

ISR と WEP 暗号化および LEAP 認証を使用するワイヤレス LAN 接続の設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ネットワーク図](#)

[表記法](#)

[871W ルータの設定](#)

[クライアント アダプタの設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、WEP 暗号化と LEAP 認証を使用する無線 LAN の接続用に Cisco 870 シリーズ Integrated Services Router (ISR; サービス統合型ルータ) を設定する方法について説明します。

Cisco ISR 無線シリーズの他のモデルにも、同じ設定が適用されます。

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 870 シリーズ ISR の基本パラメータを設定する方法についての知識。
- Aironet Desktop Utility (ADU) を使用して 802.11a/b/g 無線クライアント アダプタを設定する方法についての知識。

802.11a/b/g クライアント アダプタを設定する方法については、『[Cisco Aironet 802.11a/b/g ワイヤレス LAN クライアント アダプタ \(CB21AG および PI21AG \) インストレーション コンフィギュレーションガイド、リリース 2.5](#)』を参照してください。

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。

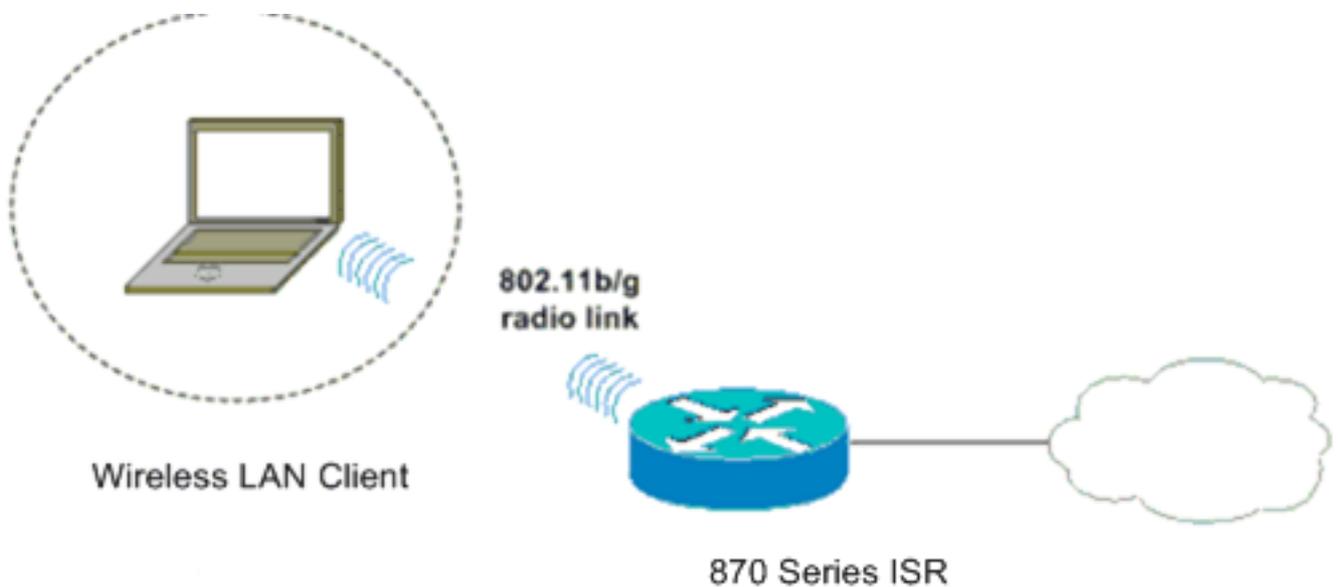
- Cisco IOS®ソフトウェアリリース12.3Y11が稼働するCisco 871W ISR
- Aironet Desktop Utility バージョン 2.5 がインストールされているラップトップ PC
- ファームウェア バージョン 2.5 が稼働する 802.11 a/b/g クライアント アダプタ

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。

ネットワーク図

このドキュメントでは、次のネットワーク設定を使用します。

このセットアップでは、ワイヤレス LAN クライアントは、870 ルータに関連付けられます。870 ルータの内部 Dynamic Host Configuration Protocol (DHCP) サーバを使用して、ワイヤレス クライアントに IP アドレスが提供されます。870 ISR と WLAN クライアントでは、WEP 暗号化が有効になっています。LEAP 認証を使用してワイヤレス ユーザが認証され、870 ルータ上のローカル RADIUS サーバ機能を使用してクレデンシャルが検証されます。



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。

871W ルータの設定

アクセスポイントとしてワイヤレスクライアントからの関連付け要求を受け付けるように 871W ISR を設定するには、次のステップを実行します。

1. Integrated Routing and Bridging (IRB) を設定し、ブリッジグループを設定します。IRB を有効にするには、グローバルコンフィギュレーションモードから次のコマンドを入力しま

す。

```
WirelessRouter<config>#bridge irb
!--- Enables IRB. WirelessRouter<config>#bridge 1 protocol ieee !--- Defines the type of
Spanning Tree Protocol as ieee. WirelessRouter<config>#bridge 1 route ip
!--- Enables the routing of the specified protocol in a bridge group.
```

2. Bridged Virtual Interface (BVI) を設定します。BVI に IP アドレスを割り当てます。グローバル コンフィギュレーション モードから次のコマンドを入力します。

```
WirelessRouter<config>#interface bvi1
!--- Enter interface configuration mode for the BVI. WirelessRouter<config-if>#ip address
172.16.1.100 255.255.0.0
```

アクセスポイントのブリッジグループの機能に関する詳細は、『[Cisco Aironetワイヤレス機器でのVLANの使用](#)』の「アクセスポイントとブリッジのブリッジグループ設定」セクションを参照してください。

3. 871W ISR に内部 DHCP サーバ機能を設定します。ルータの内部 DHCP サーバ機能を使用して、ルータに関連付けされるワイヤレス クライアントに IP アドレスを割り当てることができます。グローバル コンフィギュレーション モードで次のコマンドを実行します。

```
WirelessRouter<config>#ip dhcp excluded-address 172.16.1.100 172.16.1.100
!--- Excludes IP addresses from the DHCP pool. !--- This address is used on the BVI
interface, so it is excluded. WirelessRouter<config>#ip dhcp pool 870-ISR
WirelessRouter<dhcp-config>#network 172.16.1.0 255.255.0.0
```

注：クライアントアダプタは、DHCPサーバからIPアドレスを受け入れるように設定する必要があります。

4. 871W ISR をローカル RADIUS サーバとして設定します。グローバル コンフィギュレーション モードで次のコマンドを入力して、871W ISR をローカル RADIUS サーバとして設定します。

```
WirelessRouter<config>#aaa new-model
!--- Enable the authentication, authorization, and accounting !--- (AAA) access control
model. WirelessRouter<config>#radius-server local
!--- Enables the 871 wireless-aware router as a local !--- authentication server and enters
into configuration !--- mode for the authenticator. WirelessRouter<config-radsrv>#nas
172.16.1.100 key Cisco
!--- Adds the 871 router to the list of devices that use !--- the local authentication
server. WirelessRouter<config-radsrv>#user ABCD password ABCD
WirelessRouter<config-radsrv>#user XYZ password XYZ
!--- Configure two users ABCD and XYZ on the local RADIUS server. WirelessRouter<config-
radsrv>#exit
WirelessRouter<config>#radius-server host 172.16.1.100 auth-port 1812 acct-port 1813 key
Cisco
!--- Specifies the RADIUS server host.
```

注：ローカルRADIUSサーバの認証とアカウントングには、ポート1812と1813を使用します。

```
WirelessRouter<config>#aaa group server radius rad_eap
!--- Maps the RADIUS server to the group rad_eap
.
WirelessRouter<config-sg-radius>#server 172.16.1.100 auth-port 1812 acct-port 1813
!--- Define the server that falls in the group rad_eap. WirelessRouter<config>#aaa
authentication login eap_methods group rad_eap
!--- Enable AAA login authentication.
```

5. 無線インターフェイスを設定します。無線インターフェイスの設定には、SSID、暗号化モード、認証タイプ、速度、無線ルータの役割など、ルータのさまざまな無線パラメータの設定が含まれます。この例では、Test という名前の SSID を使用します。無線インターフェイスを設定するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

```
WirelessRouter<config>#interface dot11radio0
```

```
!--- Enter radio interface configuration mode. WirelessRouter<config-if>#ssid Test
!--- Configure an SSID test. irelessRouter<config-ssid>#authentication open eap eap_methods
WirelessRouter<config-ssid>#authentication network-eap eap_methods
!--- Expect that users who attach to SSID 'Test' !--- are requesting authentication with
the type 128 !--- Network Extensible Authentication Protocol (EAP) !--- authentication bit
set in the headers of those requests. !--- Group these users into a group called
'eap_methods'. WirelessRouter<config-ssid>#exit
!--- Exit interface configuration mode. WirelessRouter<config-if>#encryption mode wep
mandatory
!--- Enable WEP encryption. WirelessRouter<config-if>#encryption key 1 size 128
1234567890ABCDEF1234567890
!--- Define the 128-bit WEP encryption key. WirelessRouter<config-if>#bridge-group 1
WirelessRouter<config-if>#no shut
!--- Enables the radio interface.
```

この手順が終了すると、870 ルータは無線クライアントからの関連付け要求を受け付けます。ルータでEAP認証タイプを設定する場合、認証の問題を回避するために、認証タイプとして[Network-EAP]と[Open with EAP]の両方を選択することを推奨します。

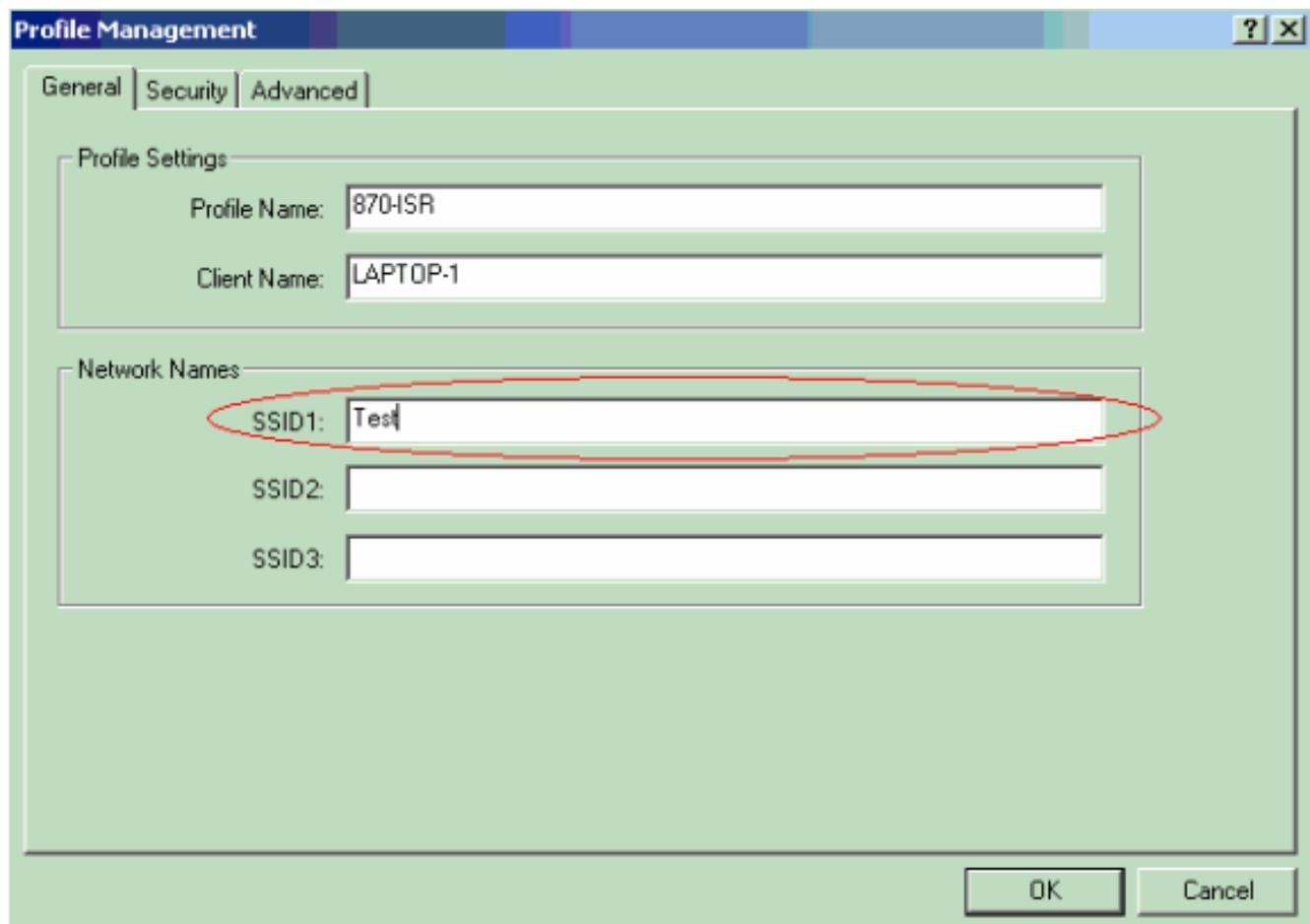
```
WirelessRouter<config-ssid>#authentication network-eap eap_methods
WirelessRouter<config-ssid>#authentication open eap eap_methods
```

注：このドキュメントでは、ネットワークにCiscoワイヤレスクライアントしかないことを前提としています。注：このドキュメントで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ([登録ユーザ専用](#)) を使用してください。

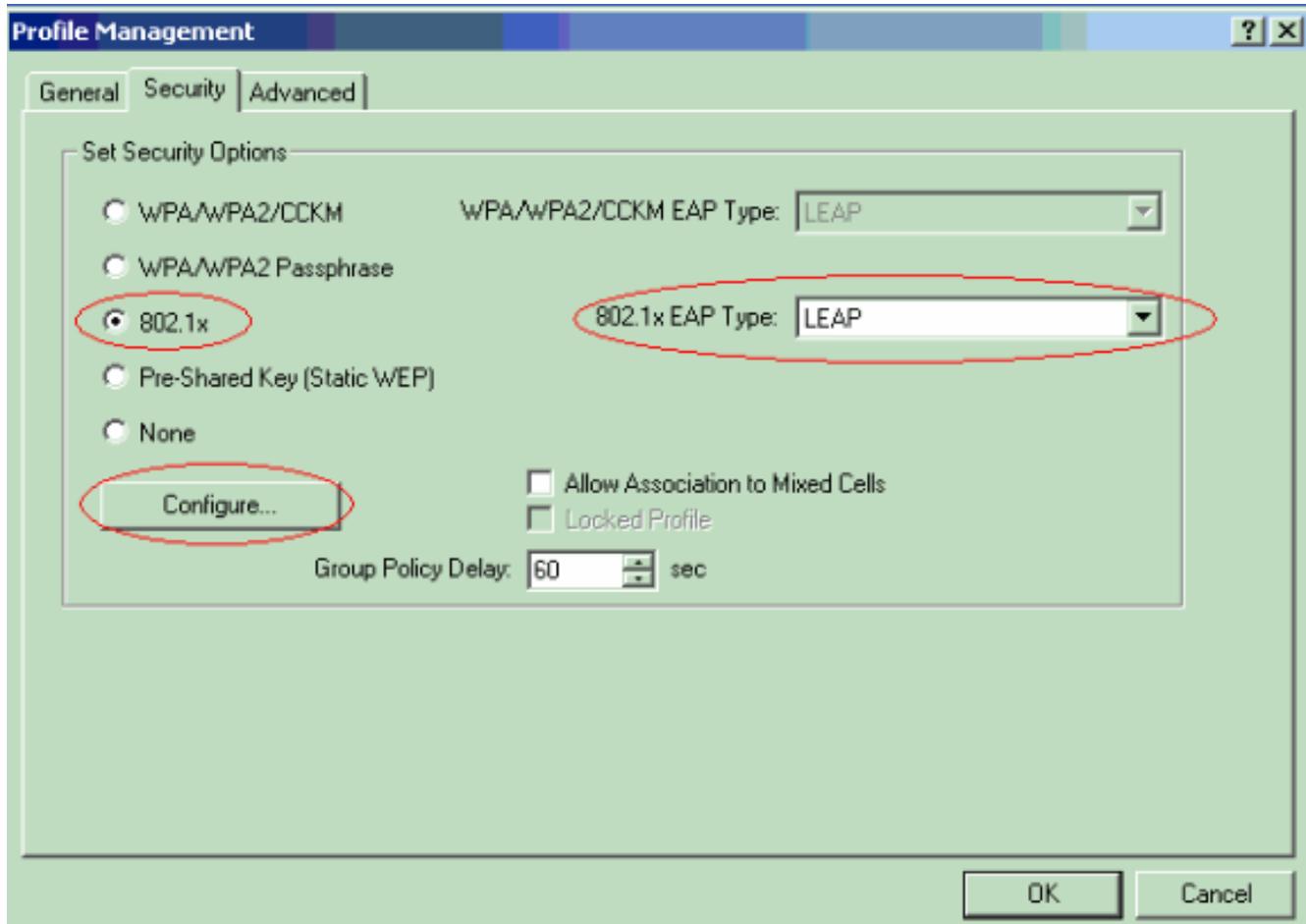
クライアント アダプタの設定

クライアント アダプタを設定するには、次のステップを実行します。この手順では、例として、ADU 上に 870-ISR という名前の新しいプロファイルを作成します。またこの手順では、SSID として Test を使用し、クライアント アダプタで LEAP 認証を有効にします。

1. ADU の Profile Management ウィンドウで、New をクリックして新しいプロファイルを作成します。General タブで、クライアント アダプタが使用するプロファイル名と SSID を入力します。この例では、プロファイル名には 870-ISR、SSID には Test を使用します。注：**SSIDは**、871W ISRで設定したSSIDと完全に一致している必要があります。SSID では大文字と小文字が区別されます。



2. Security タブに移動して、802.1x を選択し、802.1x EAP Type メニューから LEAP を選択します。これにより、クライアントアダプタで LEAP 認証が有効になります。



3. Configure をクリックして、LEAP 設定を定義します。この設定では、Automatically Prompt

for Username and Password オプションを選択しています。このオプションにより、LEAP 認証が実行されたときに、ユーザ名およびパスワードを手動入力できるようになります。

LEAP Settings [?] [X]

Always Resume the Secure Session

Username and Password Settings

Use Temporary User Name and Password

Use Windows User Name and Password

Automatically Prompt for User Name and Password

Manually Prompt for User Name and Password

Use Saved User Name and Password

User Name:

Password:

Confirm Password:

Domain:

Include Windows Logon Domain with User Name

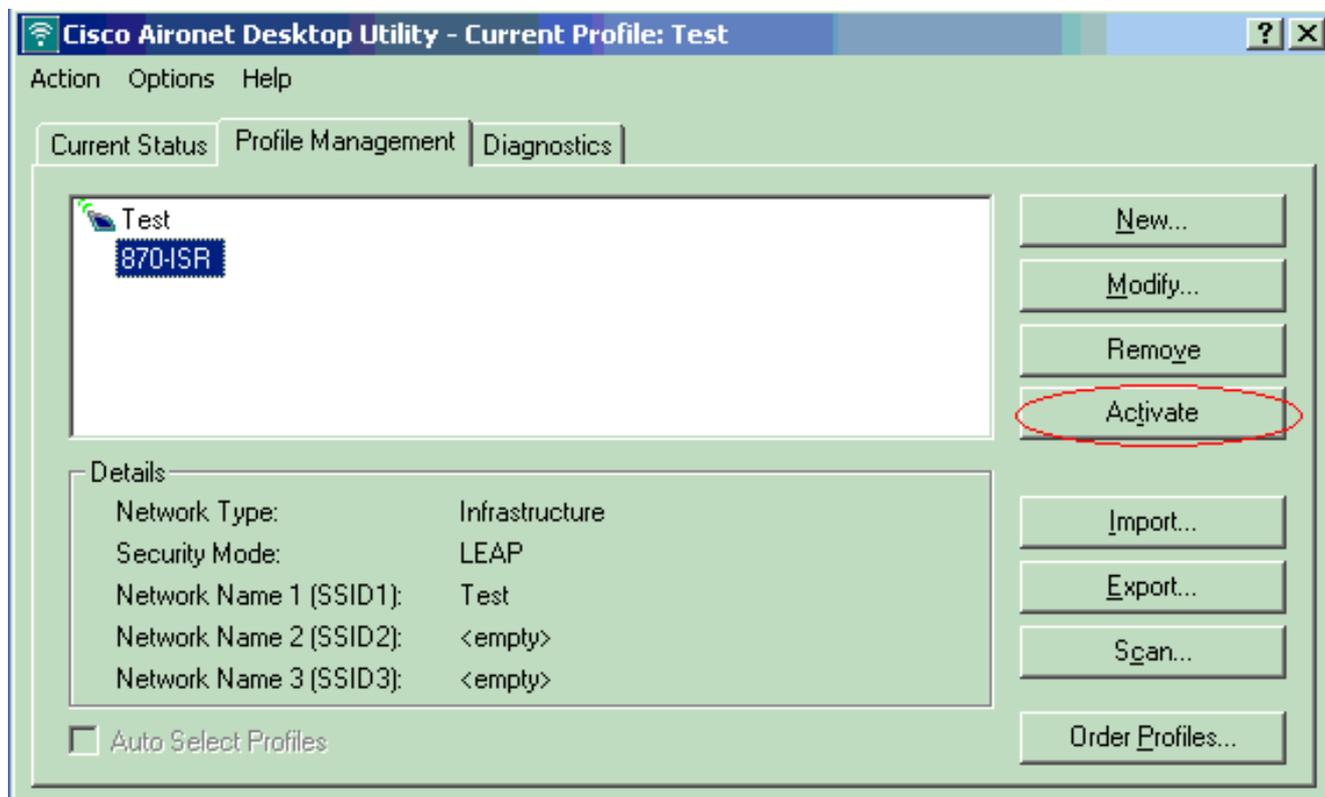
No Network Connection Unless User Is Logged In

Authentication Timeout Value (in seconds)

OK Cancel

4. OK をクリックして Profile Management ウィンドウを終了します。

5. Activate をクリックして、このプロファイルをクライアント アダプタで有効にします。



確認

ここでは、設定が正常に機能しているかどうかを確認します。

クライアントアダプタと 870 ルータの設定が終了したら、クライアントアダプタ上のプロファイル 870-ISR を有効にして、設定を確認します。

Enter Wireless Network Password ウィンドウが表示されたら、ユーザ名とパスワードを入力します。ユーザ名とパスワードは、871W ISR で設定したものに对应している必要があります。この例で使用しているプロファイルの 1 つは、ユーザ名が ABCD でパスワードが ABCD です。

Enter Wireless Network Password

Please enter your LEAP username and password to log on to the wireless network

User Name : ABCD

Password : ****

Log on to :

Card Name : Cisco Aironet 802.11 a/b/g Wireless Adapter

Profile Name : 870-ISR

OK Cancel

LEAP Authentication Status ウィンドウが表示されます。このウィンドウでは、ローカル RADIUS サーバに対するユーザのクレデンシャルが検証されます。

LEAP Authentication Status

Card Name: Cisco Aironet 802.11 a/b/g Wireless Adapter

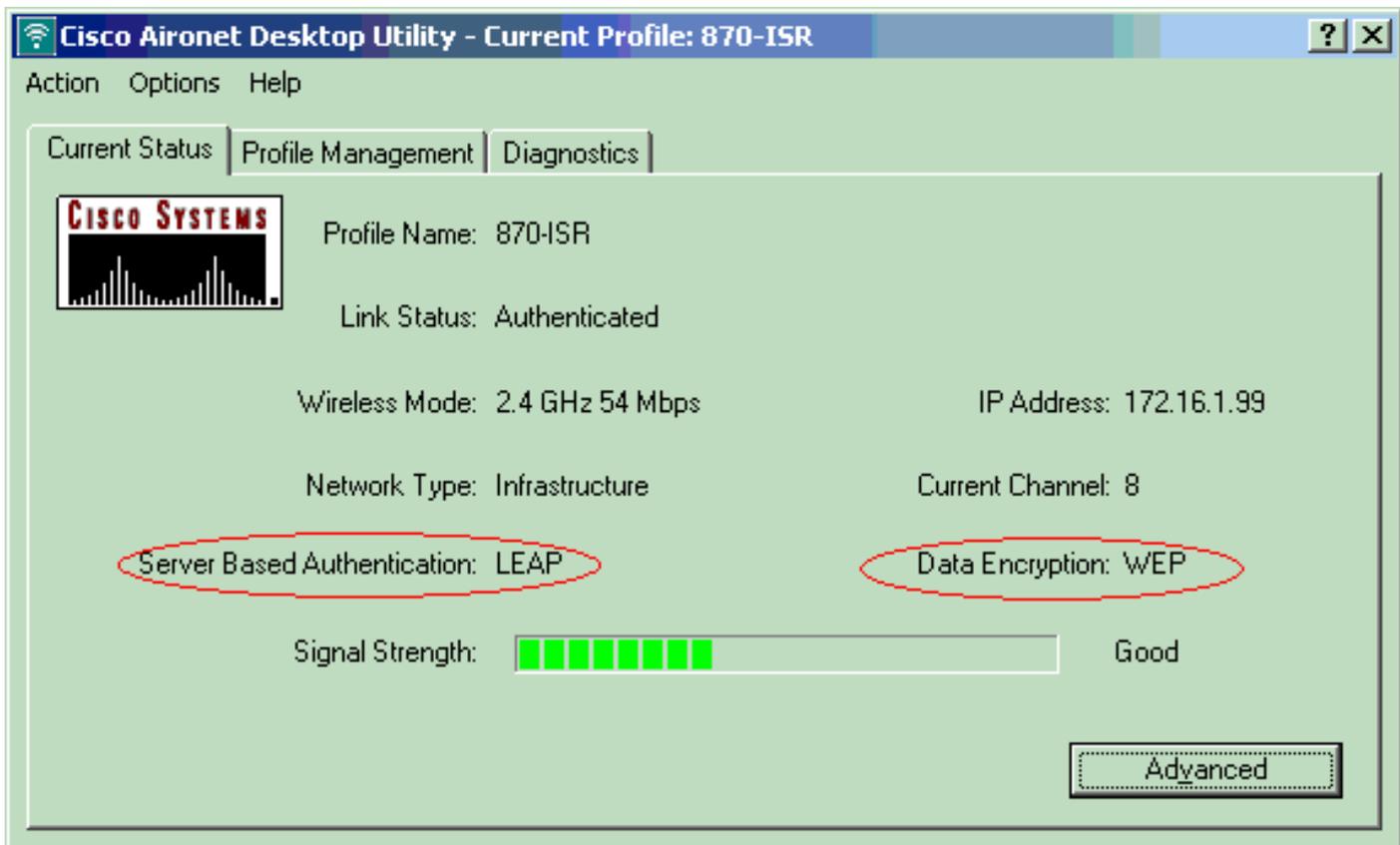
Profile Name: 870-ISR

Steps	Status
1. Starting LEAP Authentication	Success
2. Checking Link Status	Success
3. Renewing IP address	Success
4. Detecting IPX Frame Type	Success
5. Finding Domain Controller	Success

Show minimized next time

Cancel

クライアントが WEP 暗号化と LEAP 認証を使用していることを確認するには、ADU の Current Status をチェックします。



[アウトプットインタープリタ ツール \(登録ユーザ専用\) \(OIT\)](#) は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- **show dot11 association:**870ルータの設定を確認します。

```
WirelessRouter#show dot11 association
```

```
802.11 Client Stations on Dot11Radio0:
```

```
SSID [Test]:
```

MAC Address	IP Address	Device	Name	Parent	State
0040.96ac.dd05	172.16.1.99	CB21AG/PI21AG	LAPTOP-1	self	EAP-Associated

```
Others: (not related to any ssid)
```

- **show ip dhcp binding :** クライアントにDHCPサーバ経由のIPアドレスがあることを確認します。

```
WirelessRouter#show ip dhcp binding
```

```
Bindings from all pools not associated with VRF:
```

IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type
172.16.1.99	0040.96ac.dd05	Feb 6 2006 10:11 PM	Automatic

トラブルシューティング

このセクションでは、この設定に関連するトラブルシューティング情報を提供します。

1. 認証を一時的に無効にするには、SSID の方式を Open に設定します。これにより、認証の成功を妨げる Radio Frequency (RF; 無線周波数) の問題が発生する可能性が解消されます。CLI から no authentication open eap eap_methods、no authentication network-eap eap_methods、authentication open の各コマンドを使用します。クライアントが関連付けに

成功する場合には、RF はアソシエーションの問題に関係しません。

2. ワイヤレス ルータで設定されている WEP キーが、クライアントで設定されている WEP キーと一致することをチェックします。WEP キーが一致しない場合、クライアントはワイヤレス ルータと通信できません。
3. ワイヤレス ルータと認証サーバ間で共有秘密パスワードが同期していることを確認します

。

次のデバッグ 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もできます。

- `debug dot11 aaa authenticator all:MAC` および EAP 認証パケットのデバッグをアクティブにします。
- `debug radius authentication` : サーバとクライアント間の RADIUS ネゴシエーションを表示します。
- `debug radius local-server packets` : 送受信される RADIUS パケットの内容を表示します。
- `debug radius local-server client` : 失敗したクライアント認証に関するエラー メッセージを表示します。

関連情報

- [暗号化アルゴリズムと認証タイプ](#)
- [SDM による固定 ISR のワイヤレス認証種別の設定例](#)
- [固定 ISR のワイヤレス認証種別の設定例](#)
- [Cisco アクセス ルータ ワイヤレス コンフィギュレーション ガイド](#)
- [内部 DHCP とオープン認証を使用する 1800 ISR ワイヤレス ルータの設定例](#)
- [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](#)