトウェア イメージのインストールおよびアップグレード 12-3
Prime への WLC の追加 12-5
Flexible NetFlow 12-7

CHAPTER 13 QoS の設定 13-1
QoS のイネーブル化 13-1
QoS の管理 13-1
マーキング モデル 13-1
ポート別またはクライアント別のマーキング 13-2
ポリシング モデル 13-3
ワイヤレス キューイング 13-6
Wireless Multimedia 設定 13-6
QoS ポリシーの認証およびプッシュのための ISE 設定 13-7

Cisco IOS® ツール コマンド言語スクリプト 13-9

はじめに

この項では『*CT5760 コントローラ導入ガイド*』の目的、対象読者、表記法、およびマニュアルの構成について説明し、Cisco IOS ソフトウェアのマニュアルに関する一般情報を提供します。

シスコのマニュアルおよびその他の資料は、製品に同梱されている CD-ROM パッケージでご利用いただけます。Documentation CD-ROM、は Cisco Connection ファミリのメンバーで、毎月更新されます。したがって、印刷されたドキュメントより最新である可能性があります。Documentation CD-ROM の追加コピーを注文するには、営業担当者にお問い合わせいただくか、カスタマー サービスまでお問い合わせください。この CD-ROM パッケージは、単独パッケージまたは年間契約で入手することができます。

目標

このマニュアルでは、Cisco Unified Access アーキテクチャに属する 2 台の新しいコントローラを紹介し、これらの機器の導入に関する一般的なガイドラインを示します。このドキュメントでは、次のことを目的としています。

- 新しい Cisco 5760 次世代ワイヤレス LAN コントローラおよび次世代 Catalyst 3850 有線 / ワイヤレス スイッチの概要を示します。
- 一元化アクセス導入に特化した設計上の推奨事項および導入に関する考慮事項を説明します。

対象読者

このマニュアルは主にルータを設定し維持管理するユーザを対象としていますが、必ずしもタスク、タスク間の関係、または VoIP を設定する特定のタスクの実行に必要なコマンドについて熟知している必要はありません。また、このマニュアルでは、IP およびテレフォニー ネットワークに関して多少知識のある担当者を対象としています。

Cisco IOS ソフトウェアに関するマニュアル

このマニュアルに記載された情報に加えて、Cisco IOS マニュアル セットを参照する必要がある場合があります。この Cisco IOS ソフトウェア マニュアルは 9 つのモジュールと 2 つのマスター インデックスに分割されます。各モジュールは、コンフィギュレーション ガイドおよびコマンド リファレンスの 2 冊のマニュアルから成ります。コンフィギュレーション マニュアルの章ではプロトコル、設定作業、および Cisco IOS ソフトウェアの機能を説明し総合的な設定の例を示します。コマンド リファレンスの章では完全なコマンド構文の情報を提供します。各コンフィギュレーション ガイドは、それに対応するコマンド リファレンスと併せて使用できます。

マニュアルの構成

この章は、このマニュアルの各章の内容を示します。

表 1　　マニュアルの構成

章	タイトル	説明
第 1 章	製品概要	コントローラの概要
第 2 章	サポートされる機能	サポートされる機能
第 3 章	モビリティのアーキテクチャ	新しいモビリティ アーキテクチャでのモビリティ コンポーネントの概要
第 4 章	モビリティ設計と設定	ハイブリッド モードでの WLC5760、WLC5508、および Catalyst 3850 の設定
第 5 章	個人所有デバイスの持ち込み（BYOD）セキュリティ設定	個人デバイスのセルフ サービス追加の説明
第 6 章	セキュアな WLAN の設定	Catalyst 3850/WLC5508 の設定
第 7 章	無線リソース管理の設定	無線リソース管理（RRM）ソフトウェア
第 8 章	CleanAir	CleanAir：スペクトル インテリジェンス ソリューション
第 9 章	ハイ アベイラビリティ	可用性の概要
第 10 章	インターフェイス グループ	インターフェイスのグループの概要
第 11 章	マルチキャストの設定	マルチキャスト設定の概要
第 12 章	QoS の設定	WLC5760 コントローラでの Cisco IOS® ソフトウェアの概要

コマンド構文の表記法

表 2 に、このマニュアルのコマンドで使用される構文を示しています。

表 2　　コマンド構文ガイド

表記法	説明
太字	コマンドおよびキーワード。
イタリック体	ユーザによるコマンド入力。

表 2　　コマンド構文ガイド （続き）

表記法	説明
[　]	角カッコ内の要素は、省略可能です。
{ x | x | x }	選択すべきキーワード（x の部分）は、波カッコで囲み、縦棒で区切って表します。いずれか 1 つを必ず選択します。
^ または Ctrl	*Ctrl* キーを表します。たとえば、*^D* または *Ctrl-D* と表記されている場合、Ctrl キーを押さえながら D キーを押します。
`screen フォント`	画面に表示される情報の例を表します。
太字の screen フォント	入力が必要な情報の例。
<　>	パスワードのように、出力されない文字は、山カッコ（<>）で囲んで示しています。
[　]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。

製品概要

この項では、2 種類の新しいコントローラの概要を説明します。

統合アクセス CT5760 ワイヤレス コントローラ

CT5760 ワイヤレス LAN コントローラ（WLC）は次世代型ユニファイド ワイヤレス アーキテクチャで一元化されたコントローラとして導入されるようにスマート ASIC が搭載された最初の Cisco IOS® ソフトウェア ベースのコントローラです。CT5760 コントローラは従来の統合モデル中央ワイヤレス コントローラのように機能するように特別に設計されています。また、ワイヤレス アーキテクチャで次世代ワイヤレス コントローラ 3850 スイッチと共に新しいモビリティ機能をサポートします。

CT5760 コントローラはコア スイッチ/ルータの背後に配置されます。コア スイッチとルータはコントローラがネットワークへ入る唯一のゲートウェイです。コア スイッチに接続されているアップリンク ポートはポートの冗長性を保障するように EtherChannel トランクとして設定されます。

この新しいコントローラは最大 1000 個のアクセス ポイント (AP) および 12,000 クライアントまで拡張可能な、高パフォーマンスのワイヤレス コントローラです。コントローラには 8 個の 6～10 Gbps データ ポートがあります。

Cisco Unified Wireless Network のコンポーネントとして 5760 シリーズは Cisco Aironet アクセス ポイント、Cisco Prime インフラストラクチャおよびシスコ モビリティ サービス エンジンとともに動作し、ビジネス重視のワイヤレス データ、音声、およびビデオ アプリケーションをサポートします。WLC5760 概要については図 1-1 を参照してください。

図 1-1　WLC5760 の概要

統合アクセス Catalyst 3850 スイッチ

統合アクセス Catalyst 3850 スイッチは複数のプロトコルをサポートし、現在のハードウェア プラットフォームを上回る多数のメリットを備えた柔軟な ASIC ベースのハードウェアです。

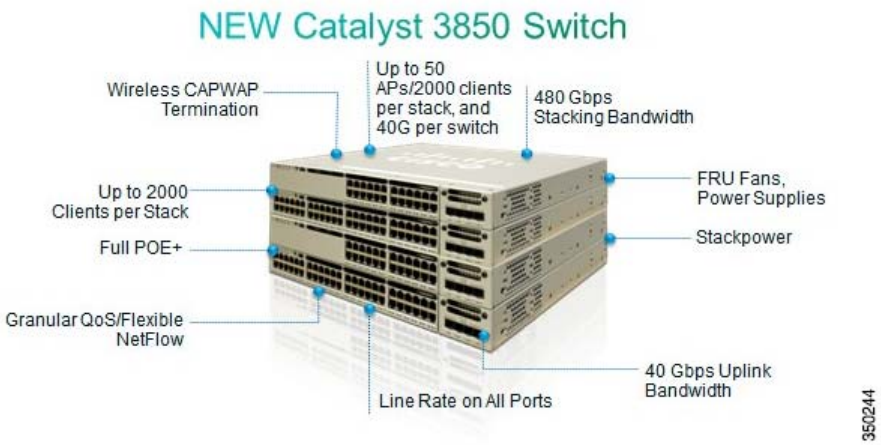
Catalyst 3850 スイッチは、ワイヤレス アクセス ポイントのコントロールとプロビジョニング（CAPWAP）およびフラグメンテーションを使用してハードウェア ベースのワイヤレス統合をサポートします。また、すべてのポートがライン レートで動作するとき、40 GB のアップリンク帯域幅があります。

Catalyst 3850 スイッチはオープンなサービス プラットフォームを提供します。また、オペレーティング システム（OS）を活用し、さまざまなサービスを提供するために 4 コア CPU を装備しています。Catalyst 3850 ハードウェアは、次世代のスイッチング ハードウェアです。

統合アクセス Catalyst 3850 スイッチは、有線とワイヤレスが統合されたアーキテクチャを持ちます。ワイヤレス オペレーティング システムは Cisco IOS® ソフトウェア ベースです。統合アクセス Catalyst 3850 スイッチは、均等な有線およびワイヤレス ポリシーを提供します。統合アクセス Catalyst 3850 スイッチは、50 アクセス ポイント（802.11n）を搭載でき、スタックごとに最大 2000 クライアントをサポートできます。図 1-2 に Catalyst 3850 のプラットフォームの概要を示します。

設定の推奨事項の詳細については、『Catalyst 3850 Configuration Guides』ページを参照してください。

図 1-2　新しい Catalyst 3850



サポートされる機能

CT5760 WLC は、802.11ac パフォーマンス用に設計された業界最先端のプラットフォームで、ミッション クリティカルなワイヤレス ネットワークに対して最大のサービス、拡張性、および復元力を提供します。拡張されたソフトウェア プログラム可能 ASIC により、表 2-1 に示す幅広い機能を提供します。

表 2-1　Cisco 5760 WLC の機能

機能	利点
拡張性	• ビジネス重視のワイヤレス サービスにおいて最大 1000 の AP、および 12,000 のワイヤレス クライアントをサポートします。 • 複数のコントローラで構成する比類のない拡張性のワイヤレス ソリューションは最大 72,000 の AP と 864,000 のワイヤレス クライアントをサポートできます。
高パフォーマンス	• 802.11ac 標準に最適化。 • 6 個の 10G Cisco SFP+（Small Form-Factor Pluggable）アップリンク。 • ダウンロード可能アクセス コントロール リスト（ACL）、Quality of Service（QoS）の詳細なキュー、公正なアルゴリズム、NetFlow v9 などのサービスで最大 60 Gbps のスループットを提供するハードウェア アシストによる処理。
高い復元性	• 統合アクセス導入モードは、障害をより小さなドメインに留める階層型ネットワーク設計を提供します。これによって、より高い復元性を実現します。ワイヤレス クライアントは、ステートフル スイッチオーバー（AP SSO）を介して、Catalyst 3850 シリーズ スイッチ スタック内のスイッチの障害を自動的に迅速に復旧します。 • 中央集中型の展開モード（別名ローカル モード）の CT5760 は 1+1 および N+1 復元力をサポートします。 • 複数リンク集約（LAG）のサポート。最適なネットワーク接続を維持しながらリンク障害から保護します。
Cisco IOS® ソフトウェア ベースのコントローラ	• 実証済みのセキュリティ強化された Cisco IOS® オペレーティング システム。 • 定評のある Cisco IOS® ソフトウェア CLI によって、カスタマーが現在の操作の管理ツールを活用することができます。 • シスコの充実した NetFlow エコ システムを使用して、カスタマーはワイヤレス ネットワークのレポート、監視、トラフィックの分析、およびトラブルシューティングをすることができます。

表 2-1　Cisco 5760 WLC の機能 （続き）

ClientLink 2.0	• Cisco ClientLink 2.0 テクノロジーによって、802.11n の 1、2、および 3 空間ストリームのデバイスなどすべてのモバイル デバイスへのダウンリンク パフォーマンスが向上し、スマート フォンやタブレットなどのモバイル デバイスのバッテリ寿命が向上します。
CleanAir	• Cisco CleanAir™ テクノロジーは、ワイヤレス干渉によるパフォーマンスの問題に予防的に対処できる高速スペクトル インテリジェンスを提供します。
無線周波数（RF）管理	• システム全体での Cisco CleanAir™ テクノロジーの統合により、コントローラ全体のネットワーク パフォーマンスに影響のある RF 干渉に関するリアルタイム情報および履歴情報の両方を提供します。
総合的なエンドツーエンド セキュリティ	• アクセス ポイントとコントローラまたはコントローラ間での暗号化を保障する CAPWAP 準拠のデータグラム トランスポート層セキュリティ（DTLS）の暗号化を提供します。
高性能ビデオ	• 有線およびワイヤレス クライアントの両方への単一ストリームによるビデオ配信を最適化します。 • ビジネス重視のマルチキャスト ビデオ アプリケーションの WLAN 全体への配信を最適化する Cisco VideoStream テクノロジーをサポートします。
エンドツーエンドの音声	• メッセージ、プレゼンス、および会議によるコラボレーションを向上させるためにユニファイド コミュニケーションをサポートします。 • コスト効率に優れたリアルタイムの音声サービスのためのすべての Cisco Unified Communications ワイヤレス IP 電話をサポートします。
高度な QoS	• モジュラ QoS CLI を介して有線およびワイヤレス QoS の両方に対する CLI の設定が統一できます。 • アクセス ポイント（AP）、サービス セット ID (SSID)、無線、およびクライアントごとの詳細な QoS ポリシーです。 • AP のワイヤレス クライアント全体に均等に帯域幅割り当てが行われます。 • ライン レート パフォーマンスを提供する実証済みの Cisco IOS® ソフトウェアおよび ASIC テクノロジーを活用します。
高度な ACL	• ダウンロード可能 ACL により、セキュリティ ポリシーを合理化および一元化します。 • ACL は、ライン レート パフォーマンスを提供するためにハードウェアで処理されます。
Flexible NetFlow v9	• ワイヤレス クライアント用の Flexible NetFlow でネットワーク全体を視覚化します。
環境への配慮	• オフピーク時に電力消費量を減らすために、組織的に AP 無線をオフにすることを選択する場合があります。 • 統合された WLC はネットワークへの追加デバイスの導入を回避します。

表 2-1　Cisco 5760 WLC の機能 （続き）

モビリティおよびセキュリティ	• 信頼性の高いワイヤレス接続、安定したエンドユーザの使用感を確保します。 • 既知の脅威に対する予防的なブロックによりネットワークの可用性を向上します。
IPv6	• 監視およびトラブルシューティングのための適切な「show」コマンドを使用してインターフェイスの IPv6 アドレッシングをサポートします。 • IPv6 ACL は、ライン レート パフォーマンスを提供するためにハードウェアで処理されます。

機能および仕様の完全なリストは、『Cisco 5760 Series Wireless Controller』ページおよび『Data Sheet』を参照してください。

シスコのコントローラの比較

この表は、シスコの大規模コントローラの比較の一覧を示します。

表 2-2　シスコのコントローラの比較

	85002	7500	5500	WiSM	5760
導入タイプ	エンタープライズ 広大な構内 + SP Wi-Fi	多数の分散したコントローラなしのブランチ オフィスに対応する中央拠点のコントローラ	企業の構内およびすべてのサービスを実施するブランチ オフィス	企業の構内	広大な構内
オペレーショナル モード	ローカル モード、FlexConnect、メッシュ	FlexConnect のみ	ローカル モード、FlexConnect、メッシュ	ローカル モード、FlexConnect、メッシュ	一元化された（ローカル モード）または統合アクセス モード
最大規模	6000 AP 64,000 クライアント	6000 AP 64,000 クライアント	500 AP 7000 クライアント	000 AP 15,000 クライアント	11000 AP 12,000 クライアント
AP カウントの範囲	300 ～ 6k AP	300 ～ 6k AP	12 ～ 500 AP	100 ～ 1000 AP	1 ～ 1000 AP

表 2-2　シスコのコントローラの比較 （続き）

ライセンス	使用権 （EULA 含む）	使用権 （EULA 含む）	CISL ベース （Unchanged）	CISL ベース （Unchanged）	使用権 （EULA 含む）
接続	2 x 10G ポート	2 x 10G ポート	8 x 1G ポート	内部接続の Catalyst バックプレーン	6 x 10G ポート
電源	AC/DC デュアル冗長	AC デュアル冗長	AC（冗長 PSU オプション）	AC/DC Catalyst シャーシ （冗長 PSU オプション）	AC（冗長 PSU オプション）
FlexConnect グループの最大数	2000	2000	100	100	該当なし
FlexConnect グループあたりの AP の最大数	100	100	25	25	該当なし
不正 AP 管理の最大数	24,000	24,000	2000	4000	4000
不正クライアント管理の最大数	32,000	32,000	2500	5000	5000
RFID の最大数	50,000	50,000	5000	10,000	10,000
RRM グループあたりの最大 AP 数	6000	6000	1000	2000	2000
最大 AP グループ数	6000	6000	500	500	1000
最大インターフェイス グループ数	512	512	64	64	64
インターフェイス グループあたりの最大インターフェイス数	64	64	64	64	64
サポートされる最大 VLAN 数	4095	4095	512	512	4096

表 2-2　シスコのコントローラの比較 （続き）

サポートされる最大 WLAN 数	512	512	512	512	512
サポートされる高速セキュアローミング (FSR) 数	64,000	64,000	14,000	30,000	24,000

Cisco IOS® ソフトウェア CLI コマンドを使用する新しいオペレーティング システム

CT5760 コントローラは、Cisco スイッチおよびルータで使用されるのと同じ Cisco IOS® ソフトウェア CLI コマンドを使用します。新しいワイヤレス CLI コマンドは既存の Cisco IOS® CLI に追加されています。ワイヤレス Cisco IOS® ソフトウェア CLI コマンドの完全なリストについては、『Cisco 5700 Series Wireless LAN Controller Command References』ドキュメントを参照してください。

ライセンス

ライセンスは使用ライセンス モデルに基づいています（Catalyst 3850 および CT5760 の AP ライセンス料金ごと）。AP ライセンスは、モビリティ コントローラでイネーブルになります。Catalyst 3850 スイッチ、CT5760、5500、または WiSM2 がモビリティ コントローラになります。モビリティ エージェントの機能（たとえばスイッチの CAPWAP 終端）別のライセンスはありません。5500/WiSM2 をモビリティ コントローラとして使用している場合は、従来と同じ AP ライセンスを使用できます。AP ライセンスは Catalyst 3850 と CT5760 間、Catalyst 3850 と Catalyst 3850 間、および CT5760 と CT5760 間で譲渡可能です。

詳細については、シスコ使用ライセンスの FAQ を参照してください。

ソフトウェア リリース番号

5760 初回リリースは、Cisco IOS XE 3.2.0SE です。

サポートされるプラットフォーム

コントローラ

- 統合アクセス モード：CT5760、CT5508、WS-SVC-WISM2、3850
- 一元化モード：CT5760、WISM2、CT5508

AP

- 1040、1140、1260、1600、2600、3500、3600

Cisco Prime 2.0（将来のリリース：2013 年 5 月）

- アプライアンスおよび仮想インスタンス

Mobility Services Engin（MSE）

- 3300 および仮想インスタンスでの MSE 7.4

Identity Services Engine（ISE）

- 3315、3355、3395 および仮想インスタンスでの ISE 1.1.1

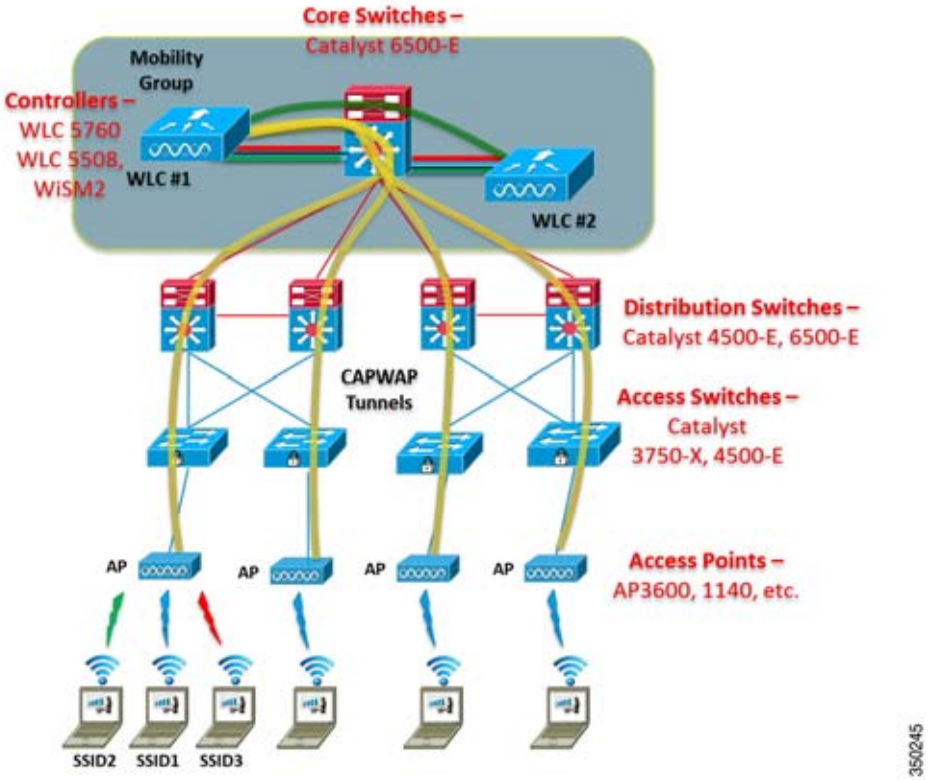
統合アクセス導入モード

CT5760 および Catalyst 3850 の導入には、2 つの Cisco Unified Access アーキテクチャ、つまり一元化および統合アクセスがあります。

一元化モード

一元化モード（従来のコントローラではローカル モード）は有線接続だけでなくワイヤレスにも設定されている Cisco Unified Wireless Network (CUWN) ソリューションのさまざまなポイントで現在使用されているものと同じ導入モデルです。現在の CUWN ではユーザ トラフィックをコントローラへ一元化してトンネリング（データ プレーンとコントロール プレーン）しチャネルおよびパワーの割り当て、不正の検出、セキュリティ攻撃、干渉、ローミングなどをシステム全体で調整します。

図 2-1　　一元化モード

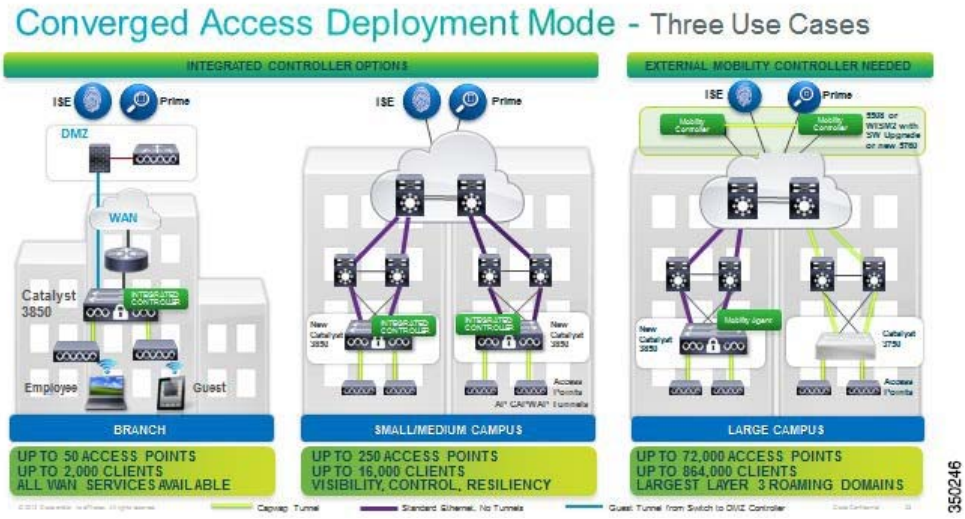


統合アクセス モード

統合モードは、既存のワイヤレス導入の進化形で、モビリティに追加の導入モードを提供します。統合アクセス モデルでは注意すべきいくつかの設計の違いがあります:

- Catalyst 3850 はローカルに接続されている AP の CAPWAP トンネルを終端するモビリティ エージェントとして動作できます。
- Catalyst 3850 は、小規模な導入では他のモビリティ エージェント スイッチのモビリティ コントローラとして機能できます。
- スイッチ ピア グループ（SPG）（L2/L3）全体のローミングを行います。
- SPG 内のモビリティ エージェントはフル メッシュ構造（SPG 形成での自動作成）です。

図 2-2　統合アクセス導入モード



統合アクセス コンポーネント

いくつかのコンポーネントは、統合アクセス モデルを理解するために強調表示されます。これらのコンポーネントを図 2-3 に示します。

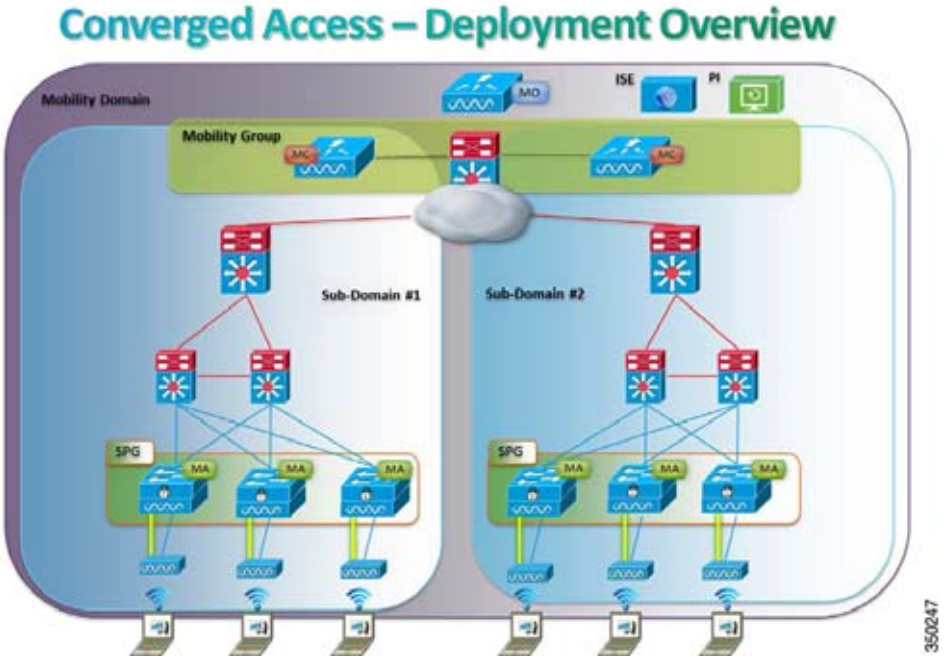
1. 物理エンティティ：

- モビリティ エージェント：AP からの CAPWAP トンネルを終端します。
- モビリティ コントローラ：サブ ドメイン内および全体でモビリティを管理します。
- モビリティ オラクル：モビリティ コントローラのスーパーセットで、ドメイン内のスケーラブルなモビリティ管理が可能になります。

2. 論理エンティティ：

- モビリティ グループ：モビリティ コントローラをグループ化して高速ローミング、無線周波数管理などを可能にします。
- スイッチ ピア グループ：ディストリビューション ブロック内をローミングするためにローカライズされたトラフィックです。

図 2-3　統合アクセス：導入の概要



この展開ガイドでは、Cisco IOS® フトウェアでの新しい CT5760 フィーチャ セットの設定に焦点を当てています。新しい Catalyst 3850 有線 / ワイヤレス スイッチおよび導入シナリオの詳細については、『Catalyst 3850 Deployment/Configuration Guides』ページを参照してください。

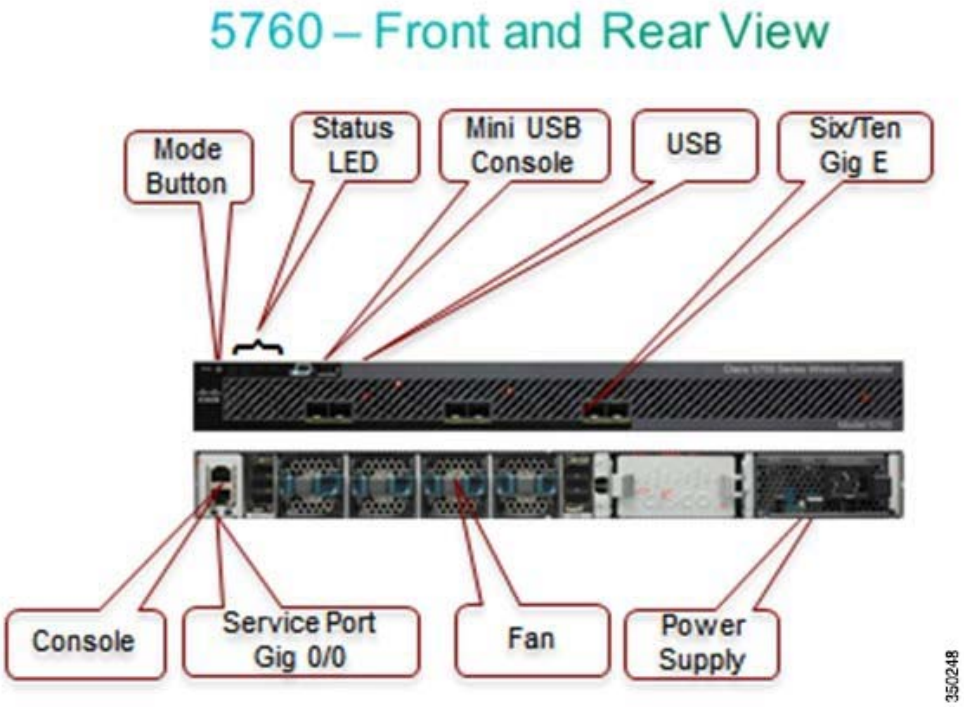
導入の基礎：ポート、インターフェイス、WLAN

この項では CT5760 ポート、インターフェイス、および WLAN に関する情報を扱います。

ポートについて

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。CT5760 コントローラで使用可能なポートを図 2-4 に示します。

図 2-4　CT5760 コントローラ：正面図および背面図



管理ポート（サービス ポート）（RJ-45）

Cisco 5760 シリーズ コントローラは 10/100/1000 銅線イーサネット管理ポート（GE0/0）を備えています。管理ポートは、コントローラのアウトオブバンド管理、システム リカバリ、およびネットワーク障害が発生した場合のメンテナンス用に確保されています。

コンソール ポート（RJ-45）およびミニ USB タイプ B ポート

CT5760 WLC には RJ-45 およびミニ USB タイプ B の 2 つのコンソール ポートがあります。

（注）　1 つのコンソール ポートのみを使用できます（RJ-45 またはミニ USB）。1 つのコンソール ポートに接続すると、もう一方のポートは無効になります。

USB ポート 0（タイプ A）：

Cisco 5760 シリーズ コントローラの USB コンソール ポートは、USB タイプ A/5 ピン ミニ タイプ B ケーブルを使用して PC の USB コネクタに直接接続します。

SFP ディストリビューション システム ポート 1 ～ 6：

Cisco 5760 コントローラには、6 個の 10 ギガビット イーサネット（GE）ディストリビューション システム ポートが搭載されていて、これらのポートを通じて複数の AP を管理できます。Cisco 5760 コントローラは、最大 1000 AP をサポートし、ポート単位の AP 数に制限はありません。ただし、負荷

を自動的に分散させるためにリンク集約 (LAG) または EtherChannel を使用することを推奨します。LAG はこのマニュアルの別の項で説明します。10GE ポートでサポートされる SFP の製品番号を表 2-3 に示します。

表 2-3　10GE でサポートされる SFP の製品番号

SFP+/SFP（サポートされる Cisco SFP のみ）	• SFP-10G-ER • SFP-10G-LR • SFP-10G-SR • SFP-10G-LRM • SFP-H10GB-CU1M • SFP-H10GB-CU3M • SFP-H10GB-CU5M • GLC-BX-D • GLC-BX-U • GLC-SX-MM • GLC-SX-MMD • GLC-T • GLC-LH-SM • GLC-ZX-SM • CWDM-SFP • DWDM-SFP • SFP-GE-L • SFP-GE-S • GLC-LH-SMD • GLC-EX-SMD • GLC-GE-100FX

インターフェイスについて

インターフェイスはコントローラ上の論理的実体です。次世代のコントローラには、複数のインターフェイスが実装されていますが、これらのインターフェイスは以下のように設定する必要があります:

1. ワイヤレス管理インターフェイス（セットアップ時に設定可能。必須）

   ワイヤレス管理インターフェイスは AP のコントローラ検出、モビリティ、および無線リソース管理（RRM）に使用されます。このインターフェイスは、インバンド管理、つまり Telnet/SSH CLI、SNMP、および WebGUI に対しても使用されます。

2. ダイナミック インターフェイスと見なされる VLAN に WLAN トラフィックがマッピングされる場所。

WLAN について

WLAN は VLAN インターフェイスにサービス セット ID（SSID）を関連付けます。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。コントローラ 1 つあたり、最大 512 AP の WLAN を設定できます。

WLAN は、物理インターフェイスにマッピングされている VLAN にマッピングされます。

（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。

コントローラ検出プロセスに接続する AP

CAPWAP 環境では、Lightweight AP は CAPWAP 検出方式によってコントローラを検知し、コントローラに CAPWAP 接続要求を送信します。これに対し、コントローラは AP に CAPWAP 接続応答を返し、AP はコントローラに接続できるようになります。AP がコントローラに接続すると、コントローラによって AP の構成、ファームウェア、制御トランザクション、およびデータ トランザクションが管理されます。

AP をネットワークでアクティブにするには、コントローラがその AP を検出する必要があります。Lightweight AP では、次のコントローラ ディスカバリのプロセスがサポートされています。

- Layer 3 CAPWAP 検出：この機能は、AP とは異なるサブネット上で有効化され、レイヤ 2 検出で使用される MAC アドレスではなく IP アドレスと UDP パケットが使用されます。
- ローカルに保存されたコントローラ IP アドレスの検出：AP が以前にコントローラに接続していた場合、第 1、第 2、第 3 のコントローラの IP アドレスが AP の不揮発性メモリに保存されています。今後の展開用に AP にコントローラの IP アドレスを保存するこのプロセスは、「AP のプライミング」と呼ばれます。
- DHCP サーバの検出：この機能は、DHCP オプション 43 を使用して AP にコントローラの IP アドレスを割り当てます。Cisco スイッチでは、通常この機能に使用される DHCP サーバ オプションをサポートしています。DHCP オプション 43 の詳細については、『Configuring DHCP Option 43 for Lightweight Access Points』ドキュメントを参照してください。
- DNS の検出：AP は DNS を使用してコントローラを検出します。AP でこれを実行するには、CISCO- CAPWAP-CONTROLLER.localdomain への応答としてコントローラの IP アドレスを返すよう、DNS を設定する必要があります。ここで、localdomain は AP ドメイン名です。AP は、DHCP サーバから IP アドレスと DNS の情報を受信すると、DNS に接続して CISCO-CAPWAP-CONTROLLER.localdomain または CISCO-CAPWAP-CONTROLLER.localdomain を解決します。DNS からコントローラの IP アドレスのリストを受信すると、AP はコントローラに検出要求を送信します。

リンク集約 / ロード バランシング / ポート冗長性

Cisco 5760 WLC にポートあたりの AP 数の制限はありませんが、自動的にロード バランシングを行うために各 10GE ポートで LAG または EtherChannel を使用することを推奨します。

LAG の機能は、Cisco IOS® ソフトウェアの EtherChannels の設定を使用して CT5760 コントローラで達成されます。EtherChannel を介して、コントローラによってポートの冗長性は動的に管理され、AP はユーザからは透過的にロード バランシングされます。

リンク集約について

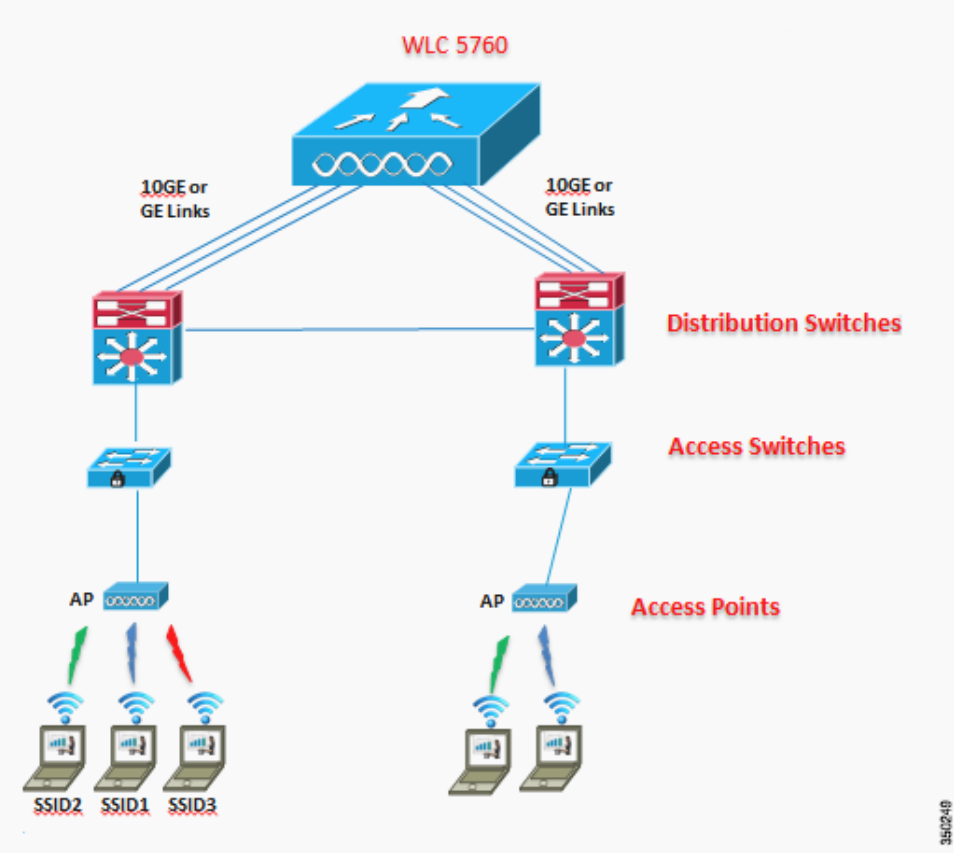
LAG は 802.3ad ポート集約標準の部分的な実装です。コントローラのすべてのディストリビューション システム ポートが 1 つの 802.3ad ポート チャネルにまとめられるので、コントローラのポートの設定に必要な IP アドレスの数を減らすことができます。LAG が有効である場合、ポートの冗長性は動的に管理され、AP はユーザからは透過的にロード バランシングされます。

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、AP はネットワークに接続されたままとなります。また、ワイヤレス クライアントは引き続きデータを送受信します。

複数 LAG

複数の LAG グループは冗長性のために複数のスイッチに接続が必要な設定をサポートするように設定できます。各 LAG グループに対する AP マネージャを設定することによって複数の LAG グループにわたって AP がロード バランスされます。

図 2-5　　複数 LAG



コントローラおよびネイバー デバイスの LAG サポートの設定

コントローラのネイバー デバイスは LAG をサポートするために正しく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ごとに次のコマンドで設定する必要があります。

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

- ネイバー スイッチのポート チャネルはこれらのコマンドで設定する必要があります。

```
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
```

WLC5760 への Cisco IOS® ソフトウェアの導入により、LAG の設定はネイバー スイッチの設定と似たものになります。

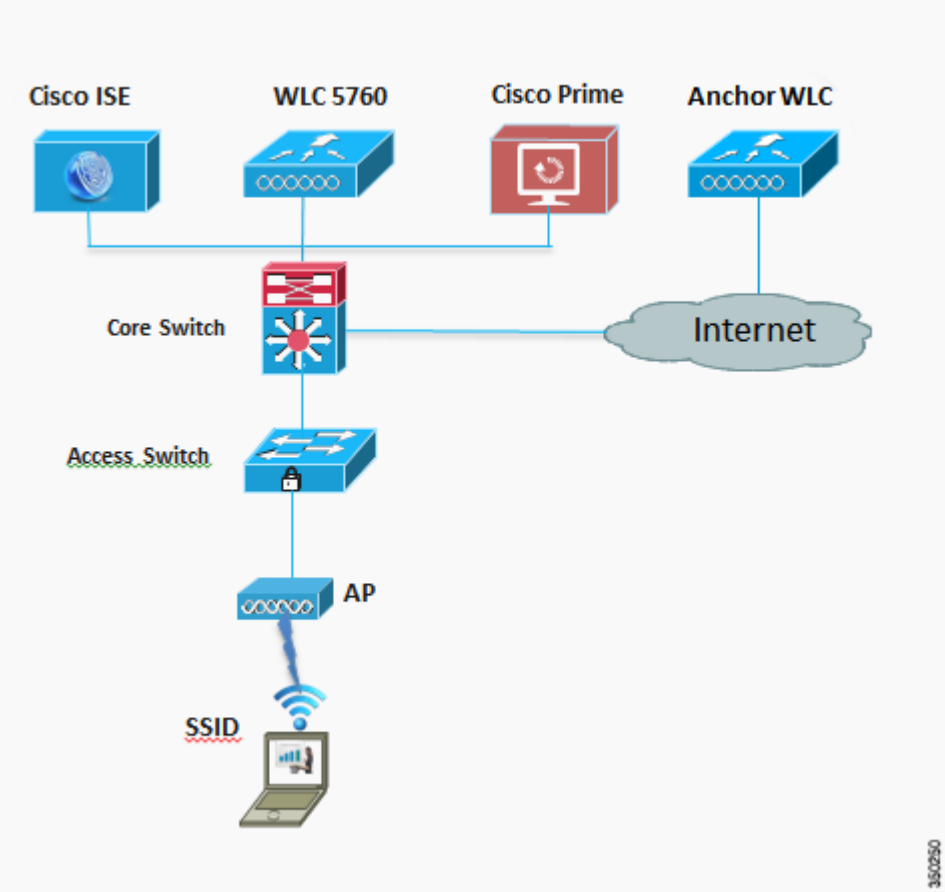
（注） 複数の AP マネージャ インターフェイスを使用するロード バランシングは、従来のコントローラとほぼ同等な CT5760 WLAN コントローラでサポートされます。ただし、冗長性とロード バランシングのために LAG を使用することを推奨します。

CT5760 の一元化設定の例

ネットワーク トポロジ

図 2-6 の図では、一元化された導入で統合アクセス CT5760 コントローラだけを使用するネットワーク トポロジを示します。

図 2-6　一元化設定のネットワーク トポロジ



VLAN および IP アドレス

表 2-4　デバイスごとの VLAN および IP アドレス

デバイス	VLAN	IP アドレス
DHCP サーバ	ゲートウェイ	10.10.100.1 / 10.10.200.1
Cisco Prime Infrastructure	200	10.10.200.30
Cisco ISE	200	10.10.200.60

表 2-4　デバイスごとの VLAN および IP アドレス （続き）

アンカー WLC	300	192.168.1.5
コア スイッチ	200、100	10.10.100.1 / 10.10.200.1
AP	200	DHCP
5760 WLC	200	10.10.200.5
クライアント VLAN	100	DHCP
管理 VLAN	200	10.10.200.5
NTP サーバ	ゲートウェイ	10.10.200.1

CLI を使用した CT5760 コントローラ設定の例

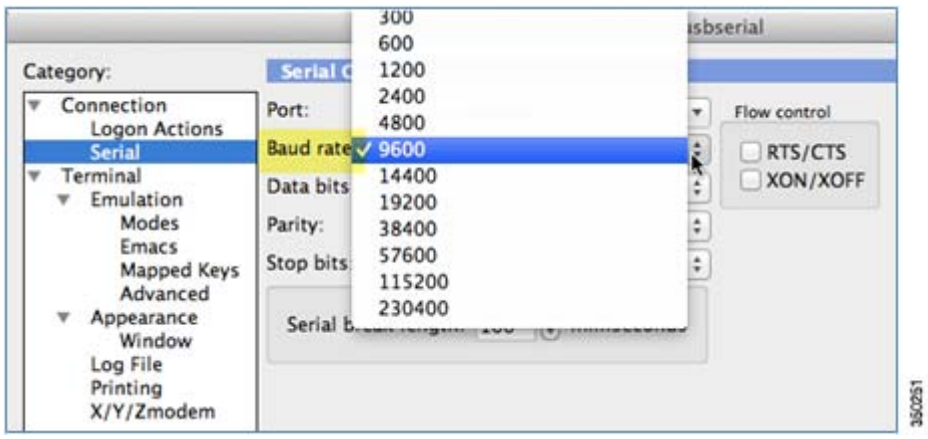
コントローラの設定を開始する前に、上記の設定のすべてのスイッチ間に完全な接続性があることを確認します。

コンソールの接続

基本動作のためにスイッチまたはコントローラを設定するまえに、VT-100 ターミナル エミュレータ（HyperTerminal、ProComm、または Putty など）を使用する PC に接続する必要があります。

コントローラには EIA/TIA-232 非同期（RJ-45）および USB 5 ピン ミニ タイプ B、2.0 準拠シリアル コンソール ポートの両方があります。コンソール ポートのデフォルト パラメータは、9600 ボー、8 データ ビット、1 ストップ ビット、およびパリティなしです。コンソール ポートはハードウェア フロー制御をサポートしていません。9600 のシリアル ボー レートを選択してください。問題がある場合は、115200 ボー レートを試してみてください。PC/Windows の Putty などとほぼ同等に使用する Mac Secure CRT の例を図 2-7 に示します。

図 2-7　Mac Secure CRT の例



スタートアップ ウィザード

スタートアップ ウィザードを起動する前に、使用可能な IP アドレスおよび VLAN の情報を用意してください。ウィザードおよび初期設定ダイアログを使用せずに開始します（初期設定を確認してください）。

```
% Please answer 'yes' or 'no'.
```

```
Would you like to enter the initial configuration dialog?[yes/no]: no
Would you like to terminate autoinstall?[yes]:
Controller>
Press RETURN to get started!

Start with the wizard/initial configuration dialog (check the initial config).
Enable secret warning
----------------------------------
In order to access the device manager, an enable secret is required
If you enter the initial configuration dialog, you will be prompted for the enable
secret
If you choose not to enter the intial configuration dialog, or if you exit setup
without setting the enable secret,
please set an enable secret using the following CLI in configuration mode-
enable secret 0 <cleartext password>
----------------------------------
Would you like to enter the initial configuration dialog?[yes/no]: yes

At any point you may enter a question mark '?' for help.Use ctrl-c to abort configuration
dialog at any prompt.Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity for management of the system,
extended setup will ask you to configure each interface on the system

Would you like to enter basic management setup?[yes/no]: yes
Configuring global parameters:

Enter host name [Controller]: CT5760-Controller

The enable secret is a password used to protect access to privileged EXEC and
configuration modes.This password, after entered, becomes encrypted in the configuration.
Enter enable secret: Cisco123

The enable password is used when you do not specify an enable secret password, with some
older software versions, and some boot images.
Enter enable password: Cisco123
The virtual terminal password is used to protect access to the router over a network
interface.Enter virtual terminal password: Cisco123
Configure a NTP server now?[yes]: yes
Enter ntp server address : 10.10.200.1

Enter a polling interval between 16 and 131072 secs which is power of 2:16
Do you want to configure wireless network?[no]: yes
Enter mobility group name: New-Mobility
```

```
Enter the country code[US]:US
Configure SNMP Network Management?[no]: no

Current interface summary

Any interface listed with OK?value "NO" does not have a valid configuration

 Interface          IP-Address    OK? Method Statu          Protocol
 Vlan1              unassigned    NO  unset  up             down
 GigabitEthernet    unassigned    YES unset  up              up
 Te1/0/1            unassigned    YES unset  down           down
 Te1/0/2            unassigned    YES unset  down           down
 Te1/0/3            unassigned    YES unset  down           down
 Te1/0/4            unassigned    YES unset  down           down
 Te1/0/5            unassigned    YES unset  down           down
 Te1/0/6            unassigned    YES unset  down           down

Enter interface name used to connect to the
management network from the above interface summary: GigabitEthernet0/0[service
port)

Configuring interface GigabitEthernet0/0: Configure IP on this interface?[no]: yes
IP address for this interface: 192.168.2.50
Subnet mask for this interface [255.255.0.0] : 255.255.255.0

Wireless management interface needs to be configured at startup
It needs to be mapped to an SVI that's not Vlan 1 (default)

Enter VLAN No for wireless management interface: 200
Enter IP address: 10.10.200.5
Enter IP address mask:: 255.255.255.0

[0] Go to the IOS command prompt without saving this config.[1] Return back to the setup
without saving this config.
[2] Save this configuration to nvram and exit.
Enter your selection [2]:2
Press RETURN to get started!
```

バージョン

```
 # show version
```

IOS XE 3.X（FCS では 3.2.0SE）が 3850/5760 の公式バージョンであり 3850/5760 を参照する際に使用できる唯一のバージョン番号です。

```
#show version running
```

WCM および IOSd バージョンを表示します。

#show ap name apname config general

AP バージョンを表示し FCS では 15.X です。

日付と時刻の設定

clock set hh:mm:ss day month year

CT5760 コントローラ Web グラフィカル ユーザ インターフェイスのイネーブル化

管理ユーザの設定

```
username admin privilege 15 password 0 Cisco123
```

コントローラの HTTP の設定

```
ip http server
ip http authentication local
username root privilege 15 password 0 cisco
```

Web Services Management Agent（WSMA）の設定

```
wsma agent exec
profile webui_service
profile httplistener
wsma agent config
profile webui_service
profile httplistener
wsma agent filesys
profile webui_service
profile httplistener
wsma agent notify
profile webui_service
profile httplistener
wsma profile listener webui_service
transport http path /webui
wsma profile listener httplistener
transport http path /index
```

基本設定

この項では、次の目的での CT5760 のコンソールからのオプションの設定を示します。

- コア スイッチへのネットワーク アップリンク
- 管理およびクライアント インタフェース
- DHCP の設定

```
Disable VLAN
```

```
1 int vlan 1
no ip address shutdown
exit
```

CT5760 での DHCP スヌーピングおよび信頼状態の設定

```
ip dhcp snooping vlan 100, 200
ip dhcp snooping wireless bootp-broadcast enable
ip dhcp snooping
interface TenGigabitEthernet1/0/1
description Connection to Core Switch
switchport trunk allowed vlan 100, 200 switchport mode trunk
ip dhcp relay information trusted ip dhcp snooping trust
interface Vlan100 description Client Vlan
ip dhcp relay information trusted
```

管理およびクライアント インターフェイスの追加

```
interface Vlan200
description "Management VLAN"
ip address 10.10.200.5 255.255.255.0
no shut
interface Vlan100
description "Client VLAN"
no shut
ip route 0.0.0.0 0.0.0.0 10.10.200.1 default-gateway 10.10.200.1
```

WLAN の設定

WLAN の設定およびクライアント VLAN の割り当て セキュリティに WPA/PSK を使用し、パス キーは **cisco123** です。

```
wlan corporate 1 corporate band-select
client vlan 100
no security wpa akm dot1x
security wpa akm psk set-key ascii 0 cisco123
no shutdown
```

ワイヤレスでの管理を許可するには、このコマンドを入力します。

```
wireless mgmt-via-wireless <cr>
```

AP の接続

L2 スイッチの任意のポートに AP を接続します。接続するまで待ってからコマンドを入力します。

show ap summary

show ap summary

```
Number of APs: 1
Global AP User Name: Not configured
Global AP Dot1x User Name: Not configured
AP Name / AP Model / Ethernet MAC / Radio MAC / State
-----------------------------------------------------------------------------
AP44d3.ca42.321a / 3602I / 44d3.ca42.321a / 64d9.8942.4090 / Registered
```

WPA キーの「cisco13」を使用して企業 SSID にワイヤレス クライアントを接続します。コントローラには、新しいクライアント関連付けについて次のように許可の成功が表示されます。

Show wireless client summary でコントローラからワイヤレス クライアントを確認します。

セキュリティ設定

この項では CT5760 のコンソールからの設定オプションを示します。

- 認証、許可、アカウンティング（AAA）をイネーブルにする
- ISE を RADIUS サーバ（10.10.200.60）として設定
- シークレットの共有：**secret**

CT5760 コンソール（Telnet またはシリアル）の形成：AAA の設定

```
aaa new-model
!
aaa group server radius Cisco
server 10.10.200.60
!
aaa authentication login no_auth none
aaa authentication dot1x default group radius
aaa authentication dot1x Cisco_dot1x group Cisco
aaa authorization network default group Cisco
aaa accounting network default start-stop group Cisco
dot1x system-auth-control
!
aaa server radius dynamic-author
auth-type any
!
radius-server attribute 6 on-for-login-auth
radius-server dead-criteria time 10 tries 3
radius-server deadtime 3
```

```
radius-server vsa send accounting
radius-server vsa send authentication
!
radius server Cisco
address ipv4 10.10.200.60 auth-port 1812 acct-port 1813
key secret
```

このコマンドは、802.1x セキュリティを使う WLAN を作成します。

```
wlan corporate1x 2 corporate1x
accounting-list Cisco
client vlan 100
security dot1x authentication-list Cisco
session-timeout 600
no shutdown
```

ワイヤレス クライアントを企業 1x に次の資格情報を使って接続します。

ユーザ名 = cisco、パスワード = Cisco123

```
Controller#show wireless client summary
```

ワイヤレス WebAuth および Guest Anchor ソリューション

次の項では、CT5760 の WebAuthentication（WebAuth）の設定および Guest Anchor の例を示します。

グローバル コンフィギュレーションの [Parameter Map] セクションの設定

parameter map コンフィギュレーション モード コマンドを使用して、接続タイプのパラメータ マップを定義することができます。接続パラメータ マップを作成したあとは、マップの TCP IP およびその他の設定を設定できます。

! 最初のセクションでは、グローバル値と内部仮想アドレスを定義します。

! これはすべての WCM のノード間で共通です。

```
PARAMETER-MAP TYPE WEBAUTH GLOBAL?
VIRTUAL-IP IPV4 192.0.2.1
PARAMETER-MAP TYPE WEBAUTH WEBPARALOCAL?
TYPE WEBAUTH?
BANNER TEXT ^C WEBAUTHX^C
REDIRECT ON-SUCCESS HTTP://9.12.128.50/WEBAUTH/LOGINSUCCESS.HTML
REDIRECT PORTAL IPV4 9.12.128.50
```

カスタマイズされた WebAuth の TAR 形式パッケージの設定

フラッシュするファイルごとに転送します。

```
copy tftp://10.1.10.100/WebAuth/webauth/ webauth_consent.htmlflash:webauth_consent.html
copy tftp://10.1.10.100/WebAuth/ webauth_success.html flash: webauth_success.html
copy tftp://10.1.10.100/WebAuth/ webauth_failure.html flash: webauth_failure.html
```

```
copy tftp://10.1.10.100/WebAuth/ webauth_expired.html flash: webauth_expired.html
```

カスタム ページを使用したパラメータ マップの設定

```
parameter-map type webauth webparalocal
type webauth
custom-page login device flash:webauth_consent.html
custom-page success device flash:webauth_success.html
custom-page failure device flash: webauth_failure.html
custom-page login expired device flash:webauth_expired.html
```

タイプ同意と電子メール オプションを使用したパラメータ マップの設定

```
parameter-map type webauth webparalocal
type consent
consent email
custom-page login device flash:webauth_consent.html
custom-page success device flash:webauth_success.html
custom-page failure device flash:webauth_failure.html
custom-page login expired device flash:webauth_expired.html
```

ローカル WebAuth 認証の設定

```
username guest password guest123
aaa new model
dot1x system-auth-control
aaa authentication login EXT_AUTH local
aaa authorization network EXT_AUTH local
aaa authorization network default local
or
aaa authentication login default local
aaa authorization network default local
```

webauth の外部 RADIUS の設定

```
aaa new model
dot1x system-auth-control
aaa server radius dynamic-author ?
client 10.10.200.60 server-key cisco ?server-key cisco ?
auth-type any

radius server cisco
address ipv4 10.10.200.60 auth-port 1812 acct-port 1813
key cisco
```

```
aaa group server radius cisco server name cisco
aaa authentication login EXT_AUTHgroup cisco
or
aaa authentication login default group cisco
```

WebAuth を使用した WLAN の設定

```
wlan Guest-WbAuth 3 Guest-WbAuth
client vlan 100
mobility anchor 192.168.5.1
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list EXT_AUTH
security web-auth parameter-map webparalocal
no shutdown
```

グローバル コンフィギュレーションでの HTTP サーバの設定

! --- Cisco IOS® ソフトウェアでの Web サービスをイネーブルにするためにこれらが必要です。

```
ip http server
ip http secure-server
ip http active-session-modules none
```

チェックを入れたりイネーブルにするその他の設定

! --- これらはグローバルなハウスキー ピング Cisco IOS® ソフトウェア コマンドの一部です。

```
ip device tracking
ip dhcp snooping
```

SNMP の設定

CT5760 コンソールから、SNMP ストリングを設定します。

snmp---s er v er co mmuni t y p ub l i c r o

snmp---s er v er co mmuni t y p r i v a t e r w

IPv6 Configuration

IPv6 は、データ パスでサポートされます。ワイヤレス クライアントは IPv6 アドレスを取得可能です。

IPv6 スヌーピングのイネーブル：CT5760

IPv6 を設定する場合には CT5760 での設定で若干の違いがあります。CT5760 で IPv6 をイネーブルにするには、次の手順を実行する必要があります。

```
ipv6 nd raguard attach-policy testgaurd
Trusted-port
Device-role router
interface TenGigabitEthernet1/0/1
description Uplink to Core Switch
switchport trunk native vlan 200
switchport mode trunk
ipv6 nd raguard attach-policy testgaurd
ip dhcp snooping trust
```

インターフェイスでの IPv6 のイネーブル：CT5760

IPv6 設定が必要なインターフェイスおよび必要なアドレスのタイプに基づいて、それぞれの設定が次のようにイネーブルにされます。IPv6 設定では、VLAN200 でイネーブルにされます。

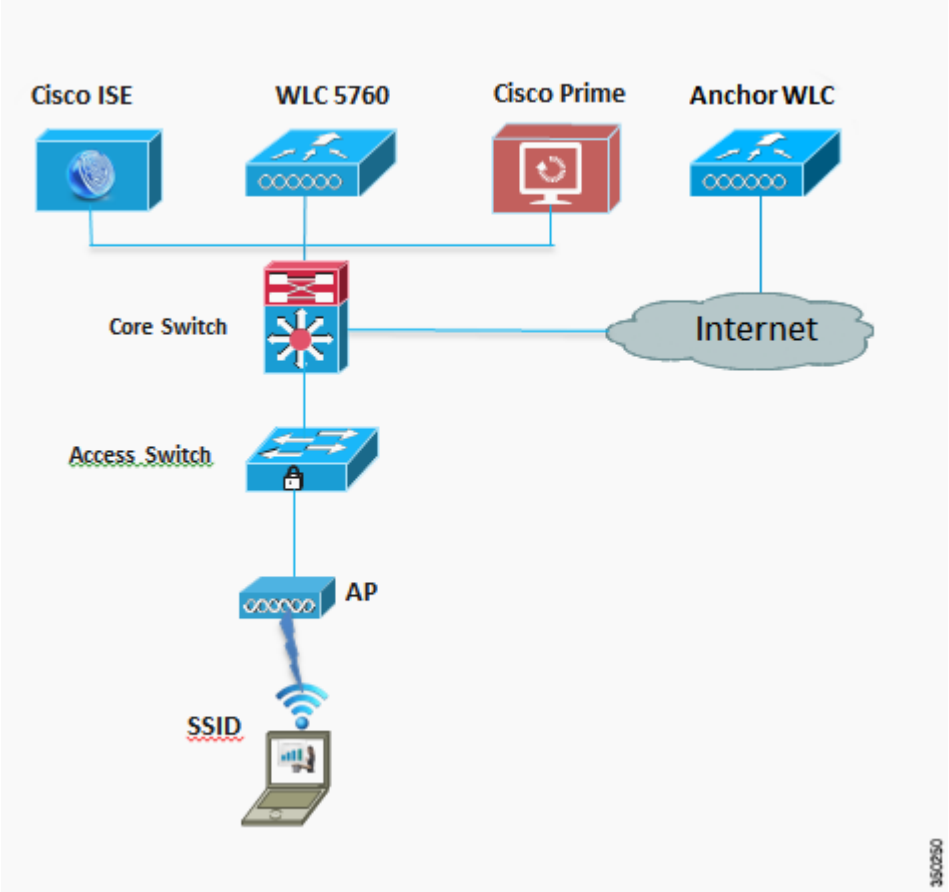
```
vlan configuration 100 200
ipv6 nd suppress
ipv6 snooping

interface Vlan100
description Client VLAN
ip address 10.10.100.5 255.255.255.0
ip helper-address 10.10.100.1 2001:DB8:0:10::1/64
ipv6 address FEC0:20:21::1/64
ipv6 enable
```

CT5760 の一元化設定の例

ネットワーク トポロジ

図 3-1 の図では、一元化された導入で統合アクセス CT5760 コントローラだけを使用するネットワーク トポロジを示します。

図 3-1　　一元化設定のネットワーク トポロジ



VLAN および IP アドレス

表 3-1　デバイスごとの VLAN および IP アドレス

デバイス	VLAN	IP アドレス
DHCP サーバ	ゲートウェイ	10.10.100.1 / 10.10.200.1
Cisco Prime Infrastructure	200	10.10.200.30
Cisco ISE	200	10.10.200.60
アンカー WLC	300	192.168.1.5
コア スイッチ	200、100	10.10.100.1 / 10.10.200.1
AP	200	DHCP
5760 WLC	200	10.10.200.5
クライアント VLAN	100	DHCP
管理 VLAN	200	10.10.200.5
NTP サーバ	ゲートウェイ	10.10.200.1

CLI を使用した CT5760 コントローラ設定の例

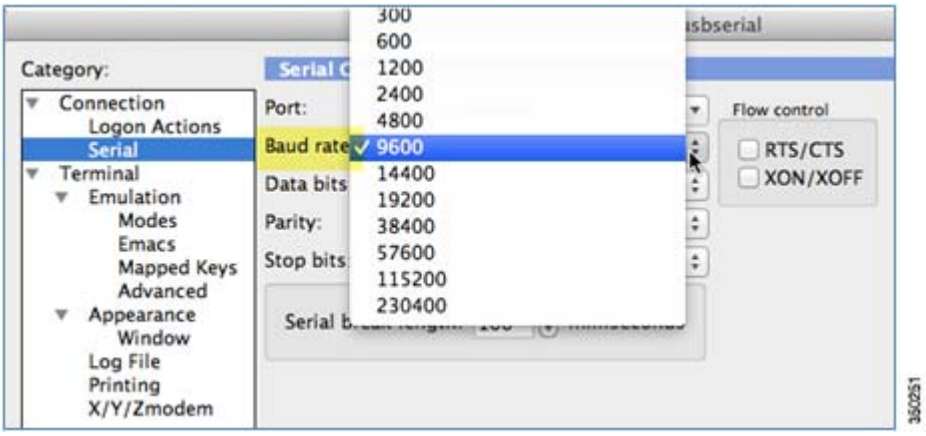
コントローラの設定を開始する前に、上記の設定のすべてのスイッチ間に完全な接続性があることを確認します。

コンソールの接続

基本動作のためにスイッチまたはコントローラを設定するまえに、VT-100 ターミナル エミュレータ（HyperTerminal、ProComm、または Putty など）を使用する PC に接続する必要があります。

コントローラには EIA/TIA-232 非同期（RJ-45）および USB 5 ピン ミニ タイプ B、2.0 準拠シリアル コンソール ポートの両方があります。コンソール ポートのデフォルト パラメータは、9600 ボー、8 データ ビット、1 ストップ ビット、およびパリティなしです。コンソール ポートはハードウェア フロー制御をサポートしていません。9600 のシリアル ボー レートを選択してください。問題がある場合は、115200 ボー レートを試してみてください。PC/Windows の Putty などとほぼ同等に使用する Mac Secure CRT の例を図 3-2 に示します。

図 3-2　Mac Secure CRT の例



スタートアップ ウィザード

スタートアップ ウィザードを起動する前に、使用可能な IP アドレスおよび VLAN の情報を用意してください。ウィザードおよび初期設定ダイアログを使用せずに開始します（初期設定を確認してください）。

```
% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog?[yes/no]: no
Would you like to terminate autoinstall?[yes]:
Controller>
Press RETURN to get started!


Start with the wizard/initial configuration dialog (check the initial config).
Enable secret warning
----------------------------------
In order to access the device manager, an enable secret is required
If you enter the initial configuration dialog, you will be prompted for the enable
secret
If you choose not to enter the intial configuration dialog, or if you exit setup
without setting the enable secret,
please set an enable secret using the following CLI in configuration mode-
enable secret 0 <cleartext password>
----------------------------------
Would you like to enter the initial configuration dialog?[yes/no]: yes


At any point you may enter a question mark '?' for help.Use ctrl-c to abort configuration
dialog at any prompt.Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity for management of the system,
extended setup will ask you to configure each interface on the system


Would you like to enter basic management setup?[yes/no]: yes
Configuring global parameters:


Enter host name [Controller]: CT5760-Controller


The enable secret is a password used to protect access to privileged EXEC and
configuration modes.This password, after entered, becomes encrypted in the configuration.
Enter enable secret: Cisco123


The enable password is used when you do not specify an enable secret password, with some
older software versions, and some boot images.
Enter enable password: Cisco123
The virtual terminal password is used to protect access to the router over a network
interface.Enter virtual terminal password: Cisco123
Configure a NTP server now?[yes]: yes
```

```
Enter ntp server address : 10.10.200.1

Enter a polling interval between 16 and 131072 secs which is power of 2:16
Do you want to configure wireless network?[no]: yes
Enter mobility group name: New-Mobility
Enter the country code[US]:US
Configure SNMP Network Management?[no]: no

Current interface summary

Any interface listed with OK?value "NO" does not have a valid configuration

 Interface          IP-Address    OK? Method Statu          Protocol
 Vlan1              unassigned    NO  unset  up             down
 GigabitEthernet    unassigned    YES unset  up              up
 Te1/0/1            unassigned    YES unset  down           down
 Te1/0/2            unassigned    YES unset  down           down
 Te1/0/3            unassigned    YES unset  down           down
 Te1/0/4            unassigned    YES unset  down           down
 Te1/0/5            unassigned    YES unset  down           down
 Te1/0/6            unassigned    YES unset  down           down

Enter interface name used to connect to the
management network from the above interface summary: GigabitEthernet0/0[service
port)

Configuring interface GigabitEthernet0/0: Configure IP on this interface?[no]: yes
IP address for this interface: 192.168.2.50
Subnet mask for this interface [255.255.0.0] : 255.255.255.0

Wireless management interface needs to be configured at startup
It needs to be mapped to an SVI that's not Vlan 1 (default)

Enter VLAN No for wireless management interface: 200
Enter IP address: 10.10.200.5
Enter IP address mask:: 255.255.255.0

[0] Go to the IOS command prompt without saving this config.[1] Return back to the setup
without saving this config.
[2] Save this configuration to nvram and exit.
Enter your selection [2]:2
Press RETURN to get started!
```

バージョン

 # show version

IOS XE 3.X（FCS では 3.2.0SE）が 3850/5760 の公式バージョンであり 3850/5760 を参照する際に使用できる唯一のバージョン番号です。

#show version running

WCM および IOSd バージョンを表示します。

#show ap name apname config general

AP バージョンを表示し FCS では 15.X です。

日付と時刻の設定

clock set hh:mm:ss day month year

CT5760 コントローラ Web グラフィカル ユーザ インターフェイスのイネーブル化

管理ユーザの設定

```
username admin privilege 15 password 0 Cisco123
```

コントローラの HTTP の設定

```
ip http server
ip http authentication local
username root privilege 15 password 0 cisco
```

Web Services Management Agent（WSMA）の設定

```
wsma agent exec
profile webui_service
profile httplistener
wsma agent config
profile webui_service
profile httplistener
wsma agent filesys
profile webui_service
profile httplistener
wsma agent notify
profile webui_service
profile httplistener
wsma profile listener webui_service
transport http path /webui
wsma profile listener httplistener
transport http path /index
```

基本設定

この項では、次の目的での CT5760 のコンソールからのオプションの設定を示します。

- コア スイッチへのネットワーク アップリンク
- 管理およびクライアント インタフェース
- DHCP の設定

```
Disable VLAN
1 int vlan 1
no ip address shutdown
exit
```

CT5760 での DHCP スヌーピングおよび信頼状態の設定

```
ip dhcp snooping vlan 100, 200
ip dhcp snooping wireless bootp-broadcast enable
ip dhcp snooping
interface TenGigabitEthernet1/0/1
description Connection to Core Switch
switchport trunk allowed vlan 100, 200 switchport mode trunk
ip dhcp relay information trusted ip dhcp snooping trust
interface Vlan100 description Client Vlan
ip dhcp relay information trusted
```

管理およびクライアント インターフェイスの追加

```
interface Vlan200
description "Management VLAN"
ip address 10.10.200.5 255.255.255.0
no shut
interface Vlan100
description "Client VLAN"
no shut
ip route 0.0.0.0 0.0.0.0 10.10.200.1 default-gateway 10.10.200.1
```

WLAN の設定

WLAN の設定およびクライアント VLAN の割り当て セキュリティに WPA/PSK を使用し、パス キーは **cisco123** です。

```
wlan corporate 1 corporate band-select
client vlan 100
no security wpa akm dot1x
security wpa akm psk set-key ascii 0 cisco123
no shutdown
```

ワイヤレスでの管理を許可するには、このコマンドを入力します。

```
wireless mgmt-via-wireless <cr>
```

AP の接続

L2 スイッチの任意のポートに AP を接続します。接続するまで待ってからコマンドを入力します。

show ap summary

show ap summary

```
Number of APs: 1
Global AP User Name: Not configured
Global AP Dot1x User Name: Not configured
AP Name / AP Model / Ethernet MAC / Radio MAC / State
-----------------------------------------------------------------------------
AP44d3.ca42.321a / 3602I / 44d3.ca42.321a / 64d9.8942.4090 / Registered
```

WPA キーの「cisco13」を使用して企業 SSID にワイヤレス クライアントを接続します。コントローラには、新しいクライアント関連付けについて次のように許可の成功が表示されます。

Show wireless client summary でコントローラからワイヤレス クライアントを確認します。

セキュリティ設定

この項では CT5760 のコンソールからの設定オプションを示します。

- 認証、許可、アカウンティング（AAA）をイネーブルにする
- ISE を RADIUS サーバ（10.10.200.60）として設定
- シークレットの共有：**secret**

CT5760 コンソール（Telnet またはシリアル）の形成：AAA の設定

```
aaa new-model
!
aaa group server radius Cisco
server 10.10.200.60
!
aaa authentication login no_auth none
aaa authentication dot1x default group radius
aaa authentication dot1x Cisco_dot1x group Cisco
aaa authorization network default group Cisco
aaa accounting network default start-stop group Cisco
dot1x system-auth-control
!
aaa server radius dynamic-author
auth-type any
!
radius-server attribute 6 on-for-login-auth
radius-server dead-criteria time 10 tries 3
radius-server deadtime 3
```

```
radius-server vsa send accounting
radius-server vsa send authentication
!
radius server Cisco
address ipv4 10.10.200.60 auth-port 1812 acct-port 1813
key secret
```

このコマンドは、802.1x セキュリティを使う WLAN を作成します。

```
wlan corporate1x 2 corporate1x
accounting-list Cisco
client vlan 100
security dot1x authentication-list Cisco
session-timeout 600
no shutdown
```

ワイヤレス クライアントを企業 1x に次の資格情報を使って接続します。

ユーザ名 = cisco、パスワード = Cisco123

```
Controller#show wireless client summary
```

ワイヤレス WebAuth および Guest Anchor ソリューション

次の項では、CT5760 の WebAuthentication（WebAuth）の設定および Guest Anchor の例を示します。

グローバル コンフィギュレーションの [Parameter Map] セクションの設定

parameter map コンフィギュレーション モード コマンドを使用して、接続タイプのパラメータ マップを定義することができます。接続パラメータ マップを作成したあとは、マップの TCP IP およびその他の設定を設定できます。

! 最初のセクションでは、グローバル値と内部仮想アドレスを定義します。

! これはすべての WCM のノード間で共通です。

```
PARAMETER-MAP TYPE WEBAUTH GLOBAL?
VIRTUAL-IP IPV4 192.0.2.1
PARAMETER-MAP TYPE WEBAUTH WEBPARALOCAL?
TYPE WEBAUTH?
BANNER TEXT ^C WEBAUTHX^C
REDIRECT ON-SUCCESS HTTP://9.12.128.50/WEBAUTH/LOGINSUCCESS.HTML
REDIRECT PORTAL IPV4 9.12.128.50
```

カスタマイズされた WebAuth の TAR 形式パッケージの設定

フラッシュするファイルごとに転送します。

```
copy tftp://10.1.10.100/WebAuth/webauth/ webauth_consent.htmlflash:webauth_consent.html
copy tftp://10.1.10.100/WebAuth/ webauth_success.html flash: webauth_success.html
copy tftp://10.1.10.100/WebAuth/ webauth_failure.html flash: webauth_failure.html
```

```
copy tftp://10.1.10.100/WebAuth/ webauth_expired.html flash: webauth_expired.html
```

カスタム ページを使用したパラメータ マップの設定

```
parameter-map type webauth webparalocal
type webauth
custom-page login device flash:webauth_consent.html
custom-page success device flash:webauth_success.html
custom-page failure device flash: webauth_failure.html
custom-page login expired device flash:webauth_expired.html
```

タイプ同意と電子メール オプションを使用したパラメータ マップの設定

```
parameter-map type webauth webparalocal
type consent
consent email
custom-page login device flash:webauth_consent.html
custom-page success device flash:webauth_success.html
custom-page failure device flash:webauth_failure.html
custom-page login expired device flash:webauth_expired.html
```

ローカル WebAuth 認証の設定

```
username guest password guest123
aaa new model
dot1x system-auth-control
aaa authentication login EXT_AUTH local
aaa authorization network EXT_AUTH local
aaa authorization network default local
or
aaa authentication login default local
aaa authorization network default local
```

webauth の外部 RADIUS の設定

```
aaa new model
dot1x system-auth-control
aaa server radius dynamic-author ?
client 10.10.200.60 server-key cisco ?server-key cisco ?
auth-type any

radius server cisco
address ipv4 10.10.200.60 auth-port 1812 acct-port 1813
key cisco
```

```
aaa group server radius cisco server name cisco
aaa authentication login EXT_AUTHgroup cisco
or
aaa authentication login default group cisco
```

WebAuth を使用した WLAN の設定

```
wlan Guest-WbAuth 3 Guest-WbAuth
client vlan 100
mobility anchor 192.168.5.1
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list EXT_AUTH
security web-auth parameter-map webparalocal
no shutdown
```

グローバル コンフィギュレーションでの HTTP サーバの設定

! --- Cisco IOS® ソフトウェアでの Web サービスをイネーブルにするためにこれらが必要です。

```
ip http server
ip http secure-server
ip http active-session-modules none
```

チェックを入れたりイネーブルにするその他の設定

! --- これらはグローバルなハウスキー ピング Cisco IOS® ソフトウェア コマンドの一部です。

```
ip device tracking
ip dhcp snooping
```

SNMP の設定

CT5760 コンソールから、SNMP ストリングを設定します。

snmp---s er v er co mmuni t y p ub l i c r o

snmp---s er v er co mmuni t y p r i v a t e r w

IPv6 Configuration

IPv6 は、データ パスでサポートされます。ワイヤレス クライアントは IPv6 アドレスを取得可能です。

IPv6 スヌーピングのイネーブル：CT5760

IPv6 を設定する場合には CT5760 での設定で若干の違いがあります。CT5760 で IPv6 をイネーブルにするには、次の手順を実行する必要があります。

```
ipv6 nd raguard attach-policy testgaurd
Trusted-port
Device-role router
interface TenGigabitEthernet1/0/1
description Uplink to Core Switch
switchport trunk native vlan 200
switchport mode trunk
ipv6 nd raguard attach-policy testgaurd
ip dhcp snooping trust
```

インターフェイスでの IPv6 のイネーブル：CT5760

IPv6 設定が必要なインターフェイスおよび必要なアドレスのタイプに基づいて、それぞれの設定が次のようにイネーブルにされます。IPv6 設定では、VLAN200 でイネーブルにされます。

```
vlan configuration 100 200
ipv6 nd suppress
ipv6 snooping

interface Vlan100
description Client VLAN
ip address 10.10.100.5 255.255.255.0
ip helper-address 10.10.100.1 2001:DB8:0:10::1/64
ipv6 address FEC0:20:21::1/64
ipv6 enable
```

CHAPTER 4

モビリティのアーキテクチャ

ここでは、新しいモビリティ アーキテクチャでのモビリティ コンポーネントを説明します。

モビリティ エージェント

モビリティ エージェントは AP 接続、AP からの CAPWAP トンネル終端を管理し、ローカルで実行されアンカー WLC からローミングされるクライアント ステーション（エンドポイント）のデータベースを構築します。インターナル モビリティ エージェントを実行中の Catalyst 3850 または CT5760 モビリティ コントローラのどちらもモビリティ エージェントになることができます。

モビリティ コントローラ：

モビリティ コントローラは SPG 内ローミング、RRM、およびゲスト アクセスなどのモビリティの管理タスクを提供します。ワイヤレス クライアントが接続やサービスを失わずに 1 つの物理的な場所から他の場所へいつでも移動するモビリティ ローミングは、ローミングが 1 つのモビリティ サブ ドメインに限定される場合は単一のモビリティ コントローラによって管理できます。1 つのモビリティ サブ ドメインから出るローミングは 1 つのモビリティ グループ内の複数のモビリティ コントローラで管理できます。このモビリティ コントローラはすべてのモビリティ コントローラのすべてのクライアントの Pairwise Master Key（PMK）のキャッシュを行い、サブ ドメインおよびモビリティ グループ内のクライアントの高速ローミングを可能にします。サブドメインのすべてのモビリティ エージェントは、モビリティ コントローラへの CAPWAP モビリティ トンネルを形成し、モビリティ コントローラにローカルのクライアントおよびローミングしたクライアントの状態をレポートします。モビリティ コントローラはすべてのモビリティ エージェントにわたるクライアント ステーションのデータベースを構築します。

モビリティ オラクル

モビリティ オラクルは複数のモビリティ グループ間のローミング アクティビティの調整により拡張性とパフォーマンスをさらに向上させ、効率とパフォーマンス向上ための異なるモビリティ グループのモビリティ コントローラ間での N2 通信の必要性がなくなります。

モビリティ グループ

モビリティ グループは、1 つのモビリティ グループのモビリティ コントローラ内のクライアントの高速ローミングを可能にするモビリティ コントローラの論理グループです。また、モビリティ グループは、選択されるか、または静的に選択したモビリティ コントローラのリーダーによって実行される、一元的な RRM を提供します。

サブ ドメインの変更

複数の SPG はグループ化され、モビリティのサブ ドメインとして一括して管理できます。1 台のモビリティ コントローラがそれぞれのモビリティ サブ ドメインに必要です。

ピア グループの切替え

統合アクセス導入は、1 台のモビリティ コントローラ（またはモビリティ サブ ドメイン）内のモビリティ エージェントの 1 つの論理グループとして SPG を定義します。SPG を実装する主な利点は、SPG を形作るスイッチへローミングのトラフィックを抑制することです。モバイル エージェントがモビリティ コントローラの 1 つの SPG で設定されている場合、ソフトウェアはモビリティ エージェントのスイッチ間で自動的にフルメッシュ CAPWAP トンネルを形成します。これらの CAPWAP トンネルは階層型ネットワーク設計（モビリティ エージェントのスイッチが VLAN にまたがった L2 隣接）またはルーテッド アクセス設計（モビリティ エージェントのスイッチが L3 隣接）で形成することができます。

SPG はユーザが頻繁にローミングするモビリティ エージェント スイッチのグループとして設計する必要があります。

（注）　SPG 内でのローミングは SPG にローカルで、モビリティ コントローラを含める必要はありません。SPG 全体のローミングでは、モビリティ コントローラを通過するトラフィックが必要です。

図 4-1　　モビリティ ドメイン

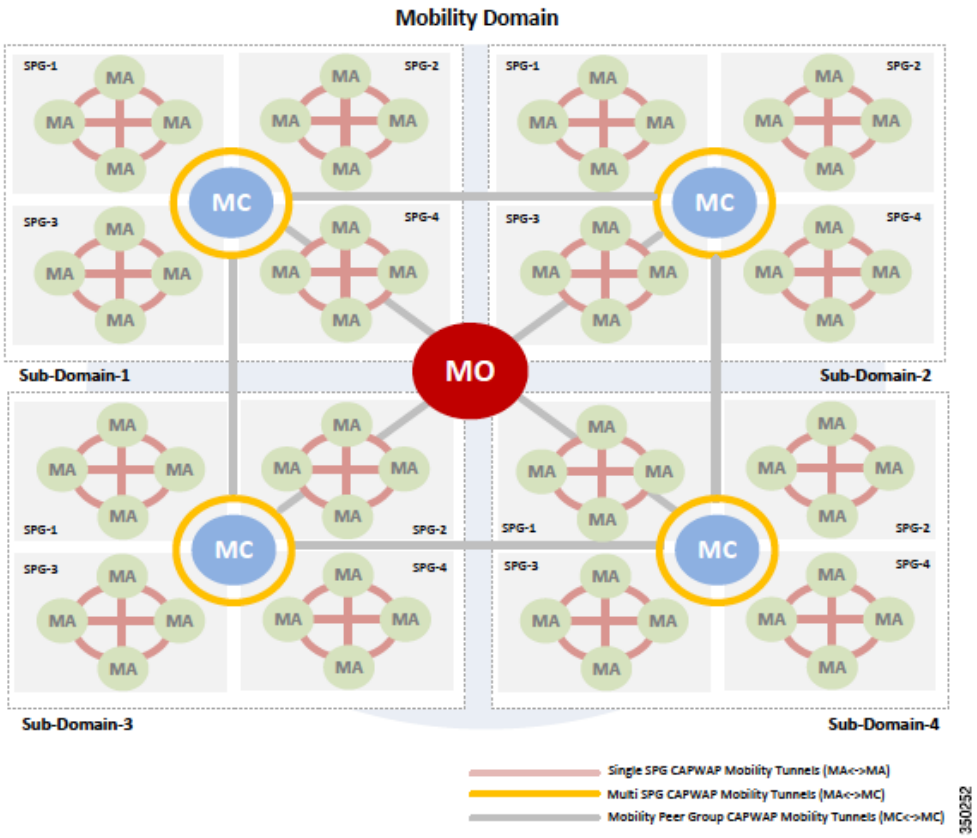
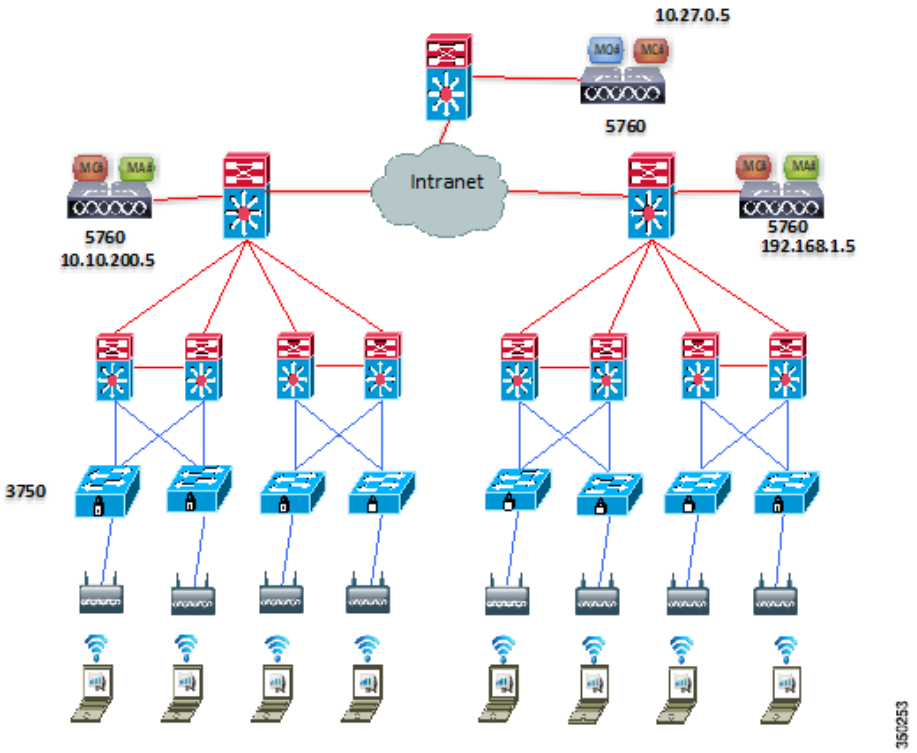


図 4-2　モビリティ設計と設定：一元化されたモードでの WLC5760



WLC5760 でのモビリティ設定：モビリティ コントローラ：モビリティ エージェント

```
wireless mobility controller
wireless mobility group member ip 10.27.0.5 public-ip 10.27.0.5
wireless mobility group member ip 192.168.1.5 public-ip 192.168.1.5
wireless mobility dscp 46
wireless mobility oracle ip 10.27.0.5
wireless management interface Vlan21
```

WLC5760 でのモビリティ設定：モビリティ コントローラ：モビリティ オラクル

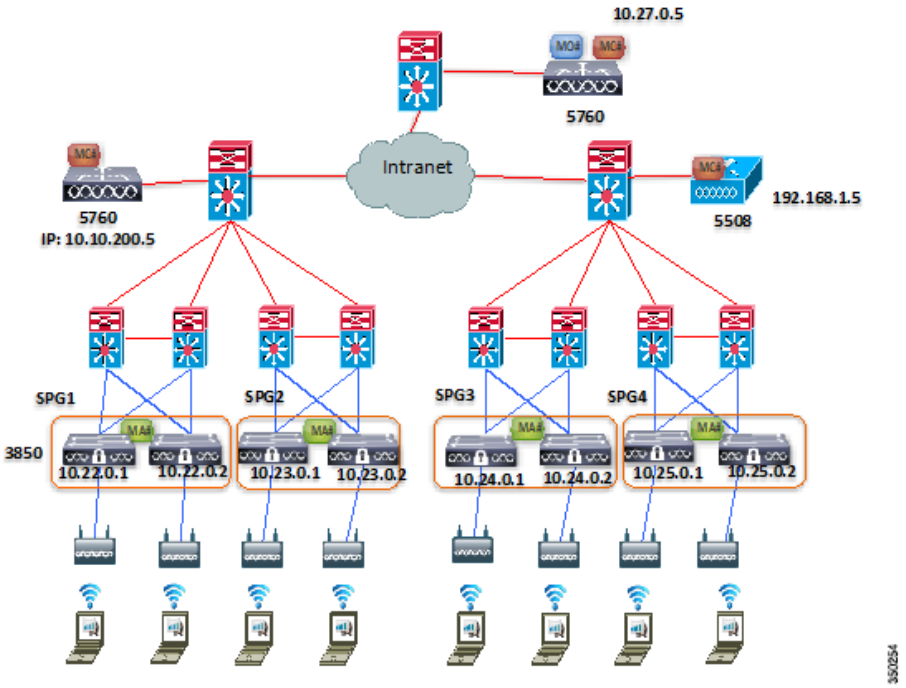
```
wireless mobility group member ip 10.10.200.5 public-ip 10.10.200.5
wireless mobility group member ip 192.168.1.5 public-ip 192.168.1.5
wireless mobility oracle
wireless management interface Vlan27
```

WLC5508 でのモビリティ設定：モビリティ コントローラ：モビリティ エージェント：

```
config mobility new-architecture enable
config mobility mobility-oracle10.27.0.5
config mobility group member add 10.10.200.5
config mobility group member add 10.27.0.5
config mobility dtls-mode enable
config mobility dscp 46
```

モビリティ設計と設定：WLC5760（モビリティ コントローラ）および統合アクセス モードの Catalyst 3850（モビリティ エージェント）

図 4-3　　統合アクセス モードでのモビリティ設計と設定



WLC5760 でのモビリティ設定：モビリティ コントローラ：モビリティ エージェント

```
wireless mobility controller
wireless mobility controller peer-group SPG1
wireless mobility controller peer-group SPG1 member ip 10.22.0.1 public-ip 10.22.0.1
```

```
wireless mobility controller peer-group SPG1 member ip 10.22.0.2 public-ip 10.22.0.2
wireless mobility controller peer-group SPG2
wireless mobility controller peer-group SPG2 member ip 10.23.0.1 public-ip 10.23.0.1
wireless mobility controller peer-group SPG2 member ip 10.23.0.2 public-ip 10.23.0.2
wireless mobility group member ip 10.27.0.5 public-ip 10.27.0.5
wireless mobility group member ip 192.168.1.5 public-ip 192.168.1.5
wireless mobility dscp 46
wireless mobility oracle ip 10.27.0.5 wireless management interface Vlan21
```

WLC5760 でのモビリティ設定：モビリティ コントローラ：モビリティ オラクル

```
wireless mobility group member ip 10.10.200.5 public-ip 10.10.200.5
wireless mobility group member ip 192.168.1.5 public-ip 192.168.1.5
wireless mobility oracle
wireless management interface Vlan27
```

WLC5508 でのモビリティ設定：モビリティ コントローラ：モビリティ エージェント

```
config mobility new-architecture enable
config mobility mobility-oracle10.27.0.5
config mobility group member add 10.10.200.5
config mobility group member add 10.27.0.5
config mobility switchPeerGroup create SPG3
config mobility switchPeerGroup member add 10.24.0.1 SPG3
config mobility switchPeerGroup member add 10.24.0.2 SPG3
config mobility switchPeerGroup create SPG4
config mobility switchPeerGroup member add 10.25.0.1 SPG4
config mobility switchPeerGroup member add 10.25.0.2 SPG4
config mobility dtls-mode enable
config mobility dscp 46
```

Catalyst 3850 でのモビリティ設定：モビリティ エージェント 1

```
wireless mobility controller ip 10.10.200.5 public-ip 10.10.200.5
wireless management interface Vlan22
```

Catalyst 3850 でのモビリティ設定：モビリティ エージェント 2

```
wireless mobility controller ip 10.10.200.5 public-ip 10.10.200.5
wireless management interface Vlan22
```

Catalyst 3850 でのモビリティ設定：モビリティ エージェント 3

```
wireless mobility controller ip 10.10.200.5 public-ip 10.10.200.5
wireless management interface Vlan23
```

Catalyst 3850 でのモビリティ設定：モビリティ エージェント 4

```
wireless mobility controller ip 10.10.200.5 public-ip 10.10.200.5
wireless management interface Vlan23
```

Catalyst 3850 でのモビリティ設定：モビリティ エージェント 5

```
wireless mobility controller ip 192.168.1.5 public-ip 192.168.1.5
wireless management interface Vlan24
```

Catalyst 3850 でのモビリティ設定：モビリティ エージェント 6

```
wireless mobility controller ip 192.168.1.5 public-ip 192.168.1.5
wireless management interface Vlan24
```

Catalyst 3850 でのモビリティ設定：モビリティ エージェント 7

```
wireless mobility controller ip 192.168.1.5 public-ip 192.168.1.5
wireless management interface Vlan25
```

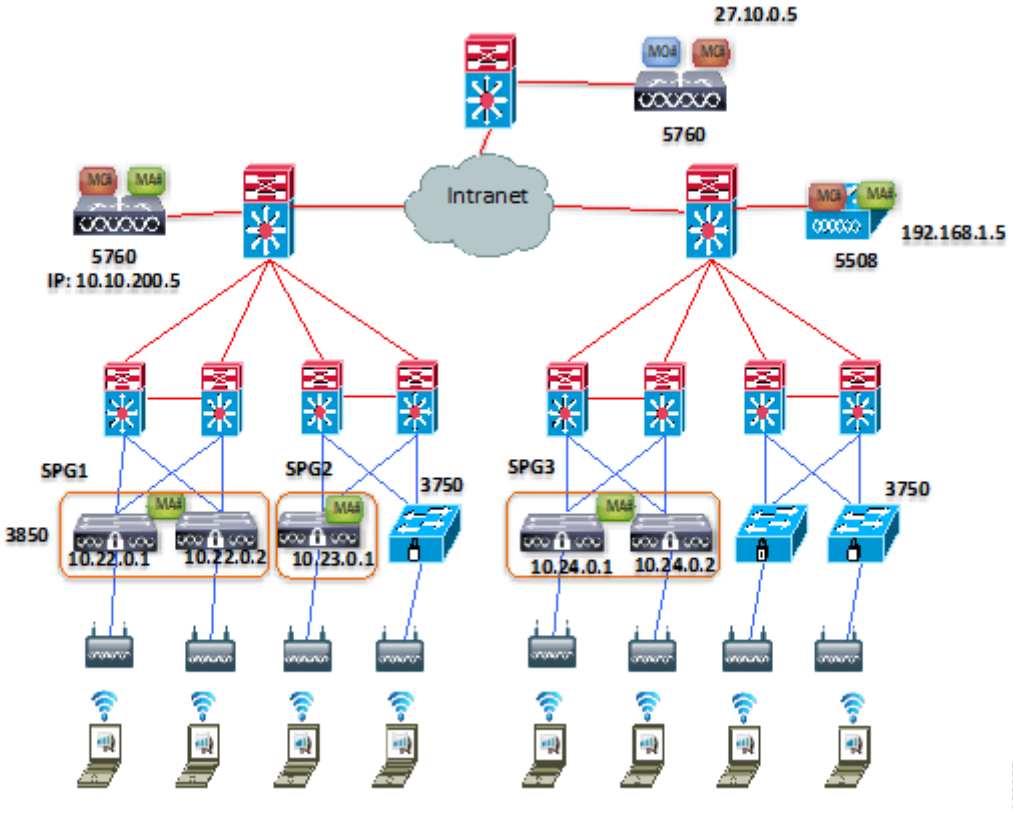
Catalyst 3850 でのモビリティ設定：モビリティ エージェント 8

```
wireless mobility controller ip 192.168.1.5 public-ip 192.168.1.5
wireless management interface Vlan25
```

モビリティ設計と設定

モビリティ設計と設定：ハイブリッド モードでの WLC5760、WLC5508、および Catalyst 3850

図 5-1　モビリティ設計と設定：ハイブリッド モードでの WLC5760、WLC5508、および Catalyst 3850



WLC5760 でのモビリティ設定：モビリティ コントローラ：モビリティ エージェント

```
wireless mobility controller
wireless mobility controller peer-group SPG1
wireless mobility controller peer-group SPG1 member ip 10.22.0.1 public-ip 10.22.0.1
wireless mobility controller peer-group SPG1 member ip 10.22.0.2 public-ip 10.22.0.2
wireless mobility controller peer-group SPG2
wireless mobility controller peer-group SPG2 member ip 10.23.0.1 public-ip 10.23.0.1
wireless mobility group member ip 10.27.0.5 public-ip 10.27.0.5
wireless mobility group member ip 192.168.1.5 public-ip 192.168.1.5
wireless mobility dscp 46
wireless mobility oracle ip 10.27.0.5
wireless management interface Vlan21
```

WLC5760 でのモビリティ設定：モビリティ コントローラ：モビリティ オラクル

```
wireless mobility group member ip 10.10.200.5 public-ip 10.10.200.5
wireless mobility group member ip 192.168.1.5 public-ip 192.168.1.5
wireless mobility oracle
wireless management interface Vlan27
```

WLC5508 でのモビリティ設定：モビリティ コントローラ：モビリティ エージェント

```
config mobility new-architecture enable
config mobility mobility-oracle10.27.0.5
config mobility group member add 10.10.200.5
config mobility group member add 10.27.0.5
config mobility switchPeerGroup create SPG3
config mobility switchPeerGroup member add 10.24.0.1 SPG3
config mobility switchPeerGroup member add 10.24.0.2 SPG3
config mobility dtls-mode enable
config mobility dscp 46
```

Catalyst 3850 でのモビリティ設定：モビリティ エージェント 1

```
wireless mobility controller ip 10.10.200.5 public-ip 10.10.200.5
wireless management interface Vlan22
```

Catalyst 3850 でのモビリティ設定：モビリティ エージェント 2

```
wireless mobility controller ip 10.10.200.5 public-ip 10.10.200.5
wireless management interface Vlan22
```

Catalyst 3850 でのモビリティ設定：モビリティ エージェント 3

```
wireless mobility controller ip 10.10.200.5 public-ip 10.10.200.5
wireless management interface Vlan23
```

Catalyst 3850 でのモビリティ設定：モビリティ エージェント 4

```
wireless mobility controller ip 192.168.1.5 public-ip 192.168.1.5
wireless management interface Vlan24
```

Catalyst 3850 でのモビリティ設定：モビリティ エージェント 5

```
wireless mobility controller ip 192.168.1.5 public-ip 192.168.1.5
wireless management interface Vlan24
```

ClientLink（ビーム形成）の設定

Cisco ClientLink は高度な信号処理技術と複数の送信パスを使用して、フィードバックなしにダウンリンク方向の 802.11a/g クライアントが受信する信号を最適化します。デフォルトでは ClientLink はディセーブルになっています。show ネットワーク コマンド **ap dot11** {24ghz | 5ghz} で ClientLink の一般ステータスを見ることができます。

グローバル コンフィギュレーション コマンド ap dot11 {24ghz | 5ghz} beamforming を使用して、すべての AP に対して ClientLink を有効にできます。ClientLink を無効にするには、コマンドの「no」形式を使用します。

```
ap dot11 5ghz shutdown
ap dot11 5ghz beamforming
no ap dot11 5ghz shutdown
```

これらのコマンドは ClientLink を全体でイネーブルにした後、特定の AP 無線で ClientLink を無効にします。

```
ap dot11 5ghz shutdown
ap dot11 5ghz beamforming
no ap dot11 5ghz shutdown
ap name 3602a dot11 5ghz shutdown
ap name 3602a no dot11 5ghz beamforming
ap name 3602a no dot11 5ghz shutdown
```

show コマンド :

```
show ap dot11 5ghz network | include Beamforming
Legacy Tx Beamforming setting : Disabled
show ap name 3602a config dot11 5ghz | include Beamforming
Legacy Tx Beamforming Setting: Enabled
```

CHAPTER 6

個人所有デバイスの持ち込みのセキュリティ設定

この項では、個人デバイスの安全なセルフ サービス追加について説明します。従業員が新しいデバイスを登録すると、証明書が各ユーザとデバイスに対して自動的にプロビジョニングされます。その証明書を使用して企業ネットワーク内のデバイスに搭載するように事前設定されたサプリカントのプロファイルとともに証明書がインストールされます。ワイヤレスのサプリカントに対してサポートされる 2 種類 BYOD 使用例は次のとおりです。

- Apple デバイスの SSID BYOD の単一認証
- Apple デバイスの SSID BYOD の二重認証

Apple デバイスの SSID BYOD の単一認証の使用例

この使用例では、保護拡張認証プロトコル（PEAP）および拡張認証プロトコル Transport Layer Security（EAP-TLS）の両方を認証および許可する企業アクセスの単一 SSID（BYOD-Dot1x）があります。

1. ユーザは BYOD-Dot1x に関連付けられます。
2. ユーザは、PEAP 認証に対する従業員のユーザ名とパスワードを入力します。
3. オーセンティケータがユーザを認証し、認可ポリシーに基づく URL リダイレクトを実行します。
4. ユーザがブラウザを開くと、デバイス登録をするセルフ登録ポータルにリダイレクトされます。
5. MAC アドレスはデバイス ID に対応するデバイス登録ページにすでに入力されており、ユーザは説明を入力し、デバイスを登録します。
6. ユーザのサプリカントはプロビジョニングされ、証明書がインストールされます。
7. 証明書のインストール後、認可変更（CoA）が発生します。サプリカントは、EAP-TLS を使用して認証および許可されます。
8. ダイナミック VLAN 割り当てが発生し、サプリカントは VLAN に配置されます

Apple デバイスの SSID BYOD の二重認証の使用例

二重 SSID の使用例では、ゲスト用の BYOD-Open および企業アクセスを認証するものの 2 つの SSID があります。

1. ユーザをゲスト用の BYOD-Open SSID に関連付けます。

2. ユーザがブラウザを開き、アイデンティティ サービス エンジン（ISE）中央 Web 認証 (CWA) のゲスト ポータルにリダイレクトされます。
3. オーセンティケータは、従業員として関連ユーザを認証し、従業員のデバイス登録のゲスト ポータルにユーザを導きます。
4. MAC アドレスはデバイス登録ページにすでに入力されており、ユーザは説明を入力し、デバイスを登録します。
5. ユーザのサプリカントはプロビジョニングされ、証明書がインストールされます。
6. ユーザはゲスト SSID から切断します。
7. ユーザは企業 SSID に接続し、認証および許可されて新しいプロファイルを使用します。

トポロジ

図 6-1　Catalyst 3850 でオーセンティケータとして使用される BYOD トポロジ

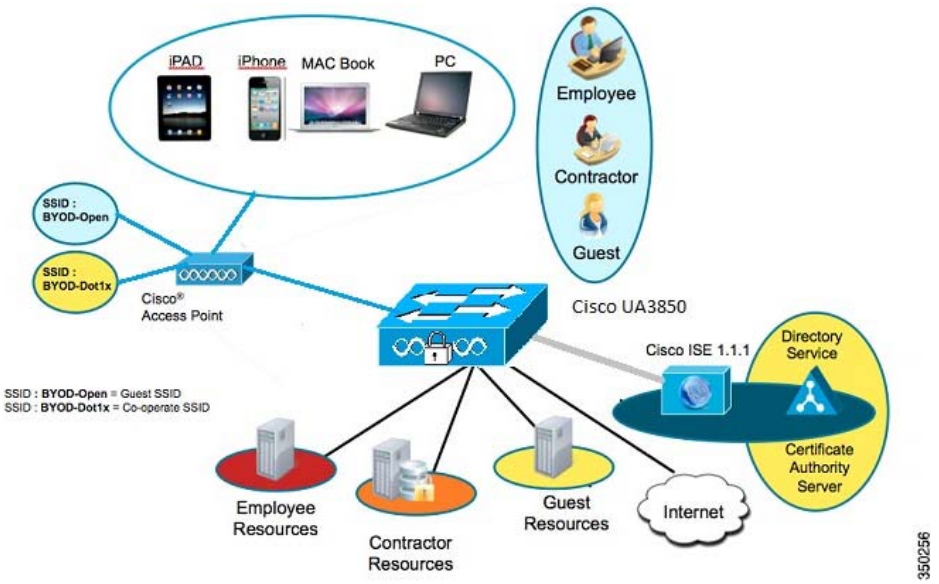
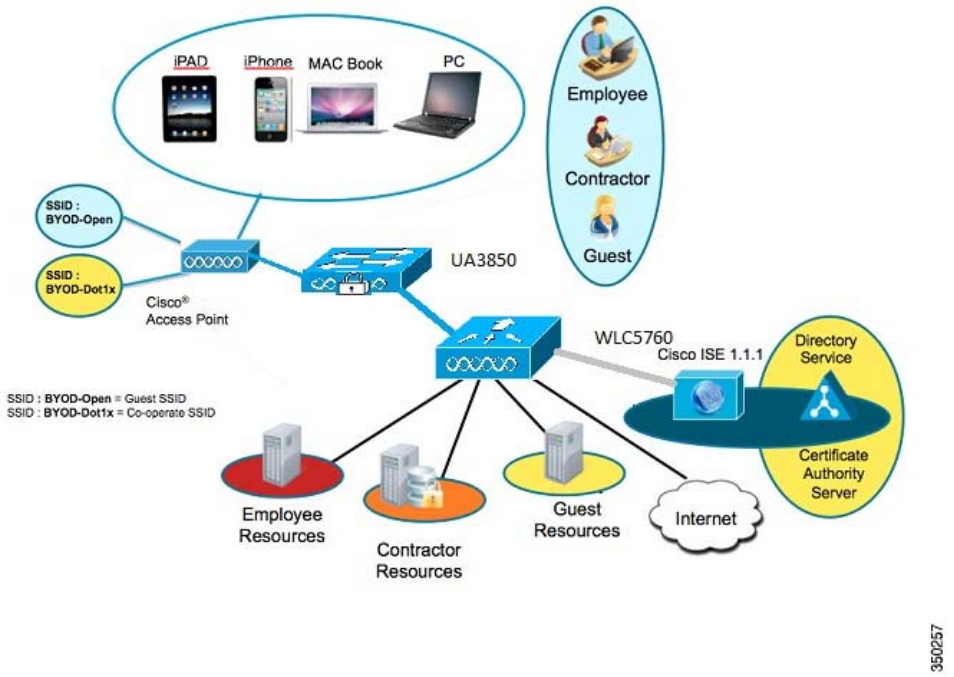


図 6-2　WLC5760 でオーセンティケータとして使用される BYOD トポロジ



コンポーネント

コンポーネント	ハードウェア	テスト対象機能	Cisco IOS® ソフトウェア リリース
ISE	UCS サーバ	AAA オーバーライド、プロファイラ、ポスチャ	ISE 1.1.1
認証局および AD Server	Windows 2008 R2 Enterprise、SP2	SCEP、認証局、Active Directory サーバ	-
ワイヤレス コントローラ	UA3850 CT5760	認証/認可、URL リダイレクト、および CoA	03.07.98.EMP
Apple iOS デバイス	Apple iPad、iPhone	-	Apple iOS 5.0

セキュアな WLAN の設定

Catalyst 3850/WLC5508 の Secure WLAN の設定

ワイヤレス Dot1x 設定

```
aaa new-model
aaa group server radius Cisco
server 10.10.200.60 auth-port 1812 acct-port 1813
aaa authentication login no_auth none
aaa authentication dot1x default group radius
aaa authentication dot1x Cisco_dot1x group Cisco
aaa authorization network default group Cisco
aaa accounting network default start-stop group Cisco
dot1x system-auth-control
```

動的認可の設定

```
aaa server radius dynamic-author
client 10.10.200.60 server-key Cisco123
auth-type any
```

RADIUS サーバの設定

```
radius-server attribute 6 on-for-login-auth
radius-server dead-criteria time 10 tries 3
radius-server host 10.10.200.60 auth-port 1812 acct-port 1813 key Cisco123
radius-server deadtime 3
radius-server vsa send accounting
radius-server vsa send authentication
radius server Cisco
```

URL リダイレクト アクセス リストの設定

```
ip access-list extended NSP-ACL?  Supplicant Provisioning ACL
denyip any host 10.10.200.60
permit ip any any
```

HTTP の設定

```
!
ip http server
ip http authentication local
ip http secure-server
ip http secure-client-auth
```

WLAN の設定

```
wireless mobility controller
wireless management interface 200
wireless client user-timeout600
wlan BYOD-Dot1x 1 BYOD-Dot1x <- Secure Corporate SSID
aaa-override
accounting-list Cisco
client vlan 100
ip access-group NSP-ACL
nac
security dot1x authentication-list Cisco
session-timeout 600
no shutdown
wlan BYOD-Open 2 BYOD-Open <- Guest SSID
aaa-override
client vlan 100
ip access-group NSP-ACL
nac
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security dot1x authentication-list Cisco
no shutdown
```

ワイヤレス Dot1x セッションの確認

```
Controller-MC#show access-session method dot1x details
Controller-MC#show access-session interface capwap 1 details
Controller-MC#show access-session mac 6420.0c37.5108 interface capwap 1
Controller-MC#show wireless client summary
```

クライアントの認証解除

```
Controller-MC#wireless client mac-address 6420.0c37.5108 deauthenticate
Controller-MC#show wireless client summary
```

無線リソース管理の設定

無線リソース管理の設定

無線リソース管理について

無線リソース管理（RRM）ソフトウェアはコントローラに組み込まれており、ワイヤレス ネットワークのリアルタイムでの無線周波数（RF）管理を常時提供する組み込みの RF エンジニアとして機能します。RRM を使用すると、コントローラは関連付けられた lightweight AP を継続的に監視できます。

- **トラフィックの負荷**：トラフィックの送受信に使用される帯域幅の合計量。これにより、ワイヤレス LAN 管理者は、ネットワークの拡大状況を追跡し、クライアントの需要以前に計画を立てることができます。
- **干渉**：他の 802.11 発信元から送られてくるトラフィック量。
- **ノイズ**：現在割り当てられているチャネルに干渉している 802.11 以外のトラフィック量。
- **カバレッジ**：接続されているすべてのクライアントの受信信号強度インジケータ（RSSI）と信号対雑音比（SNR）。
- **その他**：近くの AP 数。

RRM は、最も効率がよくなるように 802.11 RF ネットワークを定期的に再設定できます。そのために、RRM では次の機能を実行します。

- 無線リソースの監視
- 送信電力の制御
- チャネルの動的割り当て
- カバレッジ ホールの検出と修正

初期設定のために、以下で現在の WLC GUI で出現する順に項目を説明し、デフォルト値の調整が必要な予測可能な事項に焦点を当てます。

RF Group Name

RRM がグループ メンバを識別し RF グループ リーダーを選択するグループ化アルゴリズムの基礎となる RF グループ名を割り当てます。このテスト システムがすでに確立されている実稼働ネットワークと相互通信することを避けるため、明らかに異なった名前を割り当てることを推奨します。RF グループ名を設定するには、モビリティ コントローラのコマンドラインでコンフィギュレーション モードに入ります。

```
(config)#wireless rf-network <name> <cr>
802.11a/b network command
```

いくつかのコマンドは、実行するためにネットワークを無効にする必要があります。設定端末プロンプトからネットワークを簡単にイネーブルまたはディセーブルにできます。

```
Switch(config)#ap dot11 24/5ghz shut
Or use the no form to enable
config)# no ap dot11 24/5ghz shut)
```

これがデフォルトのデータ レート値の表示です。これらの内のいくつかを変更する必要があることがあります。

ap dot11 24/5ghz rate <rate> mandatory/supported/disabled:

たとえば、1、2、5.5、11 Mbps をディセーブルにして、24、54 Mbps を必須としてイネーブルにし、ほかのすべてをサポートされるようにします。5

GHz では 12、4 Mbps を必須とし、ほかのすべてがサポートされるようにします。

```
ap dot11 2 shut
ap dot11 2 rate RATE_11M disable
ap dot11 2 rate RATE_1M disable
ap dot11 2 rate RATE_2M disable
ap dot11 2 rate RATE_5_5M disable
% Unable to modify rate, Since this is the last available BSS rate.
```

上記の警告は使用可能な他の必須なレートがないために出力されます。少なくとも 1 つの必須レートがなければなりません。

```
ap dot11 2 rate RATE_24M mandatory
ap dot11 2 rate RATE_5_5M disable
ap dot11 2 rate RATE_54M mandatory
no ap dot11 2 shut
ap dot11 5 shut
ap dot11 5 rate RATE_6M supported
no ap dot11 5 shut
```

レガシー ClientLink のデフォルト設定は、ディセーブルです。

```
ap dot11 24/5ghz beamforming <cr>
```

ディセーブルにするには、no 形式を使用します。

その他のネットワーク設定は参照用に表示されます。802.11g のサポートがイネーブルです（デフォルト設定）。

```
ap dot11 24ghz dot11g <cr>
```

ビーコン間隔：デフォルトは 100 ミリ秒です。これは変更しないでください。

```
ap dot11 24/5ghz beacon(20-1000 ms)
```

short プリアンブル：Cisco AP では AP がプリアンブルを自動で調整できるように short プリアンブルはイネーブルです。常に short または long プリアンブルを使用するためにプリアンブルをセットする方法はありません。short プリアンブルがはデフォルトでイネーブルです。short プリアンブルをディセーブルにするには、コマンドの no 形式を使用します。

```
ap dot11 24/5ghz preamble short<cr>
```

フラグメンテーションしきい値：デフォルト 2346：重要な理由がない限り変更しないでください。

```
ap dot11 24/5ghz fragmentation<256-2346> (bytes)
```

送信電力の動的制御（DTPC）サポート：デフォルトはオンです。これは、Cisco Compatible Extensions（CCX）クライアントに使用されている電力レベルを伝えます。

```
ap dot11 24/5ghz dtpc <cr>
```

無効にするには、コマンドの no 形式を使用します。

CCX Location Measurement Q：デフォルトはオフです。CCX ロケーションを使用している場合は、イネーブルになります。

```
ap dot11 24/5ghz rrm ccx location-measurement <cr>
```

ディセーブルにするには、no 形式を使用します。

RRM RF グループ化と次世代のコントローラ

RF グループ化は自動またはスタティック モードに設定できます。自動モードでは、グループ リーダーが選択するためにモビリティ コントローラはグループ化アルゴリズムとネゴシエートします。スタティック モードでは、追加メンバーを手動で追加するようにユーザがグループ リーダーになるデバイスを選択することができます。メンバーはスタティック リーダーに統合するために自動に設定される必要があります。

RF グループ化モードの設定

自動 RF グループ化をするにはこのコマンドを使用します。

```
ap dot11 24/5Ghz rrm group-mode auto
```

スタティック モードで、スタティック メンバーを追加するには、メンバーのモビリティ コントローラが自動グループ化モードである必要があります。

```
ap dot11 24 rrm group-mode leader
ap dot11 24 rrm group-member Cisco_dd:f8:e4 IP address
```

RRM RF グループ化をディセーブルまたはイネーブルにするには、このコマンドを入力します。

```
ap dot11 24rrm group mode
```

RRM TPC の送信電力制御の設定

RRM の送信電力制御（TPC）を設定するには、それを実行するか、無効にするアルゴリズム用のモードを選択します。minimum/maximum コマンドを除いて、すべての TPC の設定はグローバル コマンドで、その RF グループに影響のある RF グループ リーダーで入力する必要があります。

TPC のデフォルト設定は自動に設定されます（自動）。この値を変更するには、次のコマンドを入力してください。

```
ap dot11 24 rrm txpower ?
<1-8>Enter transmit power level
autoEnables auto-RF
maxConfigures maximum auto-RF tx power
minConfigures minimum auto-RF tx power
onceEnables one-time auto-RF
```

TPC が自動に設定されている場合、TPC しきい値（デフォルトで -70 dBm）を調整する必要があります。有効な範囲は -80 dBm ~ -50 dBm です。

```
ap dot11 24 rrm tpc threshold -70
```

現在の RRM TPC 設定を表示するコマンドを示します。

```
show ap dot11 24 txpower
```

RRM DCA 設定

動的なチャネル割り当て (DCA) は、グローバル アルゴリズムです。TPC と同様に、変更は RF グループ リーダーに行う必要があります。メンバーに変更を行っても、そのメンバーをリーダーに変更しないかぎりは、アルゴリズムに影響を与えません。

デフォルト DCA は自動に設定されます。アンカーの時間や間隔の値などのその他のオプションは、オンデマンドに含まれます。

DCA が一度実行し、固定できるようにするには、次のコマンドを使用します。

```
ap dot11 24 rrm channel global once
```

DCA を自動に戻すには、次のコマンドを使用します。

```
ap dot11 24 rrm channel global auto
```

DCA を 10 分のデフォルト以外の固定間隔で実行するように設定するには、次のコマンドを使用します。

```
ap dot11 24 rrm channel dca anchor-time 1
ap dot11 24 rrm channel dca interval 8
```

これらのコマンドは、RF グループ リーダーの時間帯に 1 AM のアンカー時間を設定し、8 時間間隔で DCA を実行します。有効な間隔は 1、2、3、4、6、8、12、および 24 時間です。0 = 10 分（デフォルト）。

使用する DCA アルゴリズムの感度（デフォルトは medium）を設定するには、次のコマンドを使用します。

```
ap dot11 24 rrm channel dca sensitivity low
```

オプションは medium/low/high です。

DCA が管理するチャネルを割り当てるには、このコマンドを使用します。チャネルあたり 1 個のエントリーを使用し、2.4 および 5 Ghz 帯域の両方で実行します。

```
ap dot11 24 rrm channel dca 1
ap dot11 24 rrm channel dca 6
ap dot11 24 rrm channel dca 11
```

ノイズの回避、外部 AP 回避、ロード、CleanAir 永続型デバイスの回避、および CleanAir イベント駆動型のワイヤレス リソース管理 (EDRRM) などの DCA アルゴリズムのオプションを管理するために DCA 制御からチャネルを削除するには、このコマンドの no 形式を使用します。

```
ap dot11 24 rrm channel ?
cleanair-event - Configure cleanair event-driven RRM parameters
dca - Config 802.11b dynamic channel assignment algorithm
device - no description - CleanAir PDA
foreign - Configure foreign AP 802.11b interference avoidance
global - Configures all 802.11b Cisco APs
load - Configure Cisco AP 802.11b load avoidance
noise - Configure 802.11b noise avoidance
```

デフォルト値は foreign および noise です。

コマンドは一度に 1 行ずつ入力します。device、foreign、load、noise がオンまたはオフになる値です。オフにするには、このコマンドの no 形式を使用します。CleanAir イベントにも、関連付けられた感度レベルがあります。デフォルト値は low です。その他のオプションは、medium および high です。

チャネル アップデートに使用している回線では、AP の信号ノイズ、干渉（外部）、およびロード（SNIU）を DCA に追加された時点で示します。

RRM カバレッジ ホールの検出および軽減

カバレッジ ホールの検出と軽減（CHDM）のデフォルト値は、ほとんどの環境で十分満足のいくものです。変更する項目には、データ / 音声 RSSI しきい値などが含まれます。このしきい値により、カバレッジ ホールの状態にあるクライアント、グローバル カバレッジ例外、AP あたりの障害クライアントの割合を考慮するタイミングを決定します。コマンド ラインで公開されているその他のコントロールがあります。指示がない限りは、デフォルトを受け入れてください。

CHDM は、コントローラごとの設定ベースで、グローバルではありません。カバレッジ ホールの検出をイネーブルまたはディセーブルにするには、次のコマンドを入力します。

```
ap dot11 24 rrm coverage
```

無効にするには、コマンドの no 形式を使用します。

このコマンドは、データ/音声クライアントの RSSI しきい値を調整します。

```
ap dot11 24 rrm coverage data rssi-threshold -80
ap dot11 24 rrm coverage voice rssi-threshold -80
```

クライアントがカバレッジ ホールにあると考えるレベルを設定するには、デフォルト値は 80 dBm で、有効な範囲は -90/-60 dBm です。音声およびデータ クライアントでは、2 つのコマンドに分かれます。

このコマンドは、AP あたりの最小障害クライアントの数とカバレッジ例外レベルを設定します:

```
ap dot11 24 rrm coverage level global 3
ap dot11 24 rrm coverage exception global 25
```

3 クライアントとカバレッジ例外 25% がデフォルト値です。指定できる範囲は 1 ~ 75 クライアントおよび 0 ～ 100% です。

最小の障害クライアント数および例外レベルは、この機能のゲーティング機能として連携して機能します。3 クライアントとデフォルトの 25% は、3 クライアントがカバレッジ ホール内にある必要があり、なおかつこの 3 クライアントは現在の AP に関連付けられたクライアントの少なくとも 25% を表す必要があるという意味です。これは軽減の条件です。

ネイバー探索プロトコル

ネイバー探索プロトコル (NDP) は、ネットワーク内のすべての AP の RF プロキシミティを確立します。これはパフォーマンスのためネットワークのバランス調整に RRM で使用するすべての計算の基礎です。NDP はデフォルトで Over-the-Air オープン プロトコルです。暗号化を使用してこれを保護することは可能ですが、RF グループ内のすべてのメンバーが NDP を機能させるために同じモードである必要があります。NDP 保護をイネーブルにするには、ネットワーク上のすべてのモビリティ エージェントとモビリティ コントローラにこのコマンドを入力します。

```
ap dot11 24 rrm ndp-type protected
```

CleanAir

Cisco CleanAir は、共有ワイヤレス スペクトラムに関する問題に予防的に対応するスペクトラム インテリジェンス ソリューションです。この機能を使用すると、共有スペクトラムの全ユーザを確認できます（ネイティブ デバイスと外部干渉源の両方）。また、ネットワークにおいて、これらの情報に基づいて対処できるようになります。たとえば、干渉デバイスを手動で排除することや、システムによって自動的にチャネルを変更して干渉を受けないようにすることができます。

CleanAir について

Cisco CleanAir システムは CleanAir 対応 AP、コントローラ、および Wireless Control System（WCS）で構成されます。これらの AP は、産業、科学、医療（ISM）帯域で動作するすべてのデバイスに関する情報を収集します。AP で潜在的な干渉源として識別した情報を識別および評価し、コントローラに転送します。コントローラは AP を制御し、スペクトラム データを収集し、これらの情報を要求に応じて WCS またはシスコ モビリティ サービス エンジン（MSE）に転送します。コントローラにはローカルなユーザ インターフェイスがあり、CleanAir の基本的な機能を設定することや、基本的なスペクトラム情報を表示することができます。WCS には高度なユーザ インターフェイスがあり、Cisco CleanAir の機能の設定、情報の表示、記録の保持などを行えます。MSE は基本的な機能セットに対するオプションですが、非 Wi-Fi 干渉デバイスの位置の追跡など、高度な機能を使用するためには必須です。

Cisco CleanAir では、ライセンス不要の帯域で動作している各デバイスについて、その種類、場所、ワイヤレス ネットワークに与える影響の程度、取るべき対策を提示します。これによって RF がシンプルになり、管理者が RF のエキスパートである必要がなくなります。

ワイヤレス LAN システムは、ライセンスが不要の 2.4 GHz および 5 GHz ISM 帯域で動作します。この帯域では電子レンジ、コードレス電話、Bluetooth デバイスなどの多数の機器が動作しているため、Wi-Fi の動作に悪影響が生じる可能性があります。

Voice over Wireless や IEEE 802.11n 無線通信などの非常に高度な WLAN サービスの一部は、ISM 帯域を合法的に使用する他の機器からの干渉によって、重大な影響を受ける可能性があります。Cisco Unified Wireless Network に対する Cisco CleanAir の機能の統合は、RF 干渉の問題を解決します。

CleanAir の設定

CleanAir は WLC/ モビリティ コントローラ レベルではデフォルトで無効になっており、WLC のインストールなどすべてのモビリティ コントローラでイネーブルにする必要があります。スイッチ上で CleanAir をイネーブルにするには、次のコマンドを入力します。

```
ap dot11 24 cleanair ap dot11 5
```

```
cleanair Controller#show ap dot11 24 sum
```

単一の AP 無線上で CleanAir をイネーブルまたはディセーブルにするには、このコマンドを入力します。

```
ap name AP0022.bd18.87c0dot11 24 cleanair
```

コマンドの no 形式で CleanAir をディセーブルにします。

AP 無線およびグローバル レベルでデバイスおよび通信品質 (AQ) に関して CleanAir に問い合わせるには、次のコマンドを使用します。

```
show ap dot11 24 cleanair device type all
```

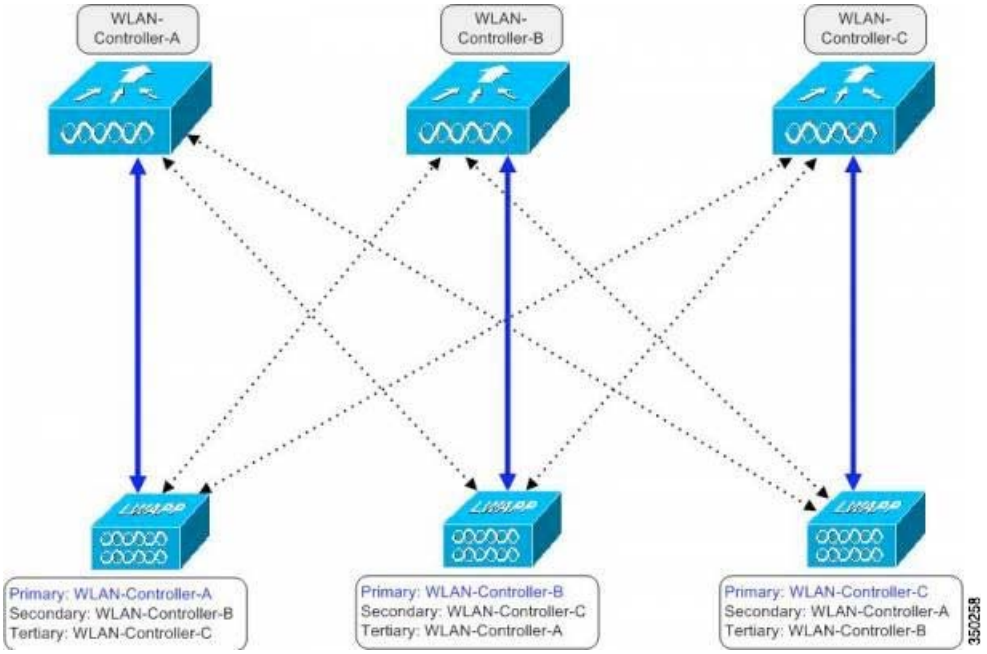
モビリティ コントローラの CleanAir 設定を表示するには次のコマンドを使用します。

```
show ap dot11 24 cleanair config
```

ハイ アベイラビリティ

WLC5760 初期リリースでは、AP は第 1、第 2、および第 3 コントローラを使用して設定できます。1 台のコントローラで管理される AP 数が原因で第 1 コントローラに障害が発生した場合、アクセス ポイントは第 2 コントローラにフェール オーバーします。第 1 コントローラが使用できないことを検出すると、AP はコントローラを再検出し、第 2 コントローラに CAPWAP トンネルを確立します。さらに、クライアントは AP で再認証される必要があります。図 10-1 は第 1、第 2、第 3 コントローラの冗長性を図示しています。

図 10-1　　WLC5760 ハイ アベイラビリティ

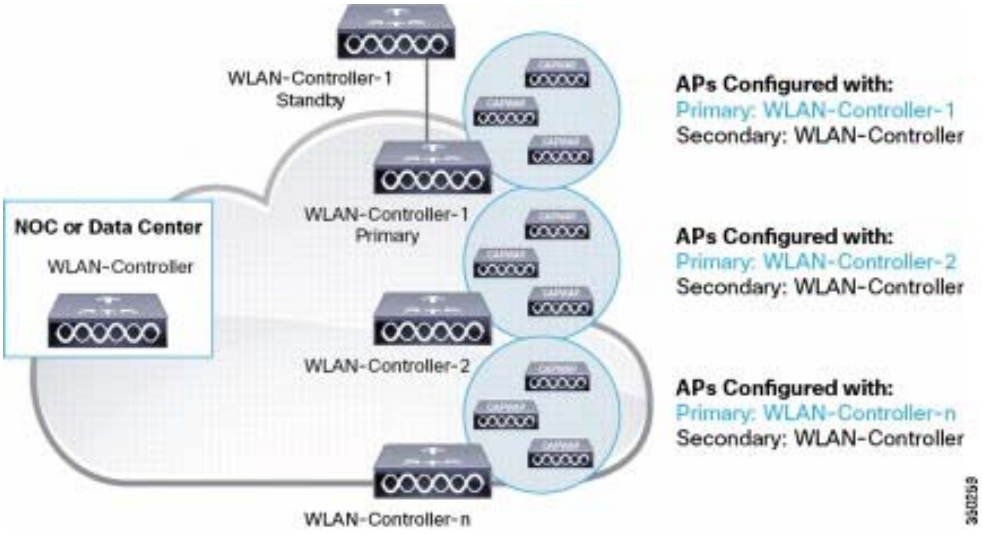


（注） リリース 7.3 以降では、従来の WLC コントローラでアクセス ポイントのステートフル スイッチオーバー（AP SSO）をサポートします。AP SSO ハイ アベイラビリティ機能に関する追加情報については、『High Availability (AP SSO) Deployment Guide』を参照してください。

N+1 冗長性

CT5760 コントローラがデータセンターに配置され複数の WLC のバックアップとして機能する場所では N+1 冗長性がサポートされます。各 AP は第 1 コントローラとして 1 台の WLC に設定され、すべての AP が第 2 として 1 台の冗長コントローラに切り替わります。

図 10-2　　N+1 冗長性



ハイ アベイラビリティ設定

```
#ap name apname controller ?
primaryConfigures primary controller
secondaryConfigures secondary controller
tertiaryConfigures tertiary controller
```

次のコマンドを使用して設定を確認します。

```
#show ap name <ap-name> config general
```

コントローラの障害検出時間を短縮するには、コントローラと AP の間のハートビート間隔に設定するタイムアウト値をより小さくします。

```
#ap capwap timers heartbeat-timeout <1-30>
```

第 1、第 2、第 3 コントローラを特定の AP に対して設定するオプションに加えて、特定の AP に対してプライマリ、セカンダリ バックアップ コントローラを設定できます。AP 側で設定された第 1、第 2、第 3 WLC がなく、コントローラ側（AP にダウンロードされる）にプライマリおよび/またはセカンダリ バックアップ コントローラが設定されている場合、このプライマリおよび/またはセカンダリ コントローラが AP のプライマリ ディスカバリ要求のメッセージ受信者のリストに追加されます。特定のコントローラのプライマリ バックアップ コントローラを設定するには、次のコマンドを使用します:

```
(config)#ap capwap backup ?
primaryConfigures primary Controller
secondaryConfigures secondary Controller
```

インターフェイス グループ

インターフェイス グループは、インターフェイスの論理的なグループです。インターフェイス グループを使用すると、同じインターフェイス グループを複数の WLAN で設定するユーザ設定や、AP グループごとに WLAN インターフェイスを上書きすることが容易になります。インターフェイス グループには隔離済みまたは隔離済みでないインターフェイスを排他的に含めることができます。1 つのインターフェイスを複数のインターフェイス グループに含めることができます。

WLAN は、インターフェイスまたはインターフェイス グループに関連付けることができます。インターフェイス グループの名前とインターフェイスの名前を同じにすることはできません。

この機能を使用すると、クライアントを特定のサブネットに、そのサブネットが接続している外部コントローラに基づいて関連付けることができます。必要に応じて、外部コントローラの MAC と特定のインターフェイスまたはインターフェイス グループ（外部マップ）との間のマッピングを維持するように、アンカー コントローラ WLAN を設定できます。このマッピングが設定されていない場合、その外部コントローラ上のクライアントが WLAN に設定されたインターフェイス グループから関連付けられた VLAN を取得します。

インターフェイス グループには AAA Override を設定することもできます。この機能では、現行の AP グループと AAA Override アーキテクチャが拡張され、AP グループと AAA Override が、インターフェイスがマッピングされているインターフェイス グループ WLAN よりも優先されるように設定できます。これは、インターフェイス グループを使用した複数のインターフェイスに対して行われます。

この機能により、ネットワーク管理者はゲスト アンカー制限を設定できます。それにより、外部ロケーションにいる無線ゲスト ユーザは、同じアンカー コントローラ内から、外部ロケーションとコントローラ上の複数のサブネットのうちの 1 つの IP アドレスを取得できます。

インターフェイス グループの設定

WLC に VLAN グループを作成するには、次のコマンドを使用します。

```
vlan group word vlan-list 100-200
show vlan group
```

WLAN に VLAN グループをマッピングするには次のコマンドを使用します。

```
wlan corporate 1 corporate client vlan word
show wlan summary
```

AP グループを設定

AP グループについて

コントローラ上に最大 512 の WLAN を作成した後では、さまざまな AP に WLAN を選択的に公開（AP グループを使用して）することで、ワイヤレス ネットワークの管理を向上させることができます。一般的な展開では、WLAN 上のすべてのユーザはコントローラ上の 1 つのインターフェイスにマップされます。したがって、その WLAN にアソシエートされたすべてのユーザは、同じサブネットまたは VLAN 上にあります。ただし、複数のインターフェイス間で負荷を分散すること、または AP グループの作成によって個々の部門（たとえばマーケティング部門）などの特定の条件に基づくグループ ユーザへと負荷を分配することを選択できます。さらに、ネットワーク管理を簡素化するために、これらの AP グループを別個の VLAN で設定できます。

図 11-1　　アクセス ポイント グループ

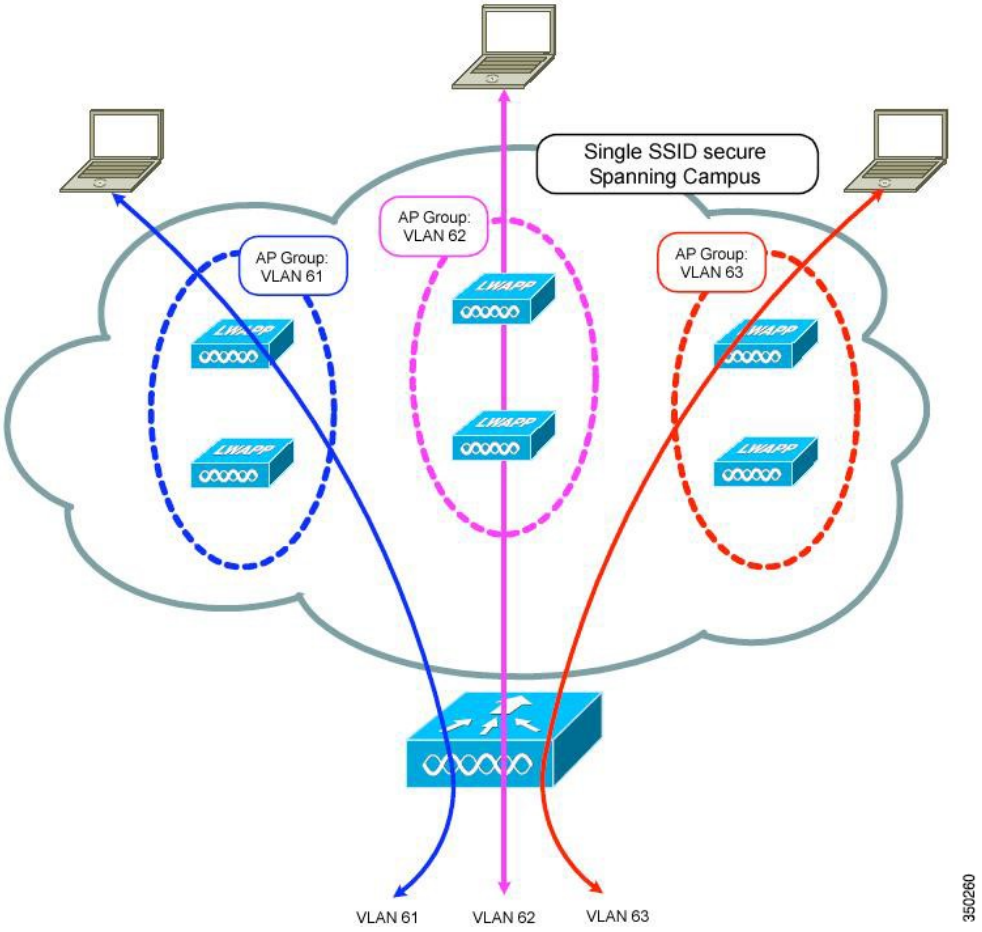


図 11-1 では、3 つの設定された動的インターフェイスが、3 つの異なる VLAN（VLAN 61、VLAN 62、および VLAN 63）にマップされています。3 つの AP グループが定義されており、各グループは異なる VLAN のメンバですが、すべてのグループが同じ SSID のメンバとなっています。ワイヤレス SSID 内のクライアントには、その AP がメンバとなっている VLAN サブネットから IP アドレスが割り当てられています。たとえば、AP グループ VLAN 61 のメンバである AP に関連する任意のユーザには、そのサブネットから IP アドレスが割り当てられます。

図 11-1 の例では、コントローラは内部的には AP 間のローミングをレイヤ 3 ローミング イベントとして扱います。

こうすることで、WLAN クライアントは元の IP アドレスを保持します。

すべての AP をコントローラに結合した後は、AP グループを作成して、最大 16 の WLAN を各グループに割り当てることができます。各 AP は、有効化されている WLAN のうち、その AP グループに属する WLAN だけをアドバタイズします。AP は、AP グループで無効化されている WLAN または別のグループに属する WLAN はアドバタイズしません。

AP グループ名を作成するには、次のコマンドを使用します。

```
ap group <WORD> wlan <apgroup> vlan < VLAN#>
```

次のコマンドは、AP グループに AP をマッピングします。

```
ap name <name> ap-groupname <apgroup>
```

AP は、上記のコマンドの実行後にリロードします。

CHAPTER 12

マルチキャストの設定

マルチキャスト転送のデフォルトは WLC5760 コントローラでディセーブルです。次のコマンドで（IPv4 または IPv6）マルチキャスト転送のサポートをイネーブルにできます。

```
(config)#wireless multicast
```

次のコマンドを使用して、Internet Group Management Protocol（IGMP）スヌーピングをコントローラでイネーブルにする必要があります。

```
(config)#ip igmp snooping
```

IPv6 の場合は、次のコマンドを使用します。

```
(config)#ipv6 mld snooping
```

WLC から AP への転送モード

マルチキャストがイネーブルにされると、マルチキャスト トラフィックを AP に転送できます。コントローラは受信したマルチキャスト パケットを CAPWAP にカプセル化し、個々の AP にこのパケットを送信します。このモードは、マルチキャスト ユニキャスト (MCUC) と呼ばれます。代わりに、コントローラがこのマルチキャスト パケットを別のマルチキャスト パケットにカプセル化して 1 回送信することができます。このモードは、1 パケットだけがコントローラで作成されるので、効率的です。このモードは、マルチキャスト マルチキャスト (MCMC) と呼ばれます。このモードを使用するには、コントローラにマルチキャスト グループを設定する必要があります。コントローラに接続されているすべての AP がこのマルチキャスト グループに加入し、マルチキャスト フローを受信できます。次のコマンドを使用して、MCMC をイネーブルにしマルチキャスト グループを設定できます。

```
(config)#wireless multicast
(config)#ap capwap multicast 239.3.3.3
```

このコマンドの no 形式を使用して、デフォルトの MCUC モードに戻すことができます。

```
(config)#no ap capwap multicast
```

従来のソリューションと同様に、マルチキャスト グループは VLAN 単位で作成されます。たとえば、WLAN が VLAN 100 にマッピングされ、クライアントがその WLAN からマルチキャスト トラフィックを要求した場合、マルチキャスト送信元、マルチキャスト アドレス、および VLAN（この例では VLAN 100）をマッピングするマルチキャスト グループ ID（MGID）をコントローラが作成します。これは、その WLAN 内のクライアント VLAN に関係なく行われます。

マルチキャスト VLAN 機能

この例では 2 つのインターフェイスを作成し、その後インターフェイス グループで 2 つの VLAN をまとめてマッピングします。

```
(config)#interface vlan 19
(config-if)#ip address 10.10.19.1 255.255.255.0
(config)#interface vlan 21
(config-if)#ip address 10.10.21.1 255.255.255.0
(config)#vlan group Group19to21 vlan-list 19,21
```

これらのコマンドは、WLAN を作成し、この WLAN を VLAN グループにマッピングします。

```
(config)#wlan open19 4 open19
(config-wlan)# client vlan Group19to21
(config-wlan)#
```

特定の VLAN にマルチキャスト トラフィックをマッピングする ip multicast vlan コマンドを使用します。

```
(config-wlan)# ip multicast vlan 21
```

コントローラは、WLAN のマルチキャスト トラフィックを処理するために、VLAN 21 インターフェイスを使用します。

（注） 一度マルチキャスト転送をコントローラで設定すると、マルチキャストをサポートするインフラストラクチャも設定する必要があります。

（注） WLC5760 は IGMP v2 を使用します。エンド ユーザがこれを変更するオプションはありません。

ブロードキャスト転送

マルチキャスト転送と同様、ブロードキャスト転送はデフォルトではディセーブルです（コントローラで受信されたブロードキャスト パケットはワイヤレス クライアントに転送されません）。ブロードキャスト転送は VLAN 単位でイネーブルになります。次の一般コマンドを使用して、特定の VLAN のブロードキャスト転送をイネーブルにできます。

```
(config)#wireless broadcast vlan 21
```

特定の VLAN を指定しない場合、すべての VLAN に対してブロードキャスト転送をイネーブルにできます。

```
(config)#wireless broadcast
```

次に、いくつかの VLAN に対するブロードキャスト転送をディセーブルにしてコマンドを制限できます。

```
(config)#no wireless broadcast vlan 20
```

設定の確認

たくさんの方法でマルチキャストを確認できます。コントローラ コンポーネントからは、マルチキャストの状態、ap マルチキャスト モード、および各 VLAN のブロードキャスト/非 IP マルチキャスト状態を表示できます。

```
#show wireless multicast
```

すべて（S、G、および V）の値および対応する MGID 値を表示できます。

```
#show wireless multicast group summary
#show ip igmp snooping
# show ip igmp snooping wireless mgid
```

これらのコマンドはすべて、IPv6 MLD の監視にも使用できます。ip キーワードの代わりに ipv6、および igmp の代わりに mld を使用する必要があります。

```
show ipv6 mld snooping, show ipv6 mld snooping wireless mgid
```

また、すべてのマルチキャスト グループとそれらの稼働中のインターフェイスを表示できます。

```
#show ip igmp groups
```

どの IGMP バージョンが使用され、どのポートがグループに関連づけられているかを確認するには、次のコマンドを使用します。

```
#show ip igmp snooping groups
```

CT5760 へのソフトウェア イメージのインストールおよびアップグレード

1. フラッシュに USB メモリから新しいイメージをコピーします。

```
Controller#copy usbflash0:/ ct5760-ipservicesk9.SSA.03.07.97.EMD.150-7.97.EMD.bin
flash:
Destination filename [ct5760-ipservicesk9.SSA.03.07.97.EMD.150-7.97.EMD.bin]?Copy in
progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
266151060 bytes copied in 36.030 secs (7386929 bytes/sec)
Controller#
```

2. 最初のインストールの場合のみ以下の CLI を使用してフラッシュからのバンドル イメージを展開します。最初のインストールでない場合は、手順 5 を参照してください。

```
Controller#software expand file flash:ct5760-ipservicesk9.SSA.03.07.97.EMD.150-
7.97.EMD.bin verbose
Preparing expand operation
[1]: Expanding bundle flash:ct5760-ipservicesk9.SSA.03.07.97.EMD.150-7.97.EMD.bin
[1]: Copying package files
[1]: Package files copied
[1]: Finished expanding bundle flash:ct5760-ipservicesk9.SSA.03.07.97.EMD.150-
7.97.EMD.bin
```

3. フラッシュから展開したファイルを確認します。

```
Controller#dir flash:
Directory of flash:/
311309-rw-266151060Mar 31 2010 05:58:22 +00:00ct5760-
ipservicesk9.SSA.03.07.97.EMD.150-7.97.EMD.bin
360451-rw-96724320Mar 31 2010 06:00:19 +00:00ct5760- base.SSA.03.07.97.EMD.pkg
360452-rw-1292972Mar 31 2010 06:00:25 +00:00ct5760- drivers.SSA.03.07.97.EMD.pkg
360453-rw-53521356Mar 31 2010 06:00:21 +00:00ct5760- infra.SSA.03.07.97.EMD.pkg
360454-rw-43506528Mar 31 2010 06:00:23 +00:00ct5760-iosd-
ipservicesk9.SSA.150-7.97.EMD.pkg
360455-rw-20646616Mar 31 2010 06:00:22 +00:00ct5760-
platform.SSA.03.07.97.EMD.pkg
360456-rw-50455240Mar 31 2010 6:00:25 +00:00ct5760-
wcm.SSA.03.07.97.EMD.pkg
360450-rw-1208 Mar 31 2010 06:00:36 +00:00packages.conf
```

4. フラッシュからのブートを設定します。

```
Controller#conf t
Controller(config)#boot system flash:packages.conf
Controller(config)#end
Controller#
```

5. 今後のアップグレードのために、次のコマンドを入力します。

```
software install file flash:ct5760-ipservicesk9.SSA.03.08.58.EMP.150-
8.58.EMP3.bin verbose
Preparing install operation ...
[1]: Starting install operation
[1]: Expanding bundle flash:ct5760-ipservicesk9.SSA.03.08.58.EMP.150-
8.58.EMP3.bin
[1]: Copying package files
[1]: Package files copied
[1]: Finished expanding bundle flash:ct5760-ipservicesk9.SSA.03.08.58.EMP.150-
8.58.EMP3.bin
[1]: Verifying and copying expanded package files to flash:
[1]: Verified and copied expanded package files to flash:
[1]: Starting compatibility checks
[1]: Finished compatibility checks
[1]: Starting application pre-installation processing
[1]: Finished application pre-installation processing
[1]: Old files list:
Removed ct5760-base.SSA.03.08.58.EMP1.pkg
Removed ct5760-drivers.SSA.03.08.58.EMP1.pkg
Removed ct5760-infra.SSA.03.08.58.EMP1.pkg
Removed ct5760-iosd-ipservicesk9.SSA.150-8.58.EMP1.pkg
Removed ct5760-platform.SSA.03.08.58.EMP1.pkg
```

```
Removed ct5760-wcm.SSA.03.08.58.EMP1.pkg
[1]: New files list:
Added ct5760-base.SSA.03.08.58.EMP3.pkg
Added ct5760-drivers.SSA.03.08.58.EMP3.pkg
Added ct5760-infra.SSA.03.08.58.EMP3.pkg
Added ct5760-iosd-ipservicesk9.SSA.150-8.58.EMP3.pkg
Added ct5760-platform.SSA.03.08.58.EMP3.pkg
Added ct5760-wcm.SSA.03.08.58.EMP3.pkg
[1]: Creating pending provisioning file
[1]: Finished installing software.New software will load on reboot.
[1]: Committing provisioning file
[1]: Do you want to proceed with reload?[yes/no]:yes
```

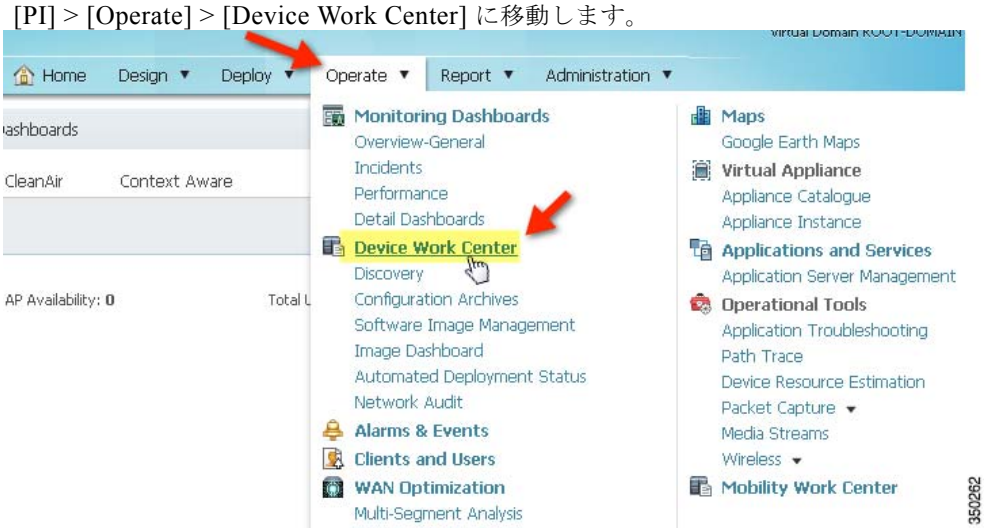
6. システムをリセットします。

Prime への WLC の追加

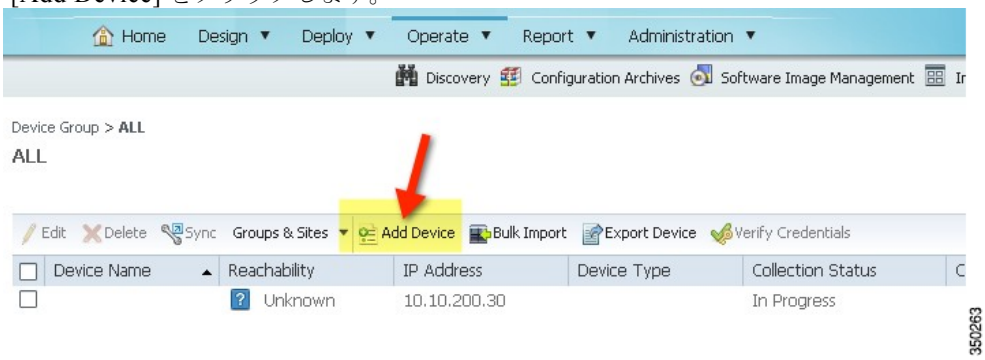
コントローラを追加するには、次の手順を完了してください。

1. CISCO PRIME にログインします。

2. [PI] > [Operate] > [Device Work Center] に移動します。



3. [Add Device] をクリックします。



4. CT5760 の以下のパラメータを入力します。

a. [IP Address] : [CT5760 mgt IP]

b. [Read-Write SNMP string (private)]

c. [Telnet credentials]

5. CISCO PRIME Infrastructure による CT5760 の検出を確認します。到達可能で成功の場合は、正しいデバイス タイプとともにステータスに完了と表示されます。

6. CT5760 を管理する CISCO PRIME Infrastructure の GUI を確認します（[client]、[statistics]、[details]、[reports] など）。

Flexible NetFlow

Cisco IOS® Flexible NetFlow は次世代のフロー テクノロジーです。ネットワーク インフラの最適化を行い、運用コストを削減し、拡大した柔軟性とスケーラビリティによって容量計画およびセキュリティ インシデント検出を改善します。IP トラフィックの特性を明確化し、トラフィックの送信元、宛先、タイミング、アプリケーション情報を特定する機能は、ネットワークの可用性、パフォーマンス、およびトラブルシューティングにとって重要となります。IP トラフィック フローが監視されている場合、容量計画の精度が向上し、リソース配置が組織の目標をサポートできるようにします。Flexible NetFlow は、リソース使用量の最適化、ネットワーク容量の計画、および QoS の最適なアプリケーション層の識別をどのように行うかを決定するために役立ちます。これは、サービス拒否（DoS）攻撃およびネットワークで伝播したワームの検出によってネットワーク セキュリティで重要な役割を果たします。

Flexible NetFlow を設定するコマンドをここに示します。

```
!
flow record IPv4flow
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match flow direction
collect counter bytes long
collect counter packets long
collect timestamp absolute first
collect timestamp absolute last
!
!
flow exporter IPv4export-1
destination 10.1.1.6(IP address of your Netflow Collector.It should be v9
netflow.
transport udp 2055
```

```
!
!
flow monitor IPv4flow (you can view the flows on the switch using CLI if netflow
Collector not available)
description Monitor all IPv4 traffic
exporter IPv4export-1
cache timeout active 30
record IPv4flow
!
```

show コマンドをここに示します。

```
show flow monitor name monitor-name cache
show flow record
show flow-sampler
show flow monitor
```

NetFlow の設定の詳細については、『Cisco Flexible NetFlow Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches)』を参照してください。

CHAPTER 13

QoS の設定

WLC5760 コントローラに Cisco IOS® ソフトウェアを導入することによって、以下の幅広い有線 / ワイヤレス QoS のサポートおよび機能が提供されます。

- モジュラ QoS CLI を介して有線およびワイヤレス QoS の両方の CLI 設定を統一
- AP、SSID、無線、およびクライアントごとの詳細な QoS ポリシー
- AP のワイヤレス クライアント全体への均等な帯域幅割り当て
- ライン レート パフォーマンスを提供する実証済みの Cisco IOS® および ASIC テクノロジーを活用

QoS のイネーブル化

モジュラ QoS CLI モデルに基づいて、QoS は WLC5760 でデフォルトでイネーブルになります。有線ポートからまたは有線ポートへのトラフィックに対するサービス クラス（CoS）または DiffServ コード ポイント（DSCP）の値を変更するためにトラフィックの明示マーキングが必要です。ワイヤレス ポートからワイヤレス ポートへ、またはワイヤレス ポートから有線ポートへのトラフィックは信頼できないものと見なされます。トラフィックが SSID を通過する場合 QoS は全体でイネーブルですが、個別にマーキングまたは信頼される必要があり、そうでない場合は、すべての QoS 値（DSCP、CoS）がデフォルト（0）に設定されます。

QoS の管理

WLC5760 の QoS ポリシーは以下の 2 つの方法でプロビジョニングされます。

- Via CLI
- Via AAA

ここでの設定例では、CLI を使用したポリシーの適用を示します。ポリシーの AAA 設定は、この特定のセクションであとで示します。実際の QoS ポリシーではなく、QoS ポリシー名が AAA サーバから WLC5760 プラットフォームに渡されます。このため、プラットフォームでの QoS の管理に使用されている方法に関係なく、QoS ポリシー設定はプラットフォームに対してローカルである必要があります。

マーキング モデル

WLC5760 では以下の複数のマーキング モデルをサポートします。

- ポート別マーキング（有線）
- クライアント別マーキング（ワイヤレス）
- SSID 別マーキング（ワイヤレス）
- VLAN 別マーキング（有線）

統合ポリシーの観点からは、ポート別およびクライアント別マーキング ポリシーは同義である可能性がありますが、異なったターゲット（ワイヤレス クライアント、物理クライアント ポート）に適用されます。各モデルを次に説明します。

ポート別またはクライアント別のマーキング

Catalyst 4500 と同様、ポート別またはクライアント別のマーキング モデルは UDP/RTP ポート 16384 ～ 32767 上の VoIP と一致します。シグナリング トラフィックは SIP ポート（TCP 5060 ～ 5061）上と同様、SCCP ポート（TCP 2000 ～ 2002）上でも一致します。トランザクションのデータ トラフィックは、さまざまなポートで一致します。Catalyst 3750-E の例とは異なり、暗黙的クラス デフォルトが WLC3850/5760 上でポリシー アクション（マーキングまたはポリシングなど）を実行するため、明示的デフォルト クラスは必要ありません。

! ACL 設定

```
ip access-list extended VOIP
remark Voice
permit udp any any range 16384 32767
ip access-list extended SIGNALING
remark SCCP
permit tcp any any range 2000 2002
remark SIP
permit tcp any any range 5060 5061
permit udp any any range 5060 5061
ip access-list extended TRANSACTIONAL-DATA
remark HTTPS
permit tcp any any eq443
remark ORACLE-SQL*NET
permit tcp any any eq1521
permit udp any any eq1521
remark ORACLE
permit tcp any any eq1526
permit udp any any eq1526
permit tcp any any eq1575
permit udp any any eq1575
permit tcp any any eq1630
permit udp any any eq14002
permit udp any any eq14006
```

! クラス マップ設定

```
class-map match-all VOIP
match access-group name VOIP
class-map match-all SIGNALING
match access-group name SIGNALING
class-map match-all TRANSACTIONAL-DATA
match access-group name TRANSACTIONAL-DATA

! ポート別またはクライアント別入力マーキング ポリシー マップ設定
policy-map PER-PORT-MARKING
class VOIP
set dscp ef
class SIGNALING
set dscp cs3
class TRANSACTIONAL-DATA
set dscp af21
class class-default
set dscp default

! インターフェイスへのポリシー適用
! WLAN OPEN に関連付けられているワイヤレス クライアント
wlan OPEN 2 OPEN
band-select
client vlan 3
ip dhcp server 10.17.1.9 load-balance
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
service-policy client input PER-PORT-MARKING
session-timeout 1800
no shutdown
```

ポリシング モデル

WLC5760 では以下の複数のポリシング モデルを使用できます。

- ポート別ポリシング
- クライアント別ポリシング
- SSID 別ポリシング

ポリシングはさまざまな方法で提供され、クライアント ベースのポリシーのインスタンスで示されるように階層的な方法で使用できます。このインスタンスでは、ポリサーは二方向で使用され、クライアントのトラフィックを集約的にポリシングし、そのクライアントに関連付けられた特定のトラフィック クラス（音声など）もポリシングすることが可能です。

以下は FLAT のポート別またはクライアント別のポリシングの設定例です。

```
! ACL 設定
ip access-list extended VOIP
remark Voice
permit udp any any range 16384 32767
ip access-list extended SIGNALING
remark SCCP
permit tcp any any range 2000 2002
remark SIP
permit tcp any any range 5060 5061
permit udp any any range 5060 5061
ip access-list extended TRANSACTIONAL-DATA
remark HTTPS
permit tcp any any eq443
remark ORACLE-SQL*NET
permit tcp any any eq1521
permit udp any any eq1521
remark ORACLE
permit tcp any any eq1526
permit udp any any eq1526
permit tcp any any eq1575
permit udp any any eq1575
permit tcp any any eq1630
permit udp any any eq14002
permit udp any any eq14006

! クラス マップ設定
class-map match-all VOIP
match access-group name VOIP
class-map match-all SIGNALING
match access-group name SIGNALING
class-map match-all TRANSACTIONAL-DATA
match access-group name TRANSACTIONAL-DATA

! ポート別またはクライアント別入力ポリシング ポリシー マップ設定
policy-map PER-PORT-POLICING
class VOIP
set dscp ef
police 128000conform-action transmitexceed-action drop
class SIGNALING
```

```
set dscp cs3
police 32000conform-action transmitexceed-action drop
class TRANSACTIONAL-DATA
set dscp af21
class class-default
set dscp default
```

! インターフェイスへのポリシー適用

! 二方向で Policing される WLAN OPEN に関連付けられているワイヤレス クライアント

```
wlan OPEN 2 OPEN
band-select
client vlan 3
ip dhcp server 10.17.1.9
load-balance
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
service-policy client input PER-PORT-POLICING
service-policy client output PER-PORT-POLICING
session-timeout 1800
```

以下は階層型のポート別またはクライアント別のポリシングの設定例です。

! ワイヤレス クライアント ポリシー マップ クライアント集約を 2 Mbps に、サブセットとしての音声を 128k に、帯域幅を 32k に Policing

```
policy-map AGG-POLICE
class class-default
police 2000000 conform-action transmit exceed-action drop
service-policy PER-PORT-POLICING
policy-map PER-PORT-POLICING
class VOIP
set dscp ef
police 128000 conform-action transmit exceed-action drop
class SIGNALING
set dscp cs3
police 32000 conform-action transmit exceed-action drop
class TRANSACTIONAL-DATA
set dscp af21
class class-default
set dscp default
```

ワイヤレス キューイング

ワイヤレス キューイングはデフォルトでキューイング ポリシーを提供します。このポリシーは、show run コマンドで表示され、変更できないスタティック トラフィック クラスが含まれています。このクラスはワイヤレス ポートだけに関連付けられた非リアルタイム トラフィックをマルチキャストするために付加されます。ワイヤレス ポートの出力でのキューの追加を可能にするには、スタティック ポリシー マップの port_child_policy は 3 個の追加クラスを含むように変更する必要があります。プライオリティ キューイングはキューの中の 2 つにサポートされ、残りのキューは class-default に設定されます。

次は出力のワイヤレス キューイング ポリシーの例です。

```
policy-map port_child_policy
class non-client-nrt-class
bandwidth remaining ratio 7
class RT1
priority level 1
police 6400000 conform-action transmit exceed-action drop
class RT2
priority level 2
police 19200000 conform-action transmit exceed-action drop
class class-default
bandwidth remaining ratio 63
```

この例では、ポリシーによって集約としてのプライオリティ キュー RT1 および RT2 を表示されているようなレートに Policing される集約に制限します。このポリシーはまた、bandwidth remaining ratio コマンドに関連付けられた帯域幅を追加の非リアルタイム クラスに提供します。使用可能な帯域幅のこの比率は、non-client-nrt（またはマルチキャストおよび非クライアントの非リアルタイム トラフィック キュー）および class-default キューに配信されます。

Wireless Multimedia 設定

Wireless Multimedia（WMM）はトラフィック タイプを 4 つの QoS アクセス カテゴリ、つまりバックグラウンド、ベスト エフォート、ビデオ、および音声に分けます。

```
(config) wlan <your WLAN name> (config-wlan) shutdown
(config-wlan) broadcast
(config-wlan) radio all (to enable this WLAN configuration on both AP radios and all Wi-Fi protocols)
(config-wlan) wmm require
(config-wlan) no security <your Current security setting>
(config-wlan) no shutdown
```

WMM の設定オプションは次のとおりです。

- WMM 必須：WMM 対応クライアントのみ WLAN に結合可能

- WMM オプショナル：非 WMM クライアントおよび WMM 対応クライアントの両方が WLAN に結合可能
  - WMM 対応クライアントは WMM QoS ヘッダーを持つすべてのパケットを送信します。
  - 非 WMM クライアントは WMM QoS ヘッダーを持つパケットを送信しません。

（注）　非 WMM が AP から WMM-QoS ヘッダーを持つパケットを受信できないことに注意してください。

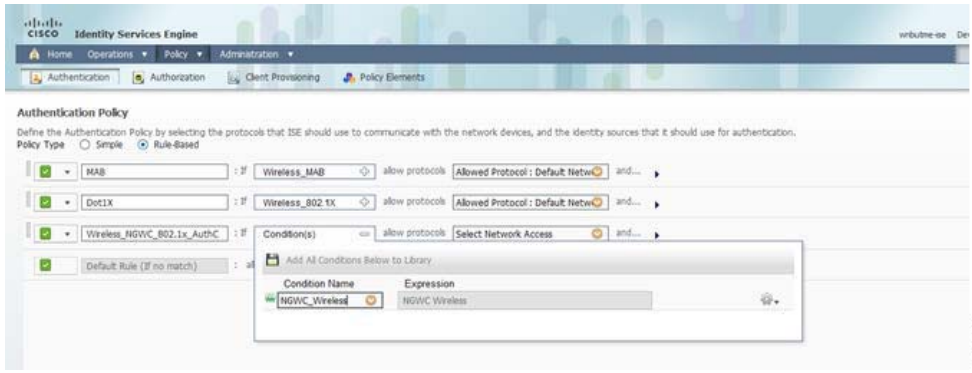
  - 非 WMM クライアントとの間のすべてのパケットはベスト エフォート Wi-Fi チャンネル アクセスで送信されます。

QoS ポリシーの認証およびプッシュのための ISE 設定

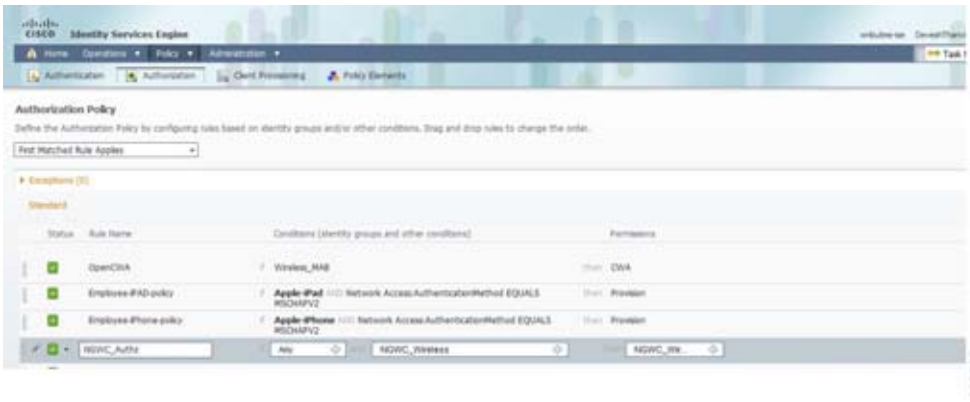
QoS ポリシーを認証しプッシュするには次の手順を実行します。

1. [NAS-Port-Type] が [Virtual] の式で条件を指定します。

2. 認証パラメータを作成します。



3. 承認：結果を定義し、同じ条件を使用します。

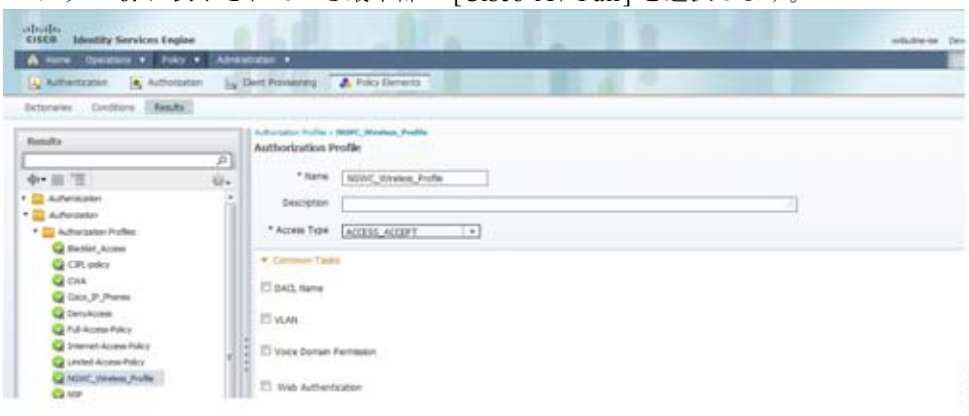


350267

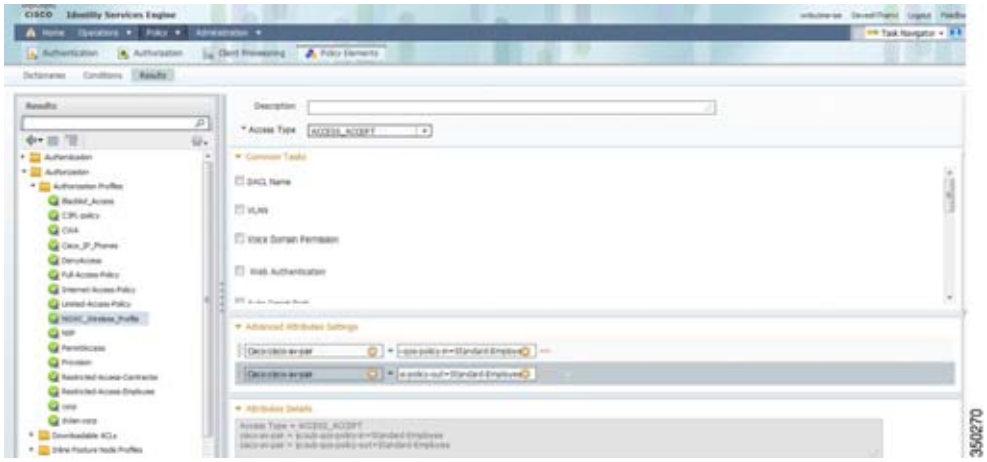
4. [Policy] > [Results] に移動します。

350268

5. ステップ 6. に表示されている最下部の [Cisco-AV-Pair] を選択します。



6. [Advanced Attribute Settings] を「Cisco av-pair name」、「ip:sub-qos-policy-in」、または「ip:sub-qos-polify-out」で修正し、WLC3850/5760 に QoS ポリシーの名前をローカルにつけます。クライアントが関連付けられて認証された場合、ポリシー名が WLC3850/5760 にプッシュされます。



Cisco IOS® ツール コマンド言語スクリプト

WLC5760 コントローラに Cisco IOS® ソフトウェアを導入すると、すぐにコントローラにツール コマンド言語（TCL）スクリプト機能を実装できます。

TCL スクリプト機能に関する詳細については、cisco.com の『Cisco IOS® Scripting with Tcl』ページを参照してください。

©2008 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。
「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)
この資料の記載内容は2008年10月現在のものです。
この資料に記載された仕様は予告なく変更する場合があります。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/