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

内容

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いています。

- ファームウェア リリース 4.2 が稼動する Cisco 4400 シリーズ WLC
- Cisco 1030 LAP
- Cisco IOS®ソフトウェアリリース12.2T13が稼働する2台のCisco 2800シリーズルータ
- ファームウェアリリース3.0が稼働するCisco Aironet 802.11a/b/gクライアントアダプタ
- Cisco Aironet Desktop Utility 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ました。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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実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 に設定されている最初の WLAN である WLAN 1 になります。このようになるのは、他のほとんどの認証方法では、コントローラと情報をやりとりする必要があるので、WAN リンクがダウンすると処理ができなくなるためです。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 ぱ両方のモードの 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

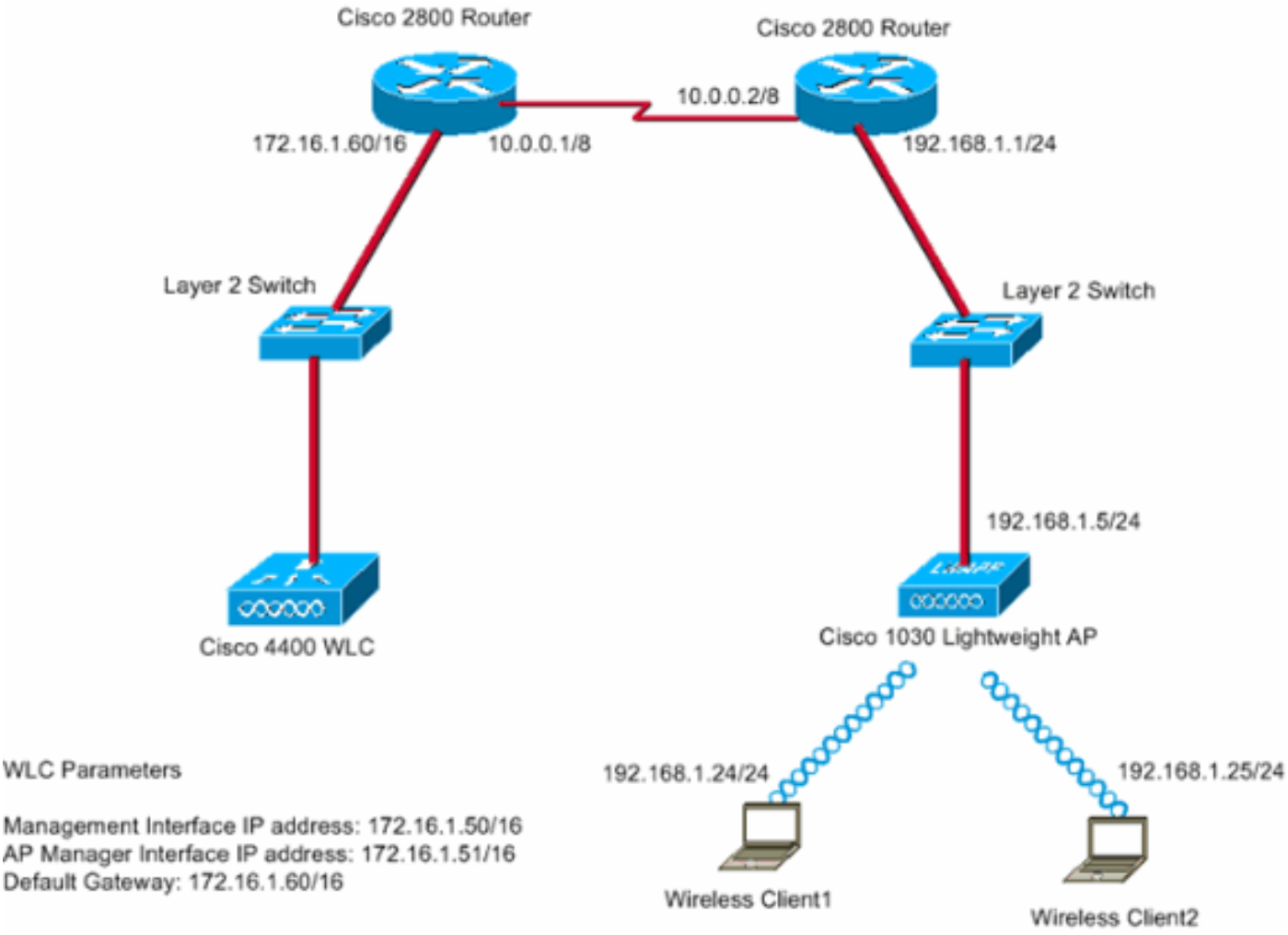
このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

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 の基本動作用の設定と 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. WAN リンクを確立するための 2800 ルータの設定
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 セットアップを使用します。



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。この専用回線は両端の 2800 シリーズ ルータで終端しています。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。本社には 4400 WLC があり、リモート オフィスには 1030 LAP を配備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。

- **WLAN 1**SSID：**SSID1**認証：**オープン**暗号化：**Temporal Key Integrity Protocol（TKIP）（WPA Pre-Shared Key [WPA-PSK]）**
- **WLAN 2**SSID：**SSID2**認証：**Extensible Authentication Protocol（EAP）**暗号化：**TKIP注**：WLAN 2の場合、このドキュメントの設定ではWPA(802.1x認証とTKIP（暗号化）を使用します。

この設定に合せて、デバイスを設定する必要があります。

WLC の基本動作用の設定と WLAN の設定

基本動作用に 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。この他、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...
```

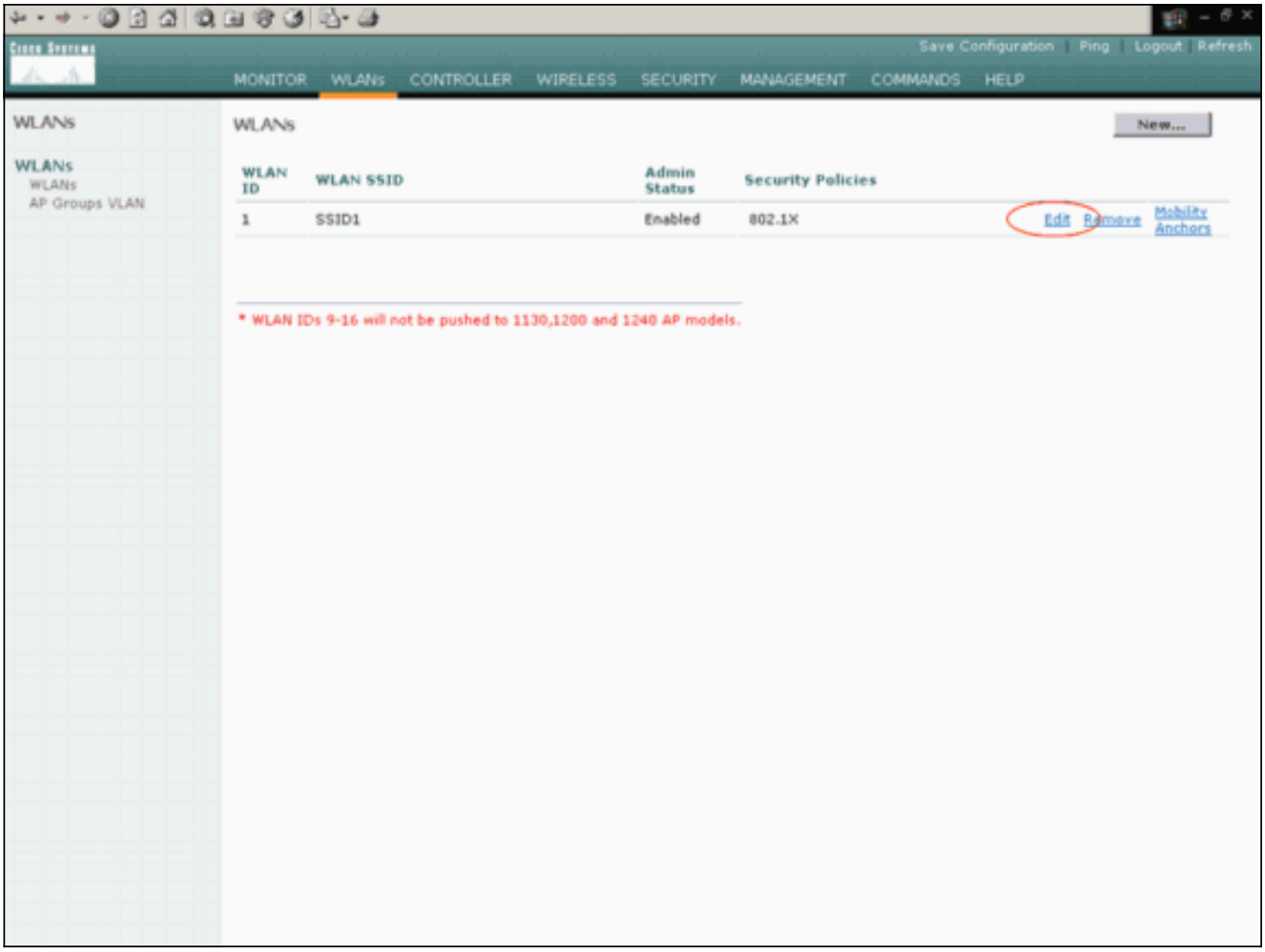
この例では、WLC で次のパラメータを設定します。

- 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 を基本動作用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。

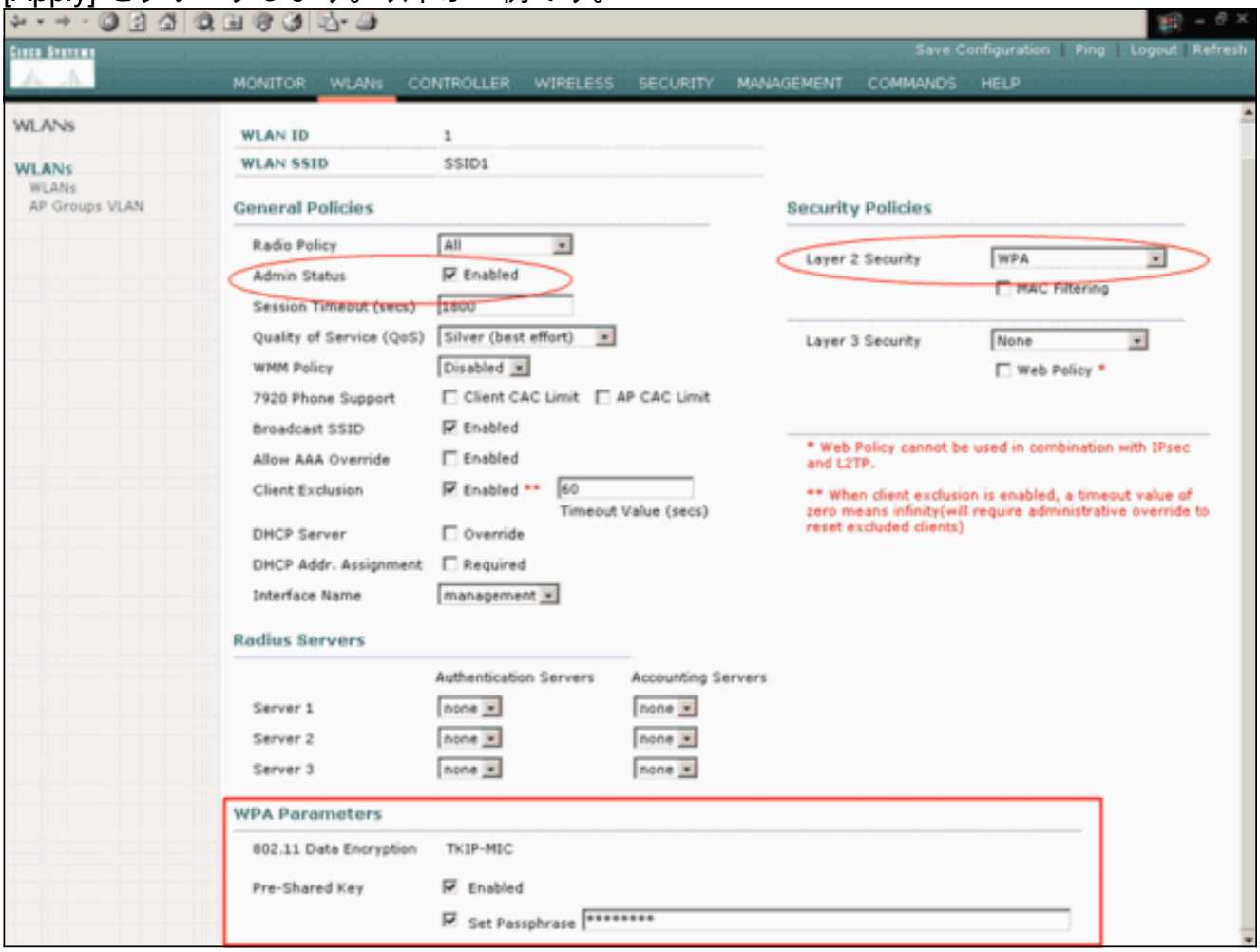
1. WLC の GUI で、ウィンドウの上部のメニューにある **WLANs** をクリックします。WLANs ウィンドウが表示されます。このウィンドウには、WLC に設定されている WLAN の一覧が表示されます。スタートアップ コンフィギュレーション ウィザードを使用して 1 つの WLAN を設定したので、この WLAN の他のパラメータを設定する必要があります。
2. WLAN SSID1 の **Edit** をクリックします。以下が一例です。



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。

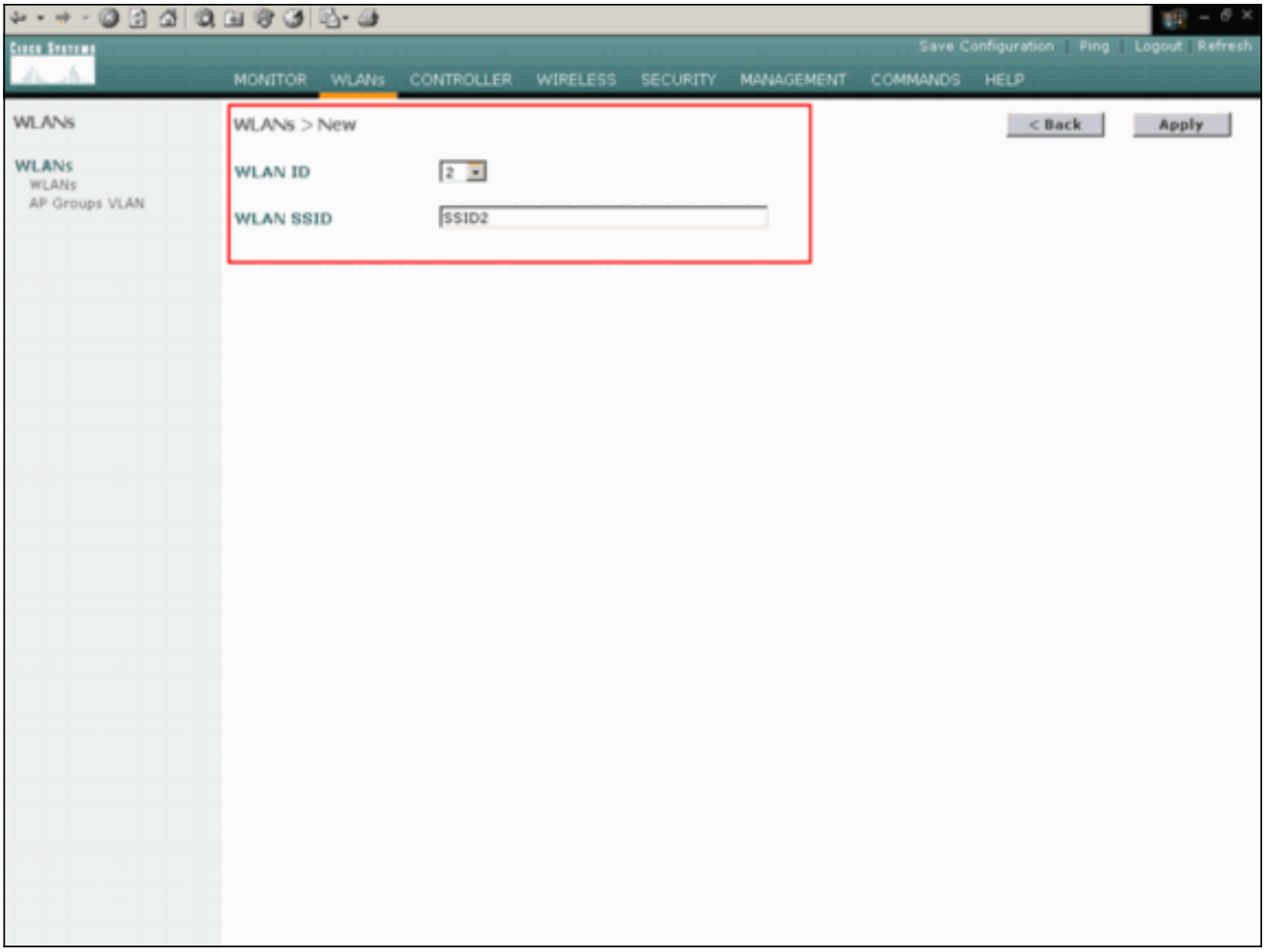
3. WLANs > Edit ウィンドウで次のように選択します。この WLAN を有効にするために、General Policies 領域にある Admin Status の横の **Enabled** チェックボックスにチェックマークを付けます。WLAN 1 で WPA を使用するために、Layer 2 Security ドロップダウン メニューから **WPA** を選択します。ウィンドウの最下部で WPA パラメータを定義します。WLAN 1 で WPA-PSK を使用するために、WPA Parameters 領域にある Pre-Shared Key の横の **Enabled** チ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パスフレーズ

は、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ている必要があります。[Apply] をクリックします。以下が一例です。



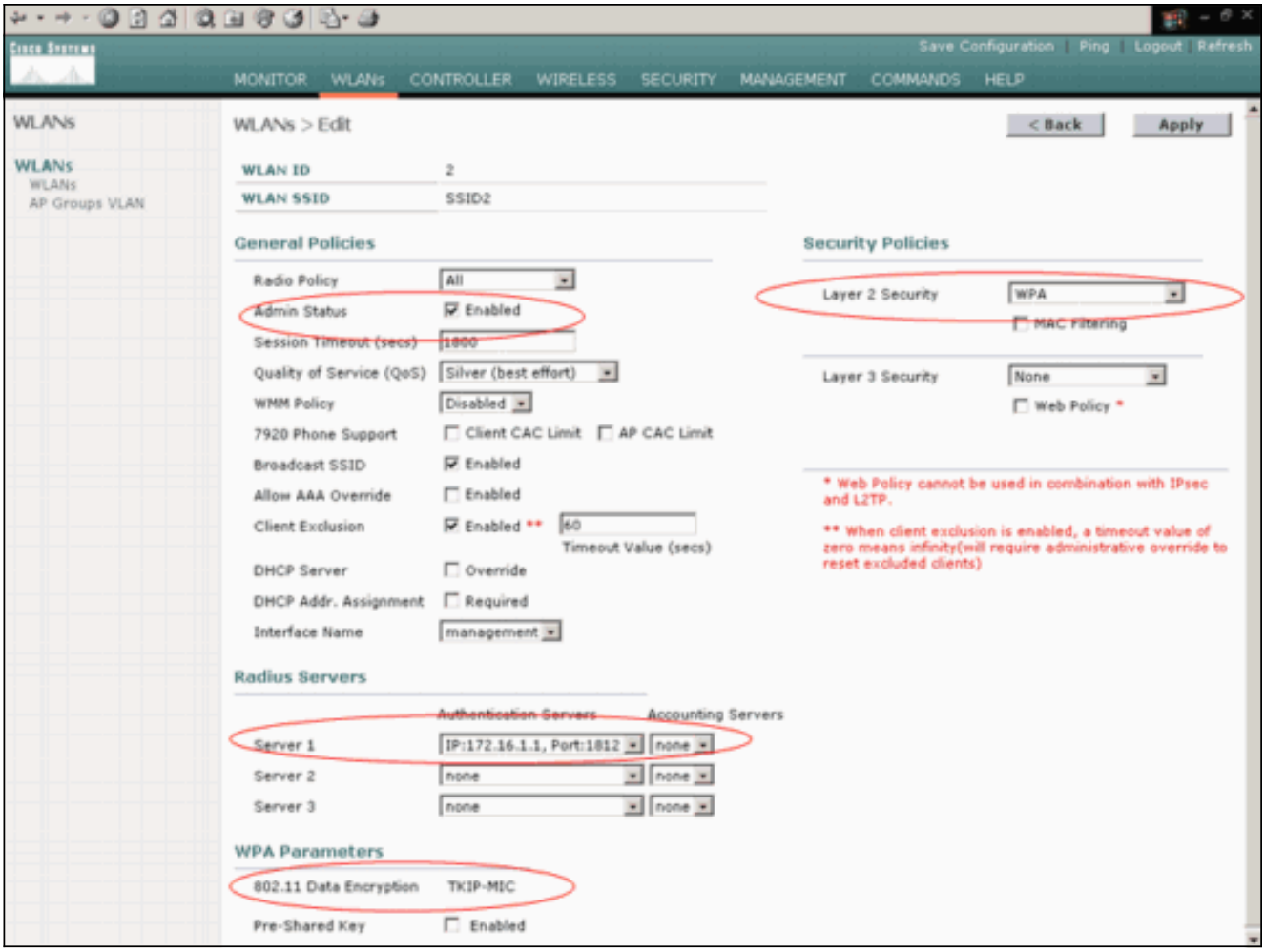
これで、WLAN 1 に WPA-PSK の暗号化を設定できました。

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。以下が一例です。



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。以下が一例です。



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について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APを出荷するためにAPをオフにする前に、APを「REAP」モードに設定してください。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。

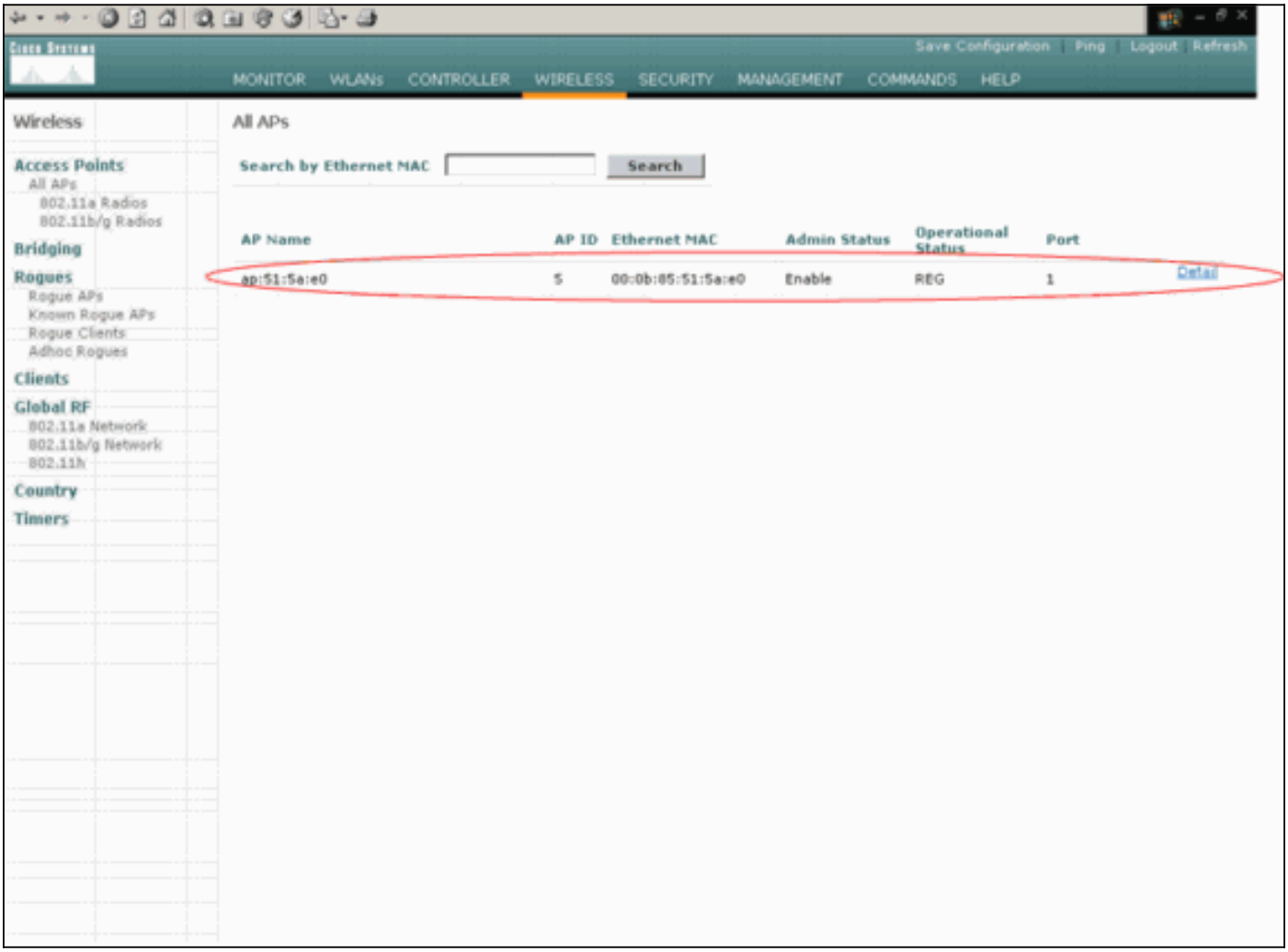
コントローラを見つけるために、LAP は次の方法のいずれかを使用できます。

- **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サーバを使用するには、LAPがWLCに直接接続されている必要があります。

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。

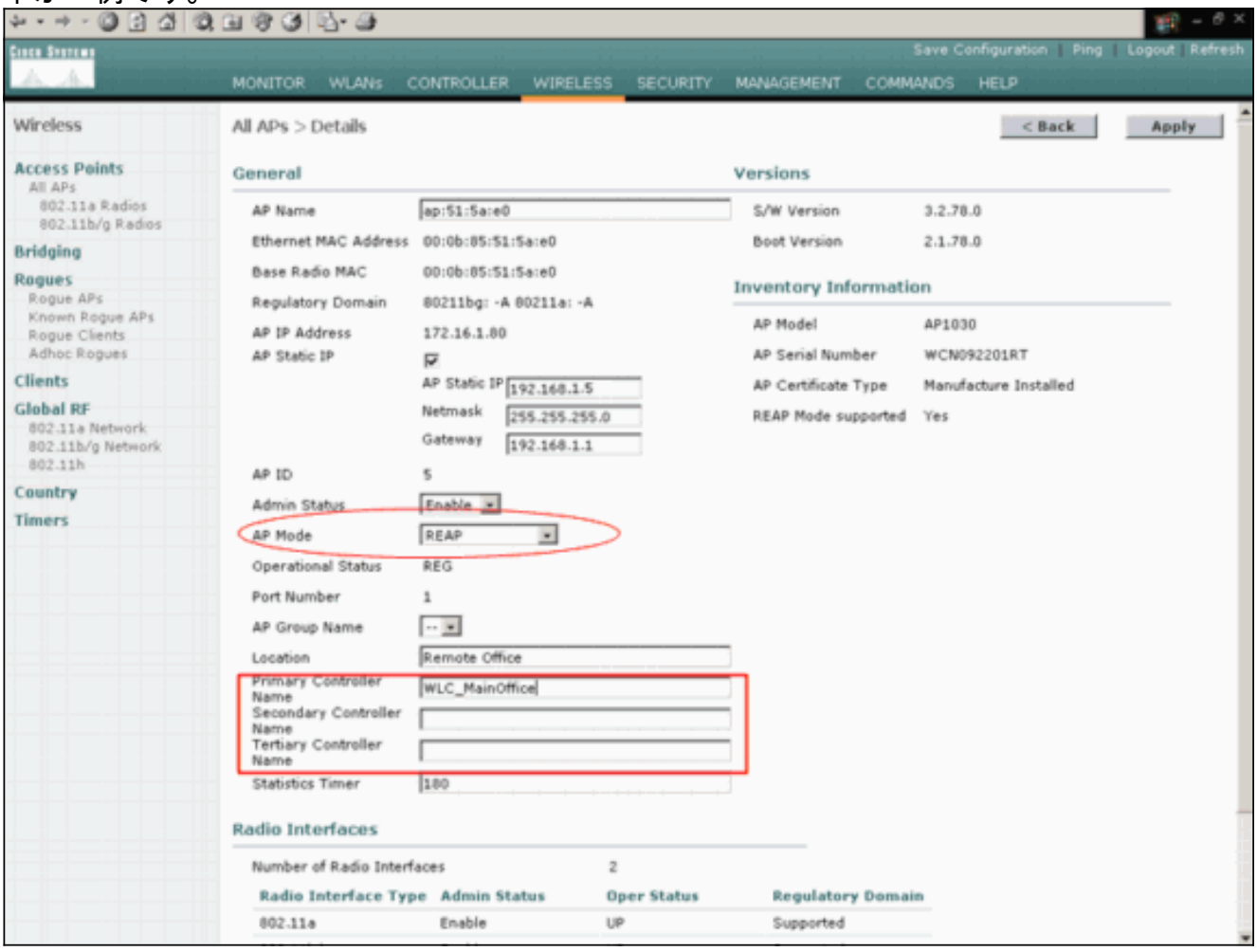
LAP がコントローラを見つけたら、AP がコントローラに登録されていることが WLC の Wireless ウィンドウに表示されます。以下が一例です。



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。以下が一例です。



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、スタティックIPアドレス192.168.1.5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。

WAN リンクを確立するための 2800 ルータの設定

この例では、WANリンクを確立するために、2台の2800シリーズルータをOSPFで使用して、ネットワーク間で情報をルーティングしています。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-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
```

ブランチオフィス

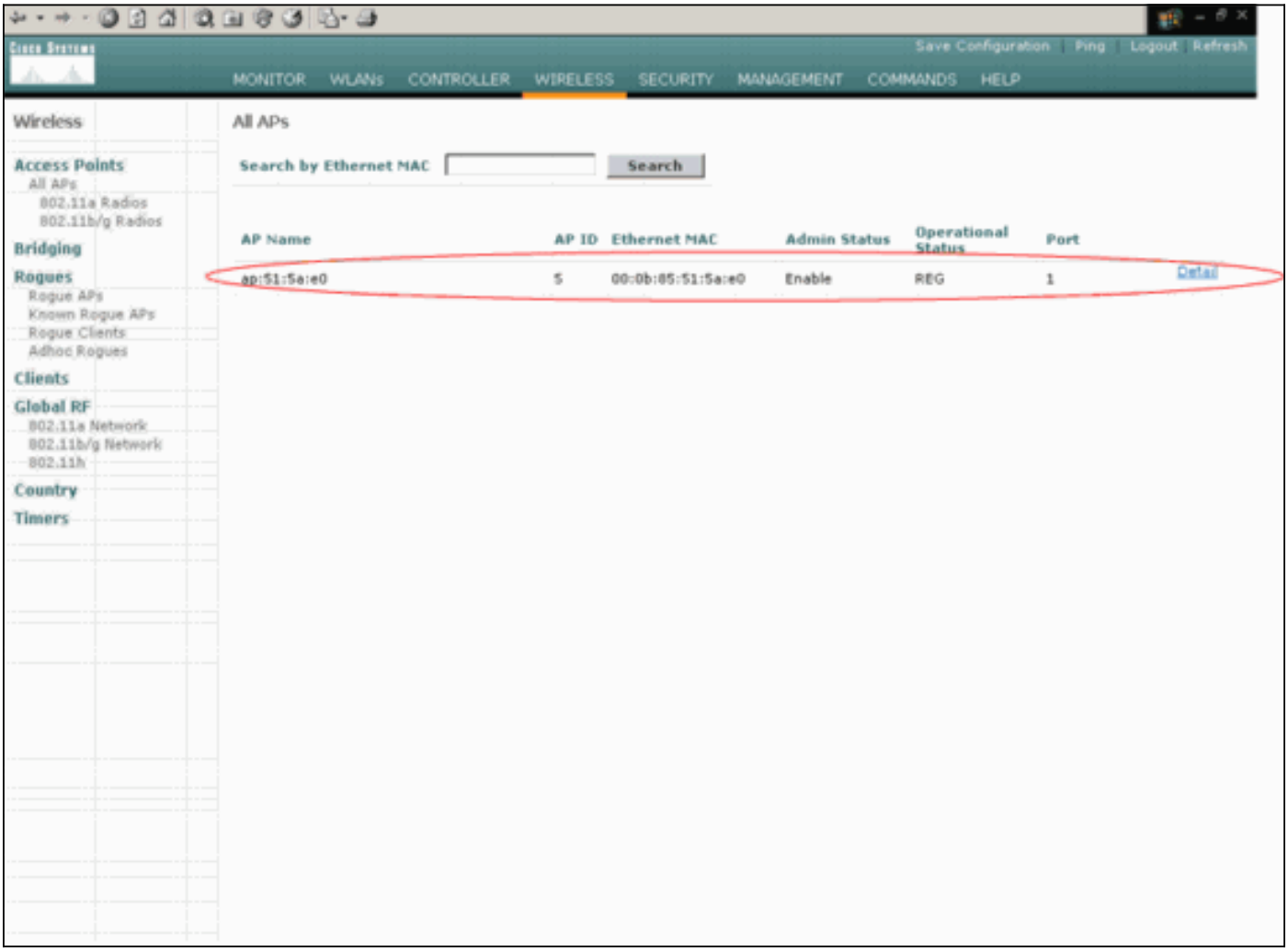
```
BranchOffice#show run
Building configuration...

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

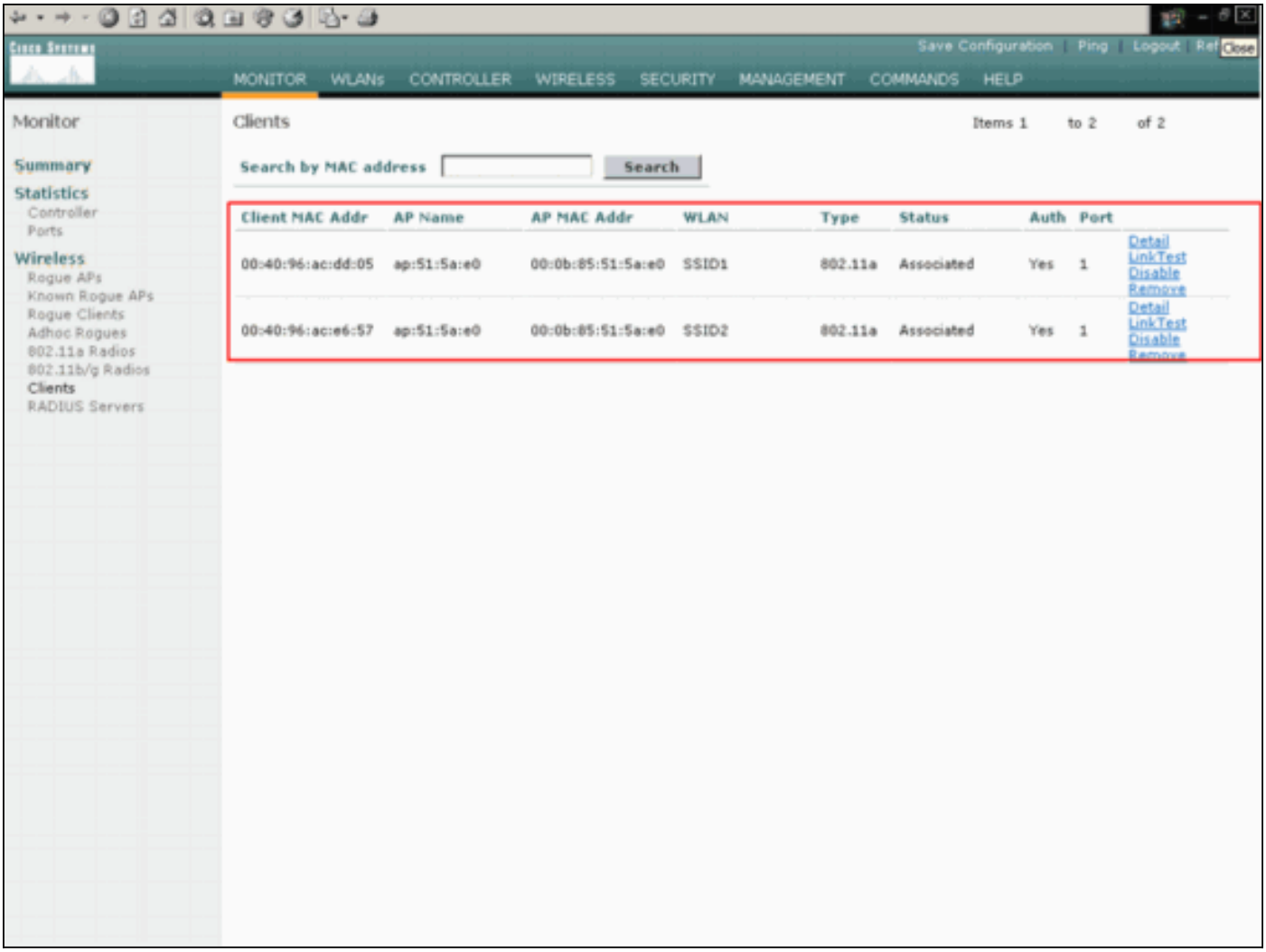
WLC での WLAN の設定、LAP のプライミング、本社とリモート オフィスの WAN リンクの確立

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。



SSID1 という SSID で WPA-PSK が有効になっているクライアントは WLAN 1 の AP に関連付けられています。**SSID2** という SSID で 802.1x 認証が有効になっているクライアントは WLAN 2 の AP に関連付けられています。次に、2 つのクライアントの例を示します。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。



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。以下が一例です。

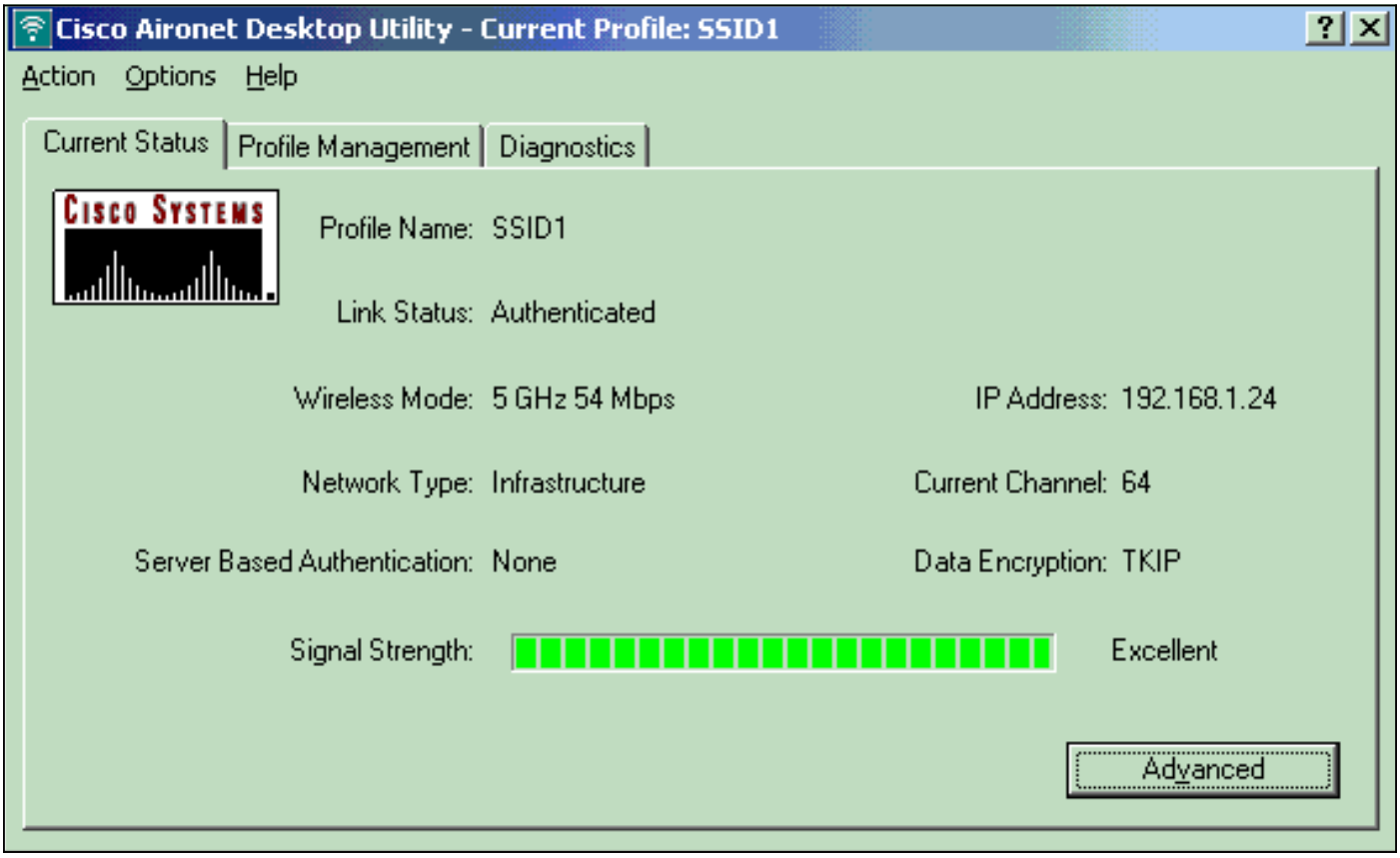
```
(Cisco Controller) >debug lwapp events enable
Wed May 17 15:04:22 2006: Did not receive heartbeat reply from AP 00:0B:85:51:5A:E0
Wed May 17 15:04:22 2006: Max retransmissions reached on AP 00:0B:85:51:5A:E0
(CONFIGURE_COMMAND, 1)
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: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

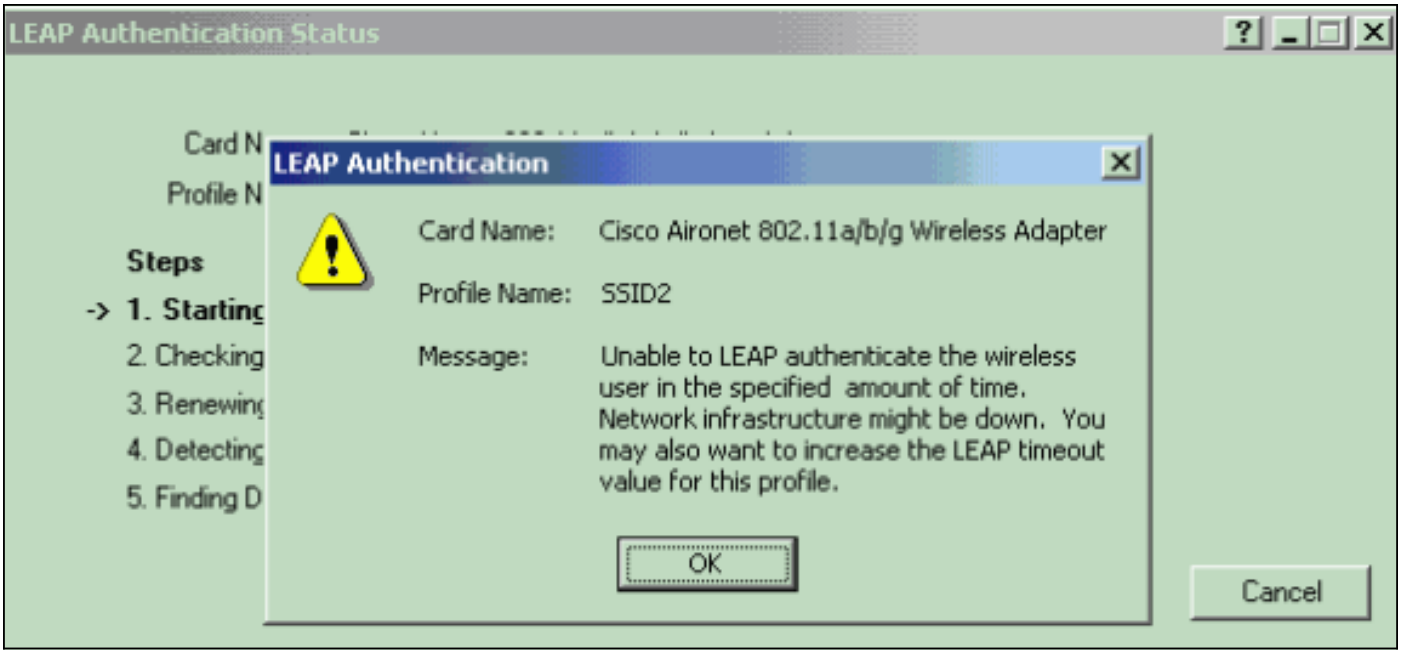
debug lwapp events enable コマンドの出力には、WLC が AP からハートビートの応答を受信しなかったので、WLC が AP の登録を解除したことが示されています。ハートビートの応答は、キープアライブ メッセージと同様のものです。コントローラは 1 秒間の間隔を空けてハートビートを 5 回連続して試みます。WLC が応答を受信しなければ、WLC は AP を登録解除します。

AP がスタンドアロン 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 の暗号化専用に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。スタンドアロン 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。

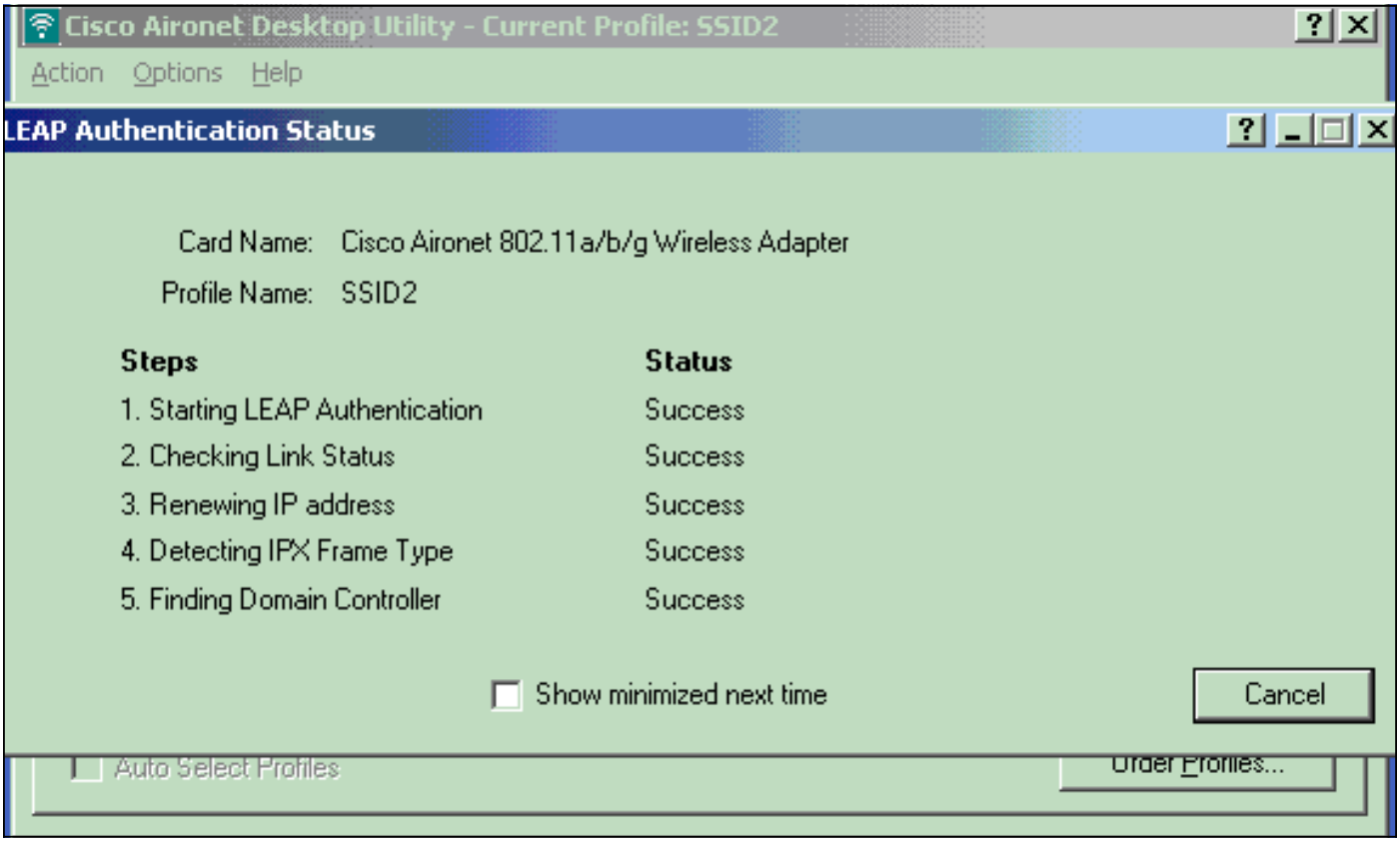
注：TKIPはWPA-PSKで使用される暗号化です。



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。以下が一例です。



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
```

トラブルシュート

このセクションは、設定のトラブルシューティングを行う際に参照してください。

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
- EAP 認証と WLAN コントローラ (WLC) の設定例
- ワイヤレス LAN コントローラと 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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。