WEP 암호화 및 LEAP 인증 구성을 사용하여 ISR을 사용하는 무선 LAN 연결 예

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[네트워크 다이어그램](#)
[표기 규칙](#)
[871W 라우터 컨피그레이션](#)
[클라이언트 어댑터 구성](#)
[다음을 확인합니다.](#)
[문제 해결](#)
[관련 정보](#)

소개

이 문서에서는 WEP 암호화 및 LEAP 인증을 사용하여 무선 LAN 연결을 위해 Cisco 870 Series ISR(Integrated Services Router)을 구성하는 방법에 대해 설명합니다.

다른 모든 Cisco ISR Wireless Series 모델에도 동일한 컨피그레이션이 적용됩니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- Cisco 870 Series ISR의 기본 매개변수를 구성하는 방법에 대한 지식
- ADU(Aironet Desktop Utility)를 사용하여 802.11a/b/g 무선 클라이언트 어댑터를 구성하는 방법에 대한 지식

802.11a/b/g 클라이언트 어댑터 구성 방법에 대한 자세한 내용은 Cisco Aironet 802.11a/b/g Wireless LAN Client Adapter(CB21AG 및 PI21AG) 설치 및 구성 설명서, 릴리스 2.5를 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® 소프트웨어 릴리스 12.3(8)YI1을 실행하는 Cisco 871W ISR

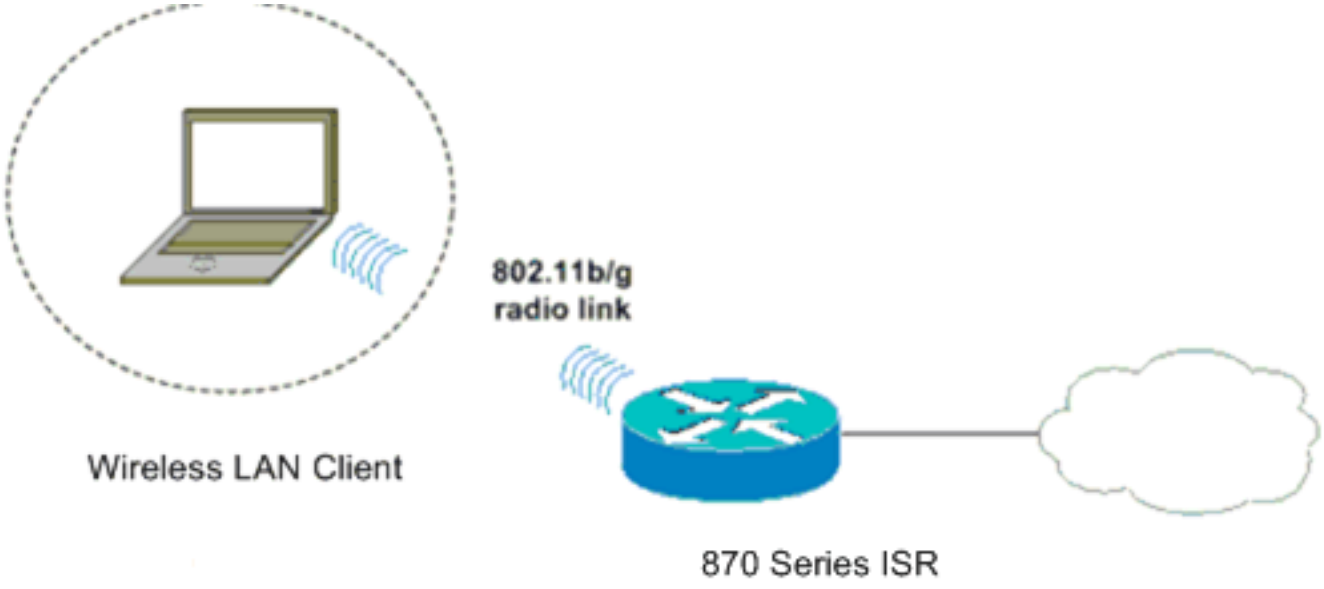
- Aironet Desktop Utility 버전 2.5가 설치된 노트북
- 펌웨어 버전 2.5를 실행하는 802.11 a/b/g 클라이언트 어댑터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.

이 설정에서는 무선 LAN 클라이언트가 870 라우터와 연결됩니다.870 라우터의 내부 DHCP(Dynamic Host Configuration Protocol) 서버는 무선 클라이언트에 IP 주소를 제공하는 데 사용됩니다.870 ISR 및 WLAN 클라이언트에서 WEP 암호화가 활성화됩니다.LEAP 인증은 무선 사용자를 인증하는 데 사용되며 870 라우터의 로컬 RADIUS 서버 기능을 사용하여 자격 증명을 검증합니다.



표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

871W 라우터 컨피그레이션

871W ISR을 액세스 포인트로 구성하여 무선 클라이언트의 연결 요청을 수락하려면 다음 단계를 완료하십시오.

1. IRB(Integrated Routing and Bridging)를 구성하고 브리지 그룹을 설정합니다.IRB를 활성화하려면 글로벌 컨피그레이션 모드에서 이 명령을 입력합니다.

```
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. BVI(bridged virtual interface)를 구성합니다.BVI에 IP 주소를 할당합니다.전역 컨피그레이션 모드에서 이 명령을 입력합니다.

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

액세스 포인트에서 브리지 그룹의 기능에 대한 자세한 내용은 Cisco Aironet Wireless Equipment를 사용하여 VLAN 사용의 액세스 포인트 및 브리지에 대한 브리지 그룹 구성 섹션을 참조하십시오.

3. 871W ISR에서 내부 DHCP 서버 기능을 구성합니다.라우터의 내부 DHCP 서버 기능을 사용하여 라우터에 연결된 무선 클라이언트에 IP 주소를 할당할 수 있습니다.전역 컨피그레이션 모드에서 이 명령을 완료합니다.

```
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
```

참고: 클라이언트 어댑터도 DHCP 서버의 IP 주소를 허용하도록 구성해야 합니다.

4. 871W ISR을 로컬 RADIUS 서버로 구성합니다.전역 컨피그레이션 모드에서 이러한 명령을 입력하여 871W ISR을 로컬 RADIUS 서버로 구성합니다.

```
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.
```

참고: 로컬 RADIUS 서버의 인증 및 계정 관리를 위해 포트 1812 및 1813을 사용합니다.

```
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. 라디오 인터페이스를 구성합니다.무선 인터페이스의 컨피그레이션에는 SSID, 암호화 모드, 인증 유형, 속도 및 무선 라우터의 역할을 비롯한 라우터의 다양한 무선 매개변수 컨피그레이션이 포함됩니다.이 예에서는 Test라는 SSID를 **사용합니다**.전역 컨피그레이션 모드에서 라디오 인터페이스를 구성하려면 다음 명령을 입력합니다.

```
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.
```

870 라우터는 이 절차를 마치면 무선 클라이언트의 연결 요청을 수락합니다.라우터에서 EAP 인증 유형을 구성할 때 인증 문제를 피하기 위해 **Network-EAP 및 Open with EAP**를 인증 유형으로 모두 선택하는 것이 좋습니다.

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

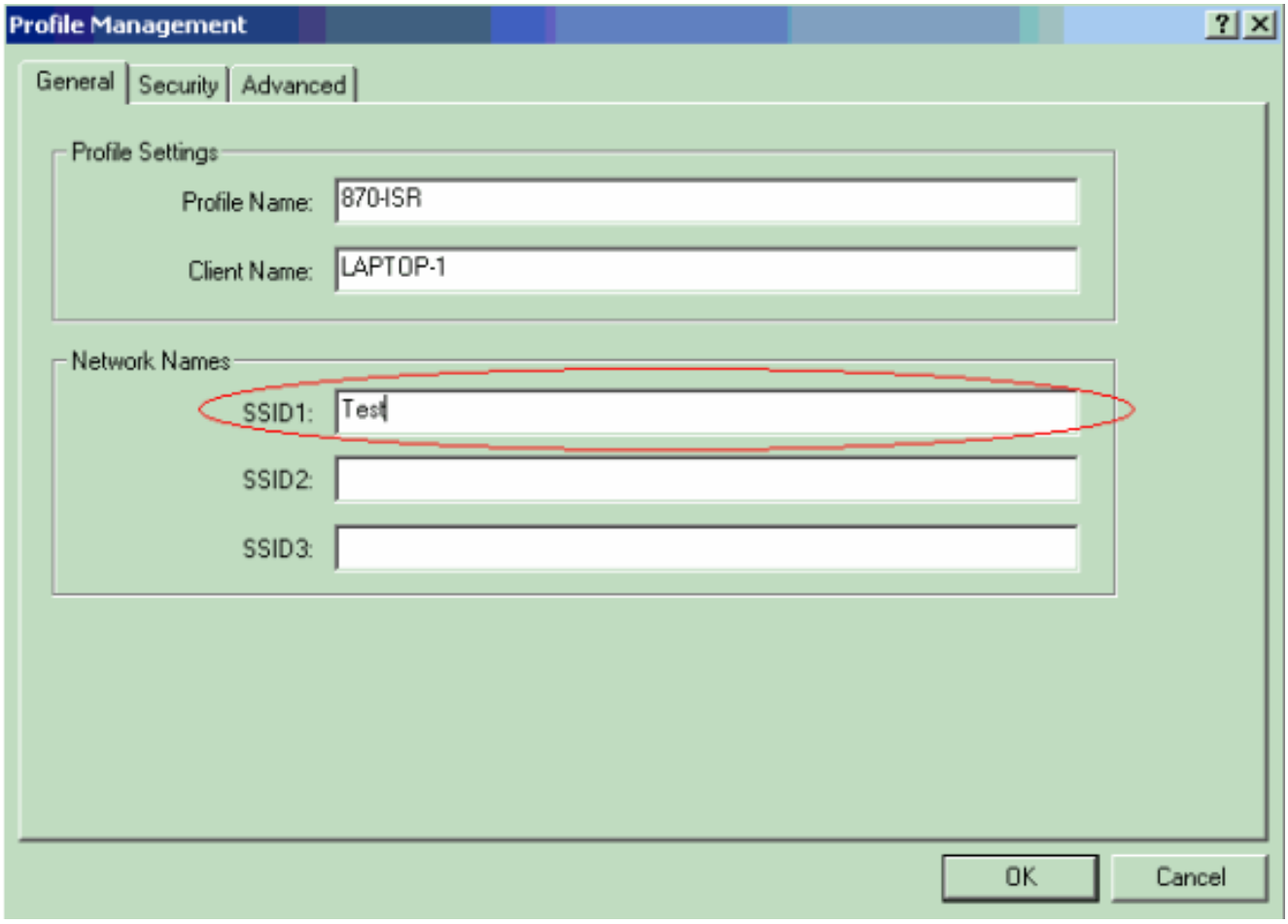
참고: 이 문서에서는 네트워크에 Cisco Wireless 클라이언트만 있다고 가정합니다.**참고:** 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 문서에 사용된 명령에 대한 자세한 내용을 확인하십시오.

클라이언트 어댑터 구성

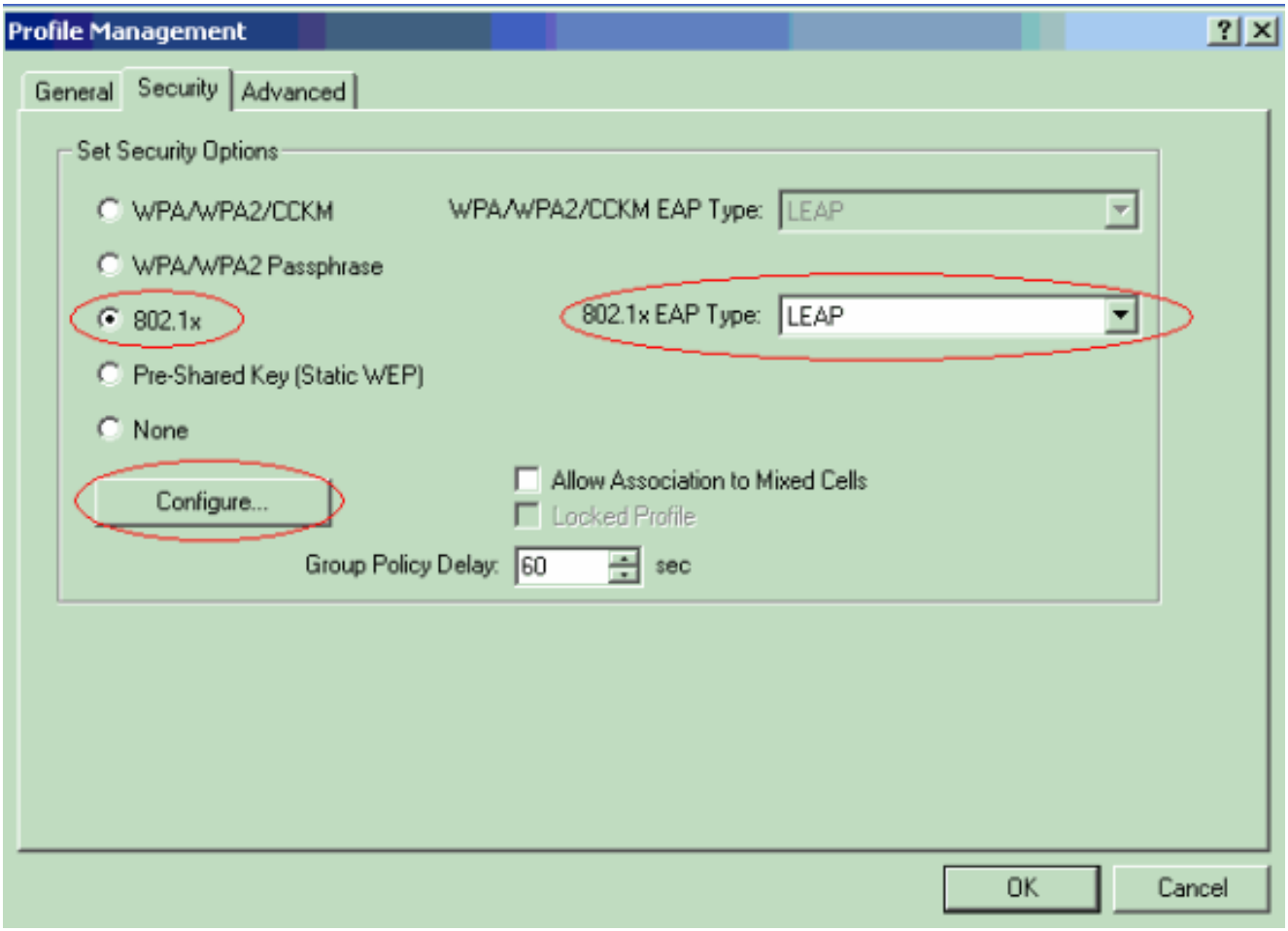
클라이언트 어댑터를 구성하려면 다음 단계를 완료합니다.이 절차에서는 ADU에 **870-ISR**이라는 새 프로파일을 예를 들어 생성합니다.이 절차에서는 Test를 SSID로 사용하고 클라이언트 어댑터에서 LEAP 인증을 활성화합니다.

1. ADU의 Profile Management(프로파일 관리) 창에서 새 프로파일을 생성하려면 New(새로 만들기)를 클릭합니다.General(일반) 탭에서 클라이언트 어댑터가 사용하는 프로파일 이름 및 SSID를 입력합니다.이 예에서 프로파일 이름은 **870-ISR**이고 SSID는 **Test입니다.참고:** SSID는 871W ISR에서 구성한 SSID와 정확히 일치해야 합니다.SSID는 대/소문자를 구분합니다

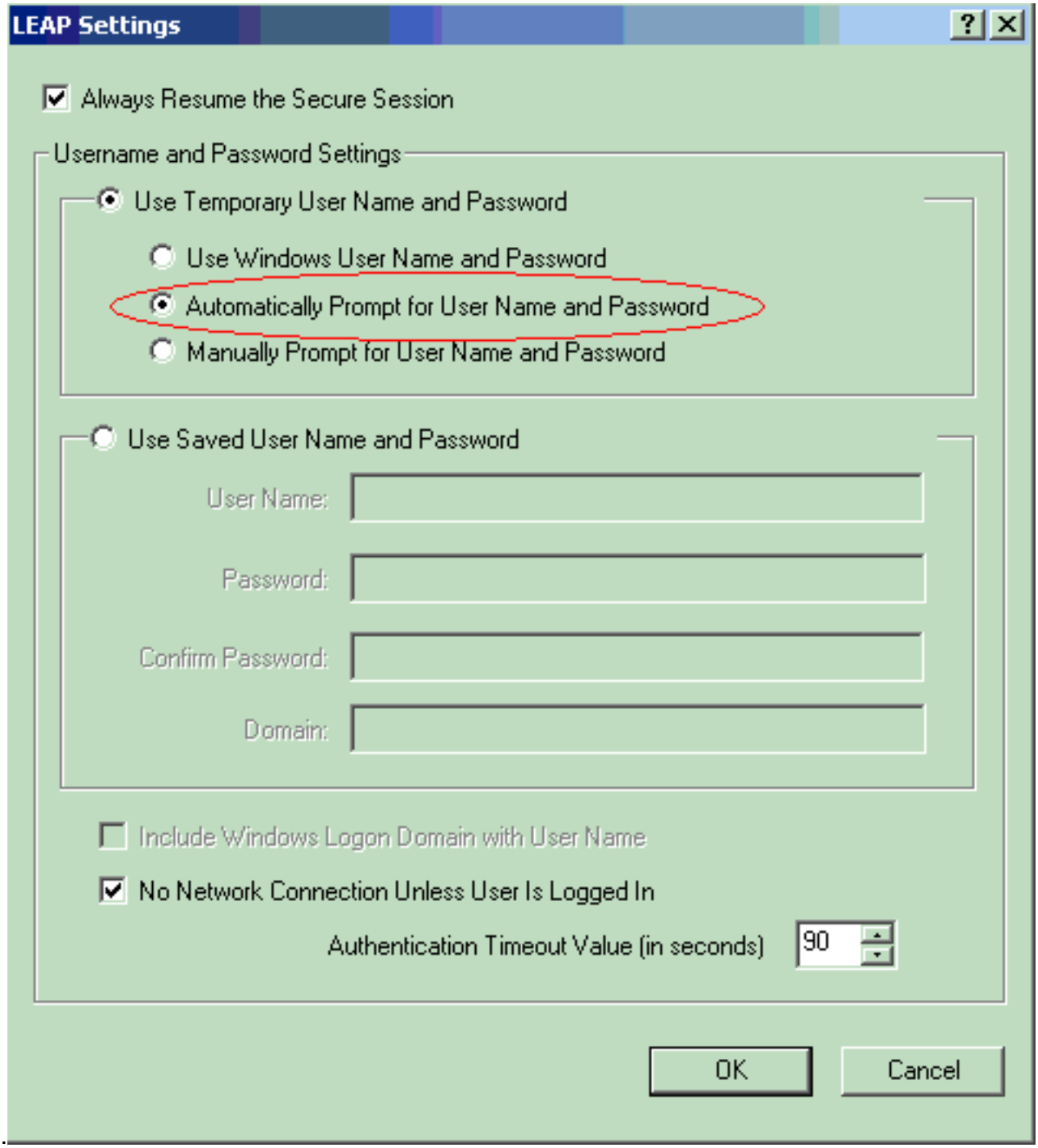
.



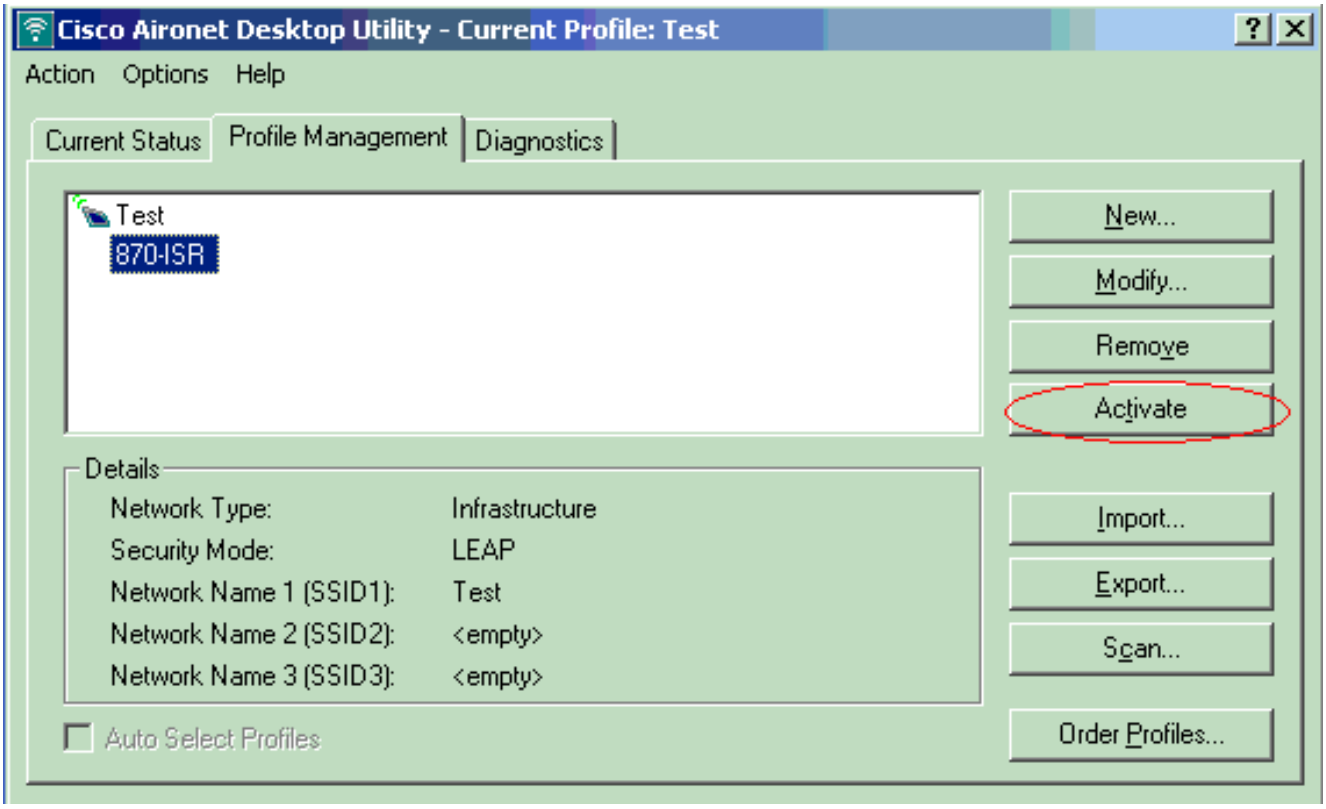
2. Security(보안) 탭으로 이동하여 **802.1x**를 선택하고 802.1x EAP Type(802.1x EAP 유형) 메뉴에서 LEAP를 선택합니다.이 작업은 클라이언트 어댑터에서 LEAP 인증을 활성화합니다
.



3. Configure(구성)를 클릭하여 LEAP 설정을 정의합니다.이 컨피그레이션에서는 **Automatically Prompt for Username and Password**(사용자 이름 **및 비밀번호 자동 프롬프트) 옵션을 선택합니다**.이 옵션을 사용하면 LEAP 인증이 발생할 때 사용자 이름과 비밀번호를 수동으로 입력할 수 있습니다



4. 확인을 클릭하여 프로파일 관리 창을 종료합니다.
5. 클라이언트 어댑터에서 이 프로파일을 활성화하려면 Activate를 클릭합니다
.

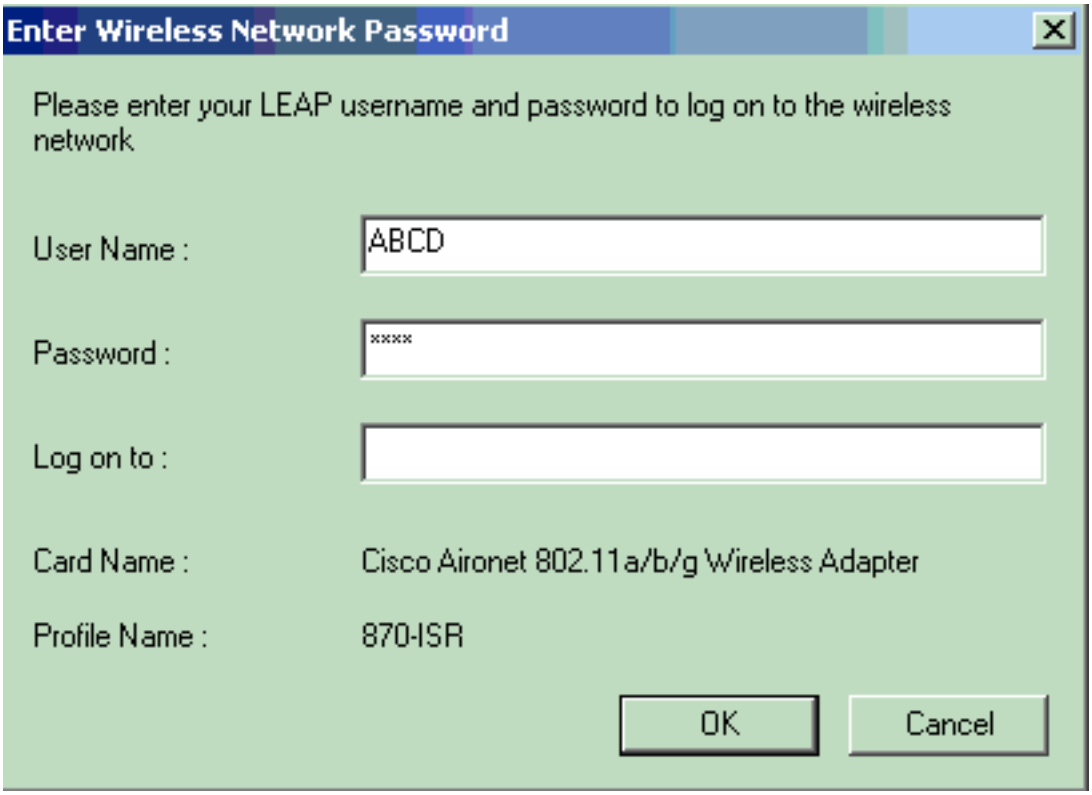


다음을 확인합니다.

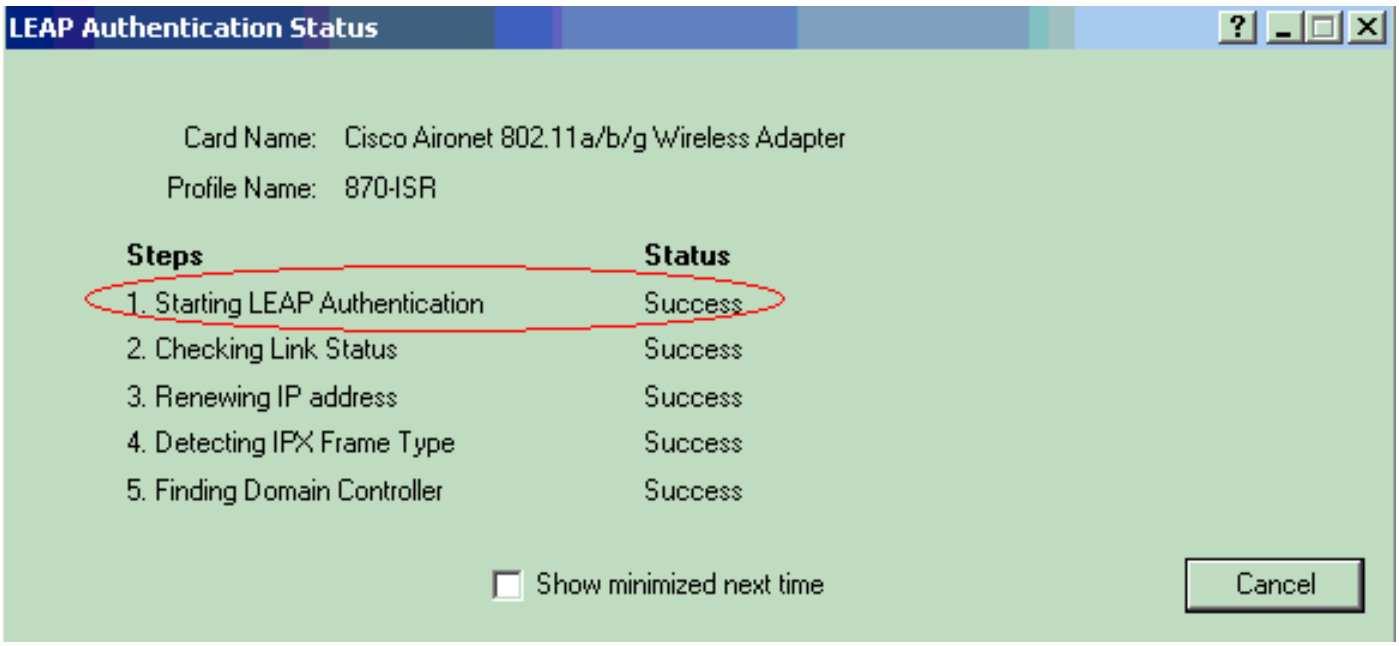
이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

클라이언트 어댑터와 870 라우터가 구성되면 클라이언트 어댑터에서 프로파일 870-ISR을 활성화하여 컨피그레이션을 확인합니다.

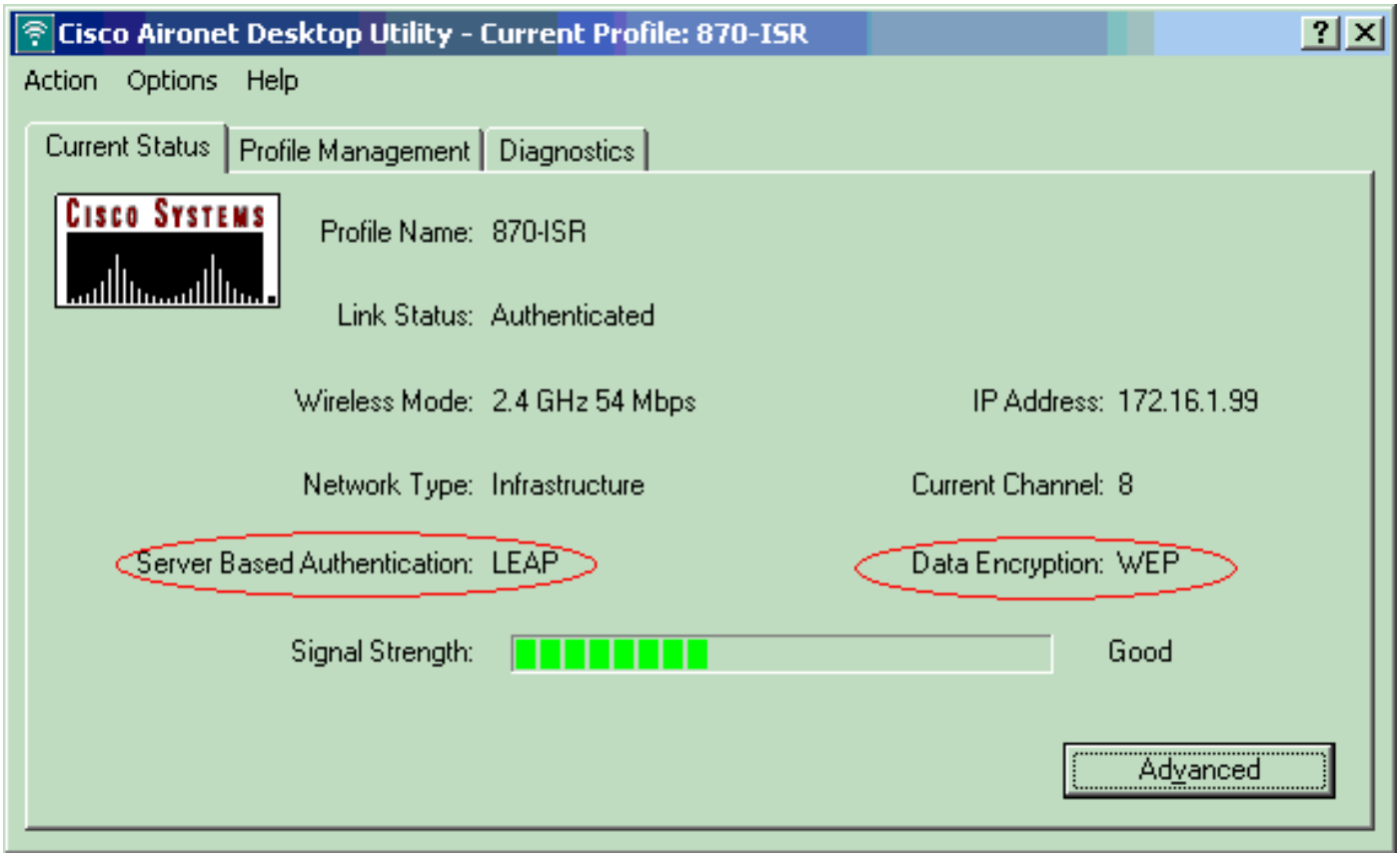
Enter Wireless Network Password(무선 네트워크 비밀번호 입력) 창이 표시되면 사용자 이름과 비밀번호를 입력합니다.이는 871W ISR에 구성된 것과 일치해야 합니다.이 예에서 사용되는 프로파일 중 하나는 User Name ABCD 및 Password ABCD입니다.



LEAP Authentication Status(LEAP 인증 상태) 창이 나타납니다.이 창은 로컬 RADIUS 서버에 대한 사용자 자격 증명을 확인합니다.



클라이언트가 WEP 암호화 및 LEAP 인증을 사용하는지 확인하려면 ADU 현재 상태를 확인합니다.



Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show dot11 association** - 870 라우터의 컨피그레이션을 확인합니다.

```
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** - 클라이언트가 DHCP 서버를 통해 IP 주소를 가지고 있는지 확인합니다.

```
WirelessRouter#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address        Client-ID/       Lease expiration      Type
                  Hardware address/
                  User name
172.16.1.99       0040.96ac.dd05     Feb 6 2006 10:11 PM  Automatic
```

문제 해결

이 섹션에서는 이 컨피그레이션과 관련된 문제 해결 정보를 제공합니다.

1. 일시적으로 인증을 비활성화하려면 SSID의 방법을 **Open**으로 설정합니다.따라서 RF(Radio Frequency) 문제가 발생하여 인증이 실패할 가능성이 없습니다.CLI에서 **no authentication open eap_methods**, **no authentication network-eap_methods** 및 **authentication open** 명령을 사용합니다.클라이언트가 성공적으로 연결되면 RF는 연결 문제에 영향을 주지 않습니다
2. 무선 라우터에 구성된 WEP 키가 클라이언트에 구성된 WEP 키와 일치하는지 확인합니다

.WEP 키가 일치하지 않으면 클라이언트가 무선 라우터와 통신할 수 없습니다.

3. 무선 라우터와 인증 서버 간에 공유 비밀 암호가 동기화되었는지 확인합니다.

이러한 debug 명령을 사용하여 컨피그레이션 문제를 해결할 수도 있습니다.

- **debug dot11 aaa authenticator all** - MAC 및 EAP 인증 패킷의 디버깅을 활성화합니다.
- **debug radius authentication(디버그 radius 인증)** - 서버와 클라이언트 간의 RADIUS 협상을 표시합니다.
- **debug radius local-server packets** - 전송 및 수신된 RADIUS 패킷의 내용을 표시합니다.
- **debug radius local-server client -** 실패한 클라이언트 인증에 대한 오류 메시지를 표시합니다.

관련 정보

- 암호화 알고리즘 및 인증 유형
- SDM을 통한 고정 ISR의 무선 인증 유형 구성 예
- 고정 ISR 컨피그레이션의 무선 인증 유형 예
- Cisco Access Router 무선 컨피그레이션 가이드
- 내부 DHCP 및 개방형 인증 컨피그레이션을 사용하는 1800 ISR 무선 라우터 예
- 무선 지원 페이지
- 기술 지원 및 문서 – Cisco Systems