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

はじめに

Cisco Unified Wireless Network ともたらされるリモート エッジ アクセス ポイント（REAP）機能は Wireless LAN（WLAN）コントローラ（WLC）からの Cisco Lightweight アクセスポイント（LAP）のリモート配備を可能にします。 これはそれらにブランチ オフィスおよび小さいリテール場所のための理想をします。 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。

- WLCs のナレッジおよび WLC 基本的なパラメータを設定する方法を
- Cisco の REAP 動作モードのナレッジ 1030 LAP
- 外部 DHCP サーバやドメイン ネーム システム（DNS）サーバの設定のナレッジ

- Wi-Fi プロテクテッド アクセス（WPA）概念のナレッジ

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

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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 モードは WAN リンクを渡って常駐することを LAP が可能にしまだ WLC と通信し、規則的な LAP の機能性を提供できます。 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。

この機能性を提供するために、1030 REAP はワイヤレス データ平面から Lightweight Access Point Protocol（LWAPP）コントロール プレーンを分けます。 すべてのユーザのデータは AP でローカルで繋がれるが規則的な LWAPP ベースのアクセス ポイント（AP）が使用されること Cisco WLCs はまだ集中制御および管理のために同じように使用されます。 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 は 2 つの動作モードをサポートします:

- 正常な REAP モード
- 独立方式

LAP は正常な REAP モードで REAP AP および WLC 間の WAN リンクが稼働しているとき設定されます。 ラップが正常な REAP モードで動作するとき、16 WLAN までサポートできます。

WLC と LAP 間の WAN リンクがダウン状態になるとき、REAP 有効に された LAP は独立方式に切り替えます。 独立方式で、REAP ラップは WLC なしで 1 WLAN だけ独自にサポートできます間、WLAN が Wired Equivalent Privacy（WEP）かローカル認証方式で設定される場合。 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。 独立方式では、ラップは最小いくつかの特性をサポートします。 この表は稼働している）（WAN リンクが WLC へのアップおよび通信のとき REAP LAP が通常モードでサポートする機能と比べて独立方式にあるとき REAP LAP サポートことをいくつかの特性に示したものです:

機能こと正常な REAP モードと独立方式の REAP LAP サポート

		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

表は複数の VLAN が Both モードの REAP ラップでサポートされないことを示したものです。 複数の VLAN は IEEE 802.1Q VLAN タギングを行うことができないので REAP ラップが単一のサブネットにしか常駐できないのでサポートされません。 従って、サービス セット識別（SSID）のそれぞれのトラフィックは有線ネットワークとして同じ サブネットで終端します。 その結果、データトラフィックは配線された側でワイヤレス トラフィックが SSID 間のセグメント化された地上波であるかもしれないのに分かれません。

REAP 配備に関する詳細については[ブランチ オフィスで REAP 配備ガイドを]、REAP および制限を管理する方法を参照すれば。

設定

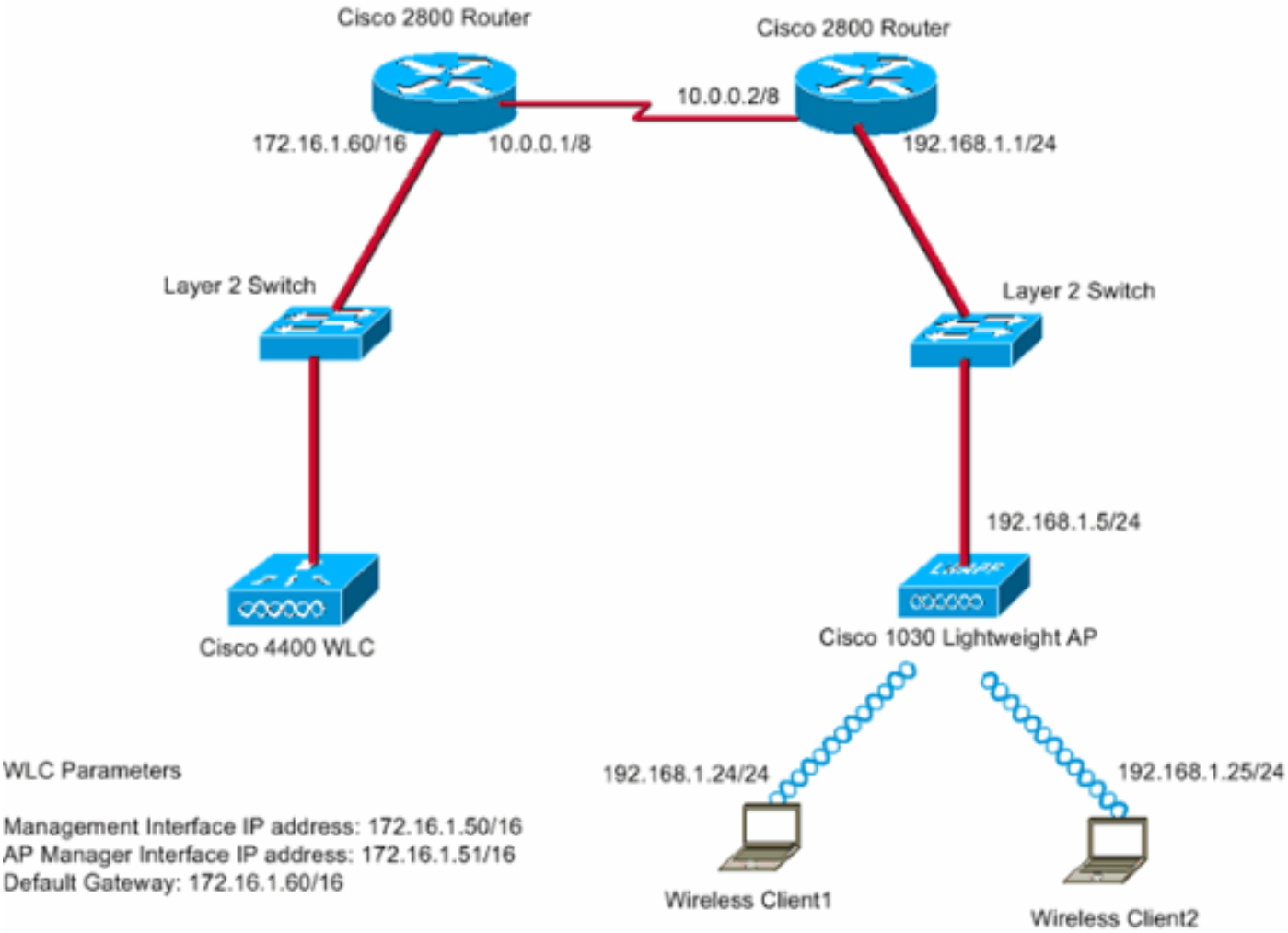
この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

デバイスをネットワーク設定を設定するために設定するためにこれらのステップを完了して下さい:

1. 基本動作のための WLC を設定し、WLAN を設定して下さい。
2. リモートサイトでインストールのための AP の発動を促して下さい。
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 REAP LAP を展開して下さい。

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。



主要なオフィスは専用回線の使用とブランチ オフィスに接続します。 専用回線は各端に 2800 シリーズ ルータで終端させます。 この例は PPP カプセル化を用いる WAN リンクのデータをルーティングするのに Open Shortest Path First (OSPF) プロトコルを使用します。 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 は 2 WLAN をサポートする必要があります。 WLAN のためのパラメータはここにあります:

- WLAN1SSID — **SSID1認証—開いて下さい**encryption — **Temporal Key Integrity Protocol (TKIP) （WPA 事前共有キー[WPA-PSK])**

- **WLAN 2**SSID — **SSID2**認証— **Extensible Authentication Protocol（EAP）** encryption — **TKIP注:** WLAN 2 に関しては、この資料の設定は WPA を使用します（暗号化のための 802.1X 認証および TKIP）。

この設定用のデバイスを設定して下さい。

基本動作のための WLC を設定し、WLAN を設定して下さい

基本動作のための WLC を設定するために Command Line Interface（CLI）のスタートアップ コンフィギュレーション ウィザードを使用できます。 また、また WLC を設定するために GUI を使用できます。 この資料は CLI のスタートアップ コンフィギュレーション ウィザードの使用の WLC の設定を説明したものです。

WLC ははじめて起動した後、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。 Configuration ウィザードを基本的な設定を行うのに使用します。 CLI または GUI のウィザードを実行できます。 スタートアップ コンフィギュレーション ウィザードの例はここにあります:

```
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...
```

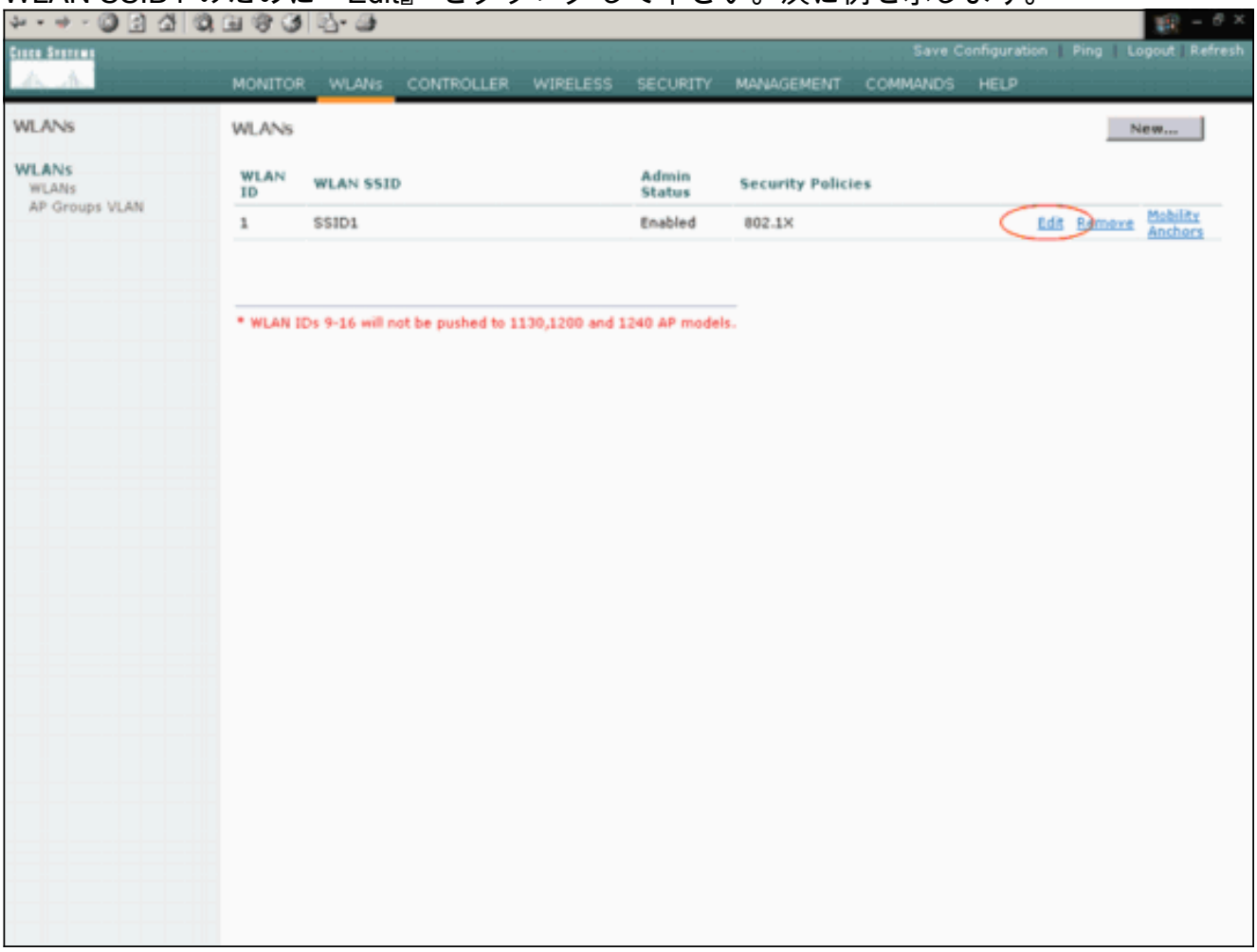
この例は WLC のこれらのパラメータを設定したものです:

- システム 名
- 管理インターフェイス IP アドレス
- AP マネージャ インターフェイス IP アドレス
- 管理インターフェイス ポート番号
- 管理インターフェイス VLAN識別名
- モビリティグループ名前
- SSID

- 他の多くのパラメータ

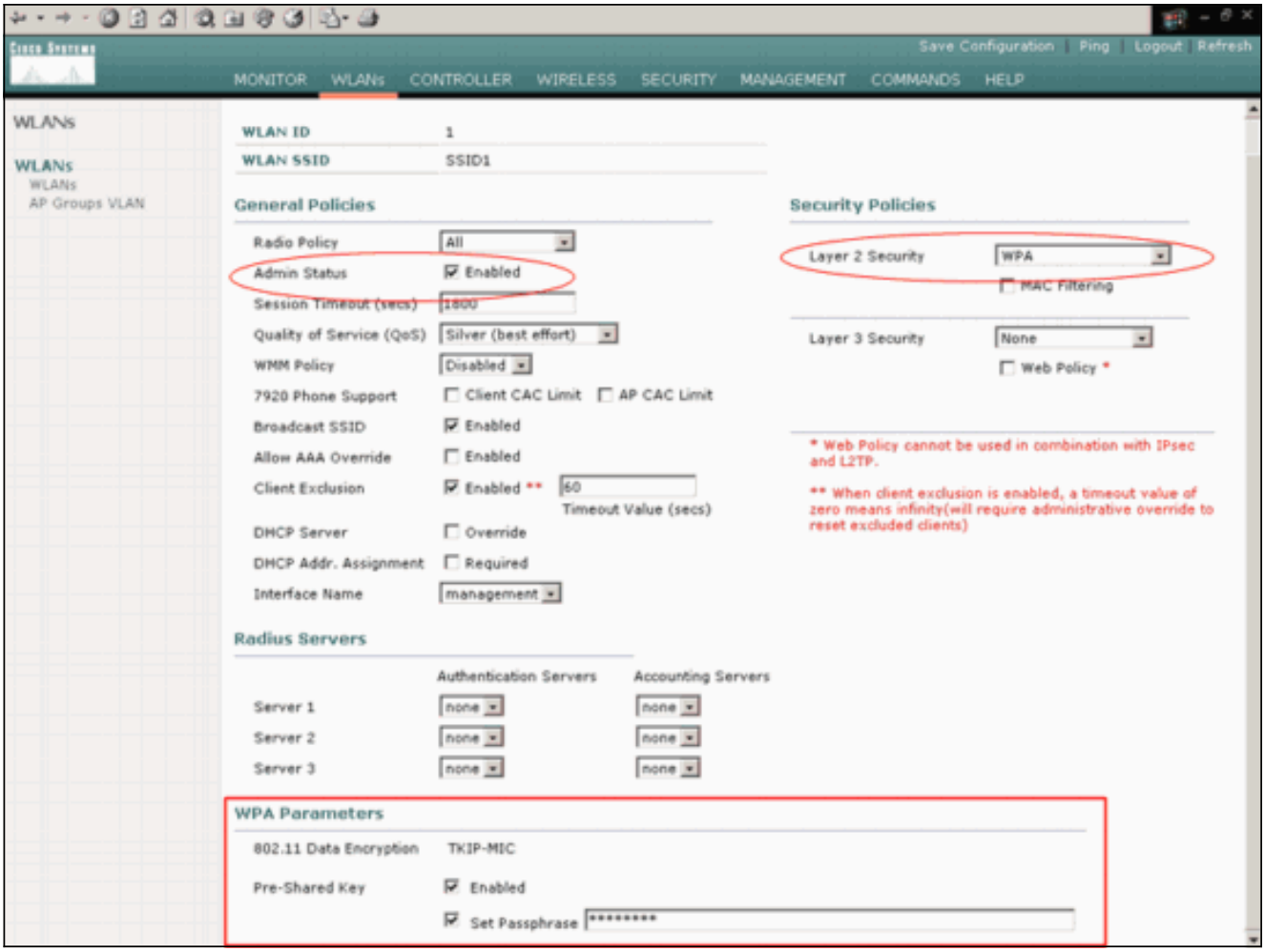
これらのパラメータが基本動作のための WLC を設定するのに使用されています。 このセクションの WLC 出力が示すと同時に、WLC は管理インターフェイス IP アドレスとして 172.16.1.50 および AP マネージャ インターフェイス IP アドレスとして 172.16.1.51 を使用します。 ネットワークのための 2 WLAN を設定するために、WLC のこれらのステップを完了して下さい:

1. WLC GUI から、ウィンドウの上でメニューで『WLAN』 をクリック して下さい。[WLANs] ウィンドウが表示されます。 このウィンドウは WLC で設定される WLAN をリストします。 スタートアップ コンフィギュレーション ウィザードの使用で 1 WLAN を設定したので、この WLAN のための他のパラメータを設定して下さい。
2. WLAN SSID1 のために『Edit』 をクリック して下さい。次に例を示します。



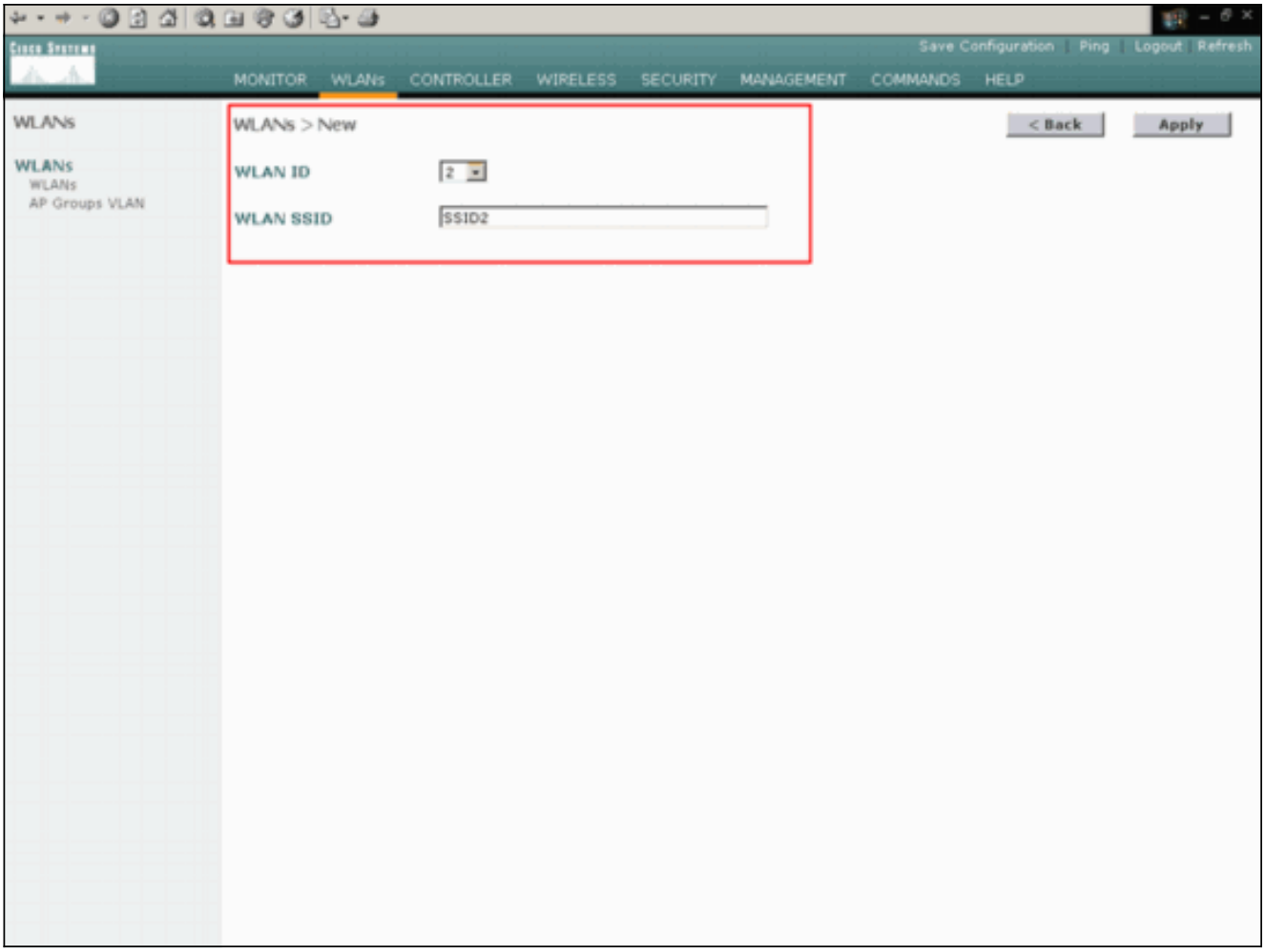
WLAN > Edit Window は現われます。 このウィンドウで、総合政策を、セキュリティポリシー、RADIUSサーバ、WLAN に特定であるパラメータを設定でき含む、他。

3. WLAN > Edit Window のこれらの選択をして下さい:総合政策領域では、この WLAN を有効に するために管理状態の側の **Enabled チェックボックスを**チェックして下さい。WLAN 1.のために WPA を使用するためにレイヤ2 セキュリティ ドロップダウン メニューから『WPA』 を選択 して下さい。ウィンドウの下部ので WPA パラメータを定義して下さい。WLAN 1 の WPA-PSK を使用するために、WPA パラメータ領域の事前共有キーの側の **Enabled チェックボックスを**チェックし、WPA-PSK のためのパスフレーズを入力して下さい。 WPA-PSK は暗号化のために TKIP を使用します。**注:** WPA-PSK パスフレーズは WPA-PSK がはたらかせることができるようにパスフレーズを一致する必要がありますクライアントアダプタで設定される。[Apply] をクリックします。次に例を示します。



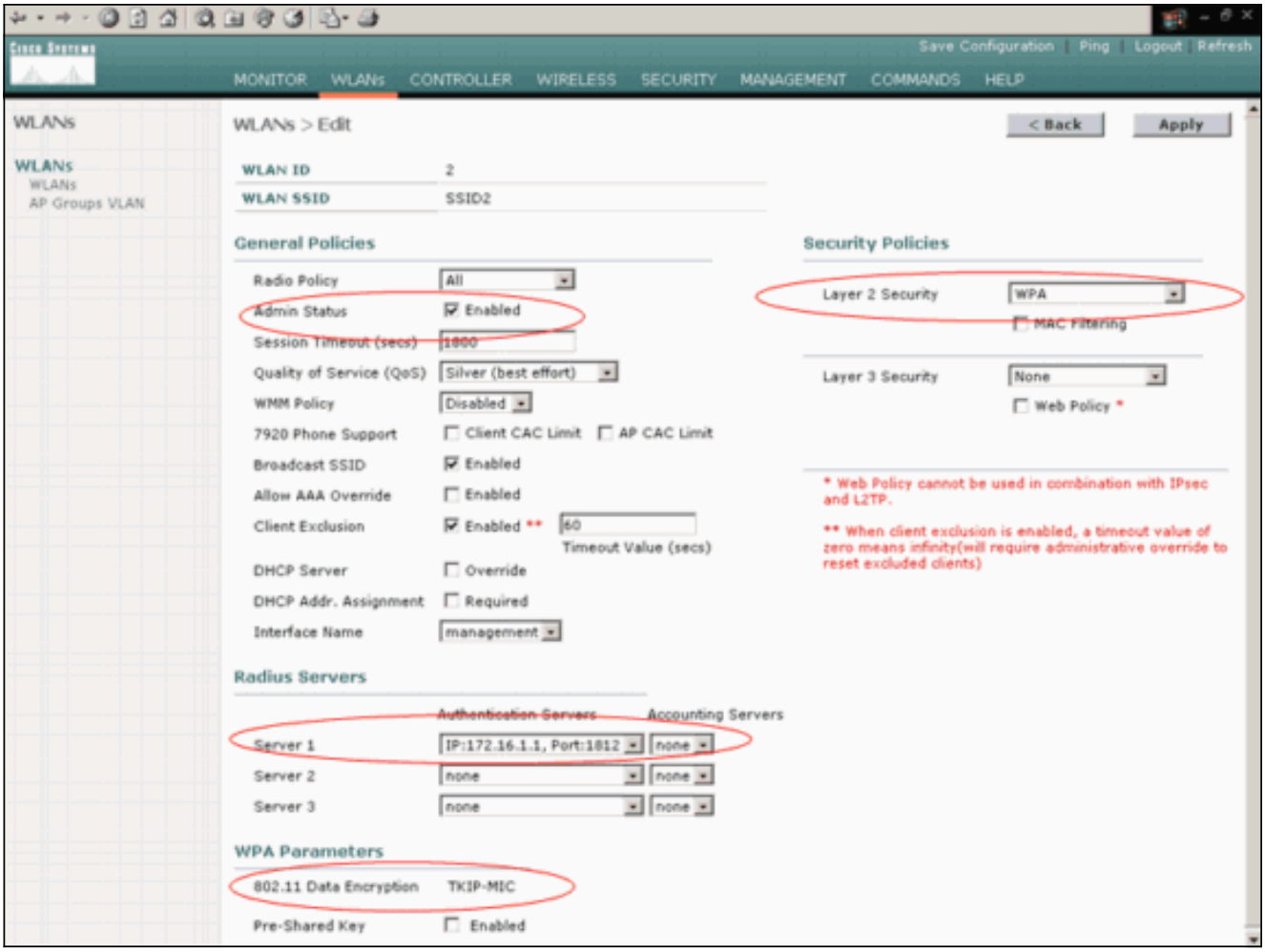
WPA-PSK 暗号化のための WLAN 1 を設定しました。

4. WLAN 2 を定義するために、WLAN ウィンドウで『New』 をクリック して下さい。WLAN > New ウィンドウは現われます。
5. では WLAN > New ウィンドウは、WLAN ID および WLAN SSID を定義し、『Apply』 をクリック します。次に例を示します。



第 2 WLAN のための WLAN > Edit Window は現われます。

6. WLAN > Edit Window のこれらの選択をして下さい:総合政策領域では、この WLAN を有効に するために管理状態の側の **Enabled チェックボックスを**チェックして下さい。この WLAN のための WPA を設定するためにレイヤ2 セキュリティ ドロップダウン メニューから『WPA』 を選択 して下さい。RADIUSサーバ エリアで、クライアントの認証のために使用するために適切な RADIUSサーバを選択して下さい。[Apply] をクリックします。次に例を示します。



注: この資料に RADIUSサーバおよび EAP 認証を設定する方法を説明されていません。 WLCs で EAP 認証を設定する方法の情報に関しては WLAN コントローラ（ WLC ）設定例の EAP 認証を参照して下さい。

リモートサイトでインストールのための AP の発動を促して下さい

起爆剤はラップが接続できるコントローラのリストを入手するプロセスです。 ラップは単一 コントローラに接続するとすぐモビリティグループのすべてのコントローラの知識のあります。 このように、ラップはグループのコントローラに加入する必要があるすべての情報を学びます。

REAP 可能な AP の発動を促すために、主要なオフィスで有線ネットワークに AP を接続して下さい。 この接続は AP が単一 コントローラを検出するようにします。 LAP が主要なオフィスでコントローラに加入した後、AP は WLAN インフラストラクチャおよび設定と対応する AP Operating System （ OS ）バージョンをダウンロードします。 モビリティグループのすべてのコントローラの IP アドレスは AP に転送されます。 AP に必要とするすべての情報があるとき、AP は遠隔地で接続することができます。 AP は IP 接続が利用できる場合そしてリストからの最少利用されたコントローラを検出し、加入できます。

注: リモートサイトにそれらを出荷するためにそれらを消す前に」モードを収獲するために AP を「設定 したことを確かめて下さい。 コントローラ CLI か GUI を通して、または Wireless Control System （ WCS ）テンプレートの使用と AP レベルでモードを設定できます。 AP は常連を、「ローカル」機能性デフォルトで行うために設定 されます。

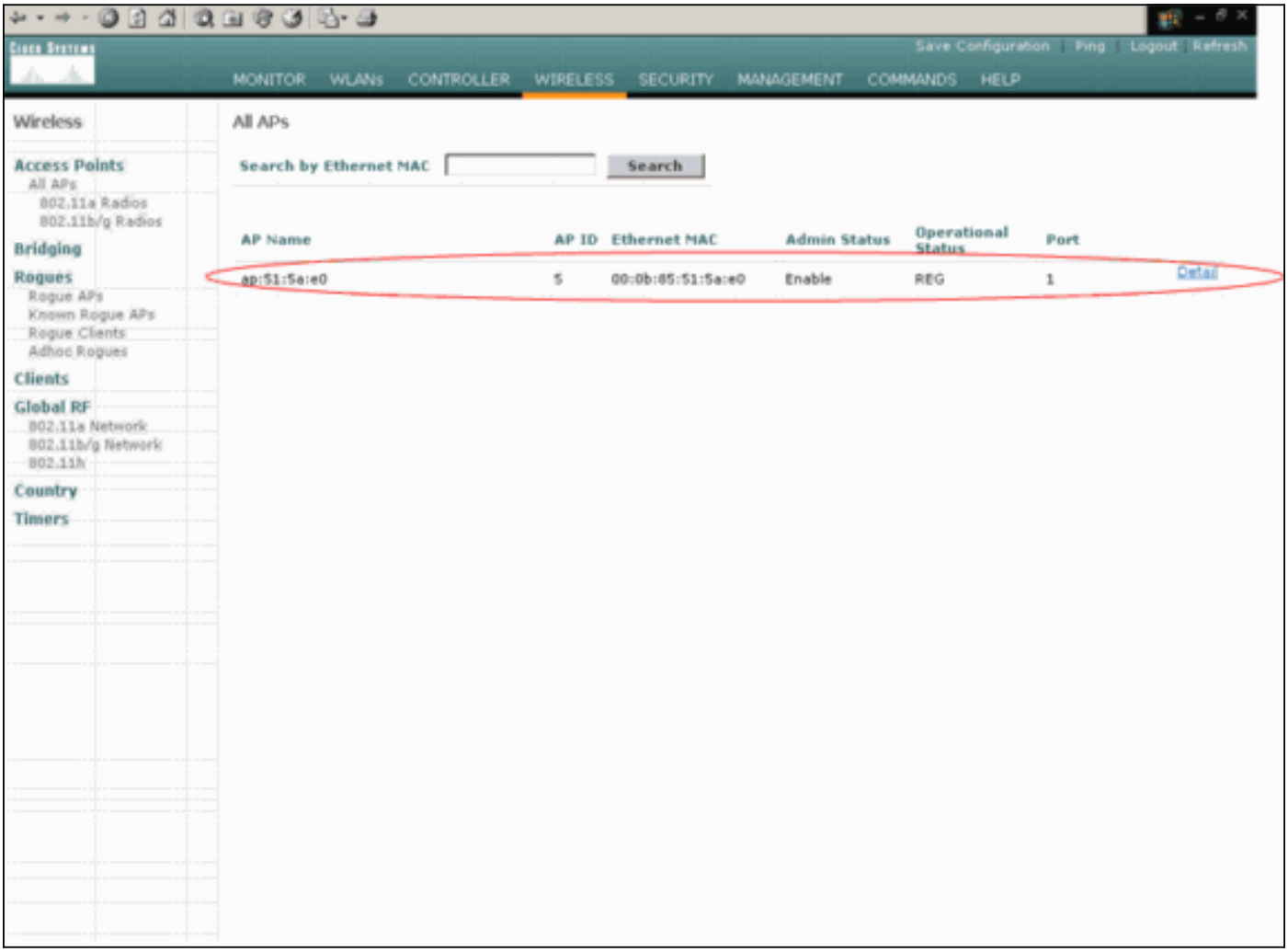
ラップはこれらのメソッドのコントローラを検出するためにどれでも使用できます:

- **レイヤ2 ディスカバリ**

- **レイヤ3 ディスカバリ**ローカル サブネットブロードキャストの使用を使ってDHCP オプション 43 の使用を使ってDNS サーバの使用を使ってを使って無線 プロビジョニング（OTAP）の使用内部 DHCP サーバの使用を使って**注:** 内部 DHCP サーバを使用するために、LAP は WLC に直接接続する必要があります。

この資料は LAP が DHCP オプション 43 ディスカバリ メカニズムの使用の WLC に登録すると仮定します。 コントローラに LAP を、また他のディスカバリ メカニズム登録する、DHCP オプション 43 の使用に関する詳細については[ワイヤレス LAN コントローラ（WLC）に簡易 AP（LAP）登録を](#)参照して下さい。

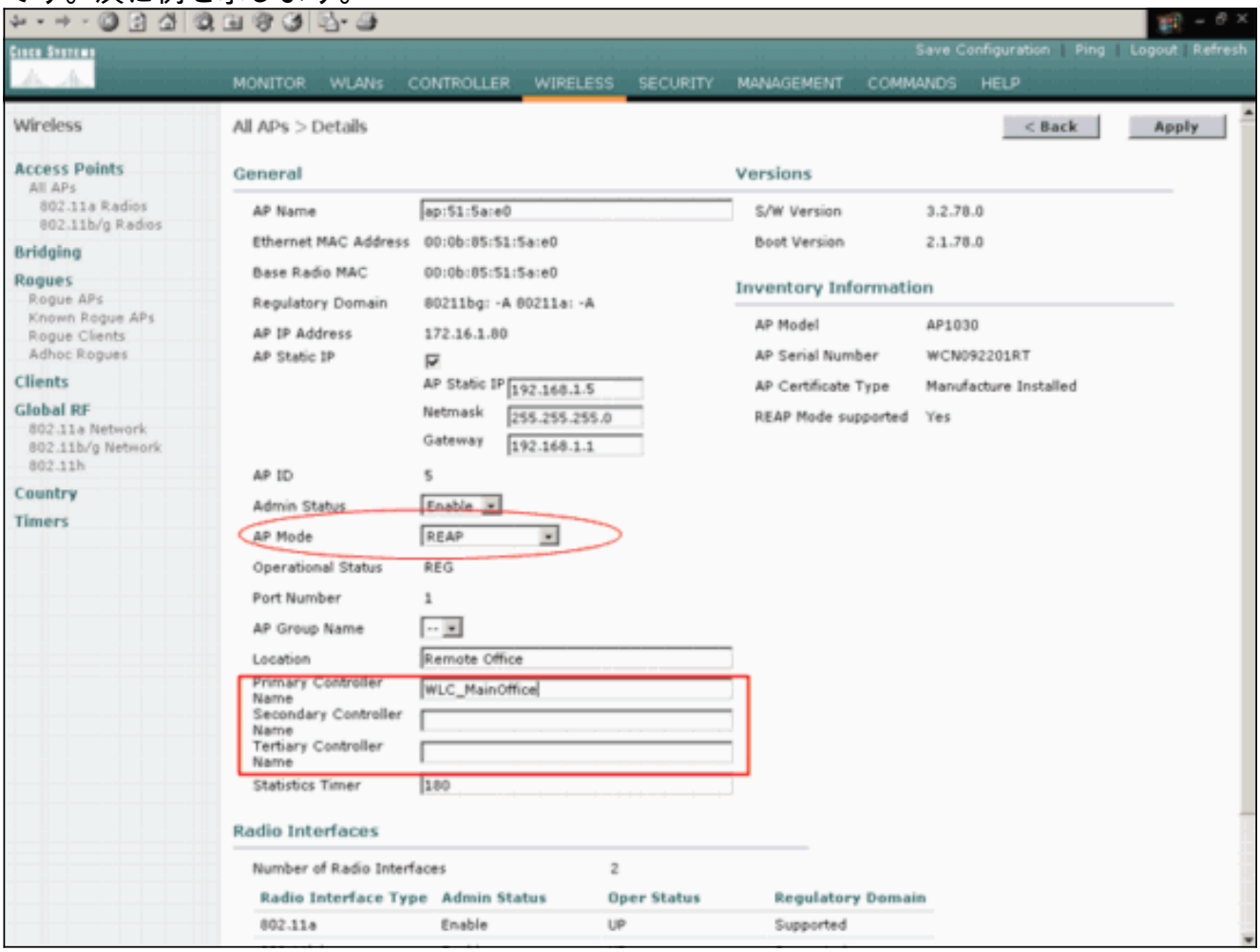
LAP がコントローラを検出した後、AP が WLC の Wireless ウィンドウのコントローラに登録されていることがわかります。 次に例を示します。



正常な REAP モードのための LAP を設定するためにこれらのステップを完了して下さい:

1. WLC GUI から、『Wireless』 をクリック して下さい。すべての AP ウィンドウは現われます。 このウィンドウは WLC に登録されている AP をリストします。
2. REAP モードのために『Detail』 をクリック する設定し、必要がある AP を選択して下さい。すべては AP > 特定の AP のための Detail ウィンドウ現われます。 このウィンドウで、下記のものを含めて AP のさまざまなパラメータを設定できます:AP 名前（スタティックに変更できる） IP アドレス管理状態セキュリティ パラメータAPモードAP が接続できる WLCs のリストその他のパラメータ
3. APモード ドロップダウン メニューから『REAP』 を選択 して下さい。このモードは REAP 可能な AP だけで利用できます。
4. AP が登録し、『Apply』 をクリック するのに使用するコントローラー名を定義して下さい

。3 つまでのコントローラー名 (プライマリ、セカンダリ、および第三) を定義できます。 AP はこのウィンドウで提供する同じ順序でコントローラを捜します。 この例が 1 人のコントローラだけ使用するので、例はプライマリ コントローラとコントローラを定義したものです。次に例を示します。



REAP モードのための AP を設定し、リモートサイトでそれを展開できます。

注: このウィンドウ例で、AP の IP アドレスがスタティックに変更され、静的IP アドレス 192.168.1.5 が割り当てられることがわかります。 この割り当てはこれがリモートオフィスで使用されるべきサブネットであるので発生します。 従って DHCP サーバからの IP アドレスを、172.16.1.80、だけ起爆剤ステージの間に使用します。 AP がコントローラに登録されていた後、静的IP アドレスにアドレスを変更します。

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。 この資料の例のシナリオのための両方のルータの設定はここにあります:

MainOffice

```
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-Template1 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
```

BranchOffice

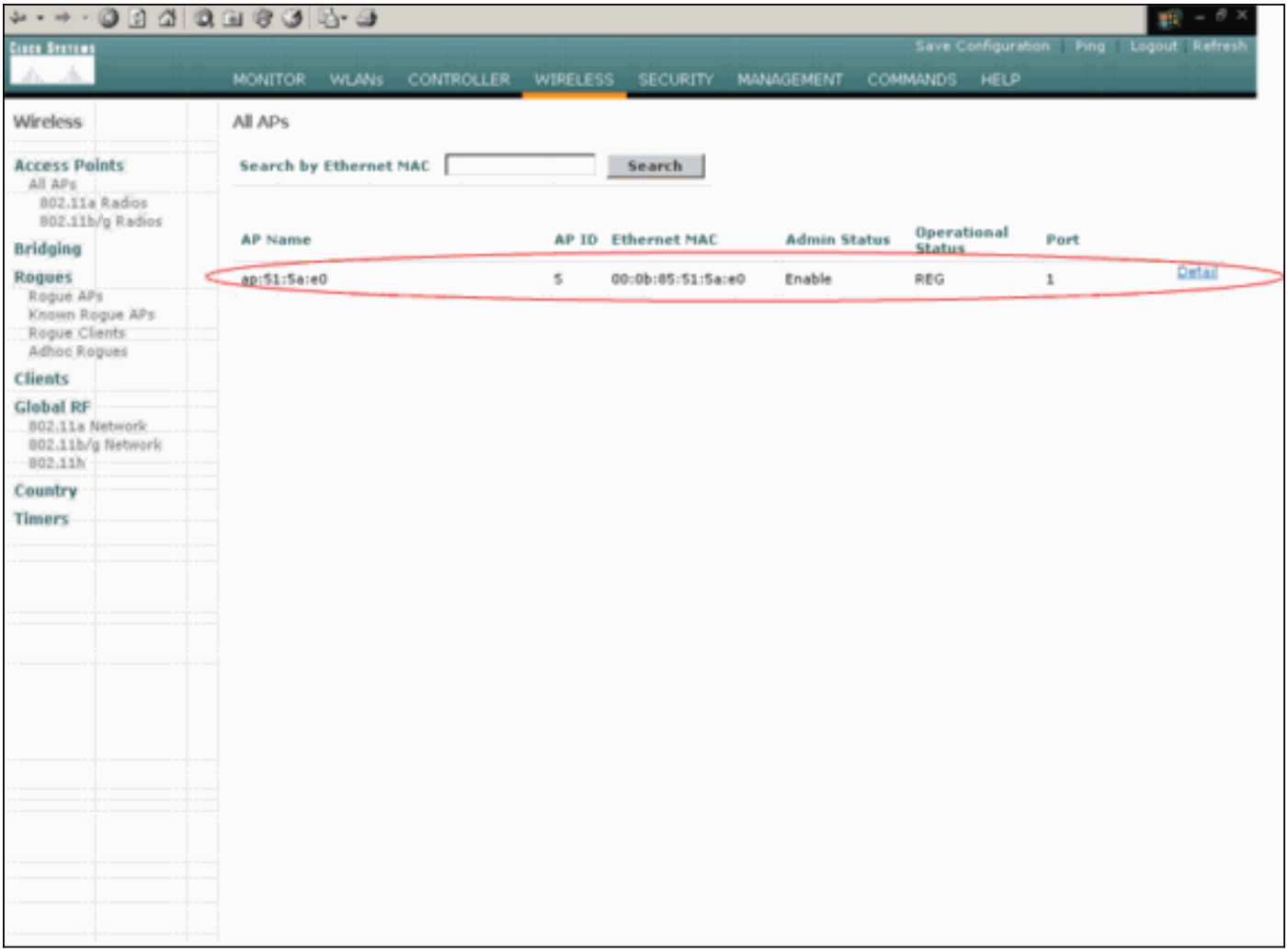
```
BranchOffice#show run
Building configuration...

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 REAP AP を展開して下さい

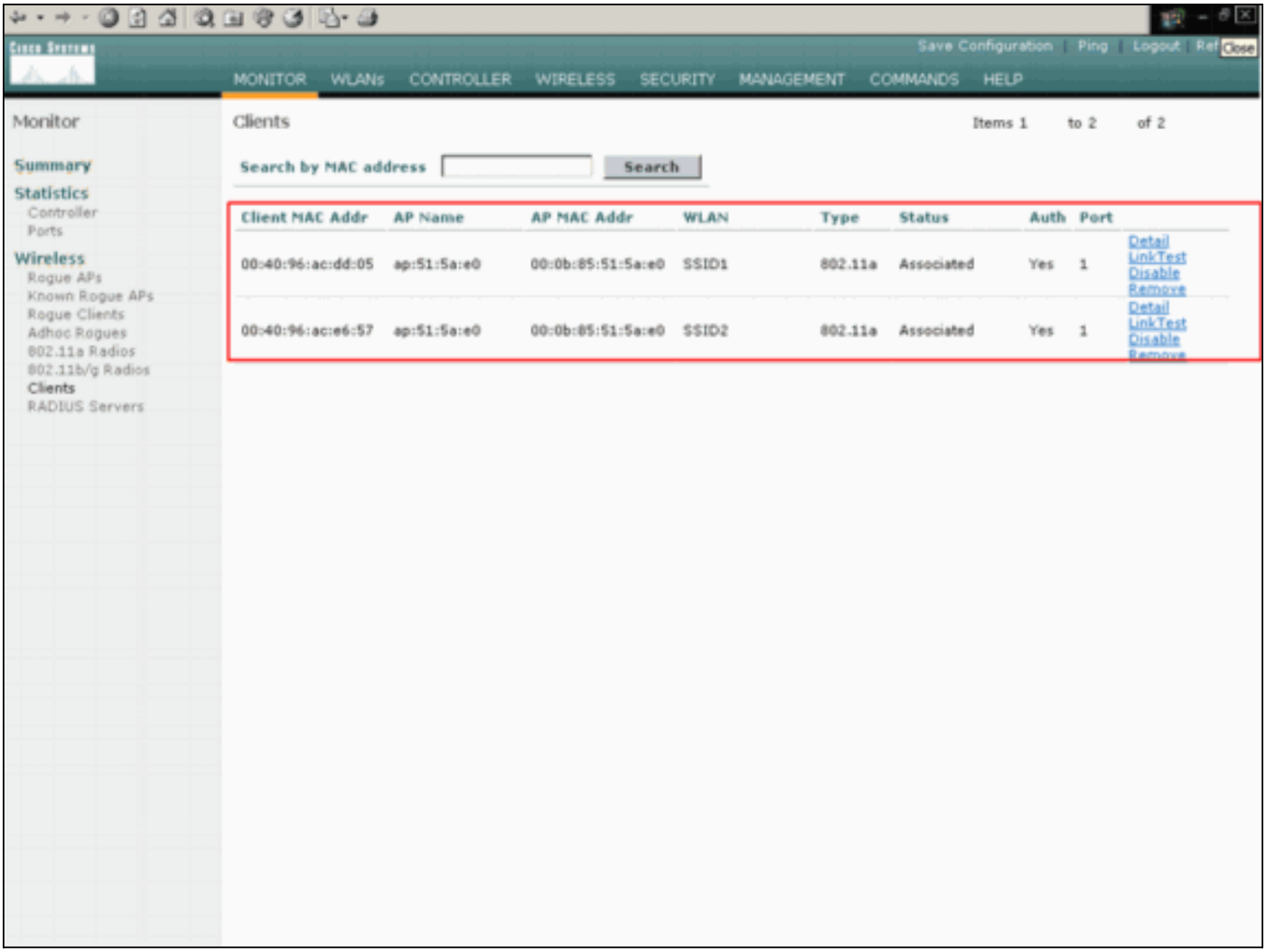
WLCs の WLAN を、LAP 発動を促されて設定し、WAN 確立される主要なオフィスとリモートオ

フィスの間でリンクしなさいので、リモートサイトで AP を展開して準備ができています。

電源投入 リモートサイトの AP、AP 起爆剤ステージで設定した順序でコントローラを探した後。AP の後でコントローラを、コントローラが付いている AP 登録見つけます。 次に例を示します。 WLC から、AP がポート 1 のコントローラに加入したことがわかります:



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 人のクライアントは WLAN 1 に接続され、他のクライアントは WLAN 2 に接続されます:



確認

REAP 設定がきちんと機能することを確認するのにこのセクションを使用して下さい。

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 リンクをダウンさせて下さい。 WAN リンクがダウンしているとき、AP は WLC の接続を失います。 WLC はそれからリストからの AP の登録を取り消します。 次に例を示します。

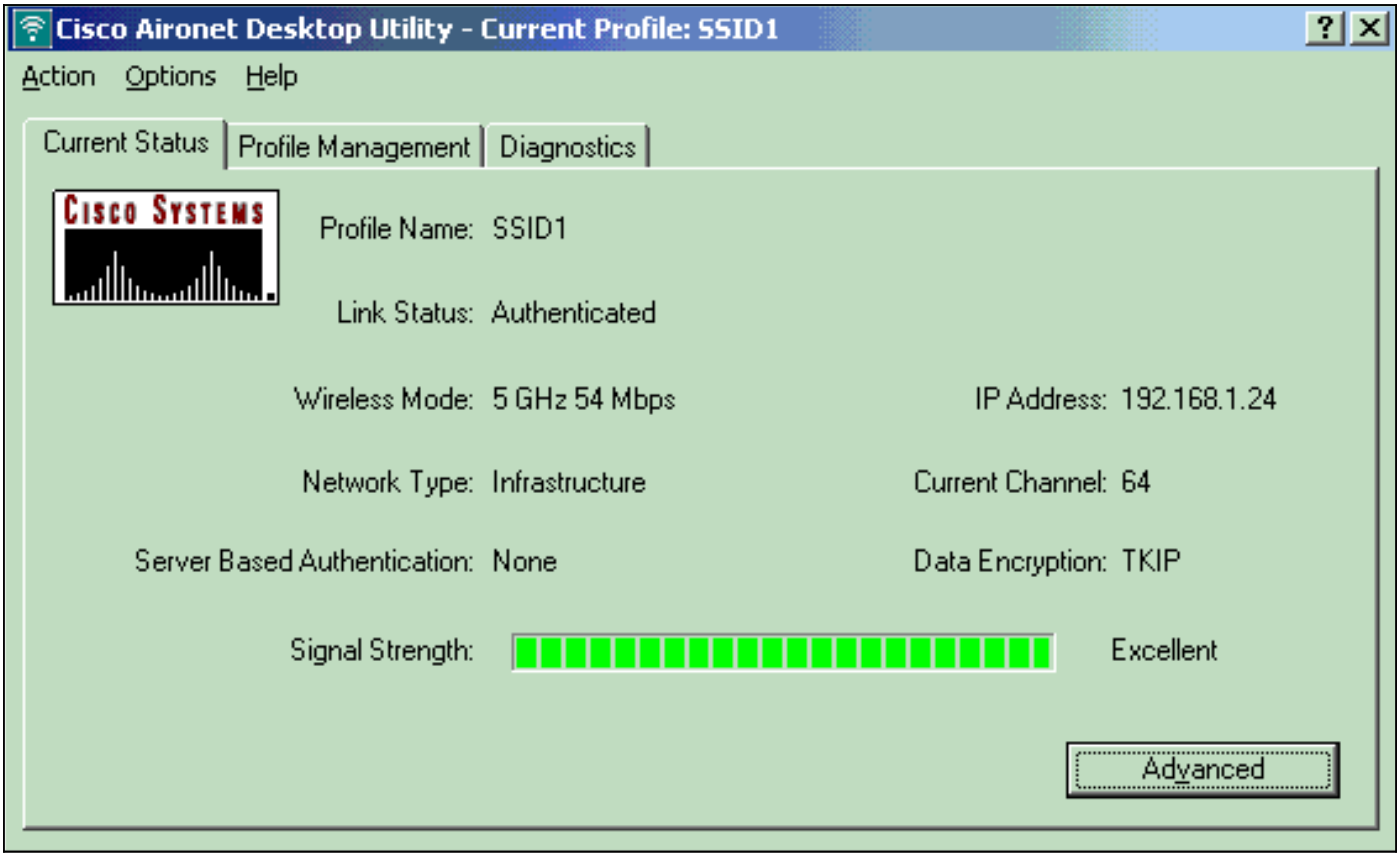
```
(Cisco Controller) >debug lwapp events enable
Wed May 17 15:04:22 2006: Did not receive heartbeat reply from AP 00:0B:85:51:5A:E0
Wed May 17 15:04:22 2006: Max retransmissions reached on AP 00:0B:85:51:5A:E0
(CONFIGURE_COMMAND, 1)
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: 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
```

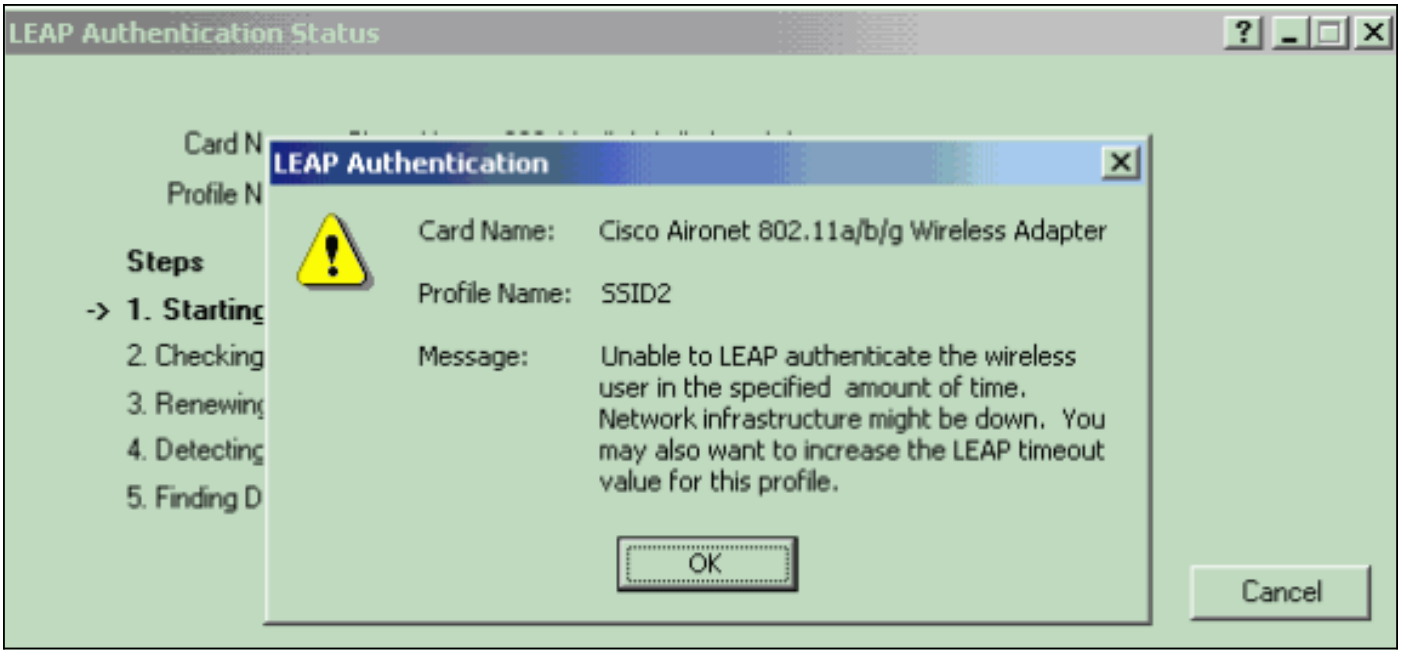
デバッグ lwapp イベント enable コマンド出力から、WLC が AP からのハートビート応答を受け取らなかったので WLC が AP の登録を取り消すことがわかります。 ハートビート応答はキープアライブ メッセージに類似したです。 コントローラは 5 つの連続した ハートビートを、1 第 2 別試みます。 WLC が応答を受け取らない場合、WLC は AP の登録を取り消します。

AP が独立方式にあるとき、AP 電源 LED は点滅します。 最初の WLAN （1） WLAN に関連付けるクライアントはまだ AP に最初の WLAN のクライアントが WPA-PSK 暗号化だけのために設定されるので関連付けられます。 LAP は独立方式の暗号化自体を処理します。 SSID1 および WPA-PSK と WLAN 1 に接続されるクライアントのステータスを（WAN リンクがダウンしているとき）表示する例はここにあります:

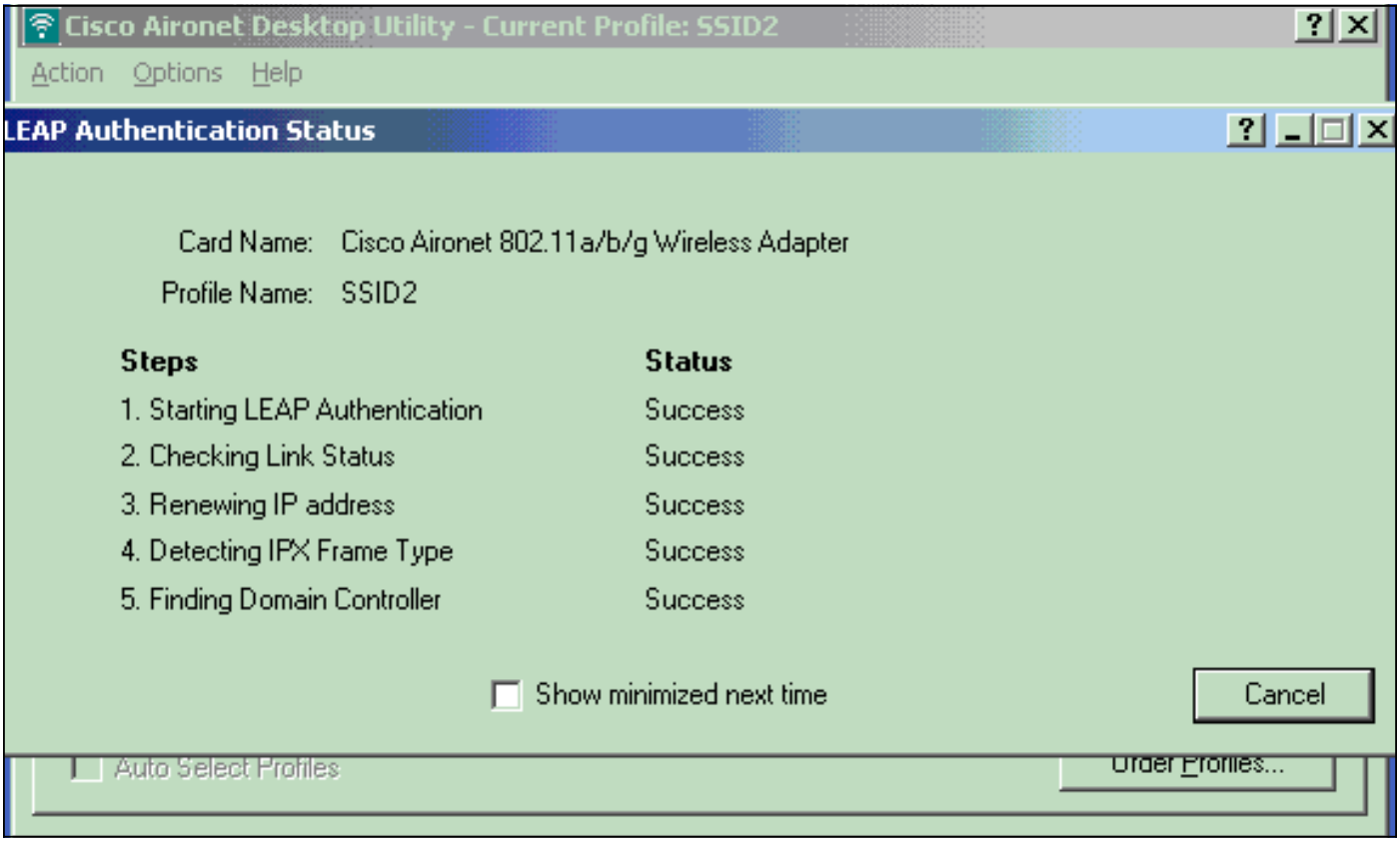
注: TKIP は WPA-PSK と使用する暗号化です。



WLAN 2 に接続されるクライアントは WLAN 2 が EAP 認証を使用するので切断されています。 この切断はので WLC と通信する EAP 認証必要を使用するクライアント発生します。 WAN リンクがダウンしていると EAP 認証は失敗することを表示するウィンドウ例はここにあります:



WAN リンクが稼働していた後、正常な REAP モードに戻る AP スイッチおよびコントローラが付いている登録。 EAP 認証をまた使用するクライアントはアップします。 次に例を示します。



コントローラの**デバッグ lwapp イベント enable コマンド**のこの出力例はこれらの結果を示します:

```
(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

設定をトラブルシューティングするこれらの **debug コマンドを**使用できます。

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。

- LAP と WLC の間に発生する **lwapp イベントを enable** —表示します出来事の順序を**デバッグして下さい。**
- **debug lwapp errors enable** — LWAPP コミュニケーションで生じるエラーを表示します。
- **デバッグ lwapp パケットは enable** — LWAPP パケット トレースのデバッグを表示します。
- **デバッグ MAC Addr** —規定 するクライアントのための MAC デバッグを有効にします。

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