# 室内メッシュの導入ガイド

# 内容

概要 概要 サポート対象ハードウェアおよびソフトウェア 屋内と屋外 コンフィギュレーション コントローラ L3 モード 最新のコードへのコントローラのアップグレード MACアドレス 無線装置への MAC アドレスの記録 コントローラへの MAC アドレスと無線装置の名前の入力 MAC フィルタリングの有効化 L3 屋内メッシュの導入 コントローラのインターフェイスの定義 無線装置のロール ブリッジ グループ名 <u>セキュ</u>リティ設定 設置 前提条件 設置 電力とチャネルの設定 RF チェック 相互接続の確認 AP コンソール アクセス セキュリティ イーサネット ブリッジング ブリッジ グループ名の拡張 ログ:メッセージ、Sys、AP、およびトラップ メッセージ ログ APログ トラップ ログ パフォーマンス スタートアップ コンバージェンス テスト WCS 屋内メッシュ アラーム メッシュ レポートおよび統計情報 リンクテスト ノードツーノ<u>ード リンク テスト</u> オンデマンド AP ネイバー リンク

# <u>概要</u>

Lightweight アクセス ポイント 1242/1131 は、選択された屋内展開用の 2 無線 Wi-Fi インフラス トラクチャ デバイスです。これは、Lightweight アクセス ポイント プロトコル(LWAPP)ベー スの製品です。802.11b/g および 802.11a と互換性のある 2.4 GHz 帯と 5.8 GHz 帯の無線を提供 します。無線の 1 つはアクセス ポイント(AP)のローカル(クライアント)アクセスに使用し 、2 つ目の無線はワイヤレス バックホール用に設定できます。LAP1242/LAP1131 は、P2P、 P2MP、およびメッシュ タイプのアーキテクチャをサポートします。

インストールを開始する前に、このガイドをよくお読みください。

このドキュメントでは、屋内メッシュ向けエンタープライズ ワイヤレス メッシュの導入について 説明します。ワイヤレス エンドユーザは、このドキュメントを読めば、屋内メッシュの基礎、屋 内メッシュを設定する場所、屋内メッシュの設定方法について理解できます。屋内メッシュは、 ワイヤレス コントローラおよび Lightweight AP を使用して導入されたシスコ エンタープライズ ワイヤレス メッシュのサブセットです。

屋内メッシュは、Unified Wireless アーキテクチャに導入されたエンタープライズ メッシュ アー キテクチャのサブセットです。屋内メッシュは、現在人気を集めています。屋内メッシュでは、 無線の 1 つ (通常は 802.11b/g)または有線イーサネット リンクを使用してクライアントに接続 し、2 つ目の無線 (通常は 802.11a)はクライアント トラフィックをバックホール接続に使用で きます。バックホールは、シングル ホップまたは複数のホップで接続されます。屋内メッシュに は、次のようなメリットがあります。

- 各 AP までのイーサネット配線が不要になります。
- AP ごとにイーサネット スイッチ ポートを用意する必要がなくなります。
- 有線では接続を提供できない場所でのネットワーク接続。
- イーサネット スイッチから 100 m の範囲内という制限がないため、柔軟に導入できます。
- アドホック ワイヤレス ネットワークを容易に導入できます。

配線に関するコストの削減と上記の理由から、屋内メッシュは大規模小売店から大きな注目を集 めています。

屋内メッシュは、インベントリスペシャリストが小売店、製造工場、その他の会社の棚卸を行う 際に利用されています。インベントリスペシャリストが望んでいるのは、ハンドヘルド デバイス を使用してリアルタイム接続をできるように、カスタマー サイトに一時的な Wi-Fi ネットワーク を迅速に導入することです。教育セミナー、会議、製造工場、およびホスピタリティ施設は、屋 内メッシュ アーキテクチャが必要となる場所の一例です。

このガイドを最後まで読むと、屋内メッシュの使用場所と設定方法について理解することができ ます。また、NEMA エンクロージャの屋内メッシュが屋外メッシュの代替物でないことを理解で きます。Autonomous AP で使用されるリンク ロールの柔軟性(シングル ホップ メッシュ)に対 する屋内メッシュの優位性についても理解できます。

#### 前提条件:

Cisco Unified Wireless Network、アーキテクチャ、および製品に関する知識があること。シスコ 屋外メッシュ製品およびいくつかのメッシュ ネットワーキング関連用語に関する知識があること

<b>字語一覧</b>

o

頭字語一覧	
LWAPP	Lightweight アクセス ポイ ント プロトコル:AP とワ イヤレス LAN コントロー ラの間のコントロールおよ びデータ トンネリング プ ロトコル。
WLAN コントローラ/コント ローラ/WLC	ワイヤレス LAN コントロ ーラ:大量の管理対象エン ドポイントを単一の統合シ ステムにまとめることで WLAN のネットワーク管理 を一元化および簡素化し、 統合されたインテリジェン ト情報 WLAN ネットワーク システムを実現するシスコ デバイス。
RAP	ルート アクセス ポイント /ルーフ アクセス ポイント : コントローラと他のワイ ヤレス AP の間のブリッジ として動作するシスコのワ イヤレス デバイス。コント ローラに有線接続されてい る AP。
MAP	メッシュ AP:802.11a で RAP または MAP に無線接 続するか 802.11b/g でサー ビス クライアントに無線接 続するシスコのワイヤレス デバイス。
親	802.11a で他の AP への無 線アクセスを提供する AP(RAP または MAP)。
ネイバー	メッシュ ネットワーク上の すべての AP はネイバーで あり、ネイバーを持ちます 。RAP は、コントローラに 有線接続されるため、ネイ バーを持ちません。
 子	コントローラから離れてい る AP は常に子になります 。メッシュ ネットワークで は、子は 1 つの親と複数の ネイバーを持ちます。親が 使用不可能になった場合、 次に容易度の値(ease value)が最も高いネイバー が親として選択されます。

SNR	信号対雑音比(SNR)
BGN	ブリッジ グループ名
EAP	Extensible Authentication Protocol(拡張認証プロト コル)
PSK	事前共有鍵
AWPP	Adaptive Wireless Path Protocol

# <u>概要</u>

Cisco 屋内メッシュ ネットワーク アクセス ポイントは、特定の屋内導入向けの、2 つの無線規格 に対応する Wi-Fi インフラストラクチャ デバイスです。これは、Lightweight アクセス ポイント プロトコル(LWAPP)ベースの製品です。802.11b/g および 802.11a 規格と互換性のある 2.4 GHz 帯と 5.8 GHz 帯の無線を提供します。無線の 1 つ(802.11b/g)はアクセス ポイント (AP)のローカル(クライアント)アクセスに使用し、2 つ目の無線(802.11a)はワイヤレス バックホール用に設定できます。このデバイスは、異なるノード(無線装置)がバックホールを 介して互いに通信しながらローカル クライアント アクセスも提供する、屋内メッシュ アーキテ クチャを提供します。この AP は、ポイントツーポイントおよびポイントツーマルチポイント ブ リッジング アーキテクチャにも使用できます。ワイヤレス屋内メッシュ ネットワーク ソリュー ションは、高いデータ レートと信頼性を最小のインフラストラクチャで実現できるため、大規模 な屋内カバレッジに最適です。この製品の最初のリリースで導入された主要な基本的特徴を次に 示します。

- ・ホップカウントが3の屋内環境向け。最大4。
- ・リレー ノードとエンドユーザ クライアントのホスト。802.11a 無線はバックホール インタ ーフェイスとして使用され、802.11b/g 無線はクライアントへのサービス用に使用されます。
- •屋内メッシュ AP のセキュリティ: EAP および PSK がサポートされます。
- メッシュ環境内の LWAPP MAP は、イーサネットに接続した AP と同じようにコントローラ と通信します。
- ポイントツーポイント無線ブリッジング。
- ポイントツーマルチポイント無線ブリッジング。
- 最適な親の選択。SNR、EASE、および BGN
- BGN の機能拡張。ヌルおよびデフォルト モード。
- ローカル アクセス。
- •ブラックリストへの親の登録。除外リスト。
- AWPP による自己修復。
- イーサネット ブリッジング。
- •4.0 リリースからの音声の基本サポート。
- 動的周波数選択。
- アンチ ストランド: default BGN および DHCP フェールオーバー。
- **注:次の機**能はサポートされません。
  - 4.9 GHz パブリック セーフティ チャネル
  - •干渉を避けるルーティング
  - バックグラウンド スキャン
  - ユニバーサル アクセス

・ワーク グループ ブリッジのサポート 屋内メッシュ ソフトウェア

屋内メッシュ ソフトウェアは、屋内 AP、特に屋内メッシュに対象が絞られている特殊なリリー スです。このリリースでは、屋内 AP は、ローカル モードとブリッジ モードの両方で動作します 。4.1.171.0 リリースに導入されている一部の機能はこのリリースに実装されていません。コマン ドライン インターフェイス(CLI)、グラフィカル ユーザ インターフェイス(GUI:Web ブラウ ザ)に加え、ステート マシン自体に機能拡張が加えられています。これらの機能拡張の目的は、 この新しい製品および機能の実行性に関してユーザの視点から貴重な情報を得ることにあります 。

屋内メッシュに固有の機能拡張:

- ・屋内環境:屋内メッシュは、LAP1242およびLAP1131を使用して実装されます。これらは、 イーサネットケーブルが使用できない屋内環境で実装されます。簡単かつ迅速に実装でき、 建物内のリモート エリア(たとえば、集配送センター、教育用セミナーまたは会議、製造工 場、ホスピタリティ施設)へのワイヤレス カバレッジを提供できます。
- ブリッジ グループ名(BGN)の機能拡張:ネットワーク管理者が屋内メッシュ AP のネット ワークをユーザによって指定されたセクターに編成できるように、ブリッジ グループ名 (BGN)と呼ばれるメカニズムが用意されています。BGN(実際はセクター名です)により 、AP は、同じ BGN を持つ他の AP に接続します。BGN と一致する適切なセクターを検出で きない場合、AP は、デフォルト モードで動作し、デフォルト BGN に応答する最適な親を選 択します。この機能は、取り残された AP 条件(BGN の設定に誤りがある場合)に対処でき るため、すでに現場から高い評価を得ています。4.1.171.0 ソフトウェア リリースでは、デ フォルト BGN が使用されている AP では屋内メッシュ ノードとして動作せず、クライアン ト アクセスも提供しません。コントローラ経由でアクセスすると AP はメンテナンス モード になります。管理者が BGN を修正しない場合、AP は 30 分後にリブートします。
- ・セキュリティの機能拡張:屋内メッシュ コードのセキュリティは、デフォルトで EAP(拡張) 認証プロトコル)用に設定されます。 これはRFC3748で定義されています。EAPプロトコル は無線LANに限定されず、有線LAN認証に使用できますが、無線LANで最も一般的に使用さ れます。802.11a/b/g ワイヤレス アクセス ポイントなどの 802.1X 対応 NAS ( ネットワーク アクセス サーバ)デバイスによって EAP が起動されたとき、最新の EAP 方式では、セキュ アな認証メカニズムを提供して、クライアントと NAS の間でセキュア PMK(ペアワイズ マ スター キー)をネゴシエートできます。この PMK は、(AES ベースの)TKIP または CCMP 暗号化を使用するワイヤレス暗号化セッションに使用できます。4.1.171.0 より前のソ フトウェア リリースでは、屋外メッシュ AP は PMK/BMK を使用してコントローラに参加し ていました。このプロセスには、3 つのサイクルが含まれていました。現在はサイクル数が 減り、より高速なコンバージェンスが可能になりました。屋内メッシュ セキュリティの全体 的な目標は、次のことを実現することにあります。セキュリティのプロビジョニングに関す るゼロ タッチの設定。データ フレームのプライバシーおよび認証。ネットワークとノード間 の相互認証。屋内メッシュ AP ノードの認証のために標準 EAP 方式を使用する機能。 LWAPP と屋内メッシュ セキュリティの切り離し。新しいセキュリティ プロトコルをサポー トするうえで必要な要素に対応するために、検出、ルーティング、および同期メカニズムが 現在のアーキテクチャから機能拡張されています。屋内メッシュ AP は、他のメッシュ AP からの gratuitous ネイバー更新をスキャンおよびリスニングして他のメッシュ AP を検出し ます。ネットワークに接続されている任意の RAP または屋内 MAP は、(802.11 ビーコン フレームと似た)NEIGH\_UPD フレーム内でコア セキュリティ パラメータをアドバタイズし ます。このフェーズが終了すると、屋内メッシュ AP とルート AP の間に論理リンクが確立 されます。

•WCSの機能拡張屋内メッシュアラームが追加されました。ホップカウント、最悪 SNR条件などの情報を示す屋内メッシュレポートを生成できます。非常にインテリジェントな情報を示すリンクテスト(親から子、子から親)をノード間で実行できます。従来よりもはるかに多くの AP 情報が表示されます。潜在的なネイバーを表示することもできます。ヘルスモニタリングが改善され、アクセスしやすくなりました。

# <u>サポート対象ハードウェアおよびソフトウェア</u>

屋内メッシュの最小ハードウェア要件およびソフトウェア要件を次に示します。

- Cisco LWAPP AP である AIR-LAP1242AG-A-K9 および AIR-LAP1131AG-A-K9 は、屋内メッシュ設定をサポートします。
- Cisco Mesh Release 2 ソフトウェアは、エンタープライズ メッシュ(屋内および屋外製品)をサポートします。 このソフトウェアは、Cisco コントローラ、Cisco 440x/210x、およびWISM にのみインストールできます。
- Cisco Enterprise Mesh Release 2 ソフトウェアは、Cisco.com からダウンロードできます。

# <u>屋内と屋外</u>

屋内メッシュと屋外メッシュの間には、次のような顕著な違いがあります。

	屋内メッシュ	屋外メッシュ			
環境	屋内のみ。屋内用の ハードウェア	屋外のみ。頑丈な ハードウェア			
ハードウェア	LAP1242 および LAP1131AG を使用 する屋内 AP	LAP15xx および LAP152x を使用す る屋外 AP			
電力レベル	2.4 GHz:20 dbm、 5.8 GHz:17 dbm	2.4 GHz:28 dbm、5.8 GHz:28 dbm			
セル サイズ	約 46 m	約 305 m			
実装の高さ	地面から約 3.6 m	地面から 9 ~ 12 m			

# <u>コンフィギュレーション</u>

新しいハードウェアを使用する場合は特に、実装を開始する前にこのガイドをよく読んでください。

## <u>コントローラ L3 モード</u>

屋内メッシュ AP は、L3 ネットワークとして導入できます。

Image: Control       Montrol       Montrol       Montrol       Montrol       Montrol       Manual         Costroll       Controll       Controll       BitD.A: None       Controll       Manual       Manua					
Controller         General         Converting Works         Converting Works         Approximation           General Investionsy         B00.2x (fairs Canned Mode Califier View)         Convert Operating Mode is Laver(3)         Convert Operating Mode is Laver(3)         Convert Operating Mode is Laver(3)           Date Faces         LAD Phale on next about         Convert Operating Mode is Laver(3)         Convert Operating Mode is Laver(3)         Convert Operating Mode is Laver(3)           Date Faces         Brance Multicast Mode         Convert Operating Mode is Laver(3)         Convert Operating Mode is Laver(3)           Note Tall CHCP Surver         Brance Multicast Mode         Convert operating Mode is Laver(3)         Convert operating Mode is Laver(3)           Portin         Porting Mode (Califier View)         Convert operating Mode is Laver(3)         Convert operating Mode is Laver(3)           Reserver Kausset         Port in Early Porting         Convert operating Mode is Laver(3)         Convert operating Mode is Laver(3)           Reserver Kausset         Port in Early Early Port in Early Ea	cisco	MONITOR WARNS CONTRALER	WHELESS SECURITY	NUMBER CONTRACT	SegeConfiguration (Eng. Lagout Beheah
General Investory     802.3 r firer Cartord Rode     Cartord Rode     Cartord Rode       Marce Cartord Rode     Cartord Rode     Cartord Rode     Content Operating Rode is Layer3)       Marce Cartord Rode     Cartord Rode     Cartord Rode     Cartord Rode       Marce Cartord Rode     Cartord Rode     Cartord Rode     Cartord Rode       Marce Cartord Rode     Cartord Rode     Cartord Rode     Cartord Rode       Marce Cartord Rode     Cartord Rode     Cartord Rode     Cartord Rode       Marce Cartord Rode     Cartord Rode     Cartord Rode     Cartord Rode       Marce Cartord Rode     Cartord Rode     Cartord Rode     Cartord Rode       Marce Cartord Rode     Cartord Rode     Cartord Rode     Cartord Rode       Marce Cartord Rode     Appresive Load Briancing     Cartord Rode     Cartord Rode       Marce Cartord Rome     Appresive Load Briancing     Cartord Rode     Cartord Rode       Marce Cartord Rome     Appresive Load Briancing     Cartord Rode     Cartord Rode       Marce Cartord Rome     Appresive Load Briancing     Cartord Rode     Cartord Rode       Marce Cartord Rome     Appresive Load Briancing     Cartord Rode     Cartord Rode       Marce Cartord Rome     Appresive Load Briancing     Soci     Cartord Rode       Marce Cartord Rode     Particle     So	Controller	General	Process Second		Apply
	General Inventory Interfaces Network Roats Internal OHCE Server Mobility Management Spanning Trees Ports Mater Controller Mote Network Time Protocol 9 QoS 9 CDP	603.3x New Cantrol Mode CAR Mole on next whoot Exame Multicast Mode Broandoat Porwarding Aggressive Ledd Brilancing Prev or two Stroking Hove Over The Air Provisioning of AP AP Failback Apple Talk Bridging Part SSC thange Dafaalt Mobility Donasn Name Rd-Researk Name User 3/8 Timeout (seconds) Avor Inmost (seconds) Avor Inmost (seconds) Avor Inmost (seconds) Stock Rafus Authentication 802.3 Bridging Operating Environment InternalTemp Alam Limits	Deabled V Liver 3 V Deabled V	(Current Operating Mode is Laver2) (LAG Hode is currently disabled).	

## <u>最新のコードへのコントローラのアップグレード</u>

#### 次のステップを実行します。

- 1. 屋内メッシュ ネットワークの Mesh Release 2 をアップグレードする場合は、4.1.185.0 ま たは Mesh Release 1(Cisco.com で入手可能)で、ネットワークを運用している必要があ ります。
- 2. コントローラの最新のコードをお使いの TFTP サーバにダウンロードします。コントローラ の GUI インターフェイスから、[Commands] > [Download file] をクリックします。
- 3. ファイル タイプで [code] を選択し、TFTP サーバの IP アドレスを指定します。ファイルの パスと名前を定義します。

cisco	HONITOR WLANS CONTROLLER	WIRLESS SCURTY NUMARHENT COMMINS HELP	Saya Configuration 1 Brig Laguat Bafrish
Commands	Download file to Controller		Clear Downlaad
Download File UploadFile Reboot	/ile Type TFTP Server	Code	
Reset to Factory Default Set Time	19 Julium Hacimur retries Timeut becondo) (* Rise Retri	10.13.05.48 10 6 // ) // ) // ) // )	

注:32 MBを超えるファイルサイズの転送をサポートするTFTPサーバを使用してください。例えば、tftpd32. File pathの下に"./"と入力します。

4. 新しいファームウェアのインストールが終了したら、CLI で show sysinfo コマンドを使用して、新しいファームウェアがインストールされていることを確認します。

0	Cisco Controller) >show sysinfe	
	anufacturer's Name. roduct Name roduct Version. TOS Version. ootloader Version. uild Type.	Cisco Systems Inc. <u>Cisco Cont</u> roller <u>4.1.175.19</u> 4.0.206.0 DATA + WPS
	ystem Name ystem Location. ystem Contact. ystem ObjectID. P Address. ystem Up Time.	CiscoImesD 1.3.6.1.4.1.14179.1.1.4.3 10.13.10.20 1 days 22 hrs 3 mins 35 secs
COHM	onfigured Country. perating Environment. Internal Temp Alarm Limits. Internal Temperature.	US - United States Commercial (0 to 40 C) 0 to 65 C +38 C
NN I ZMZ	tate of 802.11b Network tate of 802.11a Network -More or (g)uit umber of MLANS rd Party Access Point Support umber of Active Clients	Enabled Enabled 2 Disabled 3
BUUDEE	urned-in WAC Address. rypto Accelerator 1. rypto Accelerator 2. ower Supply 1. ower Supply 2.	00:18:73:34:48:60 Absent Absent Absent Present, OK

**注:公式に**は、コントローラのダウングレードはサポートされていません。

## <u>MAC アドレス</u>

MAC フィルタリングは必ず使用する必要があります。この機能により、真の「ゼロ タッチ」の Cisco 屋内メッシュ ソリューションが実現されました。 以前のリリースとは異なり、メッシュの 画面には MAC フィルタリング オプションはありません。

cisco	HONITOR MLANI CONTRILLER MIRELESS SECURITY MUNAGHENT COMMANS HELI	SayaConfiguration Bing Logout Bahash
Wireless	Mesh	Apply
Access Publits     Al JPs     Cados     Class     Class     Class     Class     Class     Class     Class     B0211a/n     B0211a/n     B0211a/n     Coatry     Tlears	Constraint Range (CostAP to RepAAP) I.2000 Avet Backhail Clant Access C thebed Security Mode Cost Access C the W Authentication Mode Local Auth 14	

注:MACフィルタリングはデフォルトで有効になっています。

## 無線装置への MAC アドレスの記録

ネットワークに導入するすべての屋内メッシュ AP 無線装置の MAC アドレスをテキスト ファイ ルに記録します。MAC アドレスは、AP の背面に示されています。ほとんどの CLI コマンドでは コマンドとともに AP の MAC アドレスまたは名前を入力する必要があるため、MAC アドレスを 記録しておくと将来テストを行うときに役立ちます。また、「建物番号-ポッド番号-AP タイプ : MAC アドレスの最後の 4 桁の 16 進文字」のように、AP の名前をより覚えやすい名前に変更 することもできます。

### コントローラへの MAC アドレスと無線装置の名前の入力

Cisco コントローラは、屋内 AP 認証 MAC アドレス リストを保持します。コントローラは、認 証リストに含まれている屋内無線装置からの検出要求のみに応答します。ネットワークで使用す るすべての無線装置の MAC アドレスをコントローラに入力します。

コントローラの GUI インターフェイスで、[Security] に移動し、画面の左側の [MAC filtering] を クリックします。次の図に示すように、[New] をクリックし、MAC アドレスを入力します。

cisco	MONITOR	W.ANE	CONTROL	ER WIRELESS	SICURITY	MONAGEMENT	Sage Co COMMANDS	nfiguration	Ping	Logaut   <u>B</u> efresh
Security	NAC Filte	ring						A	pply	New
- AAA Ceneral	RADIUS Co Node	ompatibi	ity Cisco	ACS .						
RADIUS     Authentication     Accounting	MAC Delin	niter	No De	limiter 💌						
TACACS+ LDAP	Local MA	C Filters						Items 1	to 6	of 6
MAC Filtering	NAC Addre		WLAN ID	Interface		Descriptio	n			
Disabled Chients User Login Policies	00:0h:85:5	::h5:20	n	management		MAP1				
AP Policies	C0:0b:85:5	:fa:60	0	management		Map2				
In Local EAP	(0+0h+85+5)	0.05-1.0	0	management		R 491				
Priority Order	(0:0b:85:5	5:ff:50	0	management		MAP3				
► Access Control Lists	10:0b:85:60	5:29:60	0	management						
▶ IPSec Certificates	(0:0b:05:6)	5:34:40	0	management		Indoor Rag	1			
wireless Protection Policies										
▶ Web Auth										
♦ CIDS										

さらに、[Description] に無線装置の名前(ロケーション、AP 番号など)を入力します。 この説 明は、いつでも簡単に参照できるように、無線装置が設置されている場所を示すためにも使用で きます。

### MAC フィルタリングの有効化

MAC フィルタリングはデフォルトで有効になります。

同じページで、セキュリティ モードとして EAP または PSK を選択することもできます。

スイッチの GUI インターフェイスから、次のパスを使用します。

GUI インターフェイスのパス: [Wireless] [Indoor Mesh]

CLI では、次のコマンドでのみセキュリティ モードをチェックできます。

(Cisco Controller) > **show network** 

RF-Network Name.       iMesh meD Mode.       Disable         Secure Web Mode.       Enable         Secure Web Mode.       Enable         Secure Shell (ssh)       Enable         Ethernet Milticast Mode.       Disable         Ethernet Broadcast Mode.       Disable         User Idle Timeout.       300 seconds         ARP Idle Timeout.       300 seconds         ARP Unicast Mode.       Disable         User Idle Timeout.       300 seconds         ARP Unicast Mode.       Disable         User Idle Timeout.       300 seconds         ARP Unicast Mode.       Disable         User Via Winelers Interface.       Disable         Bridge Security Mode.       Enable         Bridge Security Mode.       EAF         Mesh Hullicast Mode.       BOI: 1b/g/n         Mesh Full Sector DFS.       Enable         Disable       Dicable         Mode Talk       Disable         Apple Talk       Disable         Mode Talk       Enable         Mode Talk       Enable         Scourty Mode       EAF         Enable       Boisble         Bridging On Default       Boisble         Bridge Security Mode       Enable<	(Cisco Controller) >show network	
	RF-Network Name. meb Mode. Secure web Mode. Secure shell (ssh) Talmat. Ethernet Multicast Mode. Ethernet Broadcast Mode. User Idle Timeout. ARP Unle Timeout. ARP Unleast Mode. Cisco AP Default Master. Mget Via Wireless Interface. Gridge MAC filter Config. Bridge Scurity Mode. Mesh Full Sector DFS. Dver The Air Provisioning of AP S. Mobile Peer to Peer Blocking. Apple Talk. AP Fallback Moreor (g)uit web Auth Redirect Ports. Fast SSID Change. 802. 3 Bridging.	iMesh Disable Enable Enable Disable Mode: Ucast Disable Mode: Ucast Disable Of seconds Disable Disable Disable Enable Enable Enable Enable Enable Enable Enable Enable Enable Enable Enable Enable Enable Disable Disable Enable Enable Disable Disable Disable Disable Disable Disable Enable Enable Disable Disable Enable Disable Disable Enable Disable Disable Disable Disable Disable Disable Disable Disable Disable Disable Disable Disable Disable Disable Disable Disable Disable

## <u>L3 屋内メッシュの導入</u>

L3 屋内メッシュ ネットワークで DHCP サーバ(内部または外部)を使用しない場合は、無線装置の IP アドレスを設定します。

L3 屋内メッシュ ネットワークで DHCP サーバを使用する場合は、コントローラを L3 モードで 設定します。設定を保存し、コントローラをリブートします。DHCP サーバのオプション 43 を 必ず設定してください。コントローラを再起動した後、新しく接続された AP は、DHCP サーバ から IP アドレスを受け取ります。

<u>コントローラのインターフェイスの定義</u>

AP マネージャ

L3 の導入の場合は、AP マネージャを定義する必要があります。AP マネージャは、コントロー ラから AP への通信のソース IP アドレスとして動作します。

Path: [Controller] > [Interfaces] > [ap-manager] [edit]

	ahaha					
	CISCO	NONITOR WLANS	CONTROLLER WIRELESS	SECURETY	MANAGEMENT	COMMANDS HELP
¢	ontroller	Interfaces				
	General	Interface Name	VLAN Identifier	P Address	Interface	Type Dynamic AP Management
	Investory C	No. of Lot of Lo	untagged	31.13.10.21	Static	Enabled
	Interfaces	menagement	untagget	31.13.10.20	Static	Not Supported
	Network Routes	200,000,000	N/A	112.168.1.10	Static (	Not Supported
	Internal DIICPServer	xitted	N/A	11-1-1	Ohatie	Net Supprised
	<b>Hobility Management</b>					
	Spasning Tree					
	Ports					
	Master Controller Hode					
	Network Time Protocol					
	Qu5					
,	CDP					

AP マネージャ インターフェイスには、管理インターフェイスと同じサブネットおよび VLAN 内の IP アドレスを割り当てる必要があります。

									Logout Befre
CISCO	MONITOR WL	ANS CON	HOLLER WIRELESS	BECORITY	MANAGEMENT	COMMANDS	HELP		
Controller	Interfaces > 0	Edit						< Back	Apply
General Inventory	General Infor	mation							
Network Routes	Interface Nam MAC Address	-	ap-managar 00:18:73:34:46:63						
Hobility Management	Interface Add	Ireas							
Spanning Tree	YLAN Identifie	$\geq$	0						
Ports	1P Address		10.13.10.21						
Master Controller Mode	hetmask		255.255.255.0						
Network Time	Galeway		10.13.10.10						
▶ Quối	Physical Infor	rmation							
+ CDP	Port Number		1						
	Backup Port		0						
	Advice Port		1						
	Enable Dynam Hanagement	ie AP							
	DHCP Informe	ation							
	Primary DHCP	Server	10-13-10-10						
	Secondary DH	ICP Server							
	Access Contro	of List							
	ACL Name		none w.						
	Note: Changing 5 temporarity disat some chants.	he Interface I Net and thus	anameters causes the technology result in loss of com	Afte to be ectivity for					

## <u>無線装置のロール</u>

このソリューションにおける無線装置の主なロールには、次の2つがあります。

 ルート アクセスポイント(RAP): (スイッチ経由での)コントローラへの接続に使用する 無線装置は、RAPのロールが与えられます。RAPは、LWAPPに対応した接続により、コン トローラに有線接続されます。RAPは、任意のブリッジングまたは屋内メッシュネットワー クの親ノードとなります。コントローラは、1 つ以上の RAP を持つことができ、それぞれの RAP が同じワイヤレス ネットワークまたは異なるワイヤレス ネットワークの親として機能 します。同じ屋内メッシュ ネットワークに複数の RAP を配備して、冗長性を確保すること もできます。

 ・屋内メッシュ アクセス ポイント(MAP):コントローラへの有線接続を持たない無線装置 は、屋内メッシュ AP としてのロールが与えられます。この AP は、以前はポールトップ AP と呼ばれていました。MAP は(バックホール インターフェイスを介して)他の MAP へのワ イヤレス接続を保持し、最終的に RAP とコントローラに接続されます。また、MAP は、 LAN への有線イーサネット接続を保持し、(P2P または P2MP 接続を使用して)その LAN のブリッジ エンドポイントとしての役割を果たすこともできます。 イーサネット ブリッジ として適切に設定されている場合は、この動作を同時に実行できます。MAP は、バックホー ル インターフェイス用に使用されていない帯域上のクライアントにサービスを提供します。
 AP のデフォルト モードは MAP です。

**注:無線**の役割は、GUIまたはCLIを使用して設定できます。ロールを変更すると、AP はリブートします。

**注:コントローラ**CLIを使用して、APがスイッチに物理的に接続されている場合、またはスイッチ上のAPをRAPまたはMAPとして表示できる場合は、AP上の無線ロールを事前設定できます。

(Cisco Controller) >config ap role ?

rootAP RootAP role for the Cisco Bridge. MeshAP MeshAP role for the Cisco Bridge.

(Cisco Controller) >config ap role meshAP ?

<Cisco AP> Enter the name of the Cisco AP.

(Cisco Controller) >config ap role meshAP LAP1242-2

Changing the AP's role will cause the AP to reboot. Are you sure you want to continue? (y/n)

### <u>ブリッジ グループ名</u>

ブリッジ グループ名(BGN)は、AP の関連付けを制御します。BGN を使用して無線装置を論理 的にグループ分けしておくと、同じチャネルにある 2 つのネットワークが相互に通信することを 防止できます。この設定はまた、同一セクター(領域)のネットワーク内に複数の RAP がある 場合にも便利です。 BGN には最大 10 文字までの文字列を指定できます。

製造段階で、工場出荷時のブリッジ グループ名が割り当てられます(ヌル値)。 この値は表示さ れません。したがって、BGN を定義しない場合でも、無線装置はネットワークに参加できます。 同一セクターのネットワーク内に(より大きなキャパシティを得るために)RAP が 2 つある場合 は、別々のチャネルで 2 つの RAP に同じ BGN を設定することをお勧めします。

注:ブリッジグループ名は、コントローラのCLIとGUIから設定できます。

(Cisco Controller) >config ap bridgegroupname set ?

<bridgegroupname> Set bridgegroupname on Cisco AP.

BGN を設定すると、AP はリセットされます。

注:BGNは稼働中のネットワークで非常に慎重に設定する必要があります。最も遠い距離にある ノード(末端のノード)から開始し、RAP に向かって設定してください。その理由は、マルチホ ップの途中から BGN の設定を開始すると、このポイントの先にあるノードは異なる BGN(古い BGN)を持つことになり、ドロップされるためです。

BGN を確認するには、次の CLI コマンドを発行します。

(Cisco Controller) > show ap config general

(Cisco Controller) >show ap config general RAP1242	2
Cisco AP Identifier	0
Cisco AP Name	RAP1242
Country code	US - United States
Regulatory Domain allowed by Country	802.11bg:-AB 802.11a:-A2
AP Country code	US - United States
AP Regulatory Domain	802.11bg:-A 802.11a:-A
Switch Port Number	1
MAC Address	00:18:74:fa:7d:1f
IP Address Configuration	DHCP
IP Address	10.13.13.11
IP NetMask	255.255.255.0
Gateway IP Addr	default legation
Cisco AP Location	default_oroup
Drimary Circo Switch	12106-1
Consider Circo Switch	32100-1
Tertiary Cisco Switch	
Administrative State	ADMIN ENABLED
Operation State	REGISTERED
Mirroring Mode	Disabled
AP Node	Bridge
Mare or (g)uit	orroge
AP Role	ROOTAP
Ethernet Bridging	Enabled
Bridge GroupName	test123
Public Safety	Disabled
Remote AP Debug	Disabled
S/W Version	4.1.175.19
Boot Version	12.3.7.1
Mini IOS Version	3.0.51.0
Stats Reporting Period	180
LED State	Enabled
POE Pre-Standard Switch	Disabled
PoE Power Injector MAC Addr	Disabled
AD Nodel	2 ATD-1 AD1 242AC-A-VO
AP MODEL	12 4(20070808-082741)
Deset Button	Enabled
AD Conjal Number	ETV10358304
AP Serial Number	Manufacture Tostalled
Management Frame Protection Validation	Disabled
Console Login Name	015401cu
Console Login State	Unknown
AP Up Time.	0 days, 02 h 43 m 38 s
AP LWAPP Up Time	0 days, 02 h 42 m 43 s
More or (q)uit	
Join Date and Time	Sun Aug 19 11:59:07 2007
Join Taken Time	0 days, 00 h 00 m 24 s
Ethernet Port Duplex	Unknown
Ethernet Port Speed	Unknown

BGN は、コントローラ GUI を使用して設定または確認することもできます。

Path: [Wireless] > [All APs] [Details]

I	cisco	HONITOR WEARS CONTROLLER APPELLESS SECURITY HUMAGEMENT COMMINGS HELP	Segn Configuration ( ) proj Logust ( ) pri
ſ	Wireless	All APs> Details for RAP1242	< Back Apply
	* Access Points	General Inventory Interfaces Mish Advanced	
	<ul> <li>Ratios</li> <li>802.11a/s</li> <li>802.11b/g/r</li> <li>AP Declaration</li> </ul>	AP Role LookAP V Bridge Type Shdar San San San San San San San San San San	
I	Mesh	Ethernet Bridging 😥	
	Rogues Clients	Becihaul Interfece III2.11e Bridge Data Rae (Mbps) 1e w	
	> 80211a/n > 80211b/s/n	Heater Status V/A Smanal Temperature V/A	
	Country Timers		

この新しいリリースでは、AP の環境情報も表示されます。

# <u>セキュリティ設定</u>

デフォルトの屋内メッシュ セキュリティ モードは EAP です。つまり、コントローラ上でこれら のパラメータを設定しないと、MAP は参加しません。

	0 10 0 CISCO	Rowelds Real Comparties Waterso Securit Milwerkerus Clauserso unti-	Say Configurains   Sing   agent Baland
	Wireless	Mosh	Apple
l	* Access Points	Enternal	
	<ul> <li>Relice</li> <li>NE3.35***</li> <li>N23.110**</li> <li>At Configuration</li> </ul>	Range (Russill for Health?) [1000   See	
	Heb	Security	
	<ul> <li>Repose</li> <li>Climits</li> <li>B03.114/m</li> </ul>	Beauly Hale Authentication Hice	
	+ BOJ_118/g/s		
	Timers		

#### 屋内メッシュの EAP 設定 CLI

(Cisco Controller) >config mesh local-auth enable enable Local Auth (Cisco Controller) >config advanced eap ? identity-request-timeout Configures EAP-Identity-Request Timeout in seconds. identity-request-retries Configures EAP-Identity-Request Max Retries. key-index Configure the key index used for dynamic WEP (802.1x) unicast key (PTK). max-login-ignore-identity-response Configure to ignore the same username count reaching max in the E AP identity response request-timeout Configures EAP-Request Timeout in seconds. request-timeout Configures EAP-Request Timeout in seconds.

PSK モードを保つ必要がある場合は、次コマンドを使用して PSK モードに戻します。

(Cisco Controller) >config mesh security psk ? (Cisco Controller) >config mesh security psk All Mesh AP will be rebooted Are you sure you want to start? (y/N)n

#### 屋内メッシュの EAP の show コマンド

EAP モードのときは、次の show コマンドを使用して MAP 認証を確認できます。

(Cisco Controller) >show network	
RF-Network Name	jaggi123 Disable
Secure Web Mode	Enable Enable
Ethernet Multicast Mode	Disable Mode: Mcast 224.1.1.1
User Idle Timeout. ARP Idle Timeout.	300 seconds 300 seconds
ARP Unicast Mode. Cisco AP Default Master	Disabled Disable
Mgmt Via Dynamic Interface	Disable
Bridge Security Mode Mesh Multicast Mode	EAP otherwise PSK 802.11b/g/n
Mesh Full Sector DFS. Over The Air Provisioning of AP's	Enable Enable
Mobile Peer to Peer Blocking AP Fallback Web Auth Redirect Ports	Enable 80
More or (q)uit Fast SSID Change	D1sabled
802.3 Bridging	Disable

(Cisco Controller) >**show wlan 0** 

(Cisco Controller) >show wlan 0

	WLAN Identifier	0
	Drofile Name	Mesh profile
	Notwork Name (SSTD)	Mosh_srid
	Vectoric Maile (3310)	Disabled
	status	Disabled
	MAC Filtering	Disabled
	Broadcast SSID	Enabled
	AAA Policy Override	Disabled
	Number of Active Clients	2
	Exclusionlist Timeout	60 seconds
	Carrien Timoout	1800 seconds
	Session Theorem.	1000 Seconds
	Interface	management
	WLAN ACL	unconfigured
	DHCP Server	Default
l	DHCP Address Assignment Required	uisabled
	Duality of Service	Silver (best effort)
	MM	Allowed
	CCV AinopotTo Support	Englished
	CCX - Aironette Support	Enabled
	CCX - Gratuitous ProbeResponse (GPR)	Disabled
	Dot11-Phone Mode (7920)	Disabled
	Wired Protocol	None
	Mare or (a)uit	
	IPv6 Support	Disabled
	Padio Policy	411
	ocal EAD Authortication	Enabled (Profile JacfWap1500) ]SAuth021)
	LOCAT EAP AUCHENCICACION	Enabled (Profile primaP1500LIEAUCI95
	security	
	802.11 Authentication:	Open System
	Static WEP Keys	Disabled
	802 1X	Disabled
	Wi-Ei Drotostad Accass (WDA/WDA2)	Enabled
	UNA (CON TO)	Displad
	WPA (SSN 1E)	Disabled
	WPAZ (RSN IE)	Enabled
	TKIP Cipher	Disabled
	AES Cipher	Enabled
		Auth Key Management
	802.1x	Enabled
	PSK	Disabled
		Disabled
	CCRM	Disabled
	CKIP	Disabled
	IP Security Passthru	Disabled
	Web Based Authentication	Disabled
	web-Pass through	Disabled
	Conditional web Redirect	Disabled
	Auto Anchon	Disabled
	-Mere or (a)uit	Ursaureu
	- More- or (q)ure	Direction of the second s
	H-REAP Local Switching	Disabled
	Infrastructure MFP protection	Enabled (Global Infrastructure MFP Disabled)
	Client MFP	Optional
	Tkip MIC Countermeasure Hold-down Timer	60
	Mobility Anchor List	
	WI AN TO TO Addross Status	

(Cisco Controller) >show local-auth config

(Cisco Controller) >show advanced eap

屋内メッシュの EAP の debug コマンド

EAP モードのすべての問題をデバッグするには、コントローラで次のコマンドを使用します。

(Cisco Controller) >debug dot1x all enable (Cisco Controller) >debug aaa all enable

# 設置

### <u>前提条件</u>

コントローラで推奨バージョンのコードが実行されている必要があります。ソフトウェア バージョンを確認するには、[Monitor] をクリックします。CLI を使用してソフトウェア バージョンを確認することもできます。

Cisco Controller) >show sysinfe
anufacturer's Name
vstem         CiscoImesh           vstem         Contact
onfigured CountryUS - United States perating EnvironmentCommercial (0 to 40 C) nternal Temp Alarm Limits
tate of 802.11b Network Enabled tate of 802.11a Network Enabled -More or (g)uit umber of MLANS
urned-in WAC Address

DHCP サーバ、ACS サーバ、WCS サーバなどのシステムに到達可能である必要があります。

## <u>設置</u>

 管理 IP アドレスと同じサブネット上のレイヤ 3 ネットワークにすべての LAP(1131AG/1242AG)を接続します。すべての AP は、ローカル モードの AP としてコ ントローラに参加します。このモードで、プライマリ コントローラ名、セカンダリ コント ローラ名、およびターシャリ コントローラ名を使用して AP をプライミングします。

ahaha							Logout Sefresh
CISCO	MONITOR WLANS CONTROL	LLER WIRELESS S	ECURITY	MANAGEMENT COMMANDS H	ELP		
Wireless	AI APs > Details for API01	9.2f7e.3b02				< Back	Apply
* Access Points	General Inventory 1	nterfaces Advance					
Radios	Coneral			Versions			
802.11b/p/n	AP Name	AP0019.2/7e.3602		W Version	4.1.175.19		
Mach	Location	default location		Boot Version	12.37.1		
> Romes	Ethernet MAC Address	0013H2f17e130102	]	105 Version	12.4(20070709)172245		
Clients	Base Radio MAC	00:13:74:fb:27:60	1	Mini 105 Version	3.0.51.0		
> 802.11a/n	Status	Fnalls W		IP Config			
E 802.11b/o/o	CAP Mode	loca v		AP IP Address	10.13.10.47		
Country	Operational Status	REG		AP Static IP			
Timers	Port Number	1					
	Primary Controller Name	Ciscilmesh		Time Statistics			
	Secondary Controller Name			UP Time			
	Tertiary Controller Name			Controller Associated Time			
				Controller Association Latercy			
	Fardware Reset		Set to Fa	actory Defaults			
	Perform a hardware reset on Reset AP how	this AP	Clear default	configuration on this AP and reset it to ear Config	o factory		

- 2. AP のベース無線 MAC アドレス(たとえば、00:18:74:fb:27:60)をキャプチャします。
- 3. AP をブリッジ モードで参加させるために、AP の MAC アドレスを追加します。
- 4. [Security] > [MAC-filtering] > [New] をクリックします。
- 5. コピーした MAC アドレスを追加し、MAC フィルタ リストおよび AP リストに AP を指定 します。
- 6. [AP Mode] リストから [Bridge] を選択します。

cisco	MONITOR WANN CONTRO	LLAR WIRELESS S	FOLIETY	мульскиемт сумналась н	F,D	Sage Configuration   Eng	Ligout Briresh
Wireless Access Points Al APy Radios BOL.116/1	All APs > Details for AP00 General	19.217e.3502 Interfaces Advance	N	Versions		< Back	Apply
<ul> <li>acconfiguration</li> <li>result</li> <li>Request</li> <li>Clients</li> <li>B02.11a/r</li> <li>B02.11b/g/n</li> <li>Country</li> <li>Timers</li> </ul>	AP Name Locaton Ethernet MAC Address Base Radio MAC status AP Node Operational Status Port Rumber Primary Controller Name Secondary Costroller Name Tertiary Controller Name	Atoo19-279-3802 defeuit location Oct29121794130-02 Exable V local V local V local V Ropue Detector South	Setto Fa	S/W Version Boot version IOS Version Mixi DS Version IP Cents AP 1F Address AP 548tic SP Time Statistics UP Time Controller Associated Time Controller Association Latency Ctery Defaults	4.1.175.19 12.3.7.1 12.4(20070709:172245) 3.0.51.0 10.13.10.47		
	Perform a hardware reset or Reset APNew	this AP.	Dear o default	configuration on this AP and reset it to s	a lactory		

7. AP のリブートを確認するプロンプトが表示されます。

Micro	soft Internet Explorer 🛛 🔀
2	Warning: Changing AP Mode will reboot the AP. Are you sure you want to continue
	OK Cancel

 AP がリブートし、ブリッジ モードでコントローラに参加します。新しい AP ウィンドウには、追加の[MESH] タブが表示されます。[MESH] タブをクリックして、ロール、ブリッジ タイプ、ブリッジ グループ名、イーサネット ブリッジング、バック ホール インターフェイス、ブリッジ データ レートなどを確認します。

altalta cisco	MUNITOR MEANS CONTROLLER WHELESS SECURITY MEANSCHENT COMMANDS HELP	Saya Configuration Eing Logout Eefresh
Wireless	All APs > Details for NAP4	< Back Apply
Access Points     Al APs     Radios     802.11a/n     802.11b/g/n     AP Configuration	AP Role Bridge Type Bridge Group Name Bridge Gro	
Presite	Etherset Bridging	
Ropues	Backhaul Interface 002.11s	
Clients	Bridge Bate Rote (Phpp) 2+ -	
> 802.11a/r	Heater Status N/A	
> 802.11b/g/m Country	Internal Temperature	
Timers		

- 2. このウィンドウでは、AP ロール リストにアクセスし、適切なロールを選択します。この場合のデフォルトのロールは MAP です。[Bridge Group name] はデフォルトで空白になっています。バック ホール インターフェイスは 802.11a です。ブリッジ データ レート(つまり、バック ホール データ レート)は 24 Mbps です。
- 10. 目的の AP を RAP としてコントローラに接続します。目的の場所に無線装置(MAP)を導入します。無線装置の電源を入れます。コントローラ上のすべての無線装置を確認できます。 (Cisco Controller) >show ap summ

Number of APs			3			
AP Name	Slots	AP Model	Ethernet MAC	Location	Port	Country
RAP1242	2	AIR-LAP1242AG-A-K9	00:18:74:fa:7d:1f	default location	1	US
LAP1242-1	2	AIR-LAP1242AG-A-K9	00:1b:2b:a7:ad:bf	default location	1	US
LAP1242-2	2	AIR-LAP1242AG-A-K9	00:14:1b:59:07:af	default location	1	US

- 11. ノード間にラインオブサイトの状態を作るようにします。ラインオブサイトの状態が存在 しない場合は、フレネル ゾーン の空間を作り、ニアラインオブサイトの状態にします。
- 12. 同じ屋内メッシュ ネットワークに複数のコントローラが接続されている場合は、各ノード のプライマリ コントローラの名前を指定する必要があります。それ以外の場合、最初に識 別されたコントローラがプライマリとなります。

#### <u>電力とチャネルの設定</u>

RAP にはバックホール チャネルを設定できます。MAP は、RAP チャネルに合わされます。ロー カル アクセスは、MAP とは無関係に設定できます。

スイッチの GUI から、次のパスに従って移動します。[Wireless] > [802.11a radio] [configure]

cisco	HONITOR MUNIC CONTROLLER WHELESS	RCURITY HANAGERINE OPHIANDS HELP	Siye Configuration   Brg   Logo
Wireless	802.11a/s Cisco APs > Configure		< Back Ap
* Access Points	General	kF Backhoul Channel Assignment	
AP Configuration	AP Neme RAP1242 Admin Status Enable M Operational Source V <sup>a</sup>	Current Drahmel 56 Assignment Method O Gilgar In curron 56	
> Rogers	11n Parameters	Tx PowerLevel Assignment	
Clients > 80213a/m	Lin Supported No	Current Ix Power Level 6 Announced Mathematica	
> 80211b/g/m	Antenna	Coder A M	
Country Timors	Antenna Type External M Diversity Enailed M	Performance Profile	
	Artenna Jain 3 x 0.5 dli	View and edit Performance Profile for this AP Performance Profile	
	Management Frame Protection		
	Version Supported 1	Initial Charging any of the parameters causes the Radio Tube removements allesided and linus may result in fee of community for	
	Protection Capability All Pannes	some chero.	
	Validation Capability All Parmes		
	WLAN Override		
	WLAN Override disable 💌		

**注:バックホール**のデフォルトTx電力レベルは最高レベル(レベル1)で、Radio Resource Management(RRM)はデフォルトでオフです。

RAP を併置している場合は、各 RAP で代替隣接チャネルを使用することをお勧めします。これ により、同一チャネル干渉を低減できます。

# <u>RF チェック</u>

屋内メッシュ ネットワークでは、ノード間の親子関係を確認する必要があります。**ホップ**は、2 つの無線装置間のワイヤレス リンクです。親子関係は、ネットワーク内を移動するのに応じて変 化します。親子関係は、屋内メッシュ ネットワーク内の場所に依存します。

ワイヤレス接続(ホップ)においてコントローラにより近い無線装置が、ホップの他の側にある 無線装置の親となります。マルチホップ システムでは、コントローラに接続されているノードが RAP(親)となる、ツリー型構造があります。 第 1 ホップの反対側の隣接するノードは子となり 、第 2 ホップ以降の後続のノードはその特定の親の**ネイバー**となります。

#### 図1:2つのホップからなるネットワーク



図 1 では、わかりやすくするために AP 名が示されています。次のスクリーン ショットでは、 RAP(fb:10) が調査されています。このノードは、(実際の導入における)屋内メッシュ AP(fa:60 および b9:20)を子として識別し、MAP ff:60 をネイバーとして識別しています。

スイッチの GUI インターフェイスから、次のパスに従って移動します。[Wireless] > [All APs] > [Rap1] [Neighbor Info]。

		$\frown$	Sa <u>v</u> e Con	figuration   <u>Ping</u>   Logcut   <u>R</u> efresh
CISCO	MONITOR WLANS CONTRO	LLER WIRELESS SECURITY	MANASEMENT COMMANDS	15 CP
Winless	All APs > Rap1 > Neighbo	r Info		< Back
- Anne Balaka	Mesh Type	AP Name/Radio Mac	Base Radio Mac	
* Access Points All APs	Child	Mapl	00:05:85:5C:89:20	
<ul> <li>Radios</li> <li>802.11a/n</li> </ul>	Chid	Map2	00:05:85:5F:FA:60	
802.11b/g/n	Default Neighbor	Map3	00:05:85:5F:FF:60	
<ul> <li>AP Configuration</li> <li>None</li> </ul>				
Mesh				

屋内メッシュ ネットワークの親子関係が確立され、適切に保持されていることを確認します。

#### <u>相互接続の確認</u>

show Mesh は、ネットワーク内の相互接続を確認するための情報表示コマンドです。

これらのコマンドを各ノード(AP)でコントローラ CLI を使用して実行し、結果を Word ファイ ルまたはテキスト ファイルでアップロード サイトにアップロードする必要があります。

(Cisco Control)	ler) >show mesh ?
env	Show mesh environment.
neigh	Show AP neigh list.
path	Show AP path.
stats	Show AP stats.
secbh-stats	Show Mesh AP secondary backhaul stats.
per-stats	Show AP Neighbor Packet Error Rate stats.
queue-stats	Show AP local queue stats.
security-stats	Show AP security stats.
config	Show mesh configurations.
secondary-backl	naul Show mesh secondary-backhaul
client-access	Show mesh backhaul with client access.
public-safety	Show mesh public safety.
background-scar	ming Show mesh background-scanning state.
cac	Show mesh cac.

屋内メッシュ ネットワーク内で、マルチホップのリンクを選択し、RAP を出発点としてこれら のコマンドを発行します。コマンドの結果をアップロード サイトにアップロードします。

次の項に示す、すべてのコマンドは、図 1 の 2 つのホップからなる屋内メッシュ ネットワークに 対して発行されています。

#### Show Indoor Mesh Path

このコマンドは、MAC アドレス、ノードの無線装置のロール、アップリンク/ダウンリンク (SNRUp、SNRDown)の信号対雑音比(dB)、および特定のパスのリンク SNR(dB)を表示 します。

d = 1										
(Cisco Controller)	) >show me	esh pati	n RAP1242							
AP Name/Radio Mac	Channel	Snr-Up	Snr-Down	Link-Snr	Flags	State				
RAP1242 is a Root AP. (Cisco Controller) >show mesh path LAP1242-2										
AP Name/Radio Mac	Channel	Snn-Up	Snn-Down	Link-Snr	Flags	State				
LAP1242-1 RAP1242	56 56	29 41	29 32	27 34	0x86b	UPDATED UPDATED	NEIGH	PARENT	BEACON	
RAP1242	is a Root	t AP.	52		01000	0104120	HE LON	T THE TH	DENCON	

#### <u>屋内メッシュ ネイバーのサマリーの表示</u>

このコマンドは、MAC アドレス、親子関係、およびアップリンク/ダウンリンク SNR(dB)を表示します。

(Cisco Controller)	>show me	sh neig	gh ?						
detail Show summary Show (Cisco Controller)	v Link ra v Link ra >show me	ate neig ate neig esh neig	gh detail. gh summary gh summar	/. ry RAP1242	2				
AP Name/Radio Mac	Channel	Snr-Up	Snr-Down	Link-Snr	Flags	State			
LAP1242-2 LAP1242-1	56 56	0	0 33	00	0x860 0x960	BEACON CHILD BEACON			
(Cisco Controller) >show mesh neigh summary LAP1242-1									
AP Name/Radio Mac	Channe1	Snr-Up	Snr-Down	Link-Snr	Flags	State			
LAP1242-2 RAP1242	56 56	30 43	29 46	28 31	0×961 0x86b	UPDATED CHILD BEACON UPDATED NEIGH PARENT BEACON			

これで、ネットワークのノード間の関係を表示したり、各リンクの SNR 値を表示して RF 接続を 確認したりできます。

# <u>AP コンソール アクセス セキュリティ</u>

この機能により、AP のコンソール アクセスのセキュリティが強化されます。この機能を使用するには、AP 用のコンソール ケーブルが必要です。

次の項目がサポートされています。

•	指定した	APにユー	ーザ ID とノ	パスワート	ヾの組み合わ	っせをプッ	ッシュする	らため	の CLI。	
	(Cisco	Control	ler) >com	nfig ap	username	Cisco	, passwor	d Ci	sco ?	
	all <cisco< th=""><th>AP&gt;</th><th>Configur Enter th</th><th>res the ne name</th><th>Username, of the C</th><th>/Passwo isco AP</th><th>rd for</th><th>a11</th><th>connected</th><th>APs.</th></cisco<>	AP>	Configur Enter th	res the ne name	Username, of the C	/Passwo isco AP	rd for	a11	connected	APs.

ユーザ名とパスワードの組み合わせをコントローラに登録されているすべての AP にプッシュするための CLI コマンド。

(Cisco Controller) >config ap username Cisco password Cisco all

これらのコマンドを使用することにより、コントローラからプッシュされたユーザ ID とパスワー ドの組み合わせを AP のリロード後も保持できます。AP をコントローラからクリアした場合、セ キュリティ アクセス モードはありません。AP は、ログインが成功すると SNMP トラップを生 成します。AP は、コンソールへのログインが 3 回続けて失敗した場合も SNMP トラップを生成 します。

# <u>イーサネット ブリッジング</u>

セキュリティ上、デフォルトでは MAP でイーサネット ポートがディセーブルになっています。 イネーブルにするには、RAP およびその MAP でイーサネット ブリッジングを設定しなければな りません。

結果として、イーサネット ブリッジングは次の 2 つのシナリオに対してイネーブルにする必要が あります。

•屋内メッシュ ノードをブリッジとして使用する場合。

イーサネット ポートを使用して MAP 上の任意のイーサネット デバイス (PC/ラップトップ、ビデオ カメラなど)を接続する場合。

Path: [Wireless] > 任意の AP をクリック > [Mesh]



ブリッジングを行うノード間の距離を設定するための CLI コマンドがあります。ホップごとにビ デオ カメラなどのイーサネット デバイスを接続し、パフォーマンスを確認してみてください。

# <u>ブリッジ グループ名の拡張</u>

意図していない「ブリッジ グループ名」を使用して AP が不適切にプロビジョニングされる場合 があります。ネットワーク設計によって、この AP では、正しいセクターまたはツリーに到達し て見つけることができない場合もあります。互換性のあるセクターに到達できない場合は、AP が取り残される可能性があります。

**そのような取り残された AP を回復するために、3.2.xx.x コードでは「default」というブリッジ グループ名の概念が導入されました。**基本的な概念としては、設定されたブリッジ グループ名を 使用して他のどの AP にも接続できない AP は、ブリッジ グループ名として「default」という単 語を使用して接続を試みます。3.2.xx.x 以降のソフトウェアが実行されているすべてのノードは 、このブリッジ グループ名を持つ他のノードを受け入れます。

この機能は、新しいノードや不適切に設定されているノードを稼働中のネットワークに追加する 場合にも役立ちます。

稼働中のネットワークがある場合は、異なる BGN を持つ事前設定済みの AP をネットワークに 参加させます。この AP の MAC アドレスをコントローラに追加すると、この AP で「default」の BGN が使用されていることがコントローラに表示されます。 (CiscoController) > show mesh path Map3:5f:ff:60

00:0B:85:5F:FA:60 state UPDATED NEIGH PARENT DEFAULT (106B), snrUp 48, snrDown 4 8, linkSnr 49 00:0B:85:5F:FB:10 state UPDATED NEIGH PARENT BEACON (86B), snrUp 72, snrDown 63, linkSnr 57 00:0B:85:5F:FB:10 is RAP

ahaha						Sa <u>v</u> e Co	nfiguration	<u>Ping Logcut R</u> efresh
cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Wireless	All APs > Rap1 > N	eighber Info						< Back
- Accors Balats	Mesh Type		AP Name/	Radio Mac	Base R	adio Mac		
All APs	Chid		Map1		00:05:8	5:5C:89:20		
	Chid		Map2		00:05:8	5:5F:FA:60		
802.11b/g/n = NP Configuration = None	Default Neighbor		Map3		00:06:8	5:5F:FF:60		
Mesh								
Rogues								
Clients								
▶ 802.11a/n								
▶ 802.11b/g/n								
Country								
Timers								

default BGN を使用している AP は、クライアントを関連付けて屋内メッシュの親子関係を形成 する、通常の屋内メッシュ AP として動作することができます。

default BGN を使用しているこの AP が適切な BGN を持つ別の親を検出すると、その親への切り 替えが行われます。

# <u>ログ:メッセージ、Sys、AP、およびトラップ</u>

## <u>メッセージ ログ</u>

メッセージ ログのレポート レベルを有効にします。コントローラ CLI から次のコマンドを発行 します。

(Cisco Controller) >config msglog level ?

critical	Critical hardware or software Failure.
error	Non-Critical software error.
security	Authentication or security related error.
warning	Unexpected software events.
verbose	Significant system events.

(Cisco Controller) >config msglog level verbose

メッセージ ログを表示するには、コントローラ CLI から次のコマンドを発行します。

(Cisco Controller) >show msglog

Message Log Severity Level .... VERBDSE which no AP was configured from 00:0F:B5:93:71:E7 on port 0. Fri Jul 8 06:12:02 2005 [ERROR] spam\_radius.c 93: spamRadiusProcessResponse: A P Authorization failure for 00:0b:85:0e:04:80 Fri Jul 8 05:40:15 2005 [ERROR] spam\_tmr.c 501: Did not receive hearbeat reply from AP 00:0b:85:0e:05:80 8 05:38:45 2005 [ERROR] spam\_lrad.c 1310: Validation of Config Request Fri Jul failed from AP 00:0b:85:0e:05:80 8 05:38:40 2005 [ERROR] spam\_lrad.c 1310: Validation of Config Request Fri Jul failed from AP 00:0b:85:0e:14:00 8 05:38:40 2005 Previous message occurred 5 times Fri Jul 8 05:33:54 2005 [ERROR] spam\_lrad.c 1310: Validation of Config Request Fri Jul failed from AP 00:0b:85:0e:05:80 8 05:32:23 2005 [ERROR] poe.c 449: poeInitPowerSupply : poePortResync Fri Jul returned FAILURE Fri Jul 8 05:32:17 2005 [ERROR] dhcpd.c 78: dhcp server: binding to 0.0.0.0 [ERROR] rrmgroup.c 733: Airewave Director: 802.11a swi Fri Jul 8 05:32:17 2005 tch group reset 8 05:32:16 2005 [ERROR] rrngroup.c 733: Airewave Director: 802.11bg sw Fri Jul itch group reset Fri Jul 8 05:32:16 2005 Previous message occurred 2 times 8 05:31:19 2005 [CRITICAL] osapi\_sem.c 794: Error! osapiMutexTake cal Fri Jul

メッセージ ログをアップロードするには、コントローラ GUI インターフェイスを使用します。

1. [Commands] > [Upload] をクリックします。

սիսիս							Sa <u>v</u> e Co	nfiguration Ping	Logcut <u>R</u> efresh
CISCO	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Commands	Downloa	d file to (	Controller					flear	Download
Dovinload File	File Type			Code					
Rebaut	TFTP Serv	er							
<b>Reset to Factory Default</b>	IP Addres	15		10.51.1.5	Ł				
Set Time	Maximum	retries		10					
	Timeout (	seconds)		6					
	file Path			J					
	file Name			AS_4200	4_1_122_51	h+6			

 2. TFTP サーバの情報を入力します。このページでは、アップロードに関するさまざまなオプションと、送信するファイルを選択できます。メッセージ ログイベント ログトラップ ログクラッシュ ファイル(存在する場合)クラッシュ ファイルの有無をチェックするには、 [Management] > [Controller Crash] をクリックします。



## <u>AP ログ</u>

コントローラの該当する GUI ページに移動し、AP ログをチェックしてローカル AP の情報を探 します(該当する場合)。

Cance Sections						-	Save Configuratio	n   Ping   L	ogout Refresh
A. A.	MONITOR	WJANS	CONTROLLER	WIRELES:	s securativ	MANAGEMENT COM	MANDS HELP		
Management	AP Log In	formation							
Summary	AP Nemc			AP ID	MAC Address	Admin Status	Operational States	Port	
SNNP General SNMP V3 Users Communities Trap Deceivers Trap Controls Trap Logs HTTP Telret-SSH Serial Port Local Management Users Hicer Sections Syslog Mgmt Via Wireless Message logs Tech Support System Resource Information Costroller Crash APLon	Fap3:Sfff:	60		25	00:0b:85:5f:H:60	Enable	REG	1	Get

# <u>トラップ ログ</u>

コントローラの該当する GUI ページに移動し、トラップ ログをチェックします。

Croco Sverens									nfiguration	Ping Logout Refresh
▲ A.	MONT	TOR	W.ANe	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Management	Trap	Logs								Clear Log
Summary	Num	ber of	Traps sir	ce last reset	1208					
SNNP	5um	ber of	Traps su	ce log last viev	ved 1208					
SMP V3 Users Communities	Log	Syste	m Time	Тгар						
Trap Receivers	0	Tue M- 18:58:	ar 7 51 2006	Rogue AP: 0 Interface no	0:05:85:1e:53 :1(802.115/g	:66 detecte ) with RSSI:	d on Base Radio N -66 and SNR: 19	AC : CO:0b:85	5f:ft:10	
Trop Loga	1	Tos M. 18:58:	51 2006	Rogue AP: 0 Interface no	0:05:05:14:53	:66 detecte ) with RSSI:	d on Base Radio M -79 and SNR: 11	AC : CO:0b:05	5c:b9:20	
нттр	2	Tue M. 18:58:	ar 7 51 2006	Rogue AP: 0 Interface no	0:05:85:17:48	df detected	on Base Radio No -78 and SNR: 12	AC:00:0b:85:	5c:b9:20	
Telret-354 Serial Dort	3	Tue M. 18:58:	ar 7 51 2006	Rogue AP: 0 Interface no	0:02:8a:5E:46	:f2 detected ) with RSSI:	on Base Radio Na -85 and SNR: 3	AC:00:0b:85:	5c:b9:20	
Local Management	4	Tue M.	ar 7 51 2006	Rogue AP: 0 Interface no	0:05:85:17:03	4d detecte	d on Base Radio M -80 and SNR: 11	AC : CO:Ob:85	:5c:b9:20	
Users	5	Tue Ma	ar 7 51 2006	Rogue AP: 0	0:05:85:11:49	8d detecte	d on Base Radio N -82 and SNR: 9	AC : CO:0b:85	5c:b9:20	
Liser Sessions Susion	6	THE PL	ar / 51 2006	Rogue AP : U	0100185111149	ath RSSI:	d on Base Kadio M	AC   COLODIRS	5009120	
Mont Via Wireless	7	Tue Ma	ar 7	Rogue AP: 0	0:40:96:a1:61	:Za detecte	d on Base Radio M	AC : CO:0b:85	:5c:b9:20	
Message logs	8	Tue Ma	ar 7	Rogue : 00:4	0:94:a2:7d:c2	removed fr	om Base Radio M	AC:00:05:85:5	5c:b9:20	
Tech Support	9	Tue M.	40 2006 ar 7	Rogue : 00:00	5-81-15-68-5e	renoved fr	om Jase Radio M	LC + 00:0b:85:	Scib5:20	
Information	10	Tue M	ar 7	Rogue : 00:1	3:5f:55:ea:06	removed fr	om Base Radio MA	C:00:0b:85:5	c:b9:20	
AP Log	11	18:58: Tue M	152006 ar 7	Rogue : 00:01	1(802.116/g b:85:17:9c61	removed fr	om Base Radio M	AC : 00:05:85:5	5f:fb:10	
	-	18:58: Tue N.	ar 7	AP Disassici	ated. Base Br	die MAC-80	0h-65-56-66-60			
	13	Tue M	10 2006	ar's Interfor		Speration	state Dowr: Base	Radio MAC:00	0b:85:5f:ff	60
	14	18:58; Tue N	102006 ar 7	AP's Interfac	beat Timeou e-0(802.11a)	t Operation (	State Dumi: Base	Radio NAC-00	ob.ea.af.ff	0.0
		18:58: Tue M	10 2006 ar 7	Cause=Heart	beat Timeout	t.	about the sec			
	15			AP DISASSICI	ated, Base Ra	DOLCHAC(00)	00:05:51:14:60			

# <u>パフォーマンス</u>

# <u>スタートアップ コンバージェンス テスト</u>

コンバージェンスは、次に示すように、最初に起動されてから WLAN コントローラとの間で安定 した LWAPP 接続を確立するまでの、RAP/MAP による所要時間です。

コンバージェンス テスト	コンバ <sup>.</sup> )	ージェン	ѵ時間(∶	分:秒
	RAP	MAP1	MAP2	MAP3
イメージのアップグレー ド	2:34	3:50	5:11	6:38
コントローラのリブート	0:38	0:57	1:12	1:32
屋内メッシュ ネットワー クの電源投入	2:44	3:57	5:04	6:09
RAP リブート	2:43	3:57	5:04	6:09
MAP の再参加		3:58	5:14	6:25
親(同じチャネル)の MAP の変更		0:38		

# <u>WCS</u>

## <u>屋内メッシュ アラーム</u>

WCS は、コントローラからのトラップに基づいて、屋内メッシュ ネットワークに関連するこれ らのアラームおよびイベントを生成します。

- Poor Link SNR
- Parent Changed
- Child moved
- MAP Changes parent frequently
- Console port event
- MAC Authorization failure
- Authentication failures
- Child excluded Parent

[Mesh Links] をクリックします。屋内メッシュ リンクに関連するすべてのアラームが表示されます。

ahaha	Wireless Control System	Username: root   Lopout   Tefresh   Writ Vew
CISCO		
Andrew Second	R Server Depart Compet Concert Barrier Bar	
	INC. 3 NOTE	Ed. 1906 Ed. Contents
Name of Contractions	General Client Security Hish	
Secondary	Enventory Detail Mahas Count	
New Search Saved Startden Ook «Selec Search» &		
	Ceverage Ansas 🖂 Recent (overage tales (g)	8
	Name Tutul AN AGO DO Radio Clerks Assess fulnt Interface Clerks Clerks	
	Building2) 4 4 4 0 0 No Coverage Holes found	
	View All Head	
	Total APs not yet assigned to Maps : 3	
Alarm Tummary 9 Ropus of Coverage mote Sacurds Canona finds Local finds Local finds Local finds Local finds Local finds Local finds Local finds Local finds Local finds		

次のアラームは、屋内メッシュ リンクに適用されます。

- Poor link SNR: このアラームは、リンクの SNR が 12 db を下回ると生成されます。ユーザ はこのしきい値を変更できません。子または親のバックホール リンクで低い SNR が検出さ れると、トラップが生成されます。このトラップには、SNR 値と MAC アドレスが含まれま す。アラームの重大度は Major です。信号強度が高いだけでは受信側のパフォーマンスを良 好に保つことはできないため、信号対雑音比(SNR)は重要です。着信信号は、発生する雑 音や干渉のどれよりも強力でなくてはなりません。たとえば、干渉が強かったり雑音レベル が高かったりすると、信号強度が高くても無線のパフォーマンスが下がることがあります。
- Parent changed : このアラームは、子が別の親に移動したときに生成されます。親との関連 付けが失われると、子は別の親に参加し、前の親と新しい親の両方の MAC アドレスを含む トラップを WCS に送信します。アラームの重大度:情報。
- Child moved:このアラームは、子のロストトラップをWCSが受け取った場合に生成されます。親APが子との関連付けを失ったことを検出し、子との通信ができなくなると、子のロストトラップをWCSに送信します。このトラップには、子のMACアドレスが含まれます。アラームの重大度:情報。

- MAP parent changed frequently: このアラームは、屋内メッシュ AP が親を頻繁に変えた場合に生成されます。MAP の親変更カウンタが指定期間の間にしきい値を超えると、WCS にトラップを送信します。このトラップには、MAP の変更回数とその期間が含まれます。たとえば、2 分間に 5 回の変更があるとトラップが送信されます。アラームの重大度:情報。
- Child Excluded Parent:このアラームは、子が親をブラックリストに登録したときに生成されます。子は、コントローラでの認証試行が一定回数失敗すると、親をブラックリストに登録できます。子は、ブラックリストに登録された親を記憶し、子がネットワークに参加するときに、ブラックリストに登録された親のMAC アドレスとブラックリストへの登録期間を含むトラップを送信します。

屋内メッシュ リンク以外のアラーム:

- Console Port Access: コンソール ポートを使用すると、ユーザ名とパスワードを変更して、 取り残された屋外 AP を回復できます。ただし、AP への認証されたユーザ アクセスをすべ て防ぐために、WCS は、他ユーザがログインを試みるたびに、アラームを送信する必要があ ります。屋外に配置されている AP は物理的に脆弱なため、保護の目的でこのアラームが必 要になります。このアラームは、ユーザが正常に AP のコンソール ポートにログインした場 合、または続けて3回ログインに失敗した場合に生成されます。
- MAC Authorization Failure:このアラームは、屋内メッシュに参加しようとした AP が、 MAC フィルタ リストに登録されていないために認証に失敗したときに生成されます。WCS は、コントローラからトラップを受信します。トラップには、認証に失敗した AP の MAC ア ドレスが含まれます。

### メッシュレポートおよび統計情報

4.1.185.0 からの強化されたレポートおよび統計情報フレームワークが引き継がれています。

- No Alternate Path
- Mesh Node Hops
- Packets error Stats
- Packet Stats
- Worst Node Hop
- Worst SNR Links

abab	Wireless Control System Username: root   Logout   Refresh   Print W							
CISCO	Monitor - Reports -	<u>C</u> osfigure - Los	ation • <u>A</u> dministration •	Help -				
Mesh Reports	Mesh No Alternate	Parent			Select a command 💌 GO			
Nesh No Alternate Parent	Report Title	Schedule	Last Run Time	Next Scheduled Run				
Mesh Node Hops	C test	Disabled			Rur Now			
Mesh Packet Error Stats								
Mesh Packet Stats								
Mesh Worst Node Hops								
Mesh Worst SNRLinks								
Alarm Summary 🔍								
Roque AP 0 191 Coverage Hole 0 Security 0 0 0								
Controllers 0 0 0 Access Points 0 0 2								
Mesh Links 0 0 0 Location 0 0 0								

#### No Alternate Path

通常、屋内メッシュ AP は複数のネイバーを持ちます。屋内メッシュ AP が親との関連付けを失った場合、AP は代替の親を検出できます。ネイバーが示されていない場合に親との関連付けを 失うと、AP はどの親にも接続できなくなる場合もあります。そのため、代替の親を持たない AP を知っておくことはユーザにとって重要です。このレポートには、現在の親以外にネイバーを持 たないすべての AP が示されます。

#### Indoor Mesh Node Hops

このレポートには、ルート AP(RAP)からのホップ数が表示されます。 次の条件に基づいてレ ポートを作成できます。

- [AP By Controller]
- [AP By Floor]

#### Packet Error Rates

パケット エラーは、干渉やパケット廃棄によって発生します。パケット エラー率は、送信された パケットの数と正常に送信されたパケットの数に基づいて計算されます。パケット エラー率はバ ックホール リンクで測定され、ネイバーと親の両方に関して収集されます。AP は、パケット情 報をコントローラに定期的に送信します。AP は、親が切り替わるとすぐに、収集したパケット エラー情報をコントローラに送信します。WCS は、デフォルトで 10 分ごとにコントローラから のパケット エラー情報をポーリングし、最長で7日間データベースに格納します。WCS では、 パケット エラー率はグラフとして表示されます。このパケット エラー グラフは、データベース に格納されている履歴データに基づきます。

#### **Packet Stats**

このレポートには、ネイバーから送信されたパケットの合計数と、ネイバーから正常に送信され たパケットの合計数のカウンタ値が表示されます。レポートは特定の条件に基づいて作成できま す。

#### Worst SNR Links

ノイズの問題は、異なるタイミングで発生することがあります。また、ノイズは、異なるレート で増大したり、異なる期間にわたって継続したりすることがあります。次の図は、選択したイン ターフェイスに加えて無線 a と無線 b/g の両方に関してレポートを作成できることを示していま す。このレポートには、デフォルトで 10 個の 最悪条件の SNR リンクが表示されます。表示す る最悪条件のリンクの数は 5 ~ 50 個の範囲で選択できます。このレポートは、直前の 1 時間、 直前の 6 時間、前日、過去 2 日間、および最大 7 日間を指定して生成できます。データは、デフ ォルトで 10 分ごとにポーリングされます。データは、最長で 7 日間データベースに保持されま す。[Neighbor Type] の選択基準では、[All Neighbors] または [Parent/Children only] を選択できま す。



als als								Username: root   Logaut   Tefresh   Im	e vi
CIECO.	Wireless Contiol System								
cisco	👌 Bonkor • Baports • C	prigure - Loadi	on · Administration ·	849 4					
Mesh Reports	Mesh Worst SNRLinks > Worst	SNRinks					Save And Run	Run fow Cancel Delete	
Heah Alternate Parent						_			
Heah Link State	General Schedule Rosello	L							
Pleash Node Noos							R	Export   Email   Printer friendly	
Nesh Packet Force State									
		Mesh Wors	st SNR Links		Wi	reless Contr	ol System		
Plesh Peckel Queue Stats		Generalist Thullov	22 15 5655 PST 2007				CISCO		
Resh Packet Stats		Mish Worst SVR U	Jinks: 10						
Hesh Stranded Als		Neighbor Type: All	Neighbors (Table Only)						
Please Wee at Node Hope		Reporting Period.	Last 1 hours						
Heah Worst SNR Union		Name	BAC Address	Reigh AP Name	Neigh BAC	Reigh SNR	Neigh Type		
		LiP1242-3	011415-00-07x0	LUH242-2	014159070	9	parent		
		LiPtord-3	011410-00-07x0	LAPIDIO-2	0141539310	20	peret		
		LP1240-3	011416-00-07x0	UPI040-2	014180000	2	parent		
		LiP1240-3	011415-080740	LAPIDIZ-2	014150310	28	perent		
		LiPtoto 3	011410-00110	UPIDID-2	0141859310	2	parent.		

#### Worst Node Hops

このレポートには、デフォルトで 10 個の最悪条件のホップ数の AP が表示されます。AP のホッ プ数が多すぎる場合、リンクは脆弱である可能性があります。ユーザは、ルート AP からのホッ プ数が多い AP を隔離して、適切に対処できます。このノード数の基準を5~50の間で変更できま す。この図のレポート・タイプ・フィルタ基準は、表のみ、表とグラフのいずれかです。

ababa	Wireless Control System Usemania: root   Lepost   Advesh   Port Vew						
cisco	🚓 Hunder + Baseri + Configure + Landian + Jahrinistation + Hals +						
Hesh Reports	Mesh Warst Node Hops > WorstNodehps	Save Save And Run Run New Cancel Delete					
Heah Alternate Parent							
Mesh Link Stats	General Scheide Results R						
Mesh Node Hops	Report Title Worstholehos						
Heah Pucket Error State	Number Nodes 10						
March Barbard Channel State	Report Type Table Only w						
Henn Packet Quese state	Reporting Period						
Hesh Pucket Stats	🖲 Lawi Lawi I Nov 💌						
Hesh Stranded Als	Citetveen III III V Har III V Ha.						
Plesh Worst Node Hops	And I I I I Have A I I Have						
Mesh Worst SNE Links							

#### このレポートの結果を次の図に示します。

alialia	Wireless Control	System						Usemene root I Leasut I Refeah I I	
cisco	B Booker r	Beauty - D	poligere - Loosti	ion v géninistration v 🛛	ele -				
	Mesh Worst Node Hops > WorstNodehps					Save Save And Run	Run Now Cansel Odete		
Mark Alternate Passed				D.					
Pleak Link State	General Schedul	e Realts		46					
Mark Side Hope								Expet   Email   Printer Friendly	
Pesh Packet Error Mats						Winsteam	Control Surface July		
Noch Perket Queue Stat			Mesh Worst Node Hops			wireless Control System			
Nesh Packet Stats			Generated. Thu Nov	22 16 10 3 PST 2007					
Mark dependent sta			Number Noder, 1	0 h Onte					
			Reporting Paried	Last 1 hors					
Hesh Worst Node Hops									
Healt Moral Shill Links			APName	MAC Address	Node News	Parent AP Name	Parent MAC Autoress		
			LAPI042-3	10.14.15.59.07.ad	2	LAPI0.0.2	0014/00/08/07/10		
			LANDAD-1	10.10.2h a7.at b1	1	RAP1312	001074/tv7010		

#### セキュリティ統計情報

屋内メッシュ セキュリティ統計情報は、AP の詳細ページの [Bridging info] セクションの下に表示 されます。屋内メッシュ ノード セキュリティ統計情報テーブルのエントリは、子屋内メッシュ ノードが親屋内メッシュ ノードとの間で関連付けや認証を行ったときに作成されます。屋内メッ シュ ノードとコントローラとの関連付けが解除されると、エントリは削除されます。

## <u>リンク テスト</u>

WCS では、AP 間のリンク テストがサポートされています。任意の 2 つの AP を選択し、その 2 つの AP の間でリンク テストを実行できます。

これらの AP が RF ネイバーの場合は、リンク テストの結果が得られます。結果は、ページを完 全に更新することなく、MAP 上のダイアログに表示されます。ダイアログは簡単に処理できます 。

ただし、これらの 2 つの AP が RF ネイバーでない場合、WCS は、複合型の複数リンク テスト を行うために 2 つの AP 間のパスを検出しようとはしません。

2 つのノード間のリンク上の矢印にマウスを合わせると、次のようなウィンドウが表示されます 。



## <u>ノードツーノード リンク テスト</u>

このリンク テスト ツールは、任意の 2 つの AP 間のリンク品質を確認するためのオンデマンド ツールです。WCS では、この機能は AP の詳細ページに追加されます。

AP の詳細ページの、リンクが横に表示されている [Indoor Mesh Link] タブに、リンク テストを 実行するためのリンクが示されています。

コントローラ CLI リンク テスト ツールでは、オプションの入力パラメータとして、パケット サ イズ、リンク テスト パケットの総数、テスト期間、およびデータ リンク レートといったオプシ ョンの入力パラメータがあります。リンク テスト用のこれらのオプション パラメータには、デフ ォルト値があります。ノードの MAC アドレスは、唯一の必須入力パラメータです。

リンク テスト ツールは、強度、送信されたパケット数、およびノード間で受信されたパケット数 をテストします。リンク テスト用のリンクは、AP の詳細レポートに表示されます。このリンク をクリックすると、リンク テストの結果を示すポップアップ画面が表示されます。リンク テスト は、親子とネイバー間に適用されます。

リンク テストの出力には、送信されたパケット数、受信されたパケット数、エラー パケット数 (さまざまな理由のためのバケット)、SNR、ノイズ フロア、および RSSI が含まれます。

リンク テストでは、少なくとも次の詳細情報が GUI に表示されます。

- •送信されたリンク テスト パケット数
- •受信されたリンク テスト パケット数
- 信号強度(dBm)

•信号対雑音比

### <u>オンデマンド AP ネイバー リンク</u>

これは、WCS Map の新機能です。メッシュ AP をクリックすると、詳細情報を含むポップアッ プ ウィンドウが表示されます。次に [View Mesh Neighbors] をクリックすると、選択した AP の ネイバー情報が取得され、選択した屋内メッシュ AP のすべてのネイバーを含む表が表示されま す。

[View Mesh Neighbor] リンクをクリックすると、強調表示されている AP のすべてのネイバーが 表示されます。このスナップショットには、すべてのネイバー、ネイバーのタイプ、および SNR 値が表示されます。

#### <u>ping テスト</u>

ping テストは、コントローラと AP の間で ping を実行するためのオンデマンド ツールです。 ping テスト ツールは、AP の詳細ページと MAP の両方で使用できます。AP の詳細ページまたは MAP の AP 情報の [Run Ping Test] リンクをクリックすると、コントローラから現在の AP への ping を実行できます。

## 結論

エンタープライズ メッシュ(つまり、屋内メッシュ)は、有線イーサネットで接続を提供できな い場所にシスコ ワイヤレス カバレッジを拡張するものです。エンタープライズ メッシュにより 、ワイヤレス ネットワークの柔軟性および管理性が実現されます。

有線 AP で提供される機能のほとんどは、屋内メッシュ トポロジで提供されます。エンタープラ イズ メッシュは、同じコントローラ上で有線 AP と共存させることができます。

## <u>関連情報</u>

・<u>テクニカル サポートとドキュメント – Cisco Systems</u>