室内メッシュの導入ガイド

内容

概要

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

。

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

概要

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。

サポート対象ハードウェアおよびソフトウェア

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。

屋内と屋外

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。

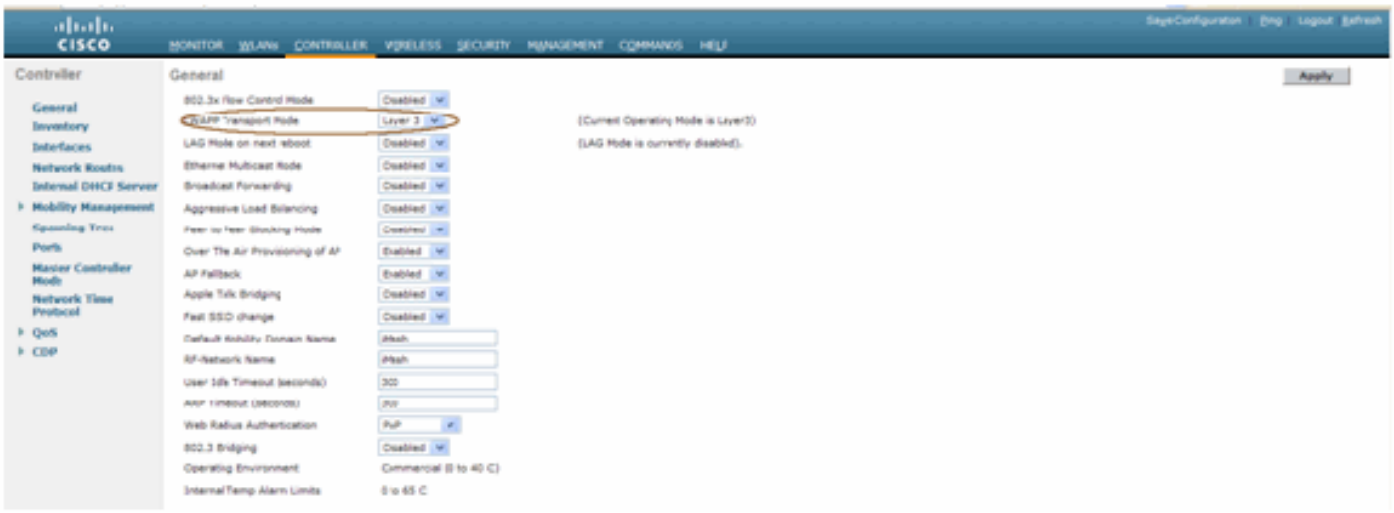
	屋内メッシュ	**屋外メッシュ**
環境	屋内のみ。屋内用のハードウェア	屋外のみ。頑丈なハードウェア
ハードウェア	LAP1242 および LAP1131AG を使用する屋内 AP	LAP15xx および LAP152x を使用する屋外 AP
電力レベル	2.4 GHz：20 dbm、5.8 GHz：17 dbm	2.4 GHz：28 dbm、5.8 GHz：28 dbm
セル サイズ	約 46 m	約 305 m
実装の高さ	地面から約 3.6 m	地面から 9 ~ 12 m

コンフィギュレーション

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。

コントローラ L3 モード

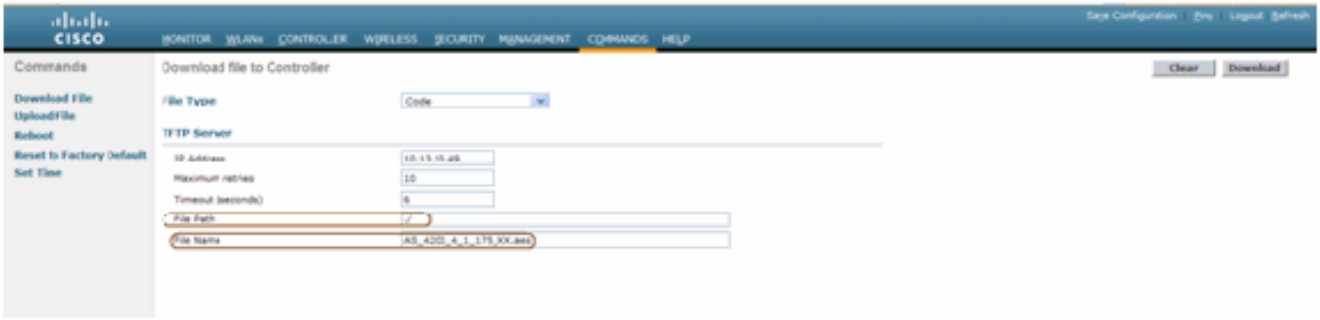
屋内メッシュ AP は、L3 ネットワークとして導入できます。



最新のコードへのコントローラのアップグレード

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。



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。

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 4.1.175.19
RTOS Version..................................... 4.1.175.19
Bootloader Version............................... 4.0.206.0
Build Type....................................... DATA + WPS

System Name...................................... CiscoImesh
System Location.....................................
System Contact......................................
System ObjectID.................................. 1.3.6.1.4.1.141/9.1.1.4.3
IP Address....................................... 10.13.10.20
System Up Time................................... 1 days 22 hrs 3 mins 35 secs

Configured Country............................... US  - United States
Operating Environment............................ Commercial (0 to 40 C)
Internal Temp Alarm Limits....................... 0 to 65 C
Internal Temperature............................. +38 C

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled
--More-- or (q)uit
Number of WLANs.................................. 2
3rd Party Access Point Support................... Disabled
Number of Active Clients......................... 3

Burned-in MAC Address............................ 00:18:73:34:48:60
Crypto Accelerator 1............................. Absent
Crypto Accelerator 2............................. Absent
Power Supply 1................................... Absent
Power Supply 2................................... 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。

MAC アドレス

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。

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。

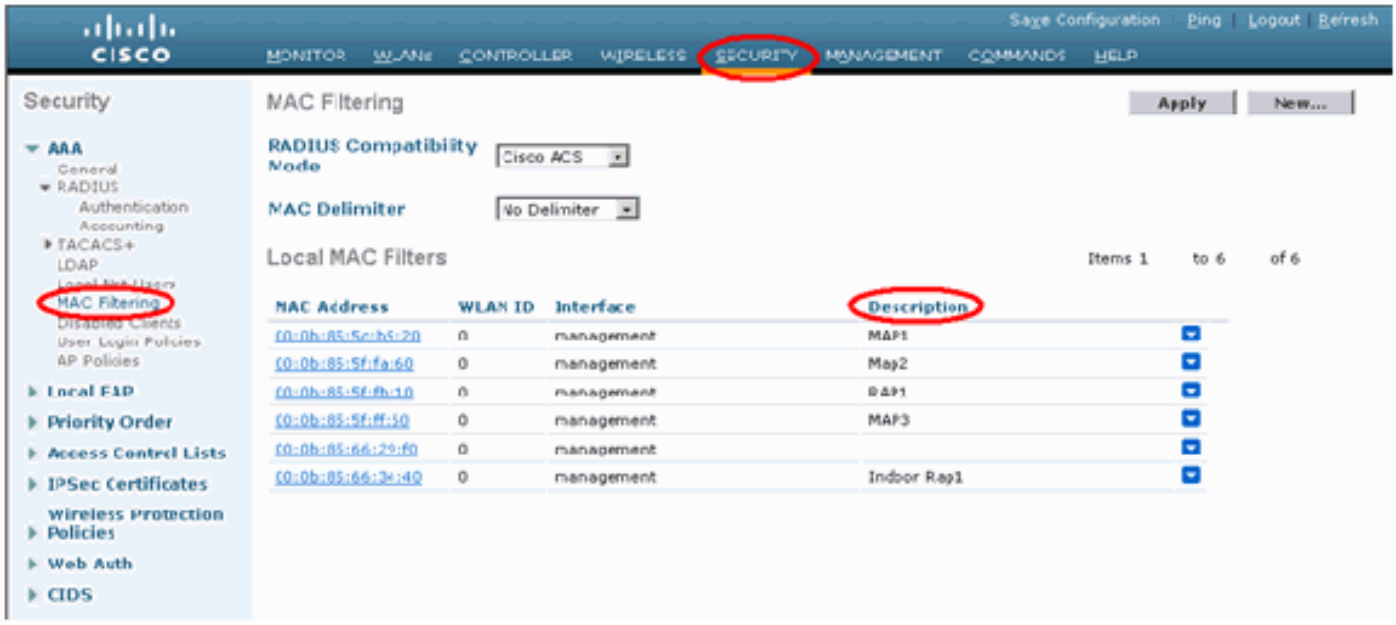
無線装置への MAC アドレスの記録

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。



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
```

```
(Cisco Controller) >show network

RF-Network Name.............................. iMesh
Web Mode..................................... Disable
Secure Web Mode.............................. Enable
Secure Shell (ssh)........................... Enable
Telnet....................................... Enable
Ethernet Multicast Mode...................... Disable   Mode: Ucast
Ethernet Broadcast Mode...................... Disable
User Idle Timeout............................ 300 seconds
ARP Idle Timeout............................. 300 seconds
ARP Unicast Mode............................. Disabled
Cisco AP Default Master...................... Disable
Mgmt Via Wireless Interface.................. Disable
Mgmt Via Dynamic Interface................... Disable
Bridge MAC filter Config..................... Enable
Bridge Security Mode......................... EAP
Mesh Multicast Mode.......................... 802.11b/g/n
Mesh Full Sector DFS......................... Enable
Over The Air Provisioning of AP's............ Enable
Mobile Peer to Peer Blocking................. Disable
Apple Talk .................................. Disable
AP Fallback ................................. Enable
--More-- or (q)uit
Web Auth Redirect Ports ..................... 80
Fast SSID Change ............................ Disabled
802.3 Bridging .............................. Disable
```

L3 屋内メッシュの導入

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。

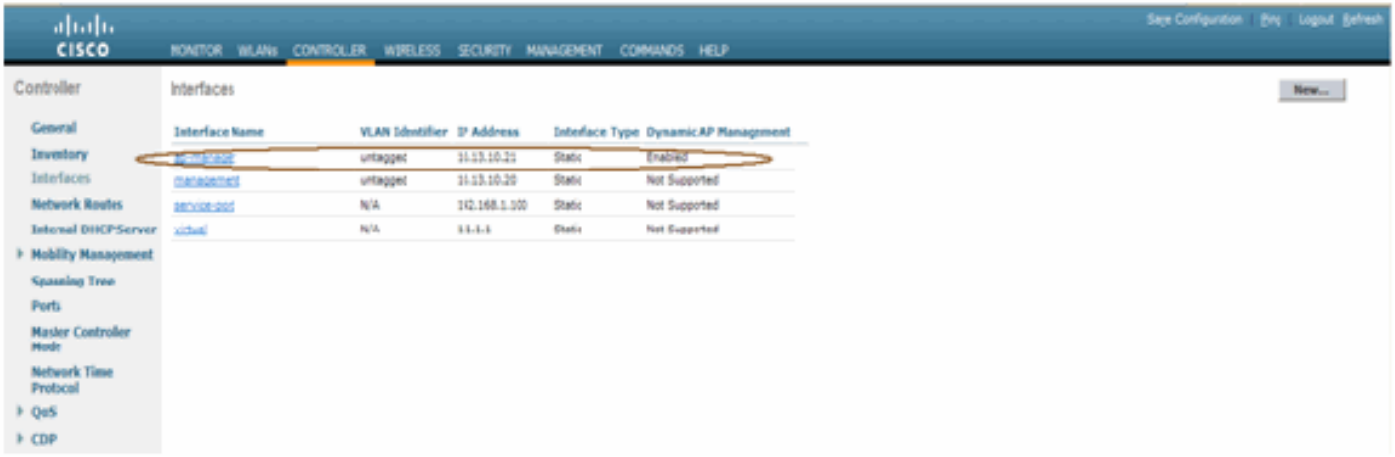
L3 屋内メッシュ ネットワークで DHCP サーバを使用する場合は、コントローラを L3 モードで設定します。設定を保存し、コントローラをリブートします。DHCP サーバのオプション 43 を必ず設定してください。コントローラを再起動した後、新しく接続された AP は、DHCP サーバから IP アドレスを受け取ります。

コントローラのインターフェイスの定義

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]**



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。

無線装置のロール

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)
```

ブリッジ グループ名

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。

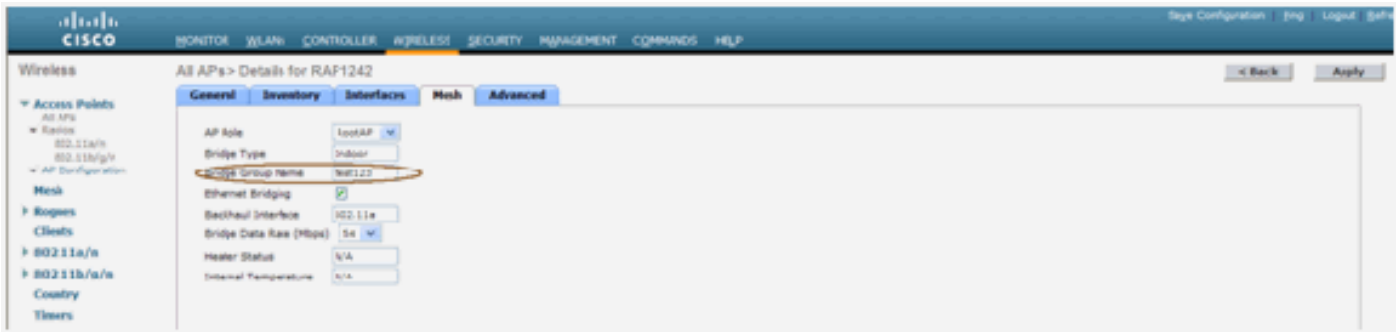
BGN を確認するには、次の CLI コマンドを発行します。

(Cisco Controller) **> show ap config general**

```
(Cisco Controller) >show ap config general RAP1242

Cisco AP Identifier.............................. 9
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.................................. 10.13.13.10
Cisco AP Location................................ default location
Cisco AP Group Name.............................. default-group
Primary Cisco Switch............................. J2106-1
Secondary Cisco Switch........................... 
Tertiary Cisco Switch............................ 
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... Bridge
--More-- or (q)uit
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
Number Of Slots.................................. 2
AP Model......................................... AIR-LAP1242AG-A-K9
IOS Version...................................... 12.4(20070808:082741)
Reset Button..................................... Enabled
AP Serial Number................................. FTX1035B3RH
AP Certificate Type.............................. Manufacture Installed
Management Frame Protection Validation.......... Disabled
Console Login Name............................... 
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]**



この新しいリリースでは、AP の環境情報も表示されます。

セキュリティ設定

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。

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-retries Configures EAP-Request Max Retries.
```

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
Web Mode..................................... Disable
Secure Web Mode.............................. Enable
Secure Shell (ssh)........................... Enable
Telnet....................................... Enable
Ethernet Multicast Mode...................... Disable   Mode: Mcast  224.1.1.1
Ethernet Broadcast Mode...................... Disable
User Idle Timeout............................ 300 seconds
ARP Idle Timeout............................. 300 seconds
ARP Unicast Mode............................. Disabled
Cisco AP Default Master...................... Disable
Mgmt Via Wireless Interface.................. Enable
Mgmt Via Dynamic Interface................... Disable
Bridge MAC filter Config..................... Disable
Bridge Security Mode......................... EAP  otherwise PSK
Mesh Multicast Mode.......................... 802.11b/g/n
Mesh Full Sector DFS......................... Enable
Over The Air Provisioning of AP's............ Enable
Mobile Peer to Peer Blocking................. Disable
AP Fallback ................................. Enable
Web Auth Redirect Ports ..................... 80
--More-- or (q)uit
Fast SSID Change ............................ Disabled
802.3 Bridging .............................. Disable
```

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

```
(Cisco Controller) >show wlan 0

WLAN Identifier.................................. 0
Profile Name..................................... Mesh_profile
Network Name (SSID).............................. Mesh_ssid
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 2
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. 1800 seconds
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Allowed
CCX - AironetIe Support.......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
Dot11-Phone Mode (7920).......................... Disabled
Wired Protocol................................... None
--More-- or (q)uit
IPv6 Support..................................... Disabled
Radio Policy..................................... All
Local EAP Authentication......................... Enabled (Profile 'prfMaP1500L1EAuth93')
Security

   802.11 Authentication:........................ Open System
   Static WEP Keys............................... Disabled
   802.1X........................................ Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Enabled
      WPA (SSN IE)............................... Disabled
      WPA2 (RSN IE).............................. Enabled
         TKIP Cipher............................. Disabled
         AES Cipher.............................. Enabled
                                                  Auth Key Management
         802.1x.................................. Enabled
         PSK..................................... Disabled
         CCKM.................................... Disabled
   CKIP ........................................... Disabled
   IP Security Passthru.......................... Disabled
   Web Based Authentication...................... Disabled
   Web-Passthrough............................... Disabled
   Conditional Web Redirect...................... Disabled
   Auto Anchor................................... Disabled
--More-- or (q)uit
   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
 WLAN ID       IP Address       Status
```

(Cisco Controller) >**show local-auth config**

```
(Cisco Controller) >show local-auth config

User credentials database search order:
    Primary ..................................... Local DB

Timer:
    Active timeout .............................. 300

Configured EAP profiles:

EAP Method configuration:
    EAP-FAST:
      Server key ................................ <hidden>
      TTL for the PAC ........................... 10
      Anonymous provision allowed ............... Yes
      Authority ID .............................. 436973636f0000000000000000000000
      Authority Information ..................... Cisco A-ID

(Cisco Controller) >show advanced eap


EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries..... 20
EAP Key-Index for Dynamic WEP..... 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds)..... 1
EAP-Request Max Retries..... 2
```

```
(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

前提条件

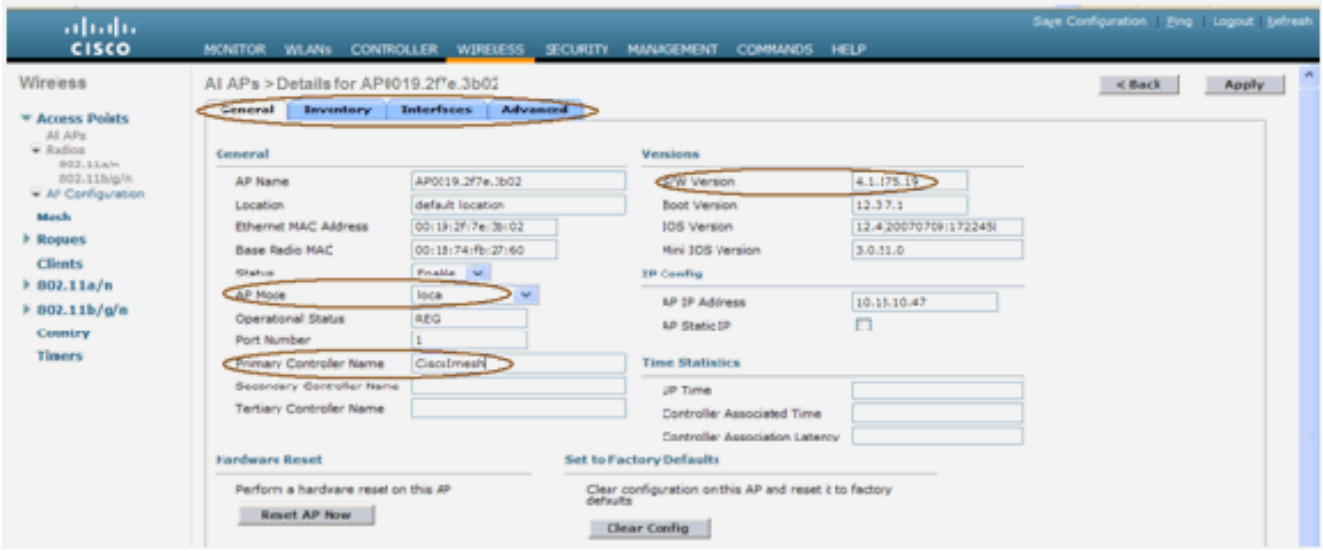
コントローラで推奨バージョンのコードが実行されている必要があります。ソフトウェア バージョンを確認するには、[Monitor] をクリックします。CLI を使用してソフトウェア バージョンを確認することもできます。

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 4.1.175.19
RTOS Version..................................... 4.1.175.19
Bootloader Version............................... 4.0.206.0
Build Type....................................... DATA + WPS

System Name...................................... CiscoImesh
System Location.....................................
System Contact......................................
System ObjectID.................................. 1.3.6.1.4.1.14179.1.1.4.3
IP Address....................................... 10.13.10.20
System Up Time................................... 1 days 22 hrs 3 mins 35 secs

Configured Country............................... US  - United States
Operating Environment............................ Commercial (0 to 40 C)
Internal Temp Alarm Limits....................... 0 to 65 C
Internal Temperature............................. +38 C

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled
--More-- or (q)uit
Number of WLANs.................................. 2
3rd Party Access Point Support................... Disabled
Number of Active Clients......................... 3

Burned-in MAC Address............................ 00:18:73:34:48:60
Crypto Accelerator 1............................. Absent
Crypto Accelerator 2............................. Absent
Power Supply 1................................... Absent
Power Supply 2................................... Present, OK
```

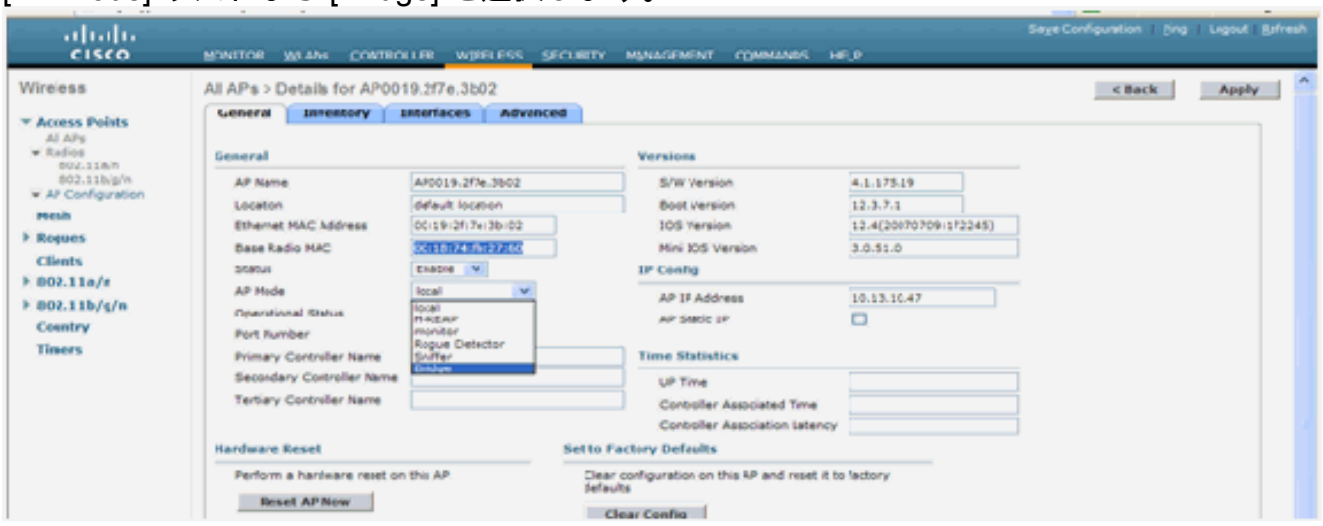
DHCP サーバ、ACS サーバ、WCS サーバなどのシステムに到達可能である必要があります。

設置

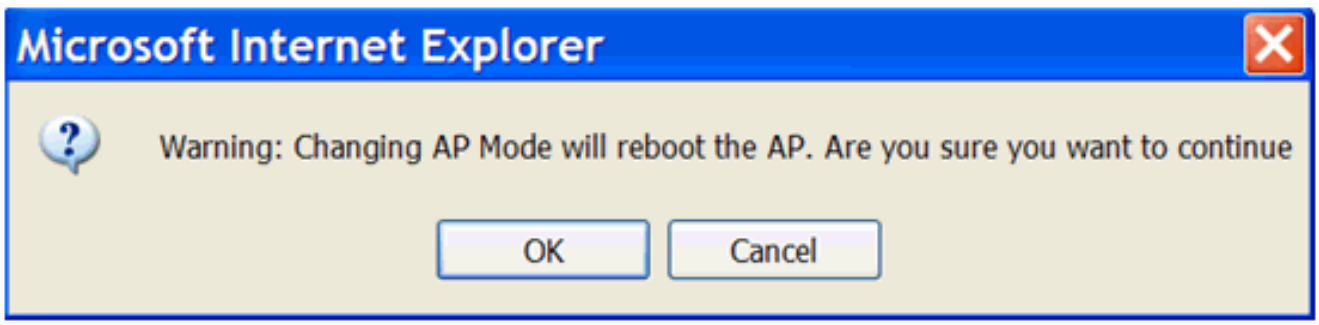
1. 管理 IP アドレスと同じサブネット上のレイヤ 3 ネットワークにすべての LAP（1131AG/1242AG）を接続します。すべての AP は、ローカル モードの AP としてコントローラに参加します。このモードで、プライマリ コントローラ名、セカンダリ コントローラ名、およびターシャリ コントローラ名を使用して AP をプライミングします。



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。



7. AP のリブートを確認するプロンプトが表示されます。



8. 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。

9. 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。

電力とチャネルの設定

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]**

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。

RF チェック

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

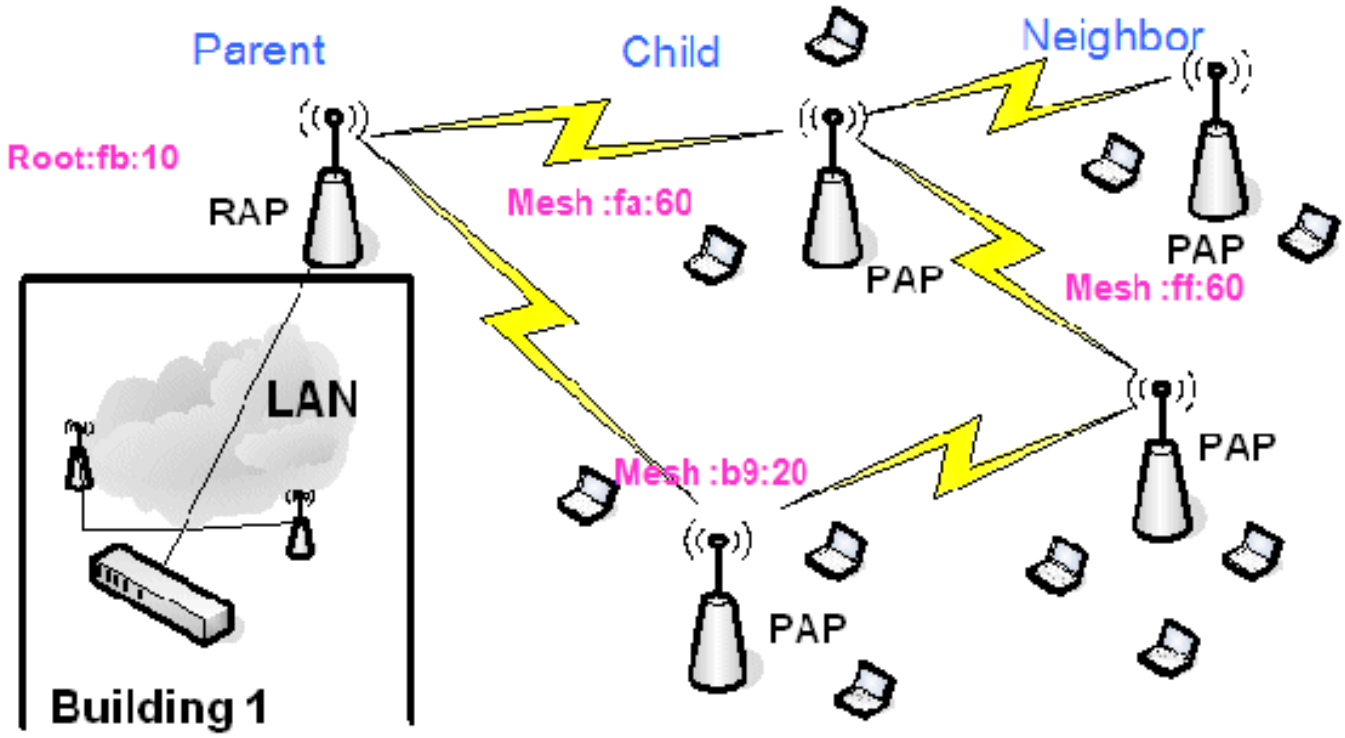


図 1 では、わかりやすくするために AP 名が示されています。次のスクリーン ショットでは、**RAP(fb:10)** が調査されています。このノードは、（実際の導入における）屋内メッシュ AP（**fa:60 および b9:20**）を子として識別し、**MAP ff:60 をネイバー**として識別しています。

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]。**

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。

相互接続の確認

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 Controller) >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-backhaul Show mesh secondary-backhaul
client-access   Show mesh backhaul with client access.
public-safety   Show mesh public safety.
background-scanning 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。

```
(Cisco Controller) >show mesh path 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 Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
LAP1242-1           56      29     29       27       0x86b    UPDATED NEIGH PARENT BEACON
RAP1242             56      41     32       34       0x86b    UPDATED NEIGH PARENT BEACON
RAP1242           is a Root AP.
```

[屋内メッシュ ネイバーのサマリーの表示]

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 mesh neigh ?

detail          Show Link rate neigh detail.
summary         Show Link rate neigh summary.
(Cisco Controller) >show mesh neigh  summary RAP1242

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
LAP1242-2           56      0      0        0        0x860    BEACON
LAP1242-1           56      0      33       0        0x960    CHILD BEACON


(Cisco Controller) >show mesh neigh  summary LAP1242-1

AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags    State
-----------------   ------- ------ -------- -------- -------  -----
LAP1242-2           56      30     29       28       0x961    UPDATED CHILD BEACON
RAP1242             56      43     46       31       0x86b    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。

AP コンソール アクセス セキュリティ

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 にユーザ ID とパスワードの組み合わせをプッシュするための CLI。

```
(Cisco Controller) >config ap username Cisco password Cisco ?

all             Configures the Username/Password for all connected APs.
<Cisco AP>      Enter the name of the Cisco AP.
```

- 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。

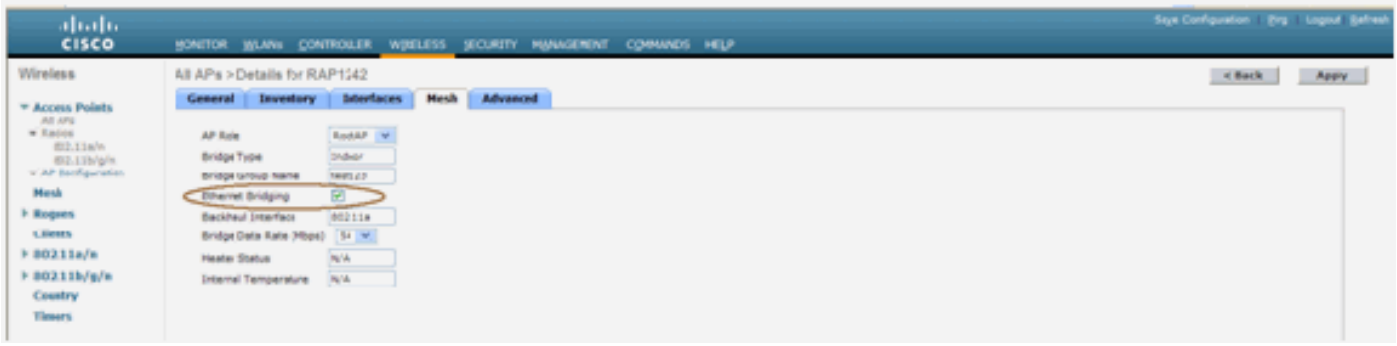
イーサネット ブリッジング

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。

ブリッジ グループ名の拡張

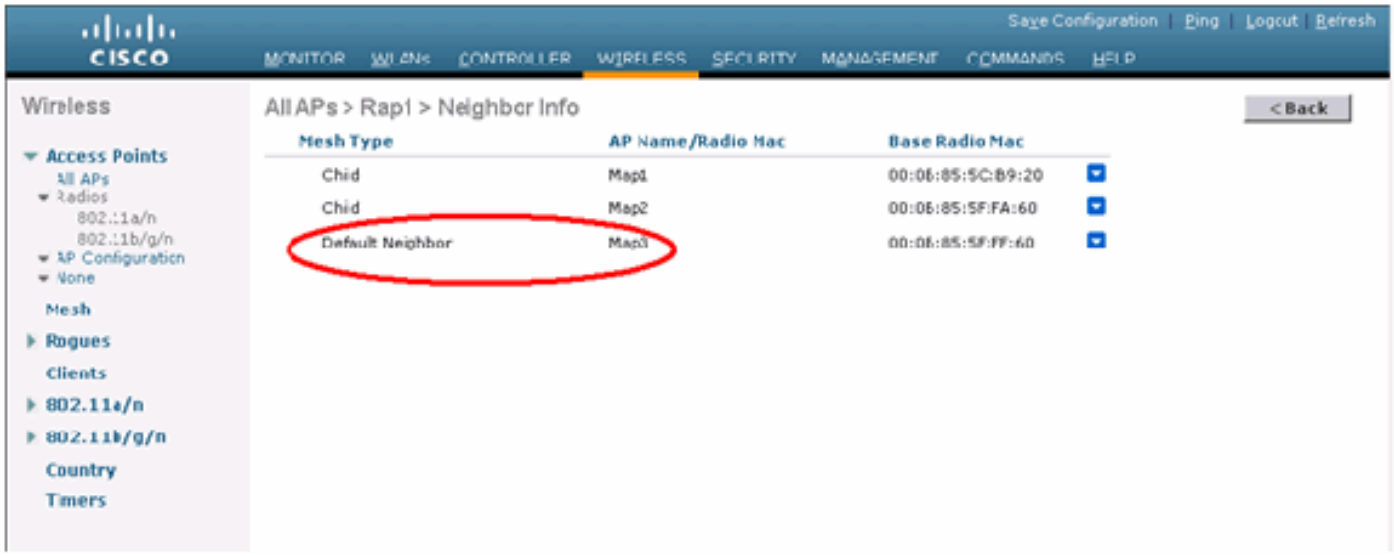
意図していない「ブリッジ グループ名」を使用して AP が不適切にプロビジョニングされる場合があります。ネットワーク設計によって、この AP では、正しいセクターまたはツリーに到達して見つけることができない場合もあります。互換性のあるセクターに到達できない場合は、AP が取り残される可能性があります。

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
```



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。

ログ：メッセージ、Sys、AP、およびトラップ

メッセージ ログ

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。

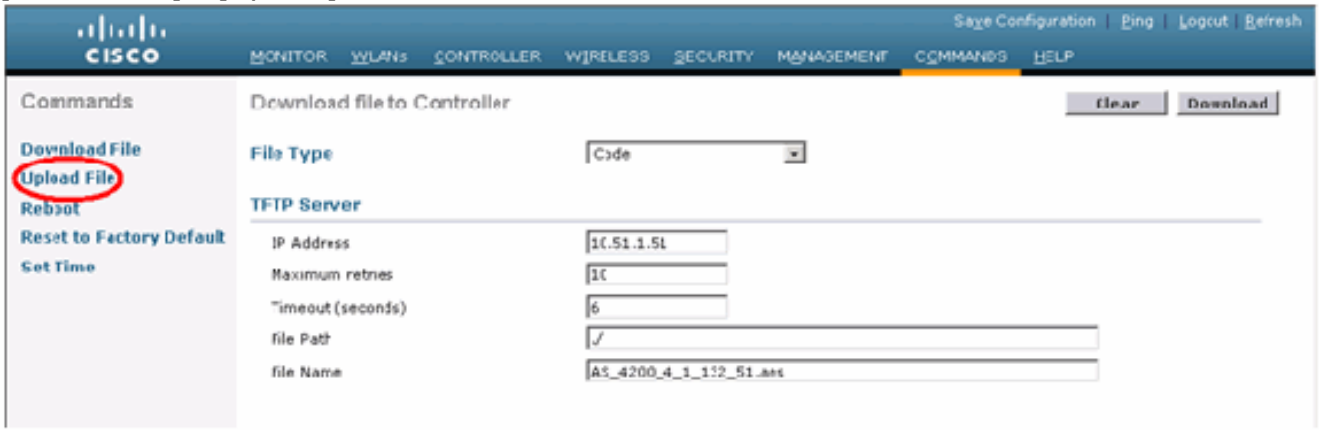
```
(Cisco Controller) >config msglog level ?

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。

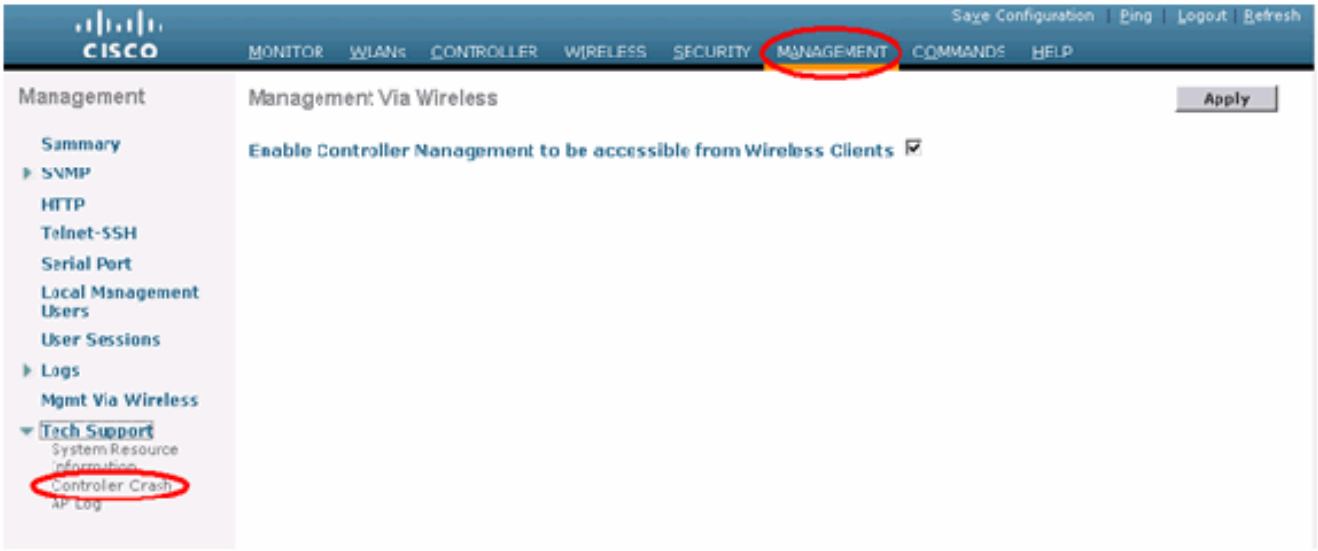
```
(Cisco Controller) >show msglog

Message Log Severity Level ..................... VERBOSE
Mon Jul 11 01:42:08 2005  [SECURITY] apf_foreignap.c 765: Received a packet for
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
Fri Jul  8 05:38:45 2005  [ERROR] spam_lrad.c 1310: Validation of Config Request
 failed from AP 00:0b:85:0e:05:80
Fri Jul  8 05:38:40 2005  [ERROR] spam_lrad.c 1310: Validation of Config Request
 failed from AP 00:0b:85:0e:14:00
Fri Jul  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
 failed from AP 00:0b:85:0e:05:80
Fri Jul  8 05:32:23 2005  [ERROR] poe.c 449: poeInitPowerSupply : poePortResync
returned FAILURE.
Fri Jul  8 05:32:17 2005  [ERROR] dhcpd.c 78: dhcp server: binding to 0.0.0.0
Fri Jul  8 05:32:17 2005  [ERROR] rrmgroup.c 733: Airewave Director: 802.11a swi
tch group reset
Fri Jul  8 05:32:16 2005  [ERROR] rrmgroup.c 733: Airewave Director: 802.11bg sw
itch group reset
Fri Jul  8 05:32:16 2005  Previous message occurred 2 times
Fri Jul  8 05:31:19 2005  [CRITICAL] osapi_sem.c 794: Error!  osapiMutexTake cal
```

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。

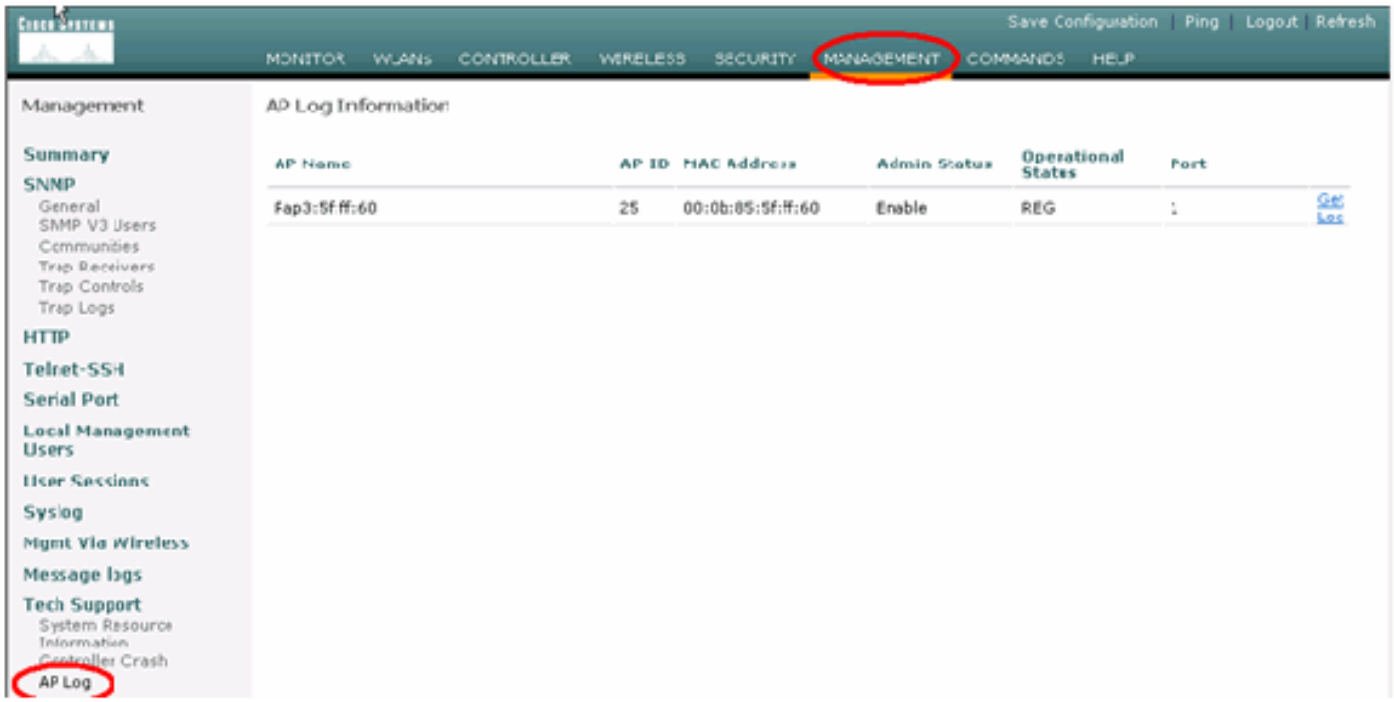


2. TFTP サーバの情報を入力します。このページでは、アップロードに関するさまざまなオプションと、送信するファイルを選択できます。メッセージ ログイベント ログトラップ ログクラッシュ ファイル（存在する場合）クラッシュ ファイルの有無をチェックするには、[Management] > [Controller Crash] をクリックします。



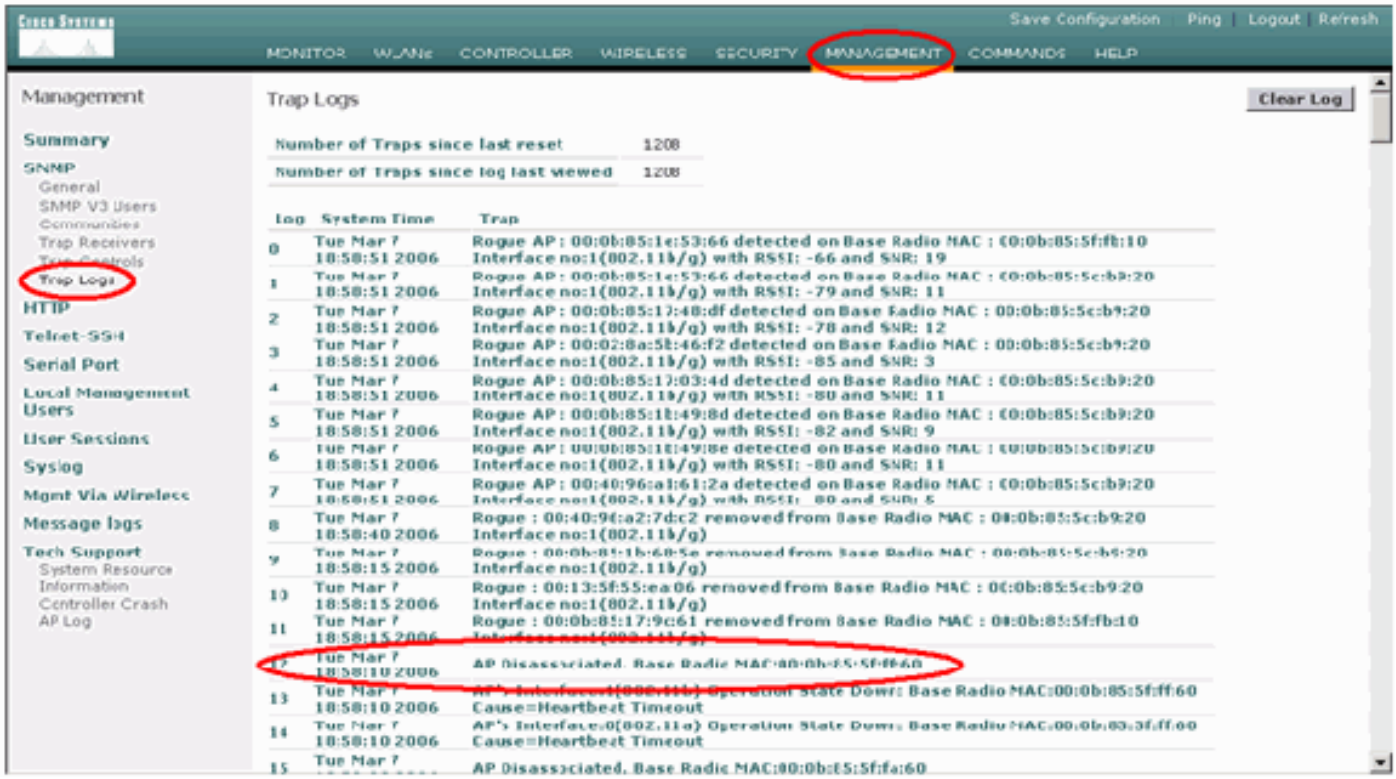
AP ログ

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）。



トラップ ログ

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。



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

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	コンバージェン時間（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		

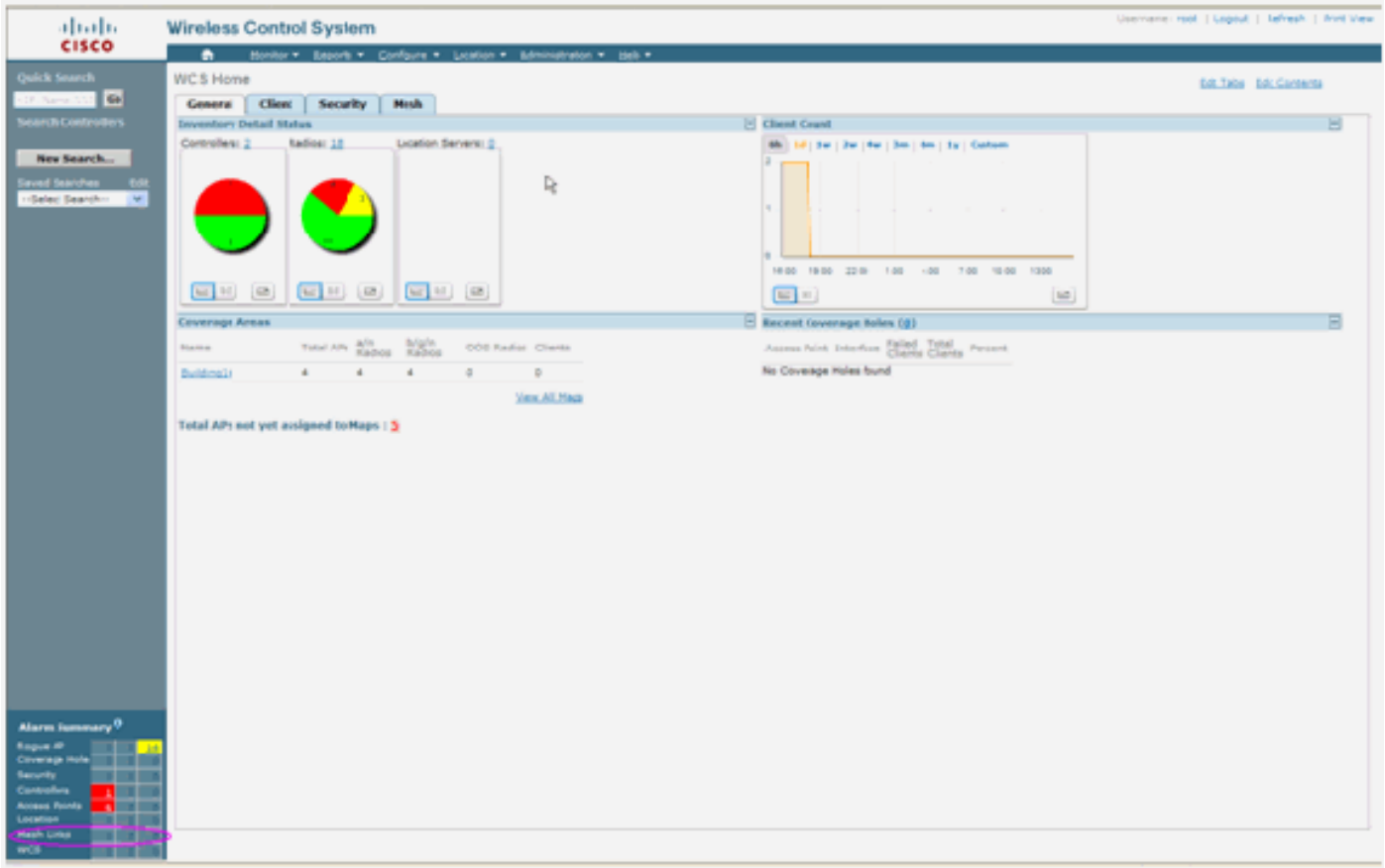
WCS

屋内メッシュ アラーム

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。



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。

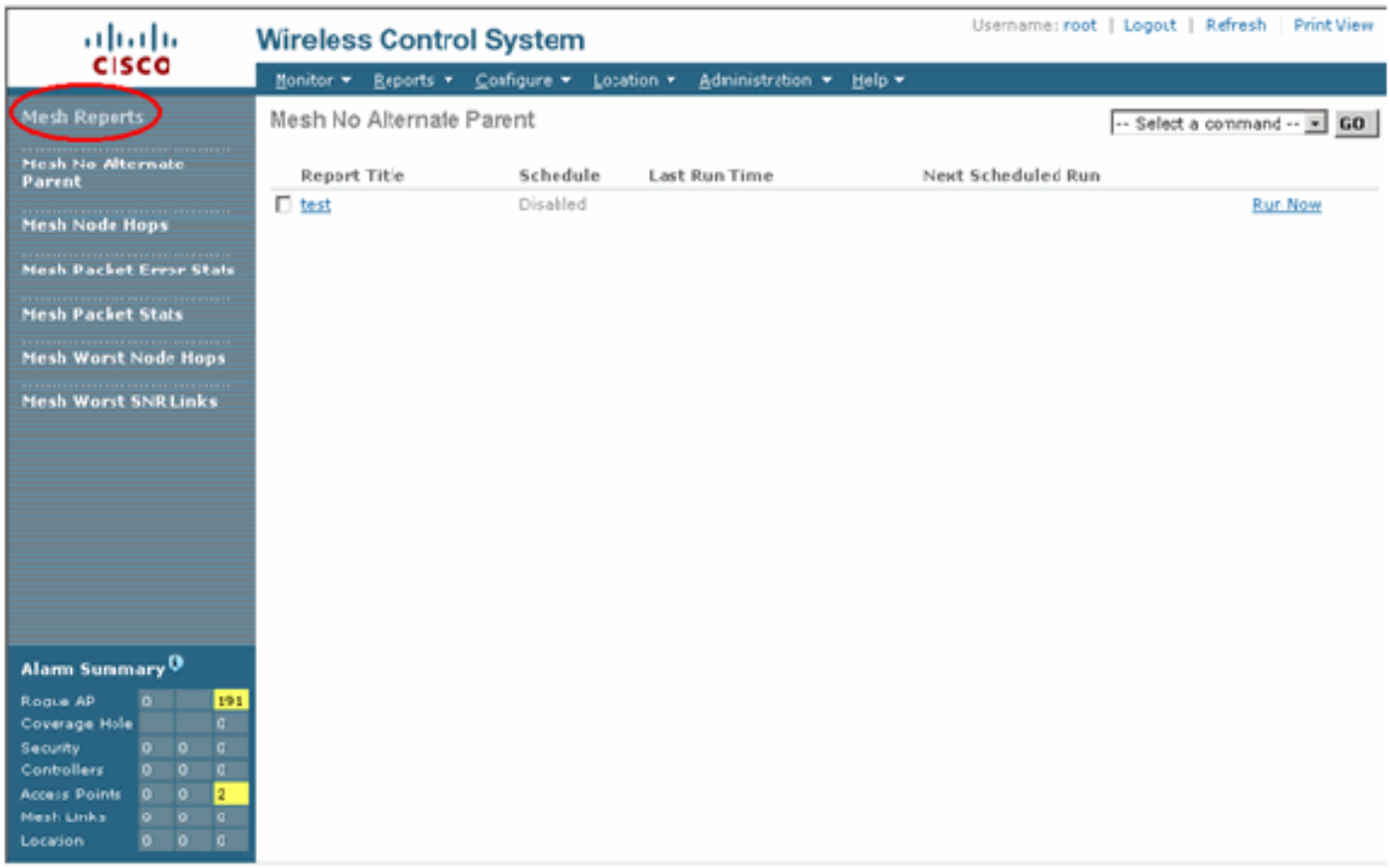
屋内メッシュ リンク以外のアラーム：

- 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



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

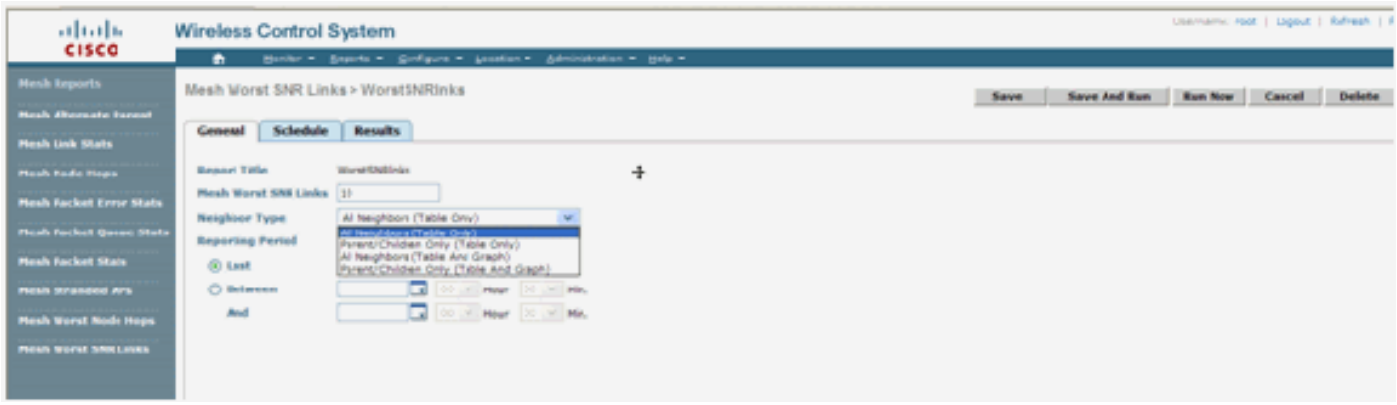
パケット エラーは、干渉やパケット廃棄によって発生します。パケット エラー率は、送信されたパケットの数と正常に送信されたパケットの数に基づいて計算されます。パケット エラー率はバックホール リンクで測定され、ネイバーと親の両方に関して収集されます。AP は、パケット情報をコントローラに定期的に送信します。AP は、親が切り替わるとすぐに、収集したパケット エラー情報をコントローラに送信します。WCS は、デフォルトで 10 分ごとにコントローラからのパケット エラー情報をポーリングし、最長で 7 日間データベースに格納します。WCS では、パケット エラー率はグラフとして表示されます。このパケ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

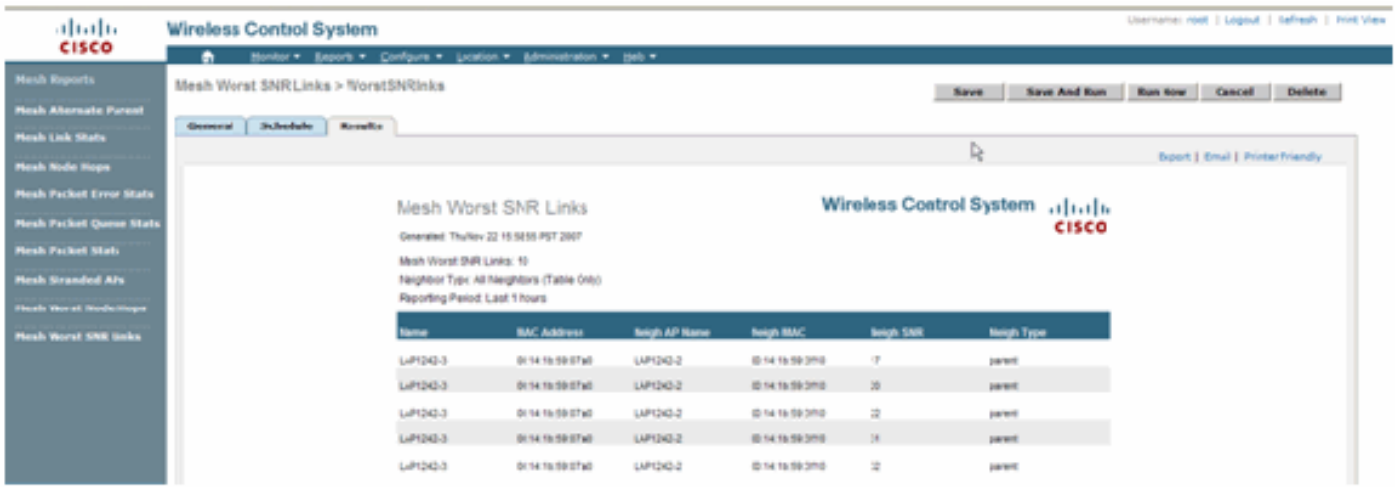
Packet Stats

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

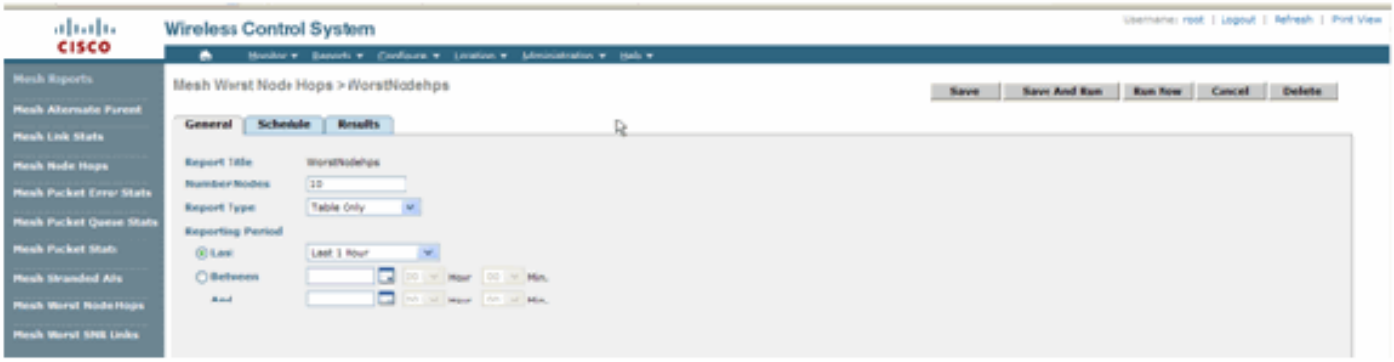
ノイズの問題は、異なるタイミングで発生することがあります。また、ノイズは、異なるレートで増大したり、異なる期間にわたって継続したりすることがあります。次の図は、選択したインターフェイスに加えて無線 a と無線 b/g の両方に関してレポートを作成できることを示しています。このレポートには、デフォルトで 10 個の 最悪条件の SNR リンクが表示されます。表示する最悪条件のリンクの数は 5 ~ 50 個の範囲で選択できます。このレポートは、直前の 1 時間、直前の 6 時間、前日、過去 2 日間、および最大 7 日間を指定して生成できます。データは、デフォルトで 10 分ごとにポーリングされま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



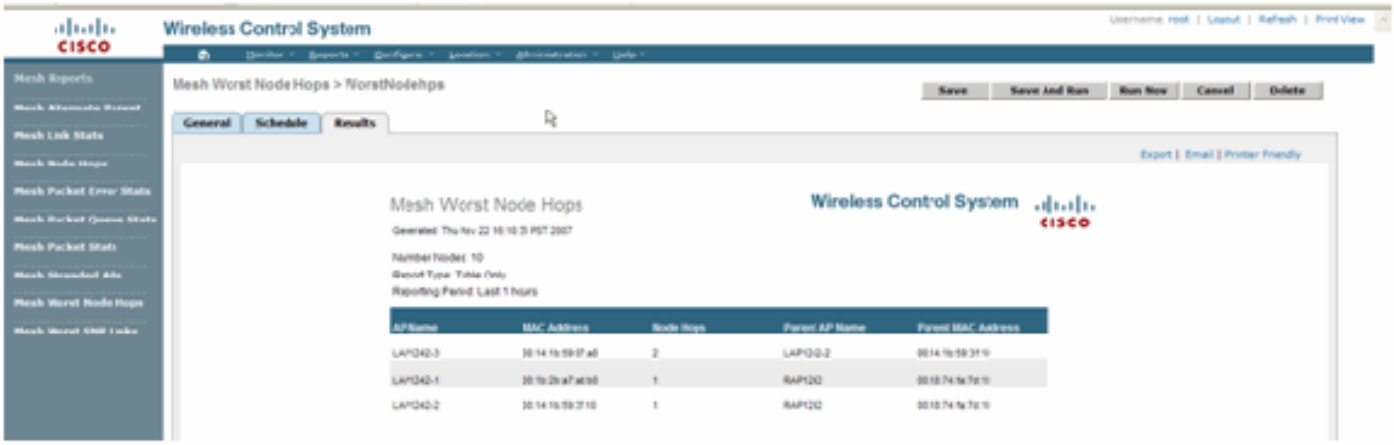


Worst Node Hops

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。



このレポートの結果を次の図に示します。



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。

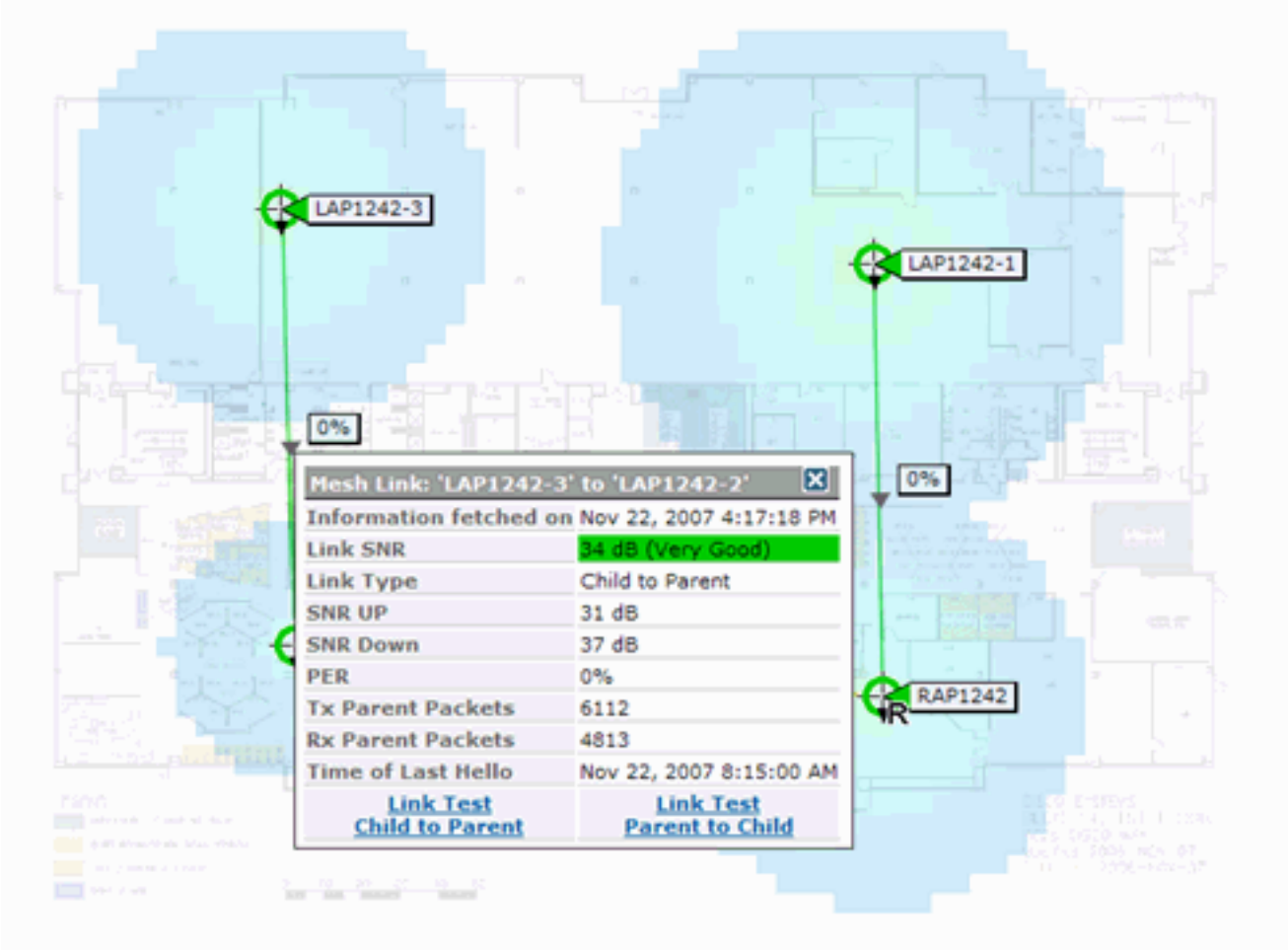
リンク テスト

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。



ノードツーノード リンク テスト

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

オンデマンド AP ネイバー リンク

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。

ping テスト

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。

関連情報

- テクニカル サポートとドキュメント – Cisco Systems