

Lightweight AP とワイヤレス LAN コントローラ (WLC) での Remote-Edge AP (REAP) の設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[WLC の基本動作の設定と WLAN の設定](#)

[リモートサイトにインストールするための AP のプライミング](#)

[2800 人のルータを WAN リンクを確立するために設定して下さい](#)

[リモートサイトでの REAP AP の配備](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[関連情報](#)

概要

Cisco Unified Wireless Network に導入された Remote-edge Access Point (REAP; リモートエッジアクセスポイント) 機能を使用すれば、ワイヤレス LAN (WLAN) コントローラ (WLC) から Cisco Lightweight アクセスポイント (LAP) をリモート配備できます。この機能は、ブランチオフィスや小規模な小売サイトに最適です。このドキュメントでは、REAP ベースの WLAN ネットワークを Cisco 1030 シリーズの LAP や 4400 WLC を使用して配備する方法について説明します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- WLC に関する知識と WLC の基本的なパラメータの設定方法に関する知識
- Cisco 1030 LAP での REAP モードの動作に関する知識
- 外部 DHCP サーバおよび Domain Name System (DNS; ドメイン ネーム システム) サーバ

のどちらかまたは両方の設定に関する知識

- Wi-Fi Protected Access (WPA) の概念に関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco 4400 シリーズ ファームウェアリリース 4.2 を実行する WLC
- Cisco 1030 LAP
- Cisco IOS® ソフトウェア リリース 12.2(13)T13 を実行する 2 Cisco 2800 シリーズ ルータ
- ファームウェアリリース 3.0 を実行する Cisco Aironet 802.11a/b/g クライアントアダプタ
- Cisco Aironet デスクトップ ユーティリティ バージョン 3.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

背景説明

REAP モードでは、WAN リンクを経由して LAP を配置し、WLC との通信を維持しながら、通常の LAP 機能を利用できます。REAP モードは、現時点では 1030 LAP でしかサポートされていません。

この機能を実現するために、1030 REAP では、Lightweight Access Point Protocol (LWAPP) のコントロールプレーンが、ワイヤレス データ プレーンと分離されています。通常の LWAPP ベースのアクセス ポイント (AP) で使用されるのと同じ方法で中央集中型の制御と管理を行うために Cisco WLC が引き続き使用されていますが、すべてのユーザ データは AP でローカルにブリッジされています。ローカル ネットワーク リソースへのアクセスは、WAN が停止していても維持されます。

REAP AP では、次の 2 つの動作モードがサポートされています。

- 通常の REAP モード
- スタンドアロン モード

REAP AP と WLC の間の WAN リンクがアップすると、LAP は通常の REAP モードに設定されます。LAP が通常の REAP モードで動作している場合は、最大 16 個までの WLAN をサポートできます。

WLC と LAP の間の WAN リンクがダウンすると、REAP が有効になっている LAP はスタンドアロン モードに切り替わります。Wired Equivalent Privacy (WEP) または任意のローカル認証方式を使用して WLAN が設定されている場合は、スタンドアロン モードでは、REAP LAP は WLC なしで WLAN を 1 つだけ単独でサポートできます。この場合、REAP AP がサポートする WLAN は AP で設定される最初の WLAN、WLAN 1.です。これは WAN リンクがダウンしているとき他の認証方式のほとんどがではない可能性のある コントローラおよび、このオペレーションに出入して情報を渡す必要があるという理由によります。スタンドアロン モードでは、最低限の機能セットが LAP でサポートされます。REAP LAP がスタンドアロン モードのときにサポート

する機能セットを、通常モードで (WAN リンクがアップしていて WLC への通信もアップしているときに) REAP LAP がサポートする機能と比較して、次の表に示します。

通常の REAP モードとスタンドアロン モードで REAP LAP がサポートする機能

		REAP (normal mode)	REAP (standalone mode)
Protocols	IPv4	Yes	Yes
	IPv6	Yes	Yes
	All other protocols	Yes (only if client is also IP enabled)	Yes (only if client is also IP enabled)
	IP Proxy ARP	No	No
WLAN	Number of SSIDs	16	1 (the first one)
	Dynamic channel assignment	Yes	No
	Dynamic power control	Yes	No
	Dynamic load balancing	Yes	No
VLAN	Multiple interfaces	No	No
	802.1Q Support	No	No
WLAN Security	Rogue AP detection	Yes	No
	Exclusion list	Yes	Yes (existing members only)
	Peer-to-Peer blocking	No	No
	Intrusion Detection System	Yes	No
Layer 2 Security	MAC authentication	Yes	No
	802.1X	Yes	No
	WEP (64/128/152bits)	Yes	Yes
	WPA-PSK	Yes	Yes
	WPA2-PSK	No	No
	WPA-EAP	Yes	No
	WPA2-EAP	Yes	No
Layer 3 Security	Web Authentication	No	No
	IPsec	No	No
	L2TP	No	No
	VPN Pass-through	No	No
	Access Control Lists	No	No
QoS	QoS Profiles	Yes	Yes
	Downlink QoS (weighted round-robin queues)	Yes	Yes
	802.1p support	No	No
	Per-user bandwidth contracts	No	No
	WMM	No	No
	802.11e (future)	No	No
	AAA QoS Profile override	Yes	No
Mobility	Intra-subnet	Yes	Yes
	Inter-subnet	No	No
DHCP	Internal DHCP Server	No	No
	External DHCP Server	Yes	Yes
Topology	Direct connect (2006)	No	No

この表には、複数の VLAN が両方のモードの REAP LAP でサポートされないことが示されています。複数の VLAN がサポートされないのは、REAP LAP が IEEE 802.1Q VLAN タギングを実行できないので、REAP LAP が存在できるのは 1 つのサブネット上だけになるためです。そのため、各 Service Set Identifier (SSID) のトラフィックは、有線ネットワークと同じサブネットで終端します。その結果、SSID 間にまたがる無線伝送中に無線トラフィックがセグメント化されることがあったとしても、有線側のデータトラフィックは分割されません。

[REAP の配備、REAP の管理および制限についての詳細は、『ブランチオフィスでの REAP 導入ガイド』を参照してください。](#)

設定

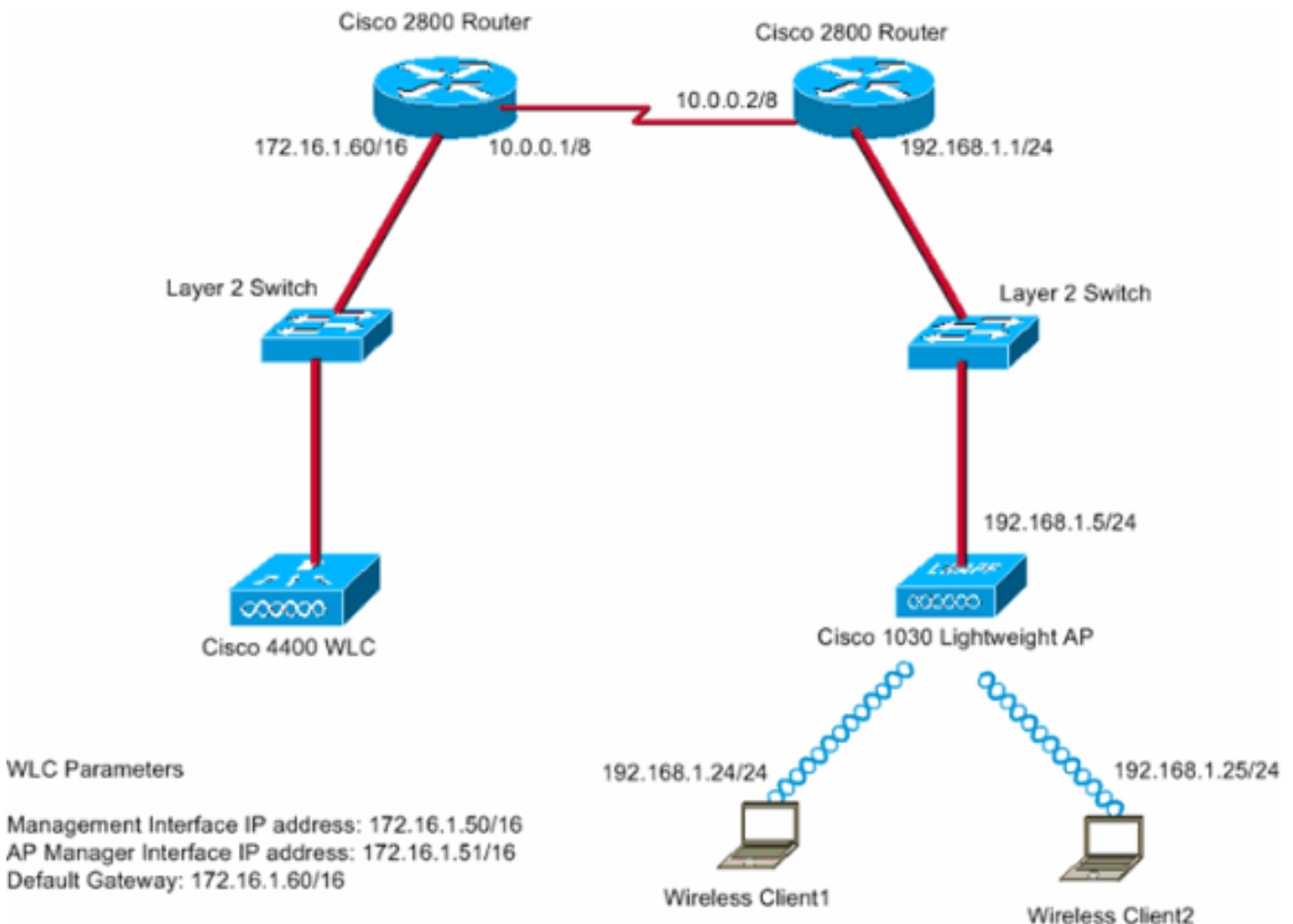
この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

デバイスを設定してネットワーク構成を実装するには、次の手順を実行します。

1. [WLC の基本動作の設定と WLAN の設定](#)
2. [リモートサイトにインストールするための AP のプライミング](#)
3. [2800 人のルータを WAN リンクを確立するために設定して下さい。](#)
4. [リモートサイトでの REAP LAP の配備](#)

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



本社とブランチオフィスは専用回線を使用して接続されています。専用回線は各端に 2800 シリーズ ルータで終端させます。この例では、Open Shortest Path First (OSPF) プロトコルを使用し、WAN リンク上で PPP カプセル化を使用してデータをルーティングしています。4400 WLC は主要な オフィスにあり、1030 LAP はリモートオフィスで展開する必要があります。1030 LAP では、2 つの WLAN をサポートする必要があります。WLAN のパラメータは次のとおりです。

- WLAN1SSID : SSID1認証 : オープン暗号化 : Temporal Key Integrity Protocol (TKIP) (WPA Pre-Shared Key [WPA-PSK])
- WLAN 2SSID : SSID2認証 : Extensible Authentication Protocol (EAP) 暗号化 : TKIP注 : WLAN 2 については、このドキュメントの設定では、WPA (802.1x 認証と TKIP による暗号化) を使用しています。

この設定に合わせて、デバイスを設定する必要があります。

WLC の基本動作の設定と WLAN の設定

基本動作に WLC を設定するには、command-line interface (CLI; コマンドライン インターフェイス) 上でスタートアップ コンフィギュレーション ウィザードを使用できます。その他、GUI を使用して WLC を設定することもできます。このドキュメントでは、CLI 上でスタートアップ コンフィギュレーション ウィザードを使用した、WLC 上の設定について説明しています。

WLC が初めて起動すると、スタートアップ コンフィギュレーション ウィザードに直接入ります。基本設定を設定するには、コンフィギュレーション ウィザードを使用します。このウィザードは、CLI または GUI で実行できます。スタートアップ コンフィギュレーション ウィザードの例を次に示します。

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: WLC_MainOffice Enter Administrative User Name (24 characters max):
admin Enter Administrative Password (24 characters max): ***** Management Interface IP Address:
172.16.1.50 Management Interface Netmask: 255.255.0.0 Management Interface Default Router:
172.16.1.60 Management Interface VLAN Identifier (0 = untagged): Management Interface Port Num
[1 to 4]: 1 Management Interface DHCP Server IP Address: 172.16.1.1 AP Manager Interface IP
Address: 172.16.1.51 AP-Manager is on Management subnet, using same values AP Manager Interface
DHCP Server (172.16.1.1): Virtual Gateway IP Address: 1.1.1.1 Mobility/RF Group Name: Main
Network Name (SSID): SSID1 Allow Static IP Addresses [YES][no]: Yes Configure a RADIUS Server
now? [YES][no]: no Warning! The default WLAN security policy requires a RADIUS server. Please
see documentation for more details. Enter Country Code (enter 'help' for a list of countries)
[US]: Enable 802.11b Network [YES][no]: Yes Enable 802.11a Network [YES][no]: Yes Enable 802.11g
Network [YES][no]: Yes Enable Auto-RF [YES][no]: Yes Configuration saved! Resetting system with
new configuration...
```

この例では、WLC で次のパラメータを設定します。

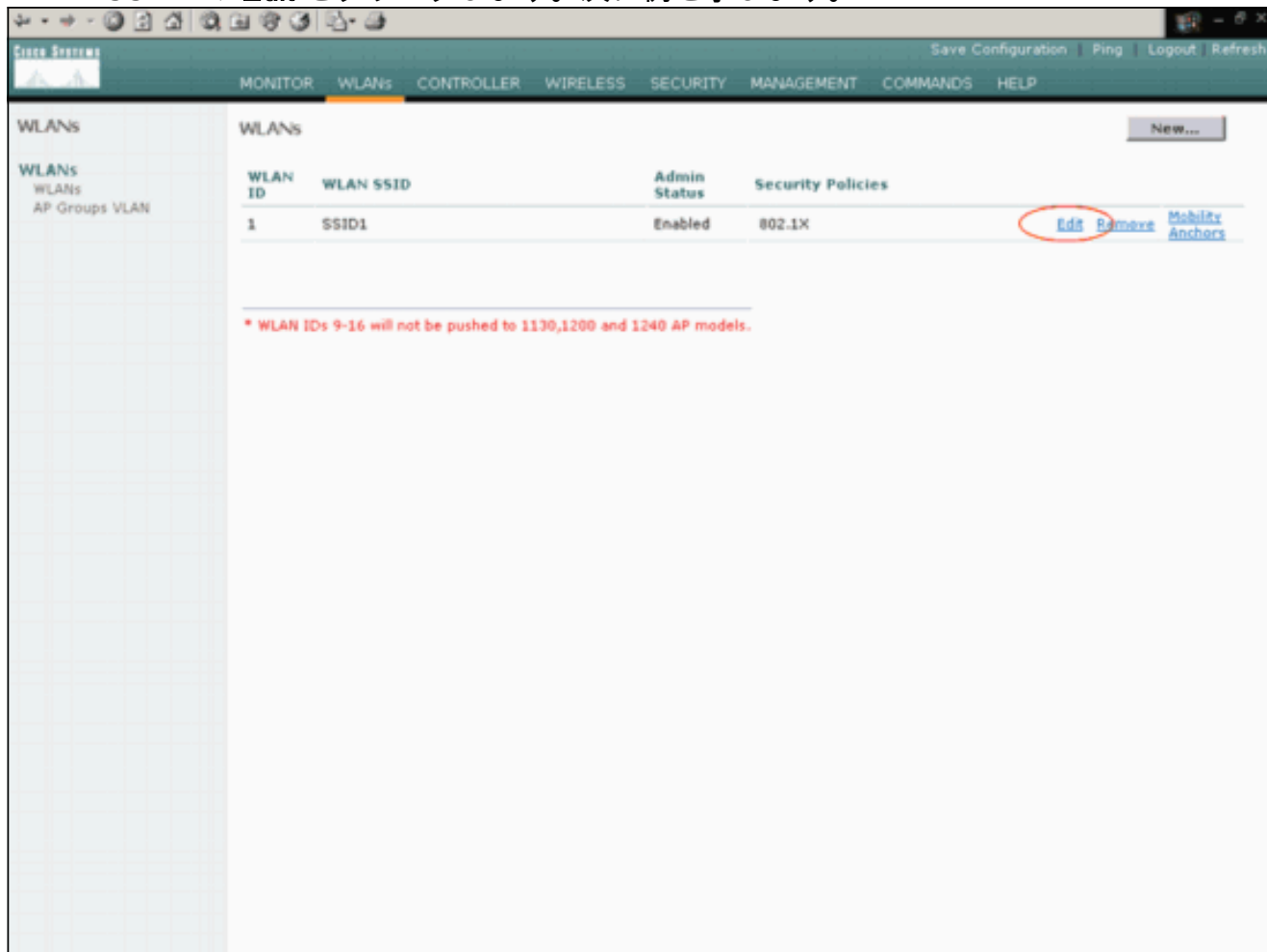
- システム名
- 管理インターフェイスの IP アドレス
- AP マネージャ インターフェイスの IP アドレス
- 管理インターフェイスのポート番号
- 管理インターフェイスの VLAN ID
- モビリティ グループの名前
- SSID
- 他の多数のパラメータ

これらのパラメータは、WLC を基本動作に設定するために使用します。このセクションの WLC 出力に示されているように、WLC では管理インターフェイス IP アドレスとして 172.16.1.50 が使用され、AP マネージャ インターフェイス IP アドレスとして 172.16.1.51 が使用されています。ネットワークに 2 つの WLAN を設定するためには、WLC で次の手順を実行します。

1. WLC の GUI で、ウィンドウの上部のメニューにある **WLANs** をクリックします。[WLANs] ウィンドウが表示されます。このウィンドウには、WLC に設定されている WLAN の一覧が表示されます。スタートアップ コンフィギュレーション ウィザードを使用して 1 つの

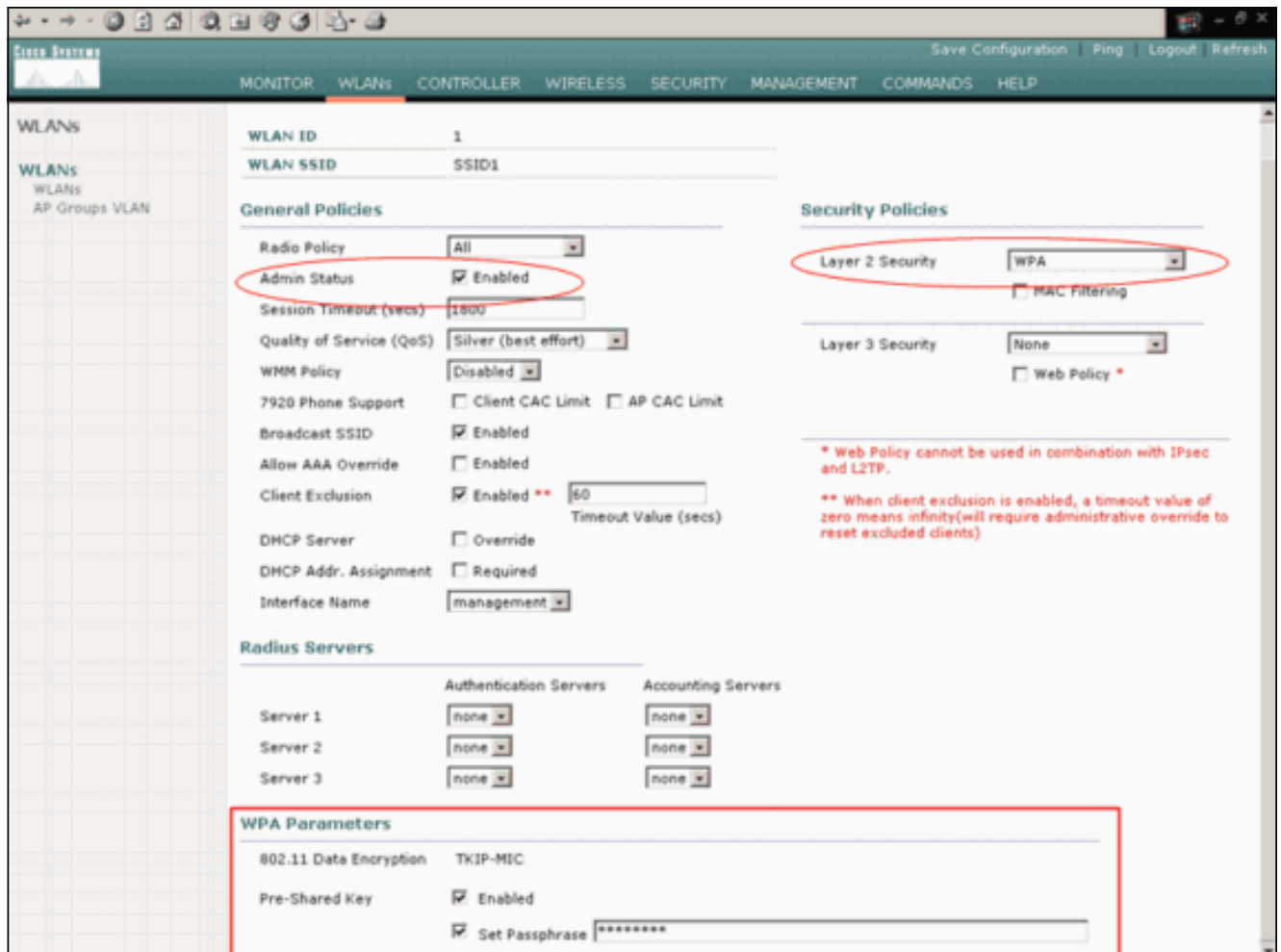
WLAN を設定したので、この WLAN の他のパラメータを設定する必要があります。

2. WLAN SSID1 の **Edit** をクリックします。次に例を示します。



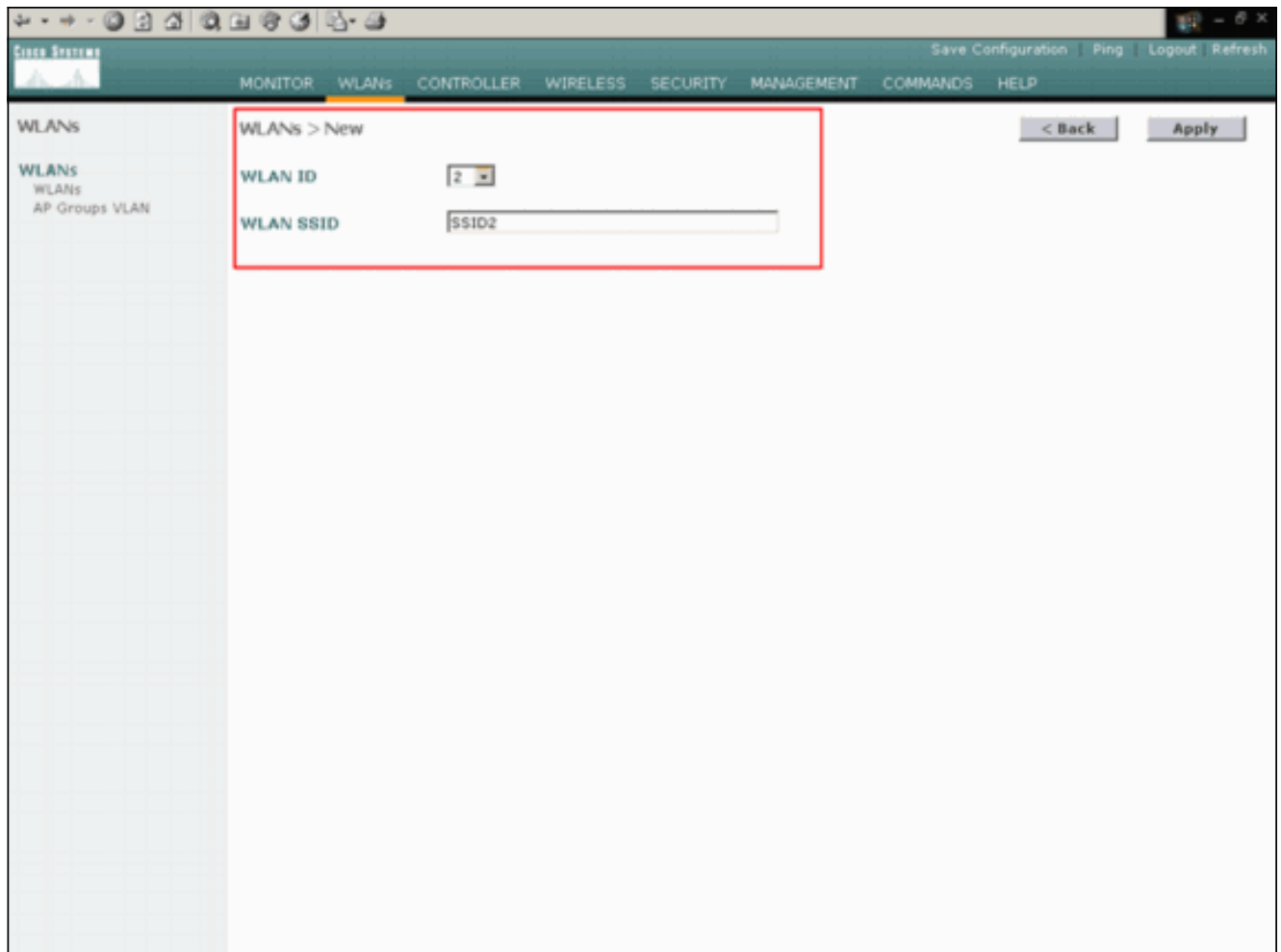
WLANs > Edit ウィンドウが表示されます。このウィンドウでは、General Policies、Security Policies、RADIUS server など、その WLAN に固有のパラメータを設定できます。

3. WLANs > Edit ウィンドウで次のように選択します。この WLAN を有効にするために、General Policies 領域にある Admin Status の横の **Enabled** チェックボックスにチェックマークを付けます。WLAN 1 で WPA を使用するために、Layer 2 Security ドロップダウンメニューから **WPA** を選択します。ウィンドウの最下部で WPA パラメータを定義します。WLAN 1 で WPA-PSK を使用するために、WPA Parameters 領域にある Pre-Shared Key の横の **Enabled** チェックボックスにチェックマークを付けて、WPA-PSK のパスフレーズを入力します。WPA-PSK では、暗号化に TKIP が使用されます。注: WPA-PSK のパスフレーズが、クライアント アダプタに設定されているパスフレーズと一致しなければ、WPA-PSK は正しく動作しません。[Apply] をクリックします。次に例を示します。



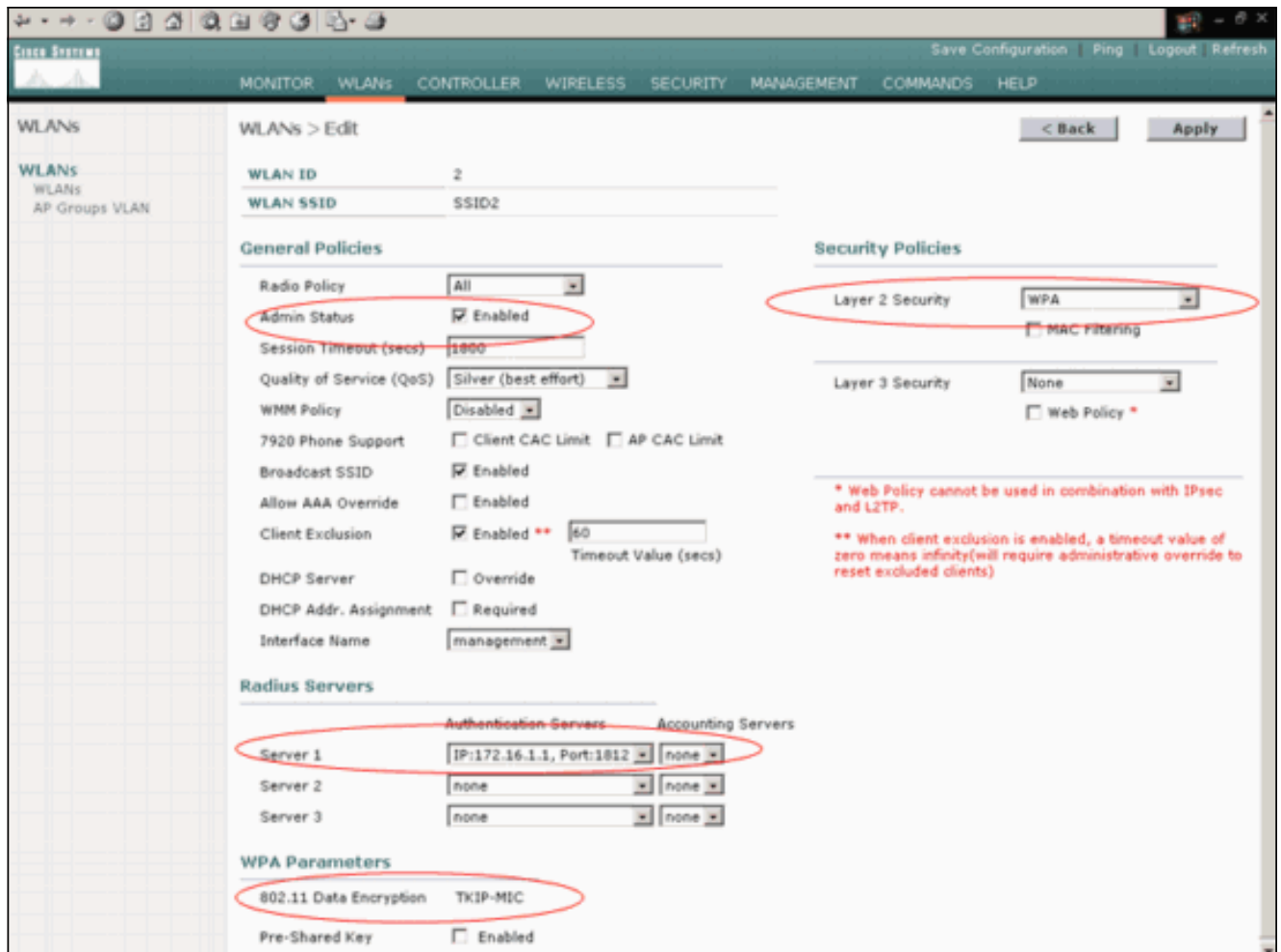
これで、WLAN 1 に WPA-PSK の暗号化を設定できました。

4. WLAN 2 を定義するために、WLANs ウィンドウにある **New** をクリックします。WLAN > New ウィンドウが表示されます。
5. WLAN > New ウィンドウで、WLAN ID と WLAN SSID を定義して、**Apply** をクリックします。次に例を示します。



2 番目の WLAN の WLAN > Edit ウィンドウが表示されます。

6. WLANs > Edit ウィンドウで次のように選択します。この WLAN を有効にするために、General Policies 領域にある Admin Status の横の **Enabled** チェックボックスにチェックマークを付けます。この WLAN に WPA を設定するために、Layer 2 Security ドロップダウンメニューから **WPA** を選択します。Radius Servers 領域で、このクライアントの認証に使用する適切な RADIUS サーバを選択します。[Apply] をクリックします。次に例を示します。



注: このドキュメントでは、RADIUS サーバと EAP 認証を設定する方法は説明していません。[WLC で EAP 認証を設定する方法については、『WLAN コントローラ \(WLC \) での EAP 認証の設定例』を参照してください。](#)

リモート サイトにインストールするための AP のプライミング

プライミングとは、自分が接続できるコントローラのリストを LAP が取得する処理のことです。1つのコントローラに LAP が接続するとすぐに、そのモビリティグループ内のすべてのコントローラが LAP に通知されます。そのようにして、LAP はグループ内の任意のコントローラに加入するために必要な情報をすべて学習します。

REAP 対応の AP のプライミングを行うためには、AP を本社の有線ネットワークに接続します。このように接続すると、AP が 1つのコントローラを見つけることができます。本社のコントローラに LAP が加入した後、WLAN のインフラストラクチャと設定に対応するバージョンの AP オペレーティングシステム (OS) のバージョンを AP がダウンロードします。モビリティグループ内のすべてのコントローラの IP アドレスが AP に転送されます。AP が必要な情報をすべて入手したら、AP をリモート サイトで接続できるようになります。IP 接続が使用できる場合は、リストから最も使用率が低いコントローラを AP が見つけて参加できます。

注: リモート サイトに発送するために電源をオフにする前に、AP が「REAP」モードに設定されていることを確認してください。コントローラの CLI か GUI を使用するか、Wireless Control System (WCS) のテンプレートを使用して、AP レベルでモードを設定できます。デフォルトでは、AP は通常の「local」機能を実行するように設定されています。

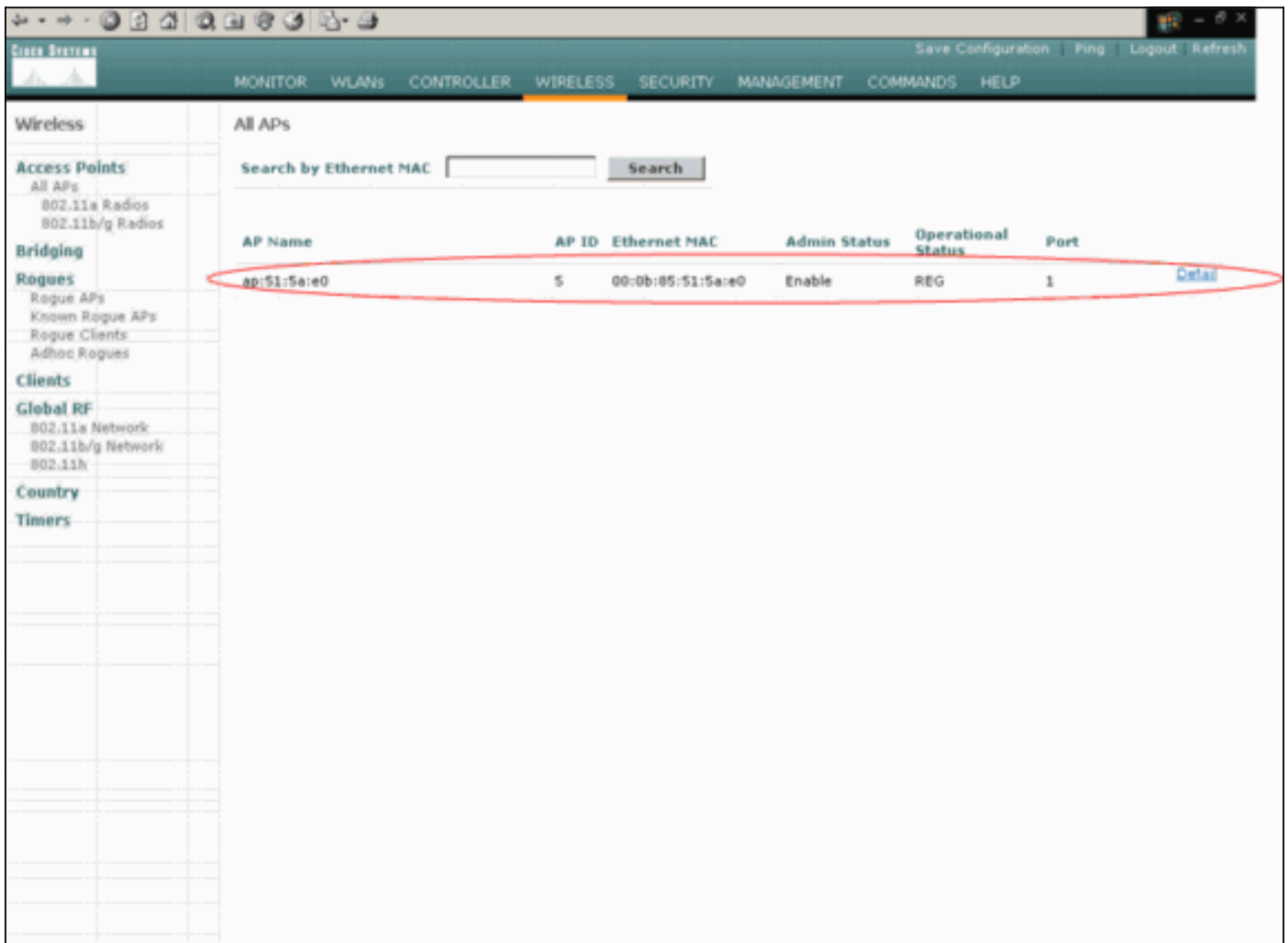
コントローラを見つけるために、LAP は次の方法のいずれかを使用できます。

- レイヤ 2 のディスカバリ

- レイヤ 3 のディスカバリローカル サブネットのブロードキャストの使用DHCP オプション 43 の使用DNS サーバの使用Over-the-Air Provisioning (OTAP) の使用内部 DHCP サーバの使用注: 内部 DHCP サーバを使用するためには、LAP を WLC に直接接続する必要があります。

このドキュメントでは、DHCP オプション 43 ディスカバリ メカニズムを使用して LAP が WLC に登録されていることを前提としています。 [DHCP オプション 43 を使用して LAP をコントローラに登録する方法および他のディスカバリ メカニズムについての詳細は、『ワイヤレス LAN コントローラ \(WLC \) への Lightweight AP \(LAP \) の登録』](#) を参照してください。

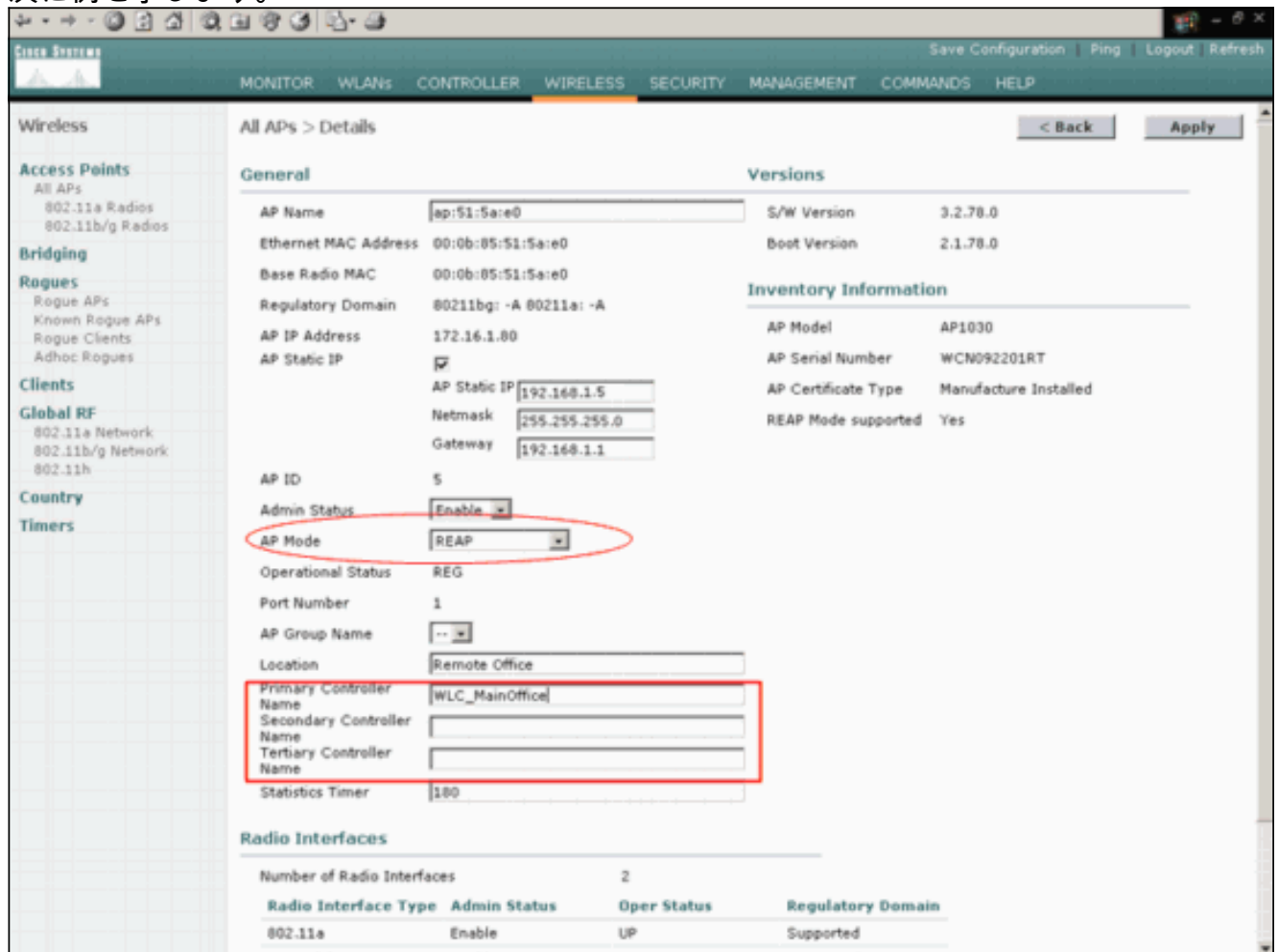
LAP がコントローラを見つけたら、AP がコントローラに登録されていることが WLC の Wireless ウィンドウに表示されます。次に例を示します。



通常の REAP モードに LAP を設定するには、次の手順を実行します。

1. WLC の GUI で、**[Wireless]** をクリックします。All APs ウィンドウが表示されます。このウィンドウには、WLC に登録されている AP の一覧が表示されます。
2. REAP モードに設定する必要がある AP を選択して、**Detail** をクリックします。その AP の All APs > Detail ウィンドウが表示されます。このウィンドウでは、次のような AP のさまざまなパラメータを設定できます。AP 名 IP アドレス (スタティックに変更できます) 管理ステータスセキュリティ パラメータ AP モード AP が接続できる WLC のリストその他のパラメータ
3. AP Mode ドロップダウン メニューから **REAP** を選択します。このモードを使用できるのは、REAP 対応の AP だけです。
4. AP が登録に使用するコントローラ名をを定義して、**Apply** をクリックします。最大 3 台

(プライマリ、セカンダリ、三次)のコントローラ名を定義できます。APは、このウィンドウに指定した順序でコントローラを検索します。この例では、コントローラを1台だけ使用しているので、そのコントローラをプライマリコントローラとして定義しています。次に例を示します。



これで AP を REAP モードに設定できたので、リモートサイトに AP を配備できます。

注: この例のウィンドウでは、AP の IP アドレスがスタティックに変更されて、192.168.1.5 という固定 IP アドレスが割り当てられていることがわかります。このように割り当てられているのは、これがリモート オフィスで使用するサブネットであるためです。そのため、DHCP サーバから取得する 172.16.1.80 という IP アドレスを使用するのは、プライミング段階の間だけです。AP がコントローラに登録された後に、アドレスをスタティック IP アドレスに変更します。

[2800 人のルータを WAN リンクを確立するために設定して下さい](#)

WAN リンクを確立するために、この例はネットワーク間のルート情報に OSPF と 2 人の 2800 シリーズ ルータを使用します。次に、このドキュメントのシナリオ例で使用する両方のルータの設定を示します。

本社

```
MainOffice#show run Building configuration... Current
configuration : 728 bytes ! version 12.2 service
timestamps debug uptime service timestamps log uptime no
service password-encryption ! hostname MainOffice ! ! ip
subnet-zero ! ! ! interface Ethernet0 ip address
172.16.1.60 255.255.0.0 !--- This is the interface which
acts as the default gateway to the WLC. ! interface
Virtual-Templatel no ip address ! interface Serial0 no
```

```
ip address ! interface Serial1 !--- This is the
interface for the WAN link. ip address 10.0.0.1
255.0.0.0 encapsulation ppp !--- This example uses PPP.
Use the appropriate !--- encapsulation for the WAN
connection. ! router ospf 50 !--- Use OSPF to route data
between the different networks. log-adjacency-changes
network 10.0.0.0 0.255.255.255 area 0 network 172.16.0.0
0.0.255.255 area 0 ! ! ip classless ip http server ! ! !
line con 0 line aux 0 line vty 0 4 ! end
```

ブランチオフィス

```
BranchOffice#show run Building configuration... Current
configuration : 596 bytes ! version 12.2 service
timestamps debug datetime msec service timestamps log
datetime msec no service password-encryption ! hostname
BranchOffice ! ! ip subnet-zero ! ! ! ! interface
Ethernet0 ip address 192.168.1.1 255.255.255.0 !--- This
is the interface which acts as the default gateway to
the LAP. ! interface Serial0 no ip address ! interface
Serial1 !--- This is the interface for the WAN link. ip
address 10.0.0.2 255.0.0.0 encapsulation ppp clockrate
56000 ! router ospf 50 !--- Use OSPF to route data
between the different networks. log-adjacency-changes
network 10.0.0.0 0.255.255.255 area 0 network
192.168.1.0 0.0.0.255 area 0 ! ip classless ip http
server ! ! ! ! line con 0 line aux 0 line vty 0 4 login
autocommand access enable-timeout 2 ! end
```

リモート サイトでの REAP AP の配備

WLC での WLAN の設定、LAP のプライミング、本社とリモート オフィスの WAN リンクの確立が完了したので、リモート サイトに AP を配布する準備が整いました。

リモート サイトで AP の電源を投入すると、プライミング段階に設定した順序で AP がコントローラを探します。AP がコントローラを見つけると、コントローラに AP が登録されます。次に例を示します。ポート 1 にあるコントローラに AP が参加したことが WLC に次のように表示されます。

The screenshot shows the Cisco Systems Wireless Management interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'WIRELESS' tab is selected. On the left, there is a sidebar menu with categories like 'Wireless', 'Access Points', 'Bridging', 'Rogues', 'Clients', 'Global RF', 'Country', and 'Timers'. The main content area is titled 'All APs' and features a search bar for 'Ethernet MAC'. Below the search bar is a table with the following columns: 'AP Name', 'AP ID', 'Ethernet MAC', 'Admin Status', 'Operational Status', and 'Port'. The first row of the table is circled in red and contains the following data: 'ap:51:5ae0', '5', '00-0b:05:51:5ae0', 'Enable', 'REG', and '1'. A 'Detail' link is visible at the end of this row.

AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port	
ap:51:5ae0	5	00-0b:05:51:5ae0	Enable	REG	1	Detail

どののために WPA-PSK が有効になるか SSID SSID1 があるクライアント、および、SSID SSID2 がある、802.1X 認証を有効にしてもらい WLAN 1.クライアントの AP への関連 WLAN 2.の AP への関連。2人のクライアントを表示する例はここにあります。1つのクライアントは WLAN 1 に接続されており、もう一つのクライアントは WLAN 2 に接続されています。

Save Configuration Ping Logout Ref Close

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Monitor Clients Items 1 to 2 of 2

Search by MAC address Search

Client MAC Addr	AP Name	AP MAC Addr	WLAN	Type	Status	Auth	Port	
00:40:96:ac:dd:05	ap:51:5a:e0	00:0b:85:51:5a:e0	SSID1	802.11a	Associated	Yes	1	Detail Link Test Disable Remove
00:40:96:ac:e6:57	ap:51:5a:e0	00:0b:85:51:5a:e0	SSID2	802.11a	Associated	Yes	1	Detail Link Test Disable Remove

Summary
Statistics
Controller Ports
Wireless
Rogue APs
Known Rogue APs
Rogue Clients
Adhoc Rogues
802.11a Radios
802.11b/g Radios
Clients
RADIUS Servers

確認

ここでは、REAP 設定が正常に動作していることを確認します。

注: [debug](#) コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

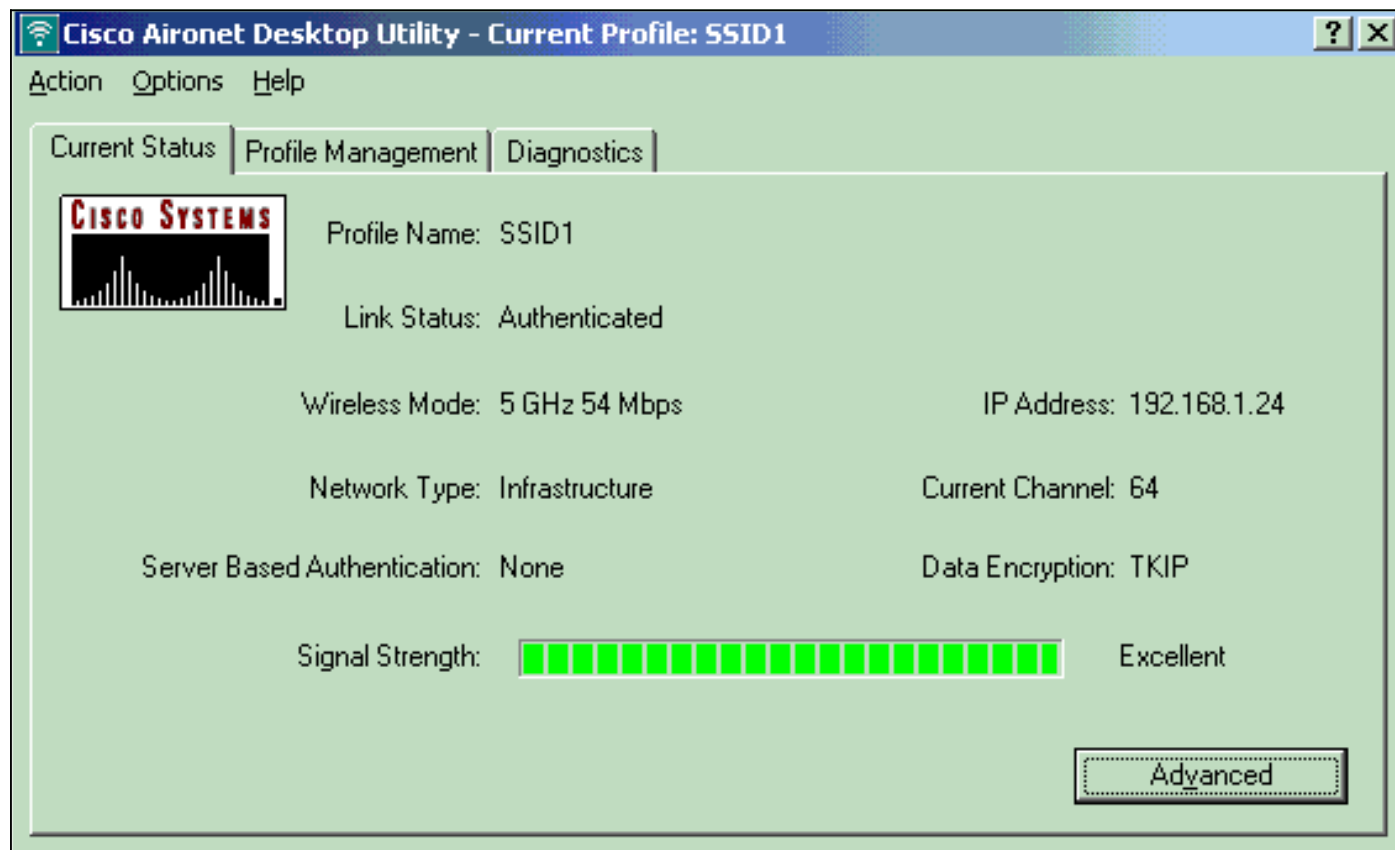
WAN リンクをダウン状態にします。WAN リンクがダウン状態になると、AP と WLC との接続が失われます。その場合、WLC は AP をリストから登録解除します。次に例を示します。

```
(Cisco Controller) >debug lwapp events enable Wed May 17 15:04:22 2006: Did not receive
heartbeat reply from AP 00:0B:85:51:5A:E0 Wed May 17 15:04:22 2006: Max retransmissions reached
on AP 00:0B:85:51:5A:E0 (CONFIGURE_COMMAND, 1) Wed May 17 15:04:22 2006:
apfSpamProcessStateChangeInSpamContext: Down LWAPP event for AP 00:0b:85:51:5a:e0 slot 0 Wed May
17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event for AP
00:0b:85:51:5a:e0 slot 0 Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Down
LWAPP event for AP 00:0b:85:51:5a:e0 slot 1 Wed May 17 15:04:22 2006:
apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event for AP 00:0b:85:51:5a:e0 slot 1
Wed May 17 15:04:22 2006: spamDeleteLCB: stats timer not initialized for AP 00:0b:85:51:5a:e0
Wed May 17 15:04:22 2006: Received LWAPP Down event for AP 00:0b:85:51:5a:e0 slot 0! Wed May 17
15:04:22 2006: Deregister LWAPP event for AP 00:0b:85:51:5a:e0 slot 0 Wed May 17 15:04:22 2006:
Received LWAPP Down event for AP 00:0b:85:51:5a:e0 slot 1! Wed May 17 15:04:22 2006: Deregister
LWAPP event for AP 00:0b:85:51:5a:e0 slot 1
```

`debug lwapp events enable` コマンドの出力には、WLC が AP からハートビートの応答を受信しなかったため、WLC が AP の登録を解除したことが示されています。ハートビートの応答は、キープアライブメッセージと同様のものです。コントローラは 1 秒間の間隔を空けてハートビートを 5 回連続して試みます。WLC が応答を受信しなければ、WLC は AP を登録解除します。

AP がスタンダアロン モードの時には、AP の電源 LED が点滅します。最初の WLAN (WLAN 1) のクライアントは WPA-PSK の暗号化専用設定されているので、最初の WLAN (WLAN 1) に関連付けられているクライアントはその AP に引き続き関連付けられています。スタンダアロン モードでは、LAP が自分で暗号化も処理します。次の例は、SSID1 および WPA-PSK を使用して WLAN 1 に接続されているクライアントの (WAN リンクがダウンしているときの) ステータスを示しています。

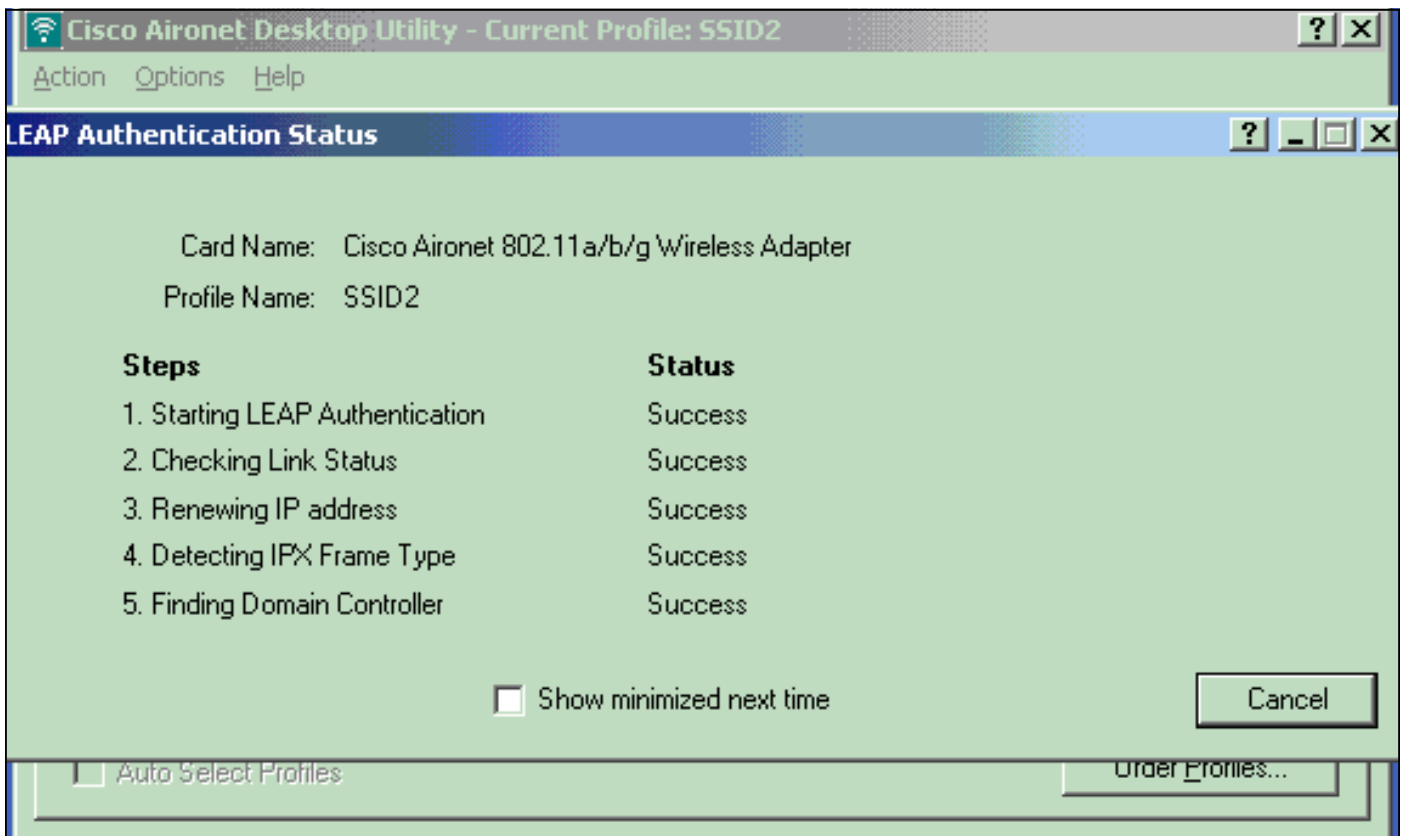
注: TKIP は WPA-PSK で使用されている暗号化アルゴリズムです。



WLAN 2 では EAP 認証が使用されているので、WLAN 2 に接続されているクライアントは接続解除されます。このように接続解除されるのは、EAP 認証を使用するクライアントは WLC と通信する必要があるためです。次のウィンドウの例には、WAN リンクがダウンしているときに EAP 認証が失敗する例が示されています。



WAN リンクがアップしたら、AP は通常の REAP モードに再び切り替わり、コントローラに登録されます。EAP 認証を使用するクライアントもアップ状態になります。次に例を示します。



この例では、コントローラの `debug lwapp events enable` コマンドの出力は、次のような結果になります。

```
(Cisco Controller) >debug lwapp events enable Wed May 17 15:06:40 2006: Successful transmission
of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1 Wed May 17 15:06:52 2006: Received
LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0to 00:0b:85:33:84:a0 on port '1' Wed May 17 15:06:52
2006: LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0is 1500, remote debug mode is 0 Wed
May 17 15:06:52 2006: Successfully added NPU Entry for AP 00:0b:85:51:5a:e0(index 51) Switch IP:
172.16.1.51, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 192.168.1.5, AP Port: 5550, next hop
MAC: 00:d0:58:ad:ae:cb Wed May 17 15:06:52 2006: Successfully transmission of LWAPP Join-Reply
to AP 00:0b:85:51:5a:e0 Wed May 17 15:06:52 2006: Register LWAPP event for AP 00:0b:85:51:5a:e0
```



```
slot 0 Wed May 17 15:06:52 2006: Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 1 Wed May 17
15:06:54 2006: Received LWAPP CONFIGURE REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:84:a0
Wed May 17 15:06:54 2006: Updating IP info for AP 00:0b:85:51:5a:e0 -- static 1,
192.168.1.5/255.255.255.0, gtw 192.168.1.1
```

トラブルシューティング

ここでは、設定に関するトラブルシューティングについて説明します。

トラブルシューティングのためのコマンド

次の `debug` コマンドを使用して、設定のトラブルシューティングを行うことができます。

注: `debug` コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

- `debug lwapp events enable` : LAP と WLC の間で発生するイベントのシーケンスが表示されます。
- `debug lwapp errors enable` : LWAPP 通信で発生するエラーが表示されます。
- `debug lwapp packet enable` : LWAPP パケットトレースのデバッグが表示されます。
- `debug mac addr` : 指定したクライアントの MAC デバッグが有効になります。

関連情報

- [ブランチオフィスでの REAP 導入ガイド](#)
- [WLAN Controller \(WLC \) での EAP 認証の設定例](#)
- [Wireless LAN Controller と Lightweight アクセス ポイントの基本設定例](#)
- [Lightweight アクセス ポイントの WLAN コントローラ フェールオーバーの設定例](#)
- [ワイヤレスに関するサポート ページ](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)