Konfigurationsbeispiel für Wireless LAN-Verbindungen mit einem ISR mit WEP Encryption und LEAP Authentication

Inhalt

Einführung

In diesem Dokument wird erläutert, wie Sie einen Cisco Integrated Services Router (ISR) der Serie 870 für Wireless LAN-Verbindungen mit WEP-Verschlüsselung und LEAP-Authentifizierung konfigurieren.

Die gleiche Konfiguration gilt für alle anderen Modelle der Cisco ISR Wireless-Serie.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Grundkenntnisse der Konfiguration der Cisco ISR der Serie 870.
- Kenntnisse zum Konfigurieren des 802.11a/b/g Wireless Client-Adapters mithilfe des Aironet Desktop Utility (ADU).

Informationen zur Konfiguration des 802.11a/b/g Client-Adapters für den Cisco Aironet 802.11a/b/g Wireless LAN Client Adapter (CB21AG und PI21AG) finden Sie im Installations- und Konfigurationsleitfaden, Version 2.5.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

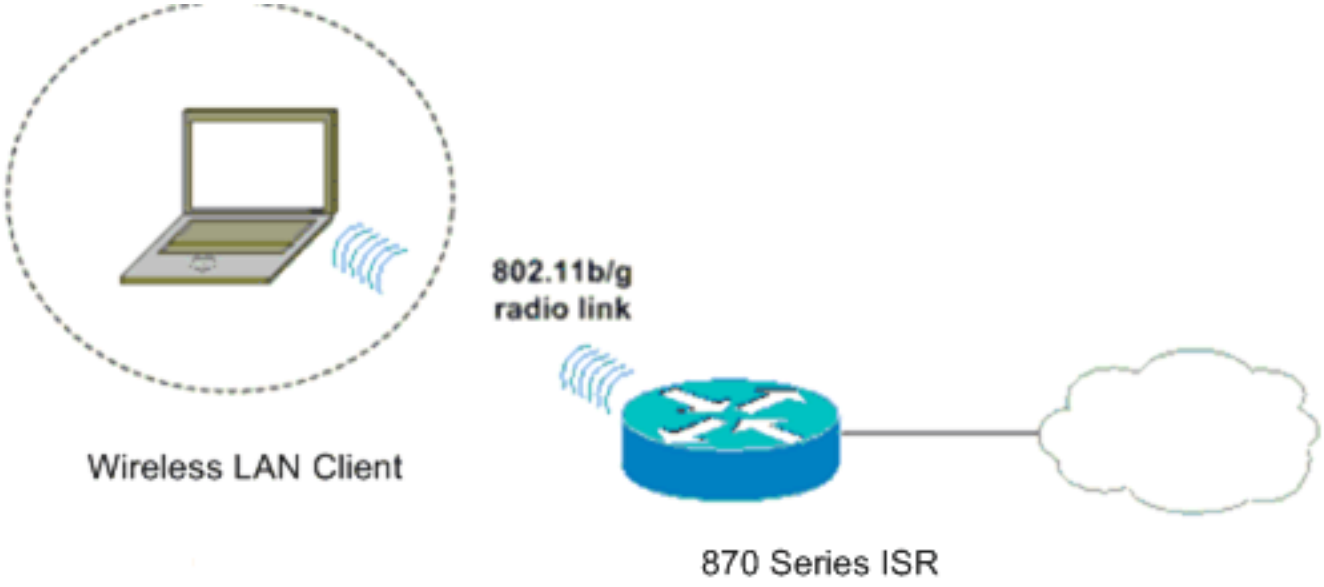
- Cisco 871W ISR mit Cisco IOS® Softwareversion 12.3(8)YI1
- Laptop mit Aironet Desktop Utility Version 2.5
- 802.11 a/b/g Client-Adapter mit Firmware-Version 2.5

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Netzwerkdiagramm

In diesem Dokument wird diese Netzwerkeinrichtung verwendet.

In dieser Konfiguration ordnet der Wireless LAN-Client dem 870-Router zu. Der interne Dynamic Host Configuration Protocol (DHCP)-Server auf dem 870-Router stellt den Wireless-Clients eine IP-Adresse zur Verfügung. Die WEP-Verschlüsselung ist auf dem 870 ISR und dem WLAN-Client aktiviert. Die LEAP-Authentifizierung dient zur Authentifizierung der Wireless-Benutzer, und die lokale RADIUS-Serverfunktion des 870-Routers dient zur Validierung der Anmeldeinformationen.



Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Router-Konfiguration 871W

Gehen Sie wie folgt vor, um den 871W ISR als Access Point zu konfigurieren, um

Assoziierungsanfragen von den Wireless-Clients zu akzeptieren.

1. Konfigurieren Sie Integrated Routing and Bridging (IRB), und richten Sie die Bridge-Gruppe ein.Geben Sie diese Befehle aus dem globalen Konfigurationsmodus ein, um IRB zu aktivieren.
```
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. Konfigurieren Sie die Bridged Virtual Interface (BVI).Weisen Sie der BVI eine IP-Adresse zu. Geben Sie diese Befehle im globalen Konfigurationsmodus ein.
```
WirelessRouter<config>#interface bvi1
!--- Enter interface configuration mode for the BVI. WirelessRouter<config-if>#ip address
172.16.1.100 255.255.0.0
```

   Weitere Informationen zur Funktionalität von Bridge-Gruppen in Access Points und Bridges finden Sie im Abschnitt Verwendung von VLANs mit Cisco Aironet Wireless Equipment unter Konfiguration der Bridge-Gruppe.
3. Konfigurieren Sie die interne DHCP-Serverfunktion des 871W ISR.Die interne DHCP-Serverfunktion des Routers kann verwendet werden, um Wireless-Clients, die dem Router zugeordnet sind, IP-Adressen zuzuweisen. Führen Sie diese Befehle im globalen Konfigurationsmodus aus.
```
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
```

   Hinweis: Der Client-Adapter sollte auch so konfiguriert sein, dass er IP-Adressen von einem DHCP-Server akzeptiert.
4. Konfigurieren Sie den 871W ISR als lokalen RADIUS-Server.Geben Sie im globalen Konfigurationsmodus diese Befehle ein, um den 871W ISR als lokalen RADIUS-Server zu konfigurieren.
```
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.
```
   Hinweis: Verwenden Sie die Ports 1812 und 1813 zur Authentifizierung und Abrechnung für den lokalen RADIUS-Server.
```
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. Konfigurieren Sie die Funkschnittstelle.Die Konfiguration der Funkschnittstelle umfasst die

Konfiguration verschiedener Wireless-Parameter auf dem Router, einschließlich SSID, Verschlüsselungsmodus, Authentifizierungstyp, Geschwindigkeit und Rolle des Wireless-Routers. In diesem Beispiel wird die SSID **Test** verwendet.Geben Sie diese Befehle ein, um die Funkschnittstelle im globalen Konfigurationsmodus zu konfigurieren.

```
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.
```

Der 870-Router akzeptiert Zuordnungsanfragen von den Wireless-Clients, sobald dieses Verfahren abgeschlossen ist.Wenn Sie den EAP-Authentifizierungstyp auf dem Router konfigurieren, wird empfohlen, sowohl **Network-EAP als auch Open mit EAP** als Authentifizierungstypen auszuwählen, um Authentifizierungsprobleme zu vermeiden.

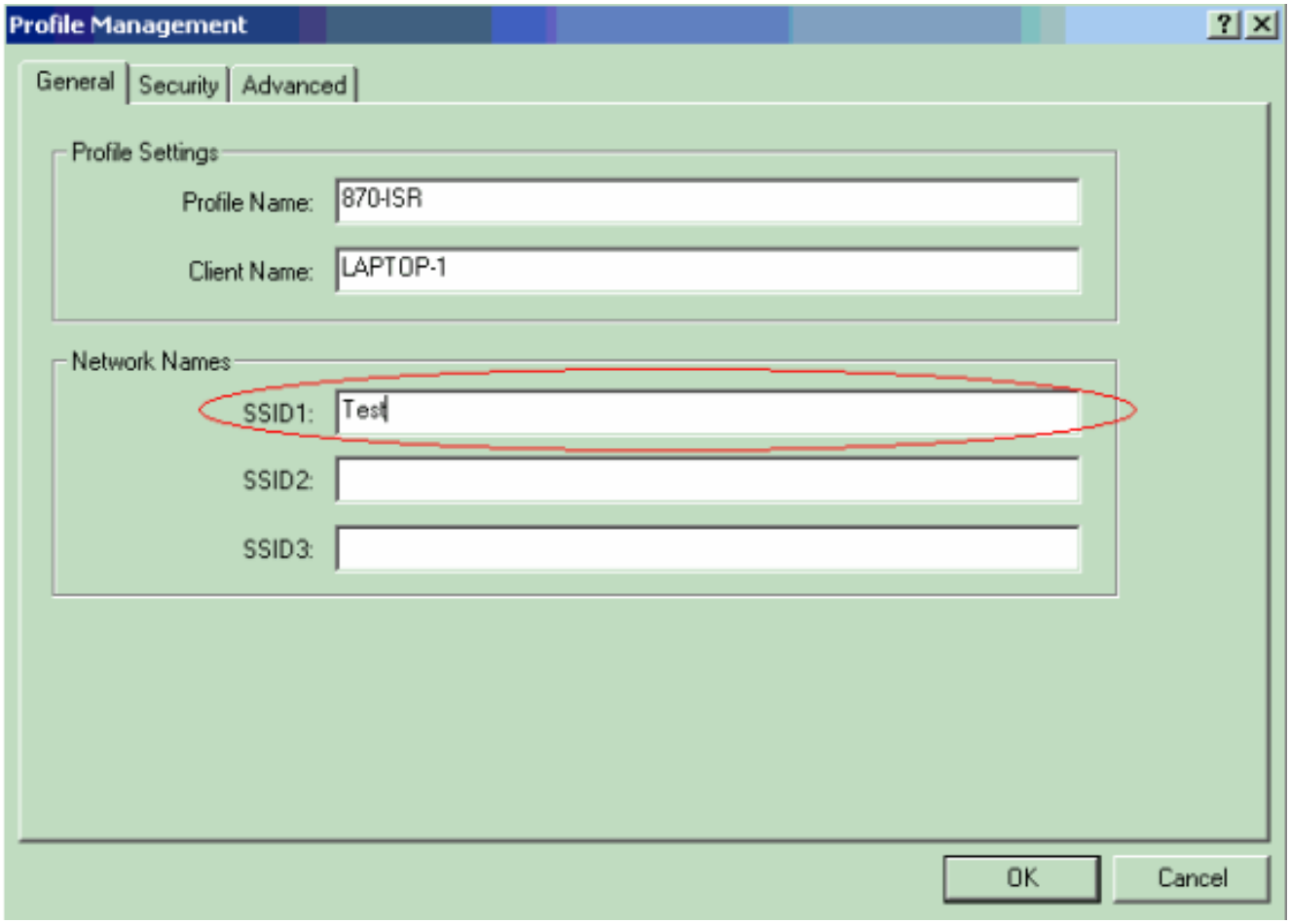
```
WirelessRouter<config-ssid>#authentication network-eap eap_methods
WirelessRouter<config-ssid>#authentication open eap eap_methods
```

Hinweis: In diesem Dokument wird davon ausgegangen, dass das Netzwerk nur über Cisco Wireless-Clients verfügt.**Hinweis:** Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

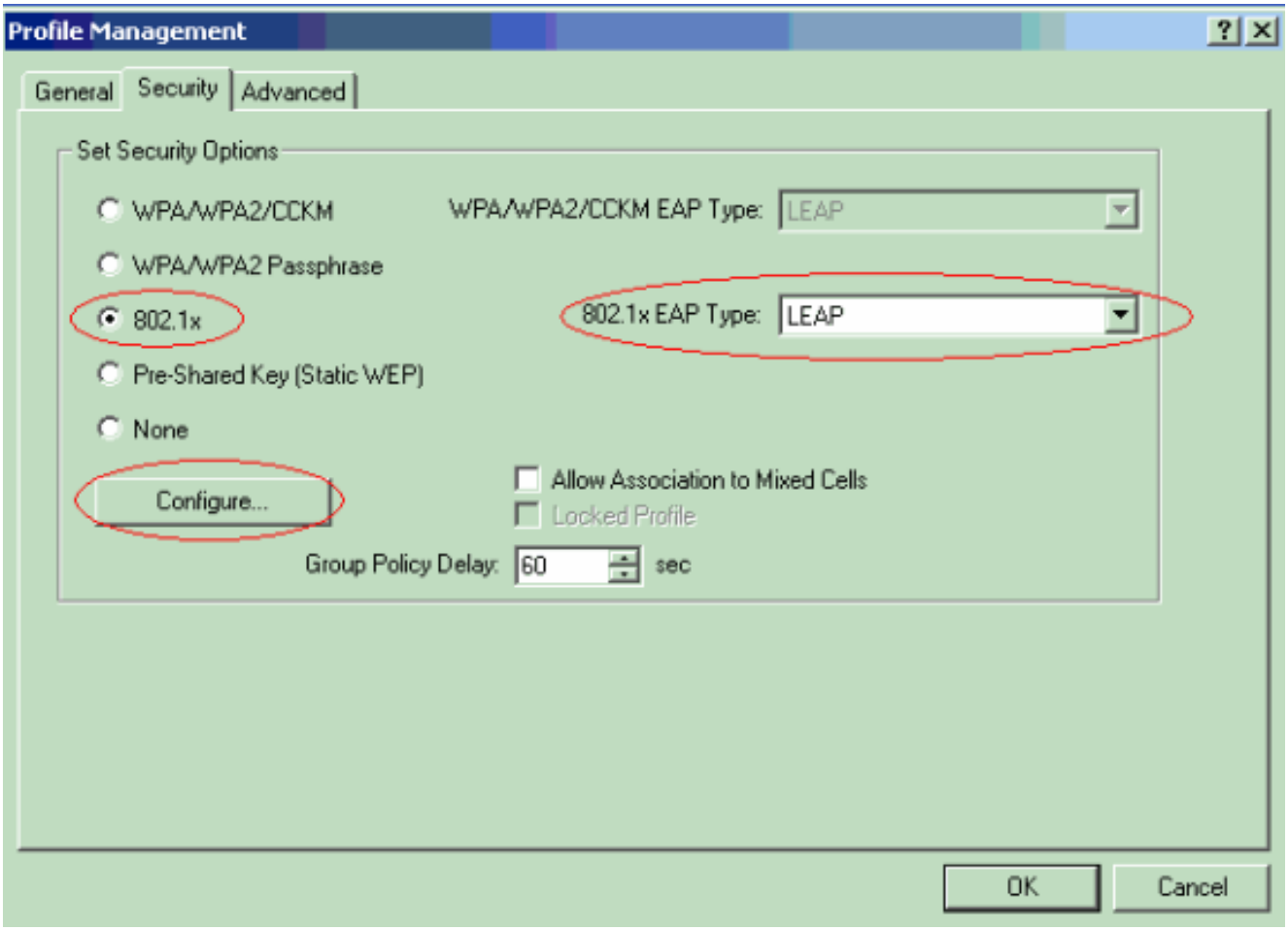
Konfiguration des Client-Adapters

Führen Sie diese Schritte aus, um den Client-Adapter zu konfigurieren. Bei diesem Verfahren wird auf der ADU ein neues Profil mit dem Namen **870-ISR** erstellt. Bei diesem Verfahren wird auch Test als SSID verwendet, und die LEAP-Authentifizierung auf dem Client-Adapter wird aktiviert.

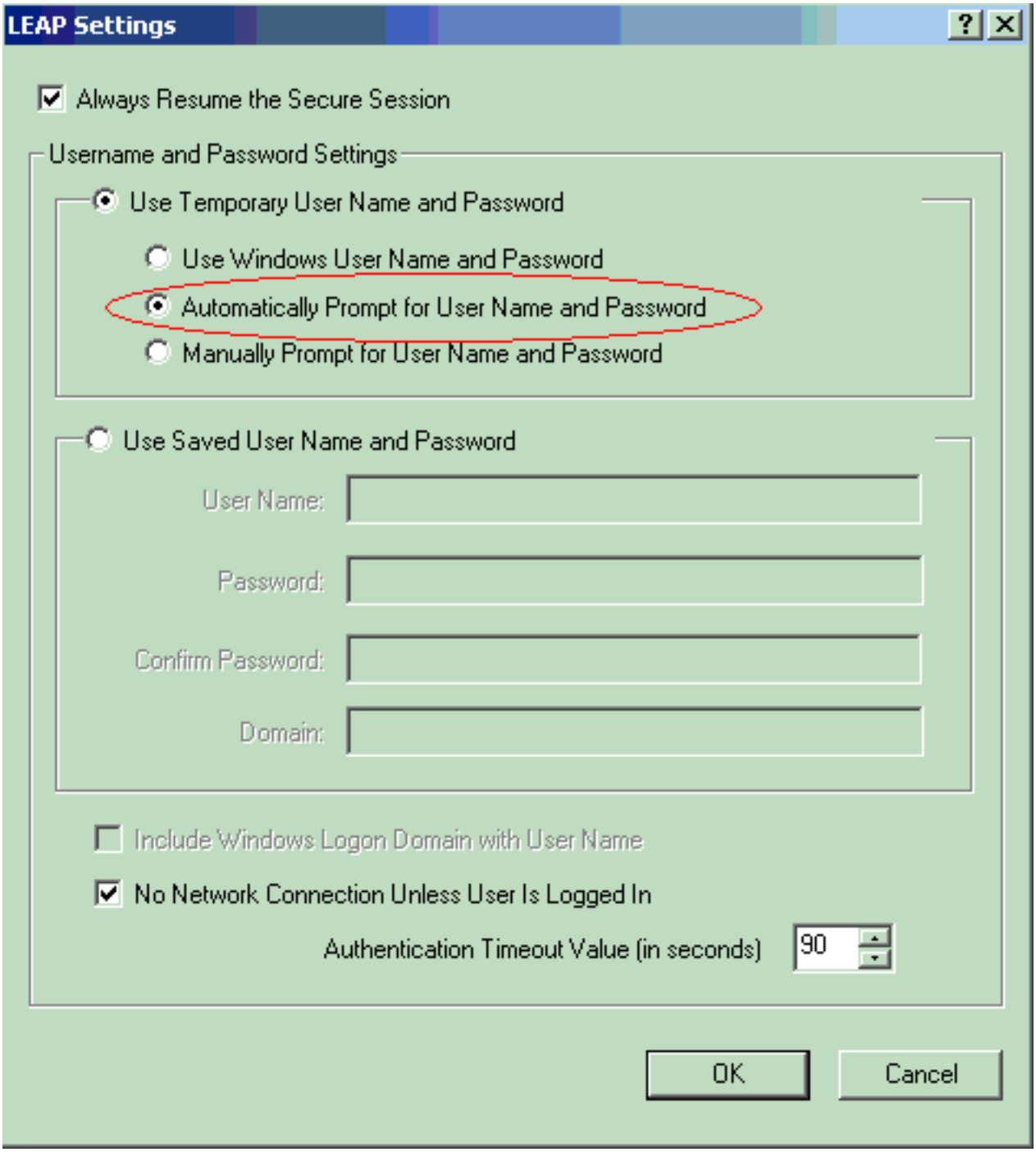
1. Klicken Sie auf **Neu**, um ein neues Profil im Fenster Profilverwaltung auf der ADU zu erstellen. Geben Sie auf der Registerkarte Allgemein den Profilnamen und die SSID ein, die der Client-Adapter verwendet.In diesem Beispiel lautet der Profilname **870-ISR** und die SSID **Test**.**Hinweis:** Die SSID muss genau mit der SSID übereinstimmen, die Sie auf dem 871W ISR konfiguriert haben. Bei der SSID wird Groß- und Kleinschreibung unterschieden.



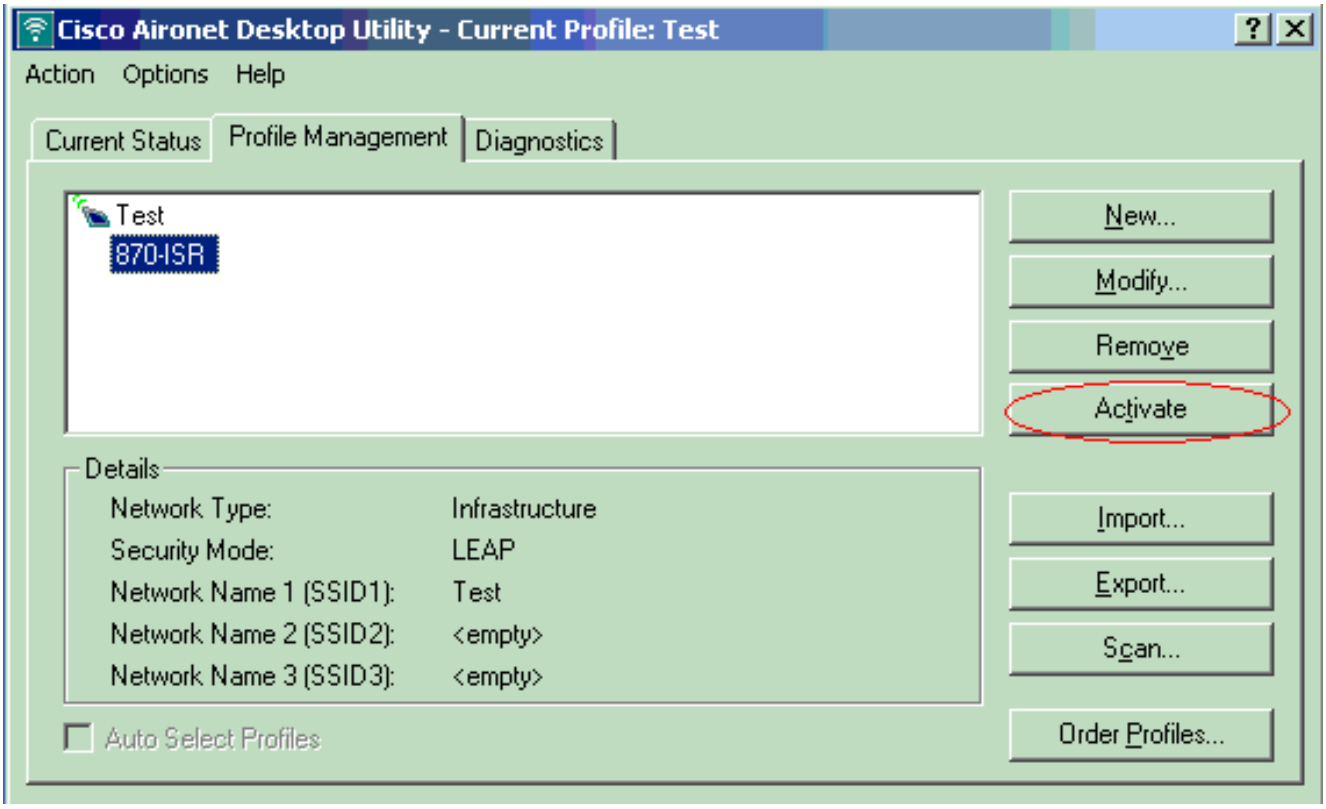
2. Öffnen Sie die Registerkarte Sicherheit, wählen Sie **802.1x aus**, und wählen Sie **LEAP** aus dem 802.1x EAP Type-Menü aus.Diese Aktion aktiviert die LEAP-Authentifizierung auf dem Client-
Adapter.



3. Klicken Sie auf **Konfigurieren**, um LEAP-Einstellungen zu definieren.Bei dieser Konfiguration wird die Option **Benutzername und Kennwort automatisch auffordern ausgewählt**. Mit dieser Option können Sie den Benutzernamen und das Kennwort manuell eingeben, wenn die LEAP-Authentifizierung
erfolgt.



4. Klicken Sie auf **OK**, um das Fenster Profilverwaltung zu schließen.
5. Klicken Sie auf **Aktivieren**, um dieses Profil auf dem Client-Adapter zu aktivieren.

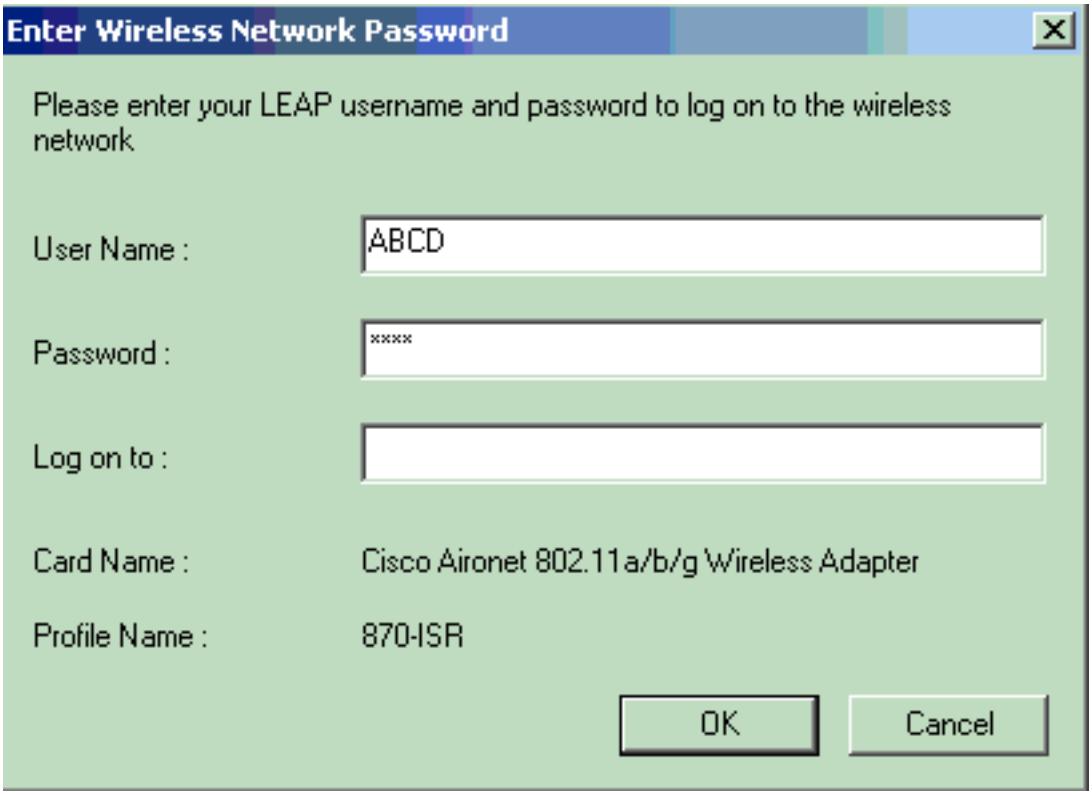


Überprüfen

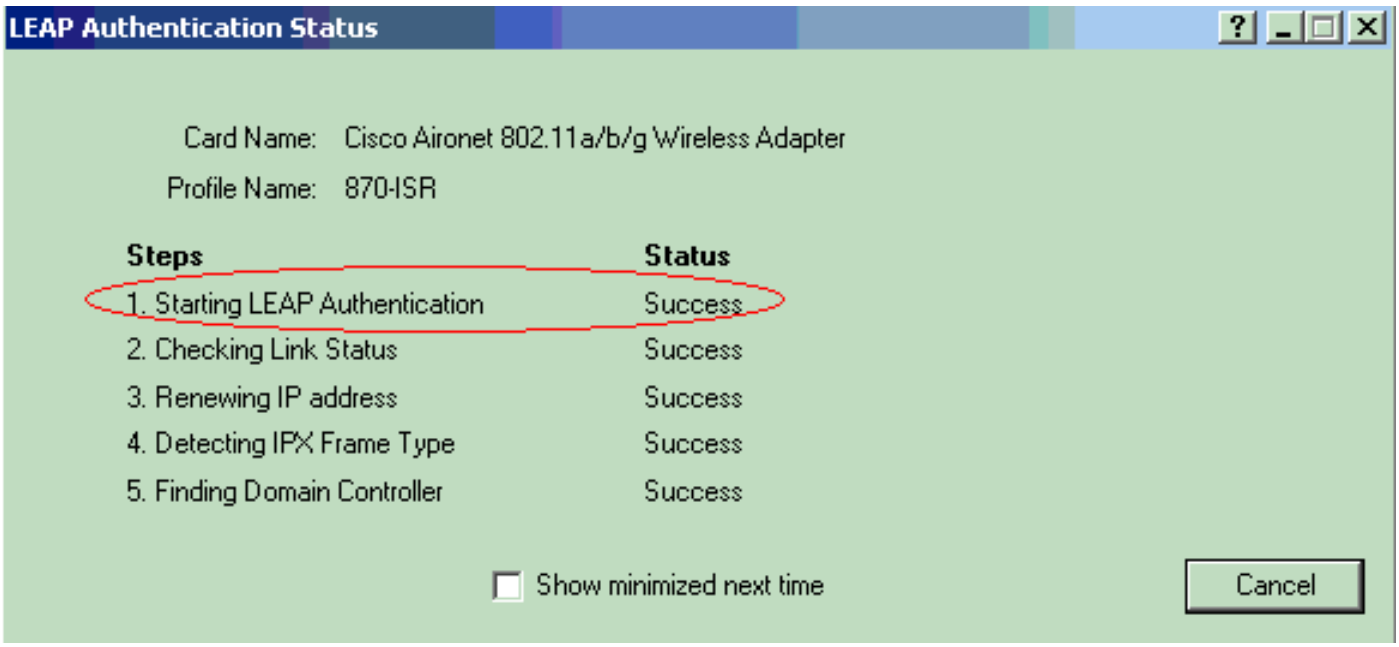
In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Sobald der Client-Adapter und der 870-Router konfiguriert sind, aktivieren Sie das Profil 870-ISR auf dem Client-Adapter, um die Konfiguration zu überprüfen.

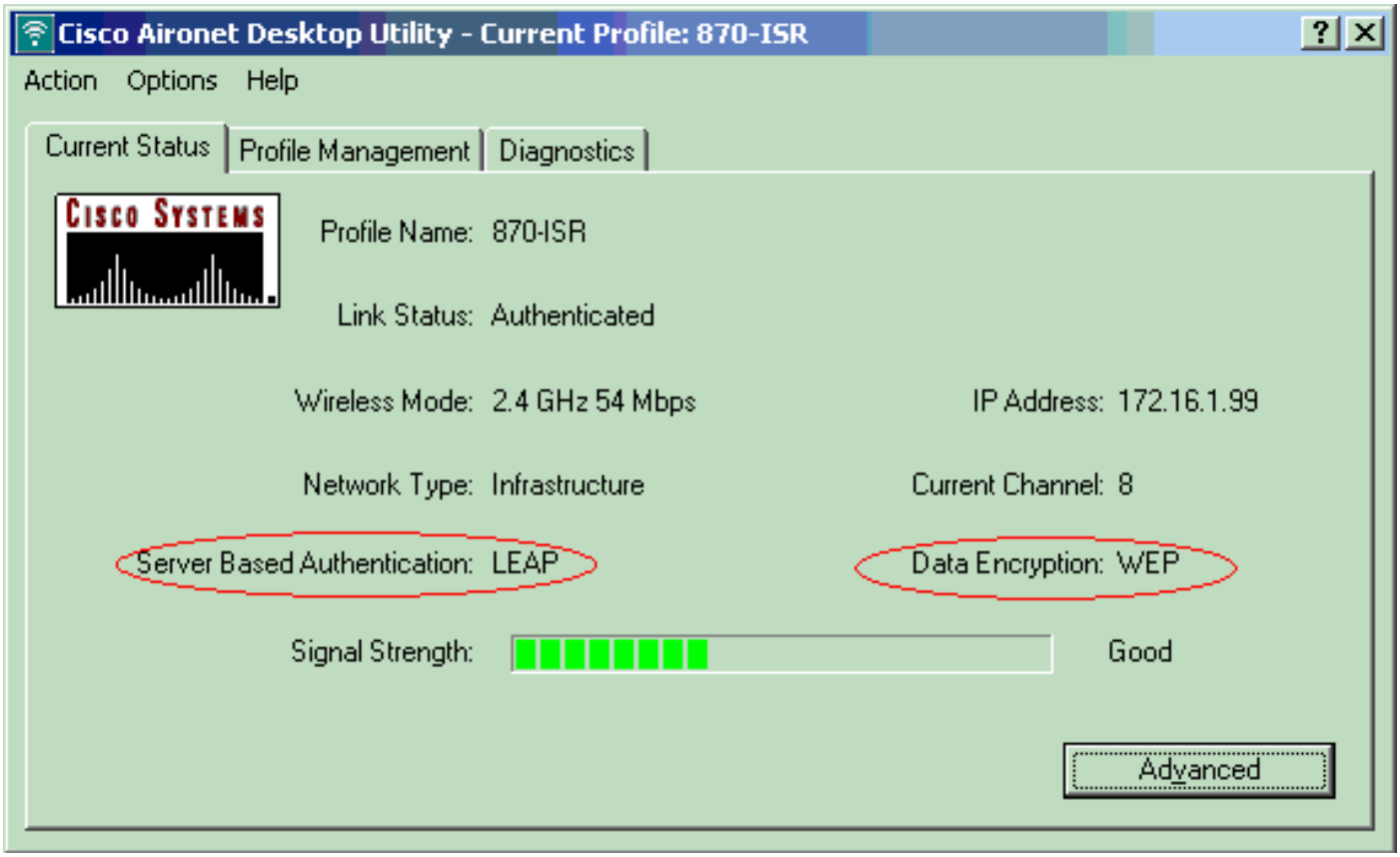
Geben Sie den Benutzernamen und das Kennwort ein, wenn das Fenster Wireless Network Password (Wireless-Netzwerkkennwort eingeben) angezeigt wird. Diese müssen den im 871W ISR konfigurierten entsprechen. Eines der Profile in diesem Beispiel ist User Name **ABCD** and Password **ABCD**.



Das Fenster LEAP Authentication Status (LEAP-Authentifizierungsstatus) wird angezeigt. In diesem Fenster werden die Benutzeranmeldeinformationen für den lokalen RADIUS-Server überprüft.



Überprüfen Sie den aktuellen ADU-Status, um zu überprüfen, ob der Client WEP-Verschlüsselung und LEAP-Authentifizierung verwendet.



Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show dot1 Association** - Überprüft die Konfiguration auf dem 870-Router.

```
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**: Vergewissert sich, dass der Client über den DHCP-Server über eine IP-Adresse verfügt.

```
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
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung, die für diese Konfiguration relevant sind.

1. Legen Sie die Methode auf der SSID auf **Öffnen** fest, um die Authentifizierung vorübergehend zu deaktivieren.Dadurch können Funkfrequenzprobleme vermieden und eine erfolgreiche Authentifizierung verhindert werden.Verwenden Sie die Befehle **no**

authentication open eap eap_methods, **no authentication network-eap eap_methods** und **authentication open** aus der CLI.Wenn der Client erfolgreich eine Verbindung herstellt, trägt RF nicht zum Zuordnungsproblem bei

2. Überprüfen Sie, ob die auf dem Wireless-Router konfigurierten WEP-Schlüssel mit den auf den Clients konfigurierten WEP-Schlüsseln übereinstimmen.Wenn die WEP-Schlüssel nicht übereinstimmen, können die Clients nicht mit dem Wireless-Router kommunizieren.
3. Überprüfen Sie, ob die gemeinsamen geheimen Kennwörter zwischen dem Wireless-Router und dem Authentifizierungsserver synchronisiert werden.

Sie können diese Debugbefehle auch verwenden, um Konfigurationsfehler zu beheben.

- **debug dot11 aaa authentication all**: Aktiviert das Debuggen von MAC- und EAP-Authentifizierungspaketen.
- **debug radius authentication**: Zeigt die RADIUS-Verhandlungen zwischen Server und Client an.
- **debug radius local-server pakets**: Zeigt den Inhalt der gesendeten und empfangenen RADIUS-Pakete an.
- **debug radius local-server client**: Zeigt Fehlermeldungen über fehlgeschlagene Client-Authentifizierungen an.

Zugehörige Informationen

- Verschlüsselungsalgorithmen und Authentifizierungstypen
- Konfigurationsbeispiel für Wireless-Authentifizierungstypen auf festem ISR über SDM
- Beispiele für Wireless-Authentifizierungstypen in einem festkonfigurierten ISR
- Konfigurationsleitfaden für Cisco Access Router Wireless
- Konfigurationsbeispiel für 1800 ISR Wireless-Router mit internem DHCP und offener Authentifizierung
- Wireless-Support-Seite
- Technischer Support und Dokumentation - Cisco Systems