Cisco Unified Wireless Network での Lightweight アクセス ポイント（LAP）の認可設定の例

目次

概要

このドキュメントでは、LAP の MAC アドレスに基づいて Lightweight アクセス ポイント（LAP）を許可するようにワイヤレス LAN コントローラ（WLC）を設定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。

- Cisco Secure Access Control Server（ACS）を無線クライアントを認証するために設定する方法の基本的な知識
- Cisco Aironet LAPs および Cisco WLCs の設定のナレッジ
- Cisco Unified Wireless Security ソリューションについての知識

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 バージョン 5.0.148.0 を実行する WLC
- Cisco Aironet 1000 シリーズ LAPs

- Cisco Aironet 1200 シリーズ LAPs
- Cisco Secure ACS サーババージョン 4.2

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。

Lightweight アクセスポイント（LAP）許可

X.509 認証を使用して LAP 登録 手続、LAPs および WLCs 相互に認証するの間。

X.509 認証は Cisco によってファクトリの Access Point （AP）および WLC 両方の保護されたフラッシュするに焼き付けられます。 AP で、プレ インストール認証は製造とインストール済み認証（MIC）呼ばれます。 の後で製造されたすべての Cisco AP に 2005 年 7月 18 日 MIC があります。

の前に 2005 年 7月 18 日製造された自律 IOS から Lightweight Access Point Protocol （LWAPP） IOS へアップグレードされた Cisco Aironet 1200、1130、および 1240 AP はアップグレード プロセスの間に自己署名証明書（SSC）を生成します。 SSCs の AP を管理する方法の情報に関しては Lightweight モードへの自律 Cisco Aironet アクセス ポイントのアップグレードを参照して下さい。

登録 手続の間に発生するこの相互認証に加えて、WLCs はまた LAPs を制限できます LAP の MAC アドレスにそれらと基づいていた登録する。

LAP の MAC アドレスの使用による強力なパスワードの欠如は RADIUSサーバを通して AP を承認する前に AP を認証するのにコントローラが MIC を使用するので問題ではないはずです。 MIC の使用は強化認証を提供します。

LAP 許可は 2 つの方法で実行されたことができます:

- WLC の内部 許可リストの使用
- AAAサーバの MAC アドレス データベースの使用

LAPs の動作は使用される認証に基づいて異なります:

- SSCs の LAPs — WLC は内部 許可リストだけを使用し、これらの LAPs のための RADIUSサーバに要求を転送しないことを。
- MIC の LAPs — WLC は WLC で設定される内部 許可リストを使用するか、または LAPs を承認するのに RADIUSサーバを使用できます

この資料は内部 許可リストおよび AAAサーバ両方を使用して LAP 許可を説明します。

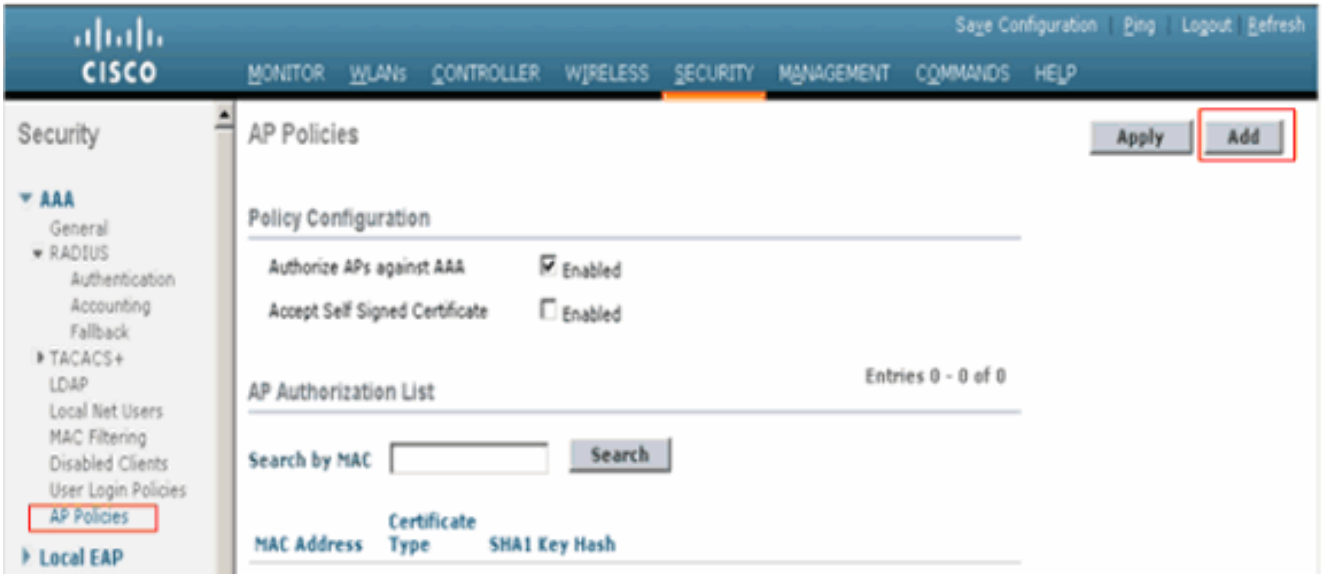
WLC の内部 許可 リストの使用

WLC で、MAC アドレスに基づいて LAPs を制限するのに AP 許可リストを使用して下さい。 AP 許可リストは WLC GUI で**セキュリティ > AP ポリシー**の下で利用できます。

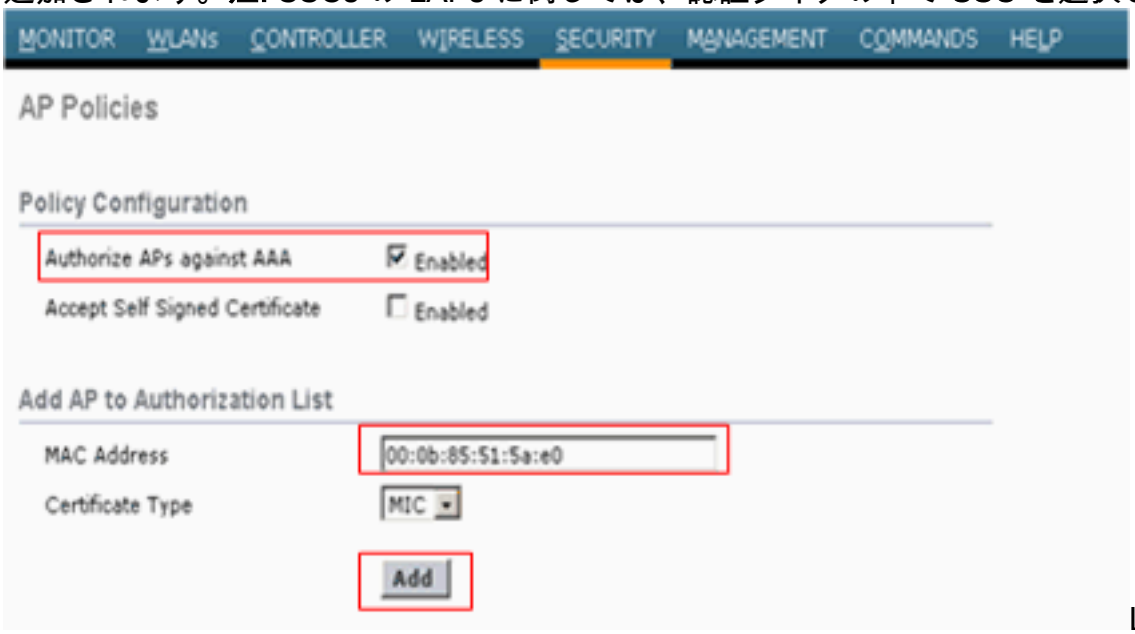
この例に MAC アドレス **00:0b:85:5b:fb:d0** の LAP を追加する方法を示されています。

次の手順を実行します。

1. WLC コントローラ GUI から、**> AP ポリシー**『Security』 をクリック して下さい。Policies ページ AP は現われます。
2. ポリシー 設定の下で、**AAA に対して Authorize AP** あるようにボックスを確認して下さい。このパラメータが選択されるとき、WLC はローカル許可リストを最初にチェックします。LAP の MAC がない場合、RADIUSサーバをチェックします。
3. 画面の右側の **Add ボタンを**クリックして下さい。



4. の下で許可 リストに AP を、入力します AP MAC アドレスを追加して下さい。 それから、認証タイプを選択し、『Add』 をクリック して下さい。この例では、MIC 認証との LAP は追加されます。**注:** SSCs の LAPs に関しては、認証タイプの下で **SSC を**選択して下さい。



LAP は AP 許可リストに追加され、**AP 許可 リスト**の下でリストされています。

確認

この設定を確認するために、LAP をネットワークへの MAC アドレス 00:0b:85:51:5a:e0 と接続し、監視する必要があります。 これを行う**デバッグ lwapp イベント イネーブル**および **debug aaa all enable** コマンドを使用して下さい。

この出力は LAP MAC アドレスが AP 許可リストに時デバッグを示したものです:

注: 出力で、スペースの制約上 2 行に分割されている行があります。

```
debug lwapp events enable Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY
REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1' Wed Sep 12 17:42:39 2007:
00:0b:85:51:5a:e0 Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on
Port 1 Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST from AP
00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1' Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0
Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1 Wed Sep 12
17:42:50 2007: 00:0b:85:51:5a:e0 Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0 to
00:0b:85:33:52:80 on port '1' Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0:
txNonce 00:0B:85:33:52:80 rxNonce 00:0B:85:51:5A:E0 Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0
LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0 Wed Sep 12
17:42:50 2007: spamRadiusProcessResponse: AP Authorization failure for 00:0b:85:51:5a:e0 debug
aaa all enable Wed Sep 12 17:56:26 2007: Unable to find requested user entry for 000b85515ae0
Wed Sep 12 17:56:26 2007: AuthenticationRequest: 0xac476e8 Wed Sep 12 17:56:26 2007:
Callback.....0x8108e2c Wed Sep 12 17:56:26 2007:
protocolType.....0x00000001 Wed Sep 12 17:56:26 2007:
proxyState.....00:0B:85:51:5A:E0-00:00 Wed Sep 12 17:56:26 2007: Packet
contains 8 AVPs (not shown) Wed Sep 12 17:56:26 2007: 00:0b:85:51:5a:e0 Returning AAA Error 'No
Server' (-7) for mobile 00:0b:85:51:5a:e0 Wed Sep 12 17:56:26 2007: AuthorizationResponse:
0xbadff7d4 Wed Sep 12 17:56:26 2007: structureSize.....28 Wed Sep 12 17:56:26
2007: resultCode.....-7 Wed Sep 12 17:56:26 2007:
protocolUsed.....0xffffffff Wed Sep 12 17:56:26 2007:
proxyState.....00:0B:85:51:5A:E0-00:00 Wed Sep 12 17:56:26 2007: Packet
contains 0 AVPs: Wed Sep 12 17:56:31 2007: Unable to find requested user entry for 000b85515ae0
Wed Sep 12 17:56:31 2007: AuthenticationRequest: 0xac476e8 Wed Sep 12 17:56:31 2007:
Callback.....0x8108e2c Wed Sep 12 17:56:31 2007:
protocolType.....0x00000001 Wed Sep 12 17:56:31 2007:
proxyState.....00:0B:85:51:5A:E0-00:00 Wed Sep 12 17:56:31 2007: Packet
contains 8 AVPs (not shown) Wed Sep 12 17:56:31 2007: 00:0b:85:51:5a:e0 Returning AAA Error 'No
Server' (-7) for mobile 00:0b:85:51:5a:e0
```

この出力は LAP の MAC アドレスが AP 許可リストに追加されるときデバッグを示したものです:

注: 出力で、スペースの制約上 2 行に分割されている行があります。

```
debug lwapp events enable Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY
REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1' Wed Sep 12 17:43:59 2007:
00:0b:85:51:5a:e0 Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on
Port 1 Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST from AP
00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1' Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0
```

Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1 Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 **Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'** Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0: txNonce 00:0B:85:33:52:80 rxNonce 00:0B:85:51:5A:E0 Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 **LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0** Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 Successfully added NPU Entry for AP 00:0b:85:51:5a:e0 (index 58)Switch IP: 10.77.244.213, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 10.77.244.221, AP Port: 5550, next hop MAC: 00:0b:85:51:5a:e0 Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 **Successfully transmission of LWAPP Join-Reply to AP 00:0b:85:51:5a:e0** Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 0 Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 **Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 1 debug aaa all enable** Wed Sep 12 17:57:44 2007: **User 000b85515ae0 authenticated** Wed Sep 12 17:57:44 2007: **00:0b:85:51:5a:e0 Returning AAA Error 'Success' (0) for mobile 00:0b:85:51:5a:e0** Wed Sep 12 17:57:44 2007: AuthorizationResponse: 0xbadff96c Wed Sep 12 17:57:44 2007: structureSize.....70 Wed Sep 12 17:57:44 2007: resultCode.....0 Wed Sep 12 17:57:44 2007: protocolUsed.....0x00000008 Wed Sep 12 17:57:44 2007: proxyState.....00:0B:85:51:5A:E0-00:00 Wed Sep 12 17:57:44 2007: Packet contains 2 AVPs: Wed Sep 12 17:57:44 2007: AVP[01] Service-Type..... 0x00000065 (101) (4 bytes) Wed Sep 12 17:57:44 2007: AVP[02] Airespace / WLAN-Identifier..... 0x00000000 (0) (4 bytes)

AAAサーバに対する AP 許可

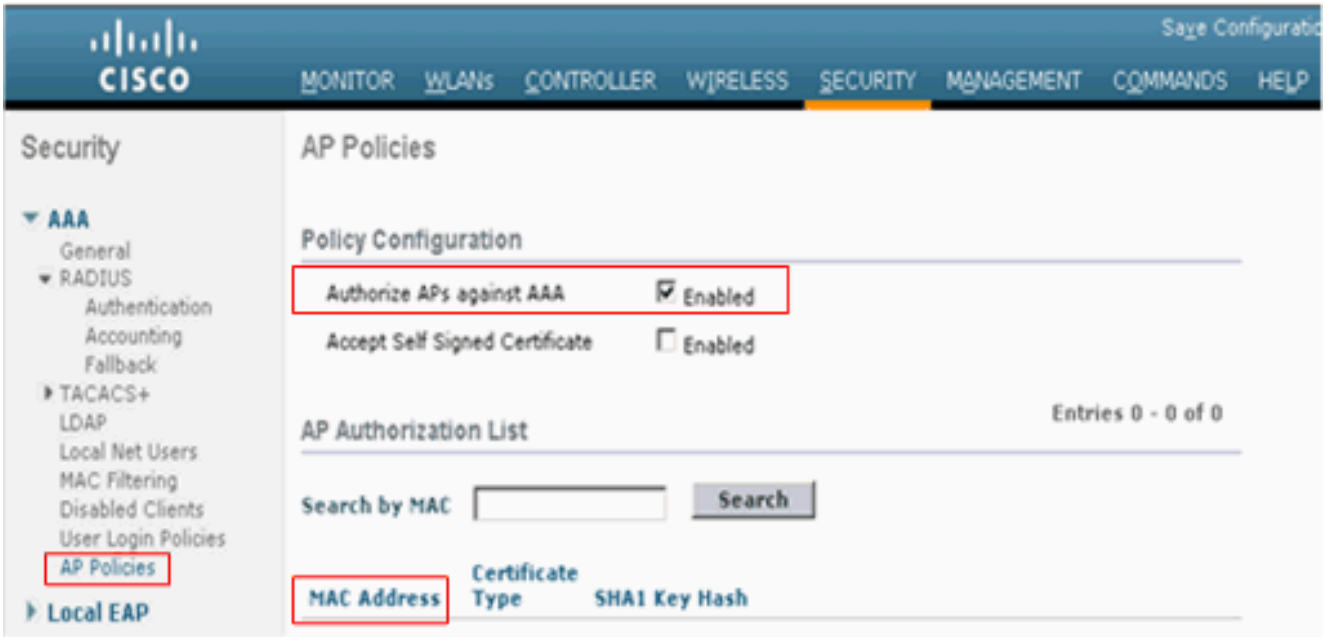
また MIC を使用して AP を承認するのに RADIUSサーバを使用するように WLCs を設定できます。 WLC は両方として情報を RADIUSサーバに送信 するとき LAP の MAC アドレスをユーザ名および パスワード使用します。 たとえば、AP の MAC アドレスが 000b85229a70 なら、両方とも AP を承認するのにコントローラが使用するユーザ名 および パスワード 000b85229a70 です。

注: RADIUS AAAサーバの AP 認証のためにユーザ名 および パスワードとして MAC アドレスを使用する場合、クライアント認証のために同じ AAAサーバを使用しないで下さい。 この理由はハッカーが AP MAC アドレスを調べる場合です、ユーザ名 および パスワード 資格情報としてネットワークに得るのにその MAC を使用できます。

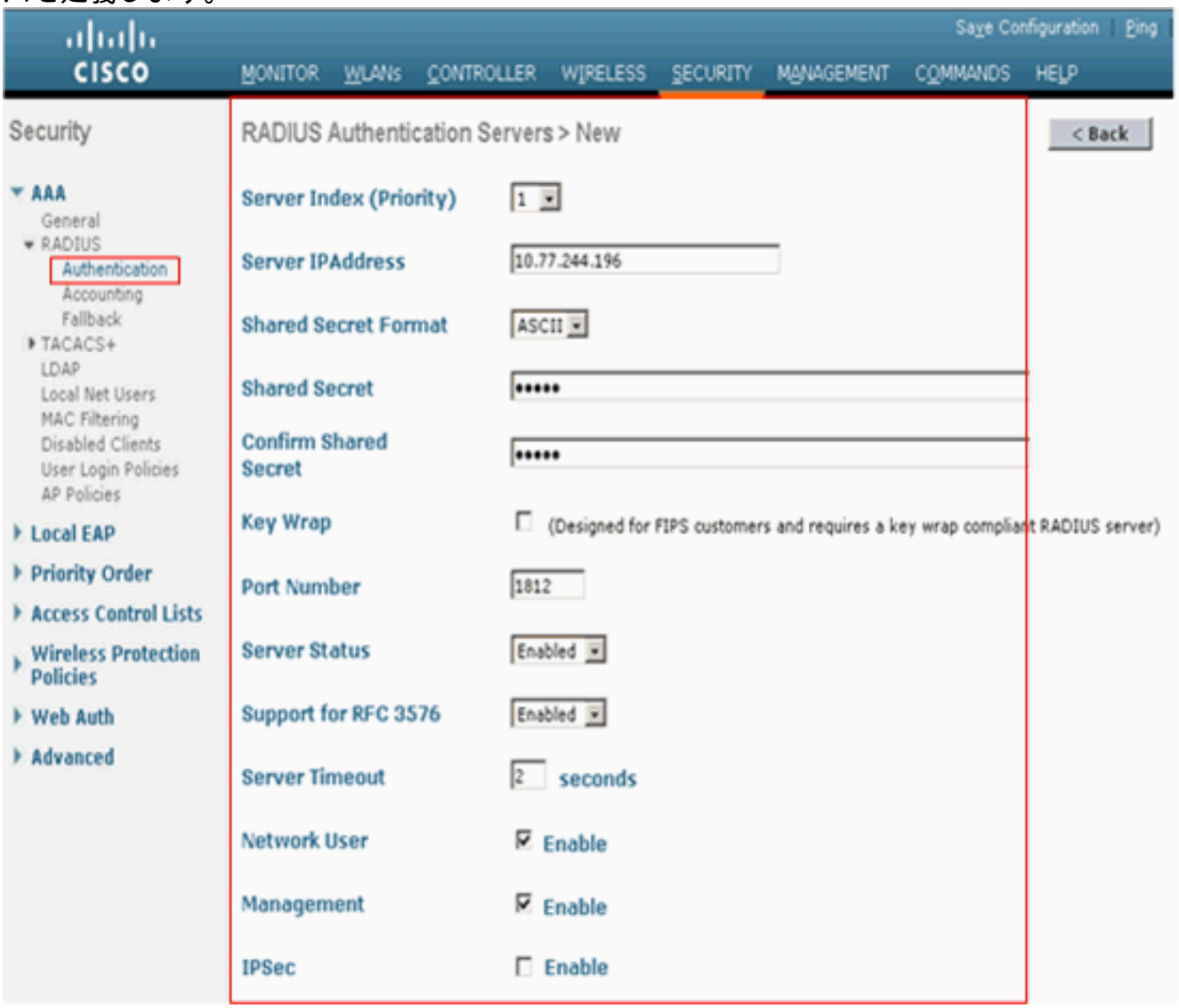
この例に Cisco Secure ACS を使用して LAPs を承認するために WLCs を設定する方法を示されています。

WLC で次の手順を実行します。

1. WLC コントローラ GUI から、**> AP ポリシー**『Security』 をクリック して下さい。Policies ページ AP は現われます。
2. ポリシー 設定の下で、**AAA に対して Authorize AP** あるようにボックスを確認して下さい。このパラメータが選択されるとき、WLC はローカルMAC データベースをまずチェックします。 従ってローカルデータベースが AP 許可 リストことをの下で MAC アドレスをクリアすることによって空であることを、確かめて下さい。 LAP MAC アドレスがない場合、それから RADIUSサーバをチェックします。



3. コントローラの GUI から Security と RADIUS Authentication をクリックして、RADIUS Authentication Servers ページを表示します。 次に、[New] をクリックして、RADIUS サーバを定義します。



4. [RADIUS Authentication Servers] > [New] ページで RADIUS サーバのパラメータを定義します。 RADIUS サーバ IP アドレス、共有秘密、ポート番号、サーバ ステータスなどのパラメータがあります。この例では、次のように、Cisco Secure ACS を IP アドレスが

10.77.244.196 である RADIUS サーバとして使用しています。
5. [Apply] をクリックします。

LAPs を承認するために Cisco Secure ACS を設定して下さい

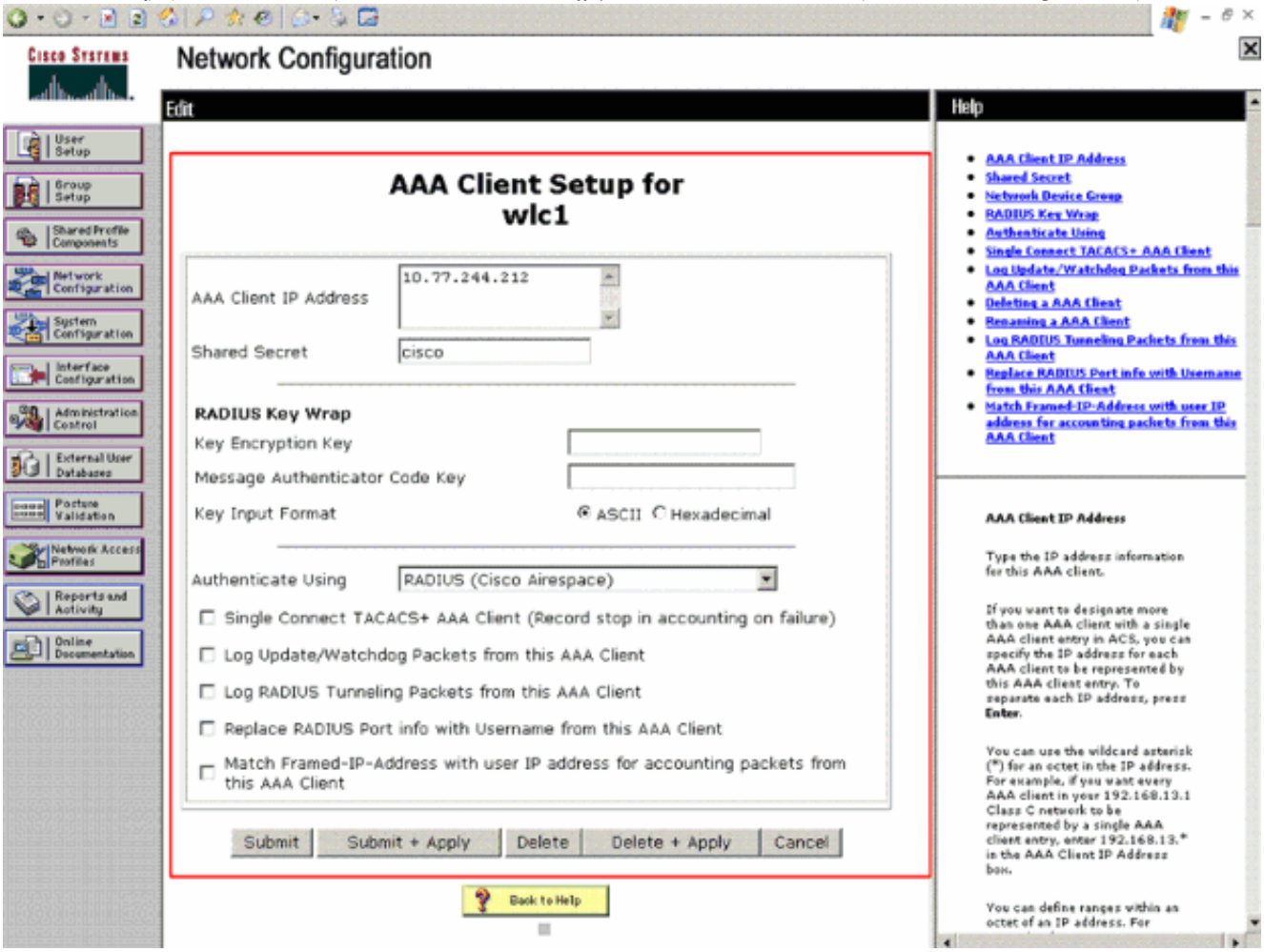
LAPs を承認することを Cisco Secure ACS が可能にするためにこれらのステップを完了する必要があります:

1. Cisco Secure ACS の AAA クライアントで WLC を設定して下さい
2. Cisco Secure ACS のユーザデータベースへの LAP MAC アドレスを追加して下さい

Cisco Secure ACS の AAA クライアントで WLC を設定して下さい

Cisco Secure ACS の AAA クライアントで WLC 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. [Network Configuration] > [Add AAA client] をクリックします。[Add AAA Client] ページが表示されます。
2. このページで、RADIUS Airespace を使用して WLC システム 名、マネージメントインターフェイス IP アドレス、共有秘密および認証するを定義して下さい。**注:** また、RADIUS Aironet を使用して認証する オプションを試みることができます。次に例を示します。

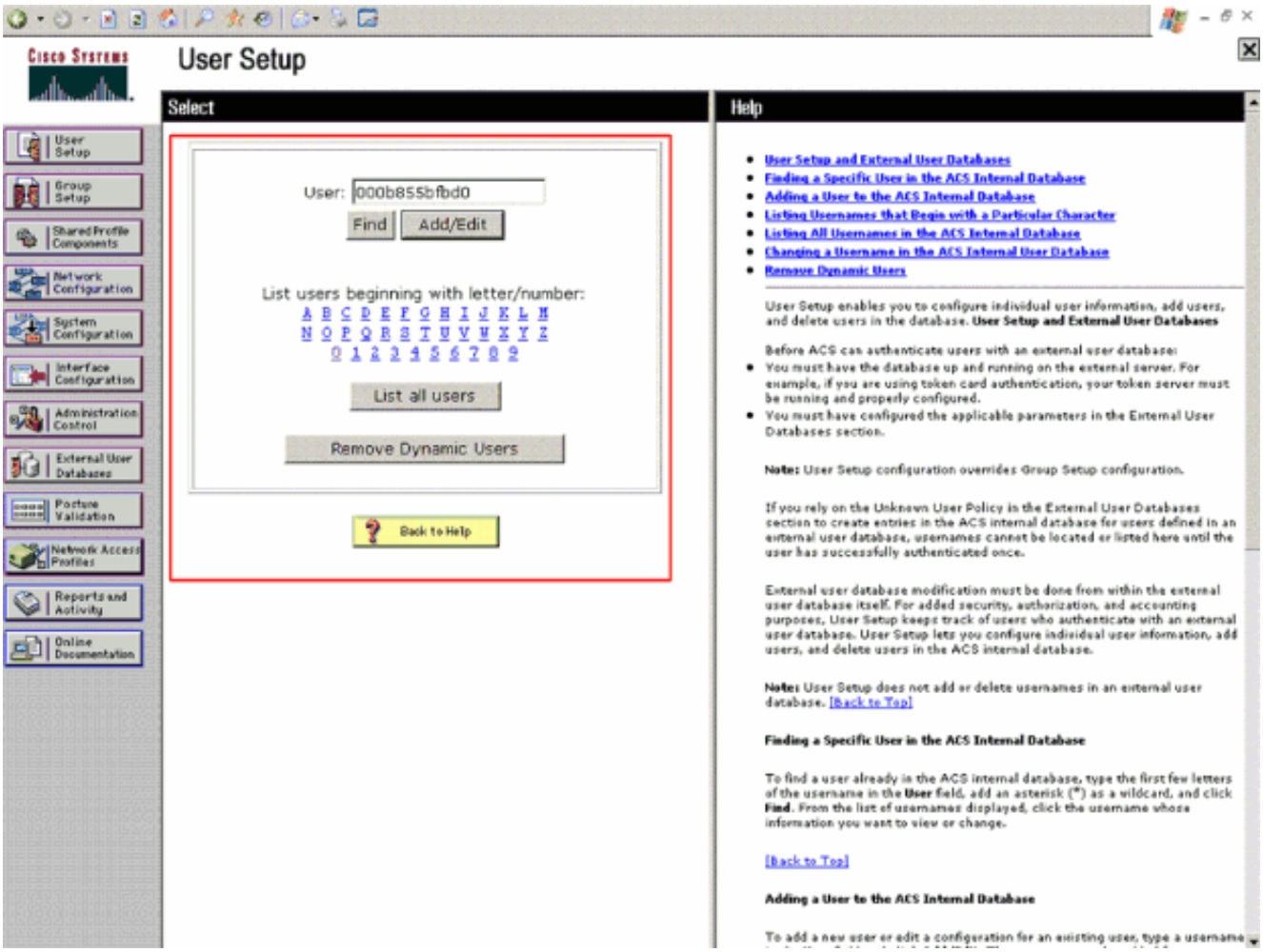


3. [Submit+Apply] をクリックします。

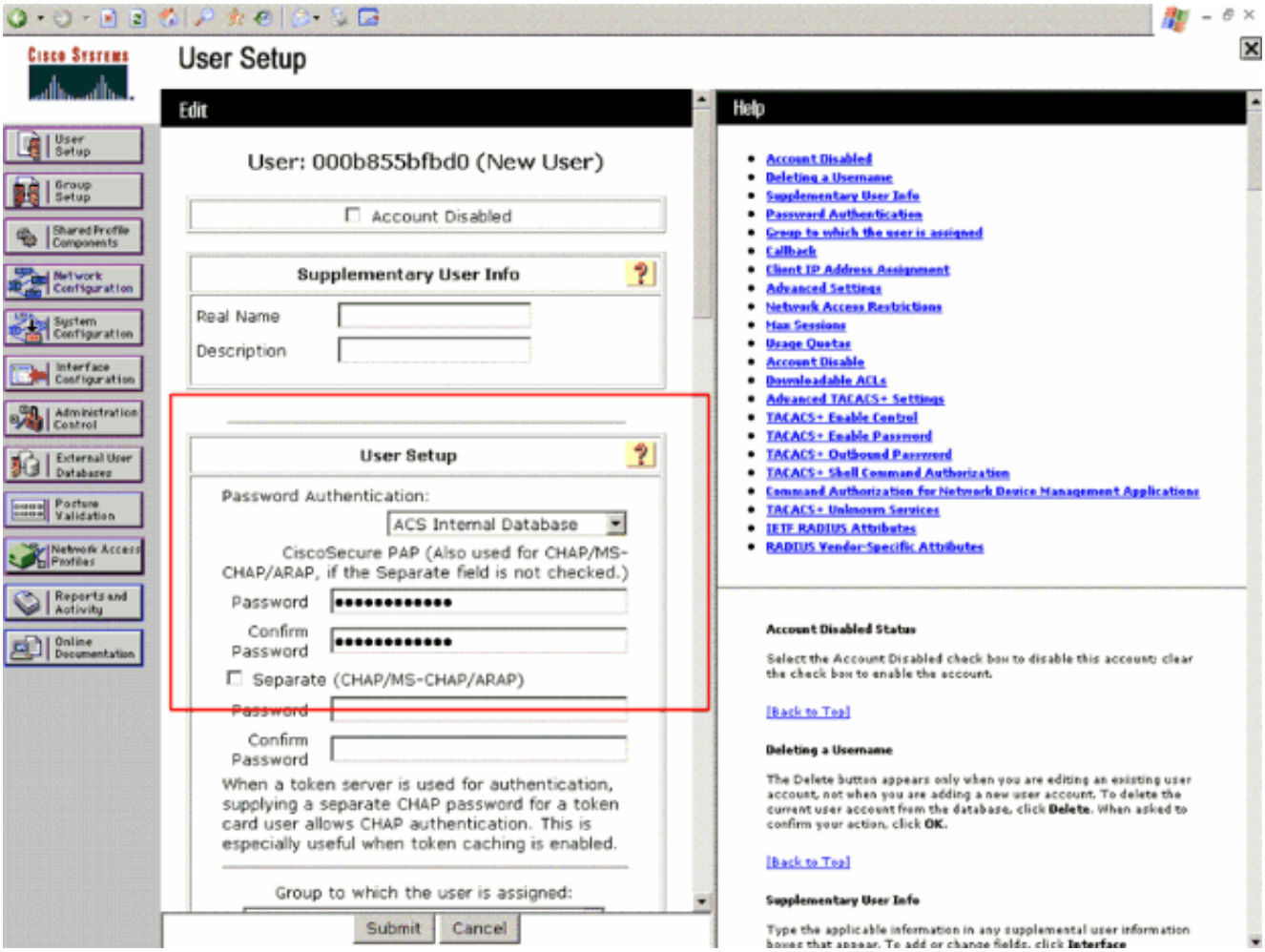
Cisco Secure ACS のユーザデータベースへの LAP MAC アドレスを追加して下さい

Cisco Secure ACS への LAP MAC アドレスを追加するためにこれらのステップを完了して下さい :

1. ACS GUI から [**User Setup**] を選択し、ユーザ名を入力して、[**Add/Edit**] をクリックします。 ユーザ名は承認したいと思う LAP の MAC アドレスであるはずです。 MAC アドレスはコロンかハイフンが含まれていてはなりません。この例では、LAP は MAC アドレス **000b855bfbd0** と追加されます :



2. User Setup ページが現われるとき、示されているとして Password フィールドのこの LAP のためのパスワードを定義して下さい。パスワードはまた LAP の MAC アドレスであるはずです。 この例では、それは **000b855bfbd0** です。



3. [Submit] をクリックします。
4. Cisco Secure ACS データベースにより多くの LAPs を追加するためにこのプロシージャを繰り返して下さい。

確認

この設定を確認するために、LAP をネットワークへの MAC アドレス 00:0b:85:51:5a:e0 と接続し、監視する必要があります。 これを行うために**デバッグ lwapp イベント イネーブル**および **debug aaa all enable** コマンドを使用して下さい。

、RADIUSサーバへの 10.77.244.196 LAP MAC アドレスで渡される WLC デバッグから見られるようにおよびサーバは LAP の認証に成功しました。 次に LAP が WLC に登録されます。

注: 出力で、スペースの制約上 2 行に分割されている行があります。

```
debug aaa all enable Thu Sep 13 13:54:39 2007: AuthenticationRequest: 0xac48778 Thu Sep 13
13:54:39 2007: Callback.....................0x8108e2c Thu Sep 13 13:54:39 2007:
protocolType.....................0x00000001 Thu Sep 13 13:54:39 2007:
proxyState.....................00:0B:85:51:5A:E0-00:00 Thu Sep 13 13:54:39 2007: Packet
contains 8 AVPs (not shown) Thu Sep 13 13:54:39 2007: 00:0b:85:51:5a:e0 Successful transmission
of Authentication Packet (id 123) to 10.77.244.196:1812, proxy state 00:0b:85:51:5a:e0-85:51 Thu
Sep 13 13:54:39 2007: 00000000: 01 7b 00 72 00 00 00 00 00 00 00 00 00 00 00 00 .{.r............
Thu Sep 13 13:54:39 2007: 00000010: 00 00 00 00 01 0e 30 30 30 62 38 35 35 31 35 61
......000b85515a Thu Sep 13 13:54:39 2007: 00000020: 65 30 1e 13 30 30 2d 30 62 2d 38 35 2d 33
33 2d e0..00-0b-85-33- Thu Sep 13 13:54:39 2007: 00000030: 35 32 2d 38 30 1f 13 30 30 2d 30 62
2d 38 35 2d 52-80..00-0b-85- Thu Sep 13 13:54:39 2007: 00000040: 35 31 2d 35 61 2d 65 30 05 06
00 00 00 01 04 06 51-5a-e0........ Thu Sep 13 13:54:39 2007: 00000050: 0a 4d f4 d4 20 06 77 6c
63 31 02 12 03 04 0e 12 .M....wlc1..... Thu Sep 13 13:54:39 2007: 00000060: 84 9c 03 8f 63 40
```

2a be 9d 38 42 91 06 06 00 00 ....c@*..8B..... Thu Sep 13 13:54:39 2007: 00000070: 00 0a .. Thu Sep 13 13:54:40 2007: 00000000: 02 7b 00 30 aa fc 40 4b fe 3a 33 10 f6 5c 30 fd .{.0..@K.:3..\0. Thu Sep 13 13:54:40 2007: 00000010: 12 f3 6e fa 08 06 ff ff ff ff 19 16 43 41 43 53 ..n.........CACS Thu Sep 13 13:54:40 2007: 00000020: 3a 30 2f 39 37 37 2f 61 34 64 66 34 64 34 2f 31 :0/977/a4df4d4/1 Thu Sep 13 13:54:40 2007: ****Enter processIncomingMessages: response code=2 Thu Sep 13 13:54:40 2007: ****Enter processRadiusResponse: response code=2 Thu Sep 13 13:54:40 2007: **00:0b:85:51:5a:e0 Access-Accept received from RADIUS server 10.77.244.196 for mobile 00:0b:85:51:5a:e0** receiveId = 0 Thu Sep 13 13:54:40 2007: AuthorizationResponse: 0x9845500 Thu Sep 13 13:54:40 2007: structureSize.....84 Thu Sep 13 13:54:40 2007: resultCode.....0 Thu Sep 13 13:54:40 2007: protocolUsed.....0x00000001 Thu Sep 13 13:54:40 2007: proxyState.....00:0B:85:51:5A:E0-00:00 Thu Sep 13 13:54:40 2007: Packet contains 2 AVPs: Thu Sep 13 13:54:40 2007: AVP[01] Framed-IP-Address..... 0xffffffff (-1) (4 bytes) Thu Sep 13 13:54:40 2007: AVP[02] Class..... CACS:0/977/a4df4d4/1 (20 bytes) **debug lwapp events enable** Thu Sep 13 14:01:51 2007: 00:0b:85:51:5a:e0 **Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'** Thu Sep 13 14:01:51 2007: 00:0b:85:51:5a:e0 Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1 Thu Sep 13 14:01:51 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1' Thu Sep 13 14:01:51 2007: 00:0b:85:51:5a:e0 **Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1** Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1' Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0: txNonce 00:0B:85:33:52:80 rxNonce 00:0B:85:51:5A:E0 Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 **LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0** Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 Successfully added NPU Entry for AP 00:0b:85:51:5a:e0(index 57)Switch IP: 10.77.244.213, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 10.77.244.221, AP Port: 5550, next hop MAC: 00:0b:85:51:5a:e0 Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 **Successfully transmission of LWAPP Join-Reply to AP 00:0b:85:51:5a:e0** Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 0 Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 **Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 1**

トラブルシューティング

設定をトラブルシューティングするこれらのコマンドを使用して下さい:

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。

- LWAPP イベントおよびエラーの **lwapp イベント** 設定デバッグを **enable —デバッグして下さい。**
- LWAPP パケットトレースの **lwapp パケット** 設定デバッグを **enable —デバッグして下さい**。
- **debug aaa all enable**：すべての AAA メッセージのデバッグを設定します。

関連情報

- Autonomous Cisco Aironet アクセス ポイントの Lightweight モードへのアップグレード手順
- LWAPP アップグレード ツールのトラブルシューティングのヒント
- 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