Ejemplo de configuración de conectividad de LAN inalámbrica mediante un ISR con encriptación WEP y autenticación LEAP

Contenido

Introducción

Este documento explica cómo configurar un Cisco 870 Series Integrated Services Router (ISR) para conectividad de LAN Inalámbrica con cifrado WEP y autenticación LEAP.

La misma configuración se aplica a cualquier otro modelo Cisco ISR Wireless Series.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento sobre cómo configurar los parámetros básicos de Cisco ISR serie 870.
- Conocimiento de cómo configurar el adaptador de cliente inalámbrico 802.11a/b/g mediante la utilidad de escritorio Aironet (ADU).

Consulte Guía de Instalación y Configuración de Cisco Aironet 802.11a/b/g Wireless LAN Client Adapters (CB21AG y PI21AG), Release 2.5 para obtener información sobre cómo configurar el 802.11a/b/g Client Adapter.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

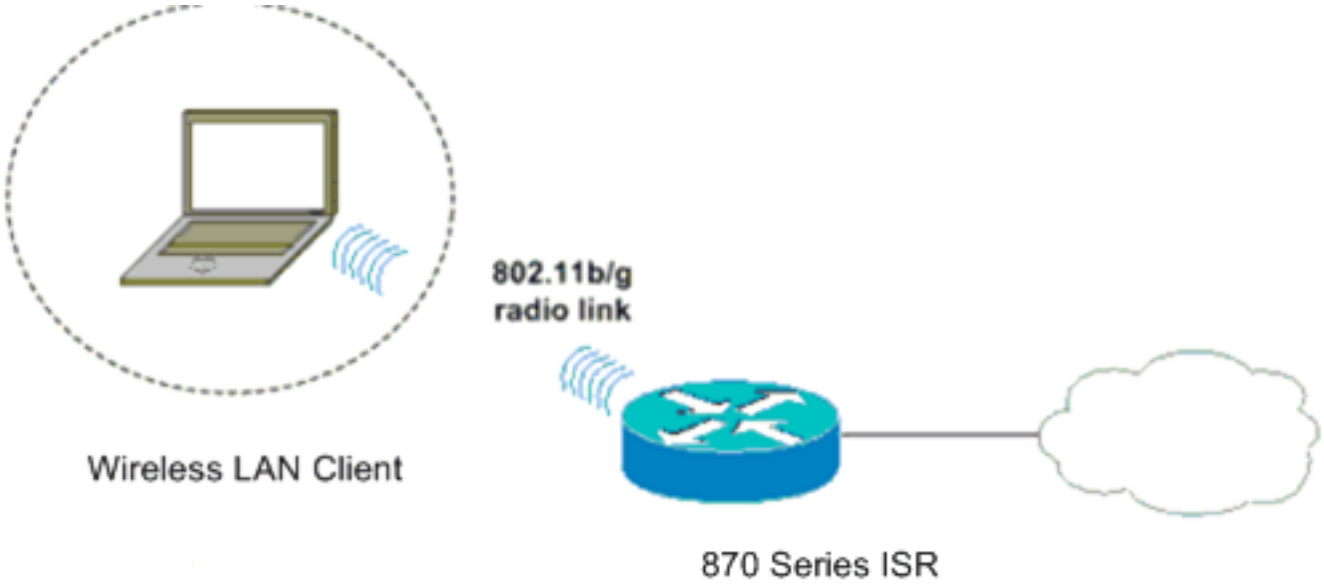
- Cisco ISR 871W que ejecuta Cisco IOS® Software Release 12.3(8)YI1
- Notebook con Aironet Desktop Utility versión 2.5
- Adaptador de cliente 802.11 a/b/g que ejecuta firmware versión 2.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Diagrama de la red

Este documento utiliza esta configuración de red:

En esta configuración, el cliente de LAN inalámbrica se asocia al router 870. El servidor interno del protocolo de configuración dinámica de host (DHCP) del router 870 se utiliza para proporcionar una dirección IP a los clientes inalámbricos. La encriptación WEP está habilitada en el ISR 870 y en el cliente WLAN. La autenticación LEAP se utiliza para autenticar a los usuarios inalámbricos y la función de servidor RADIUS local en el router 870 se utiliza para validar las credenciales.



Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Configuración del router 871W

Complete estos pasos para configurar el ISR 871W como punto de acceso para aceptar solicitudes de asociación de los clientes inalámbricos.

1. Configure el routing y el puente integrados (IRB) y configure el grupo de bridges.Escriba estos comandos desde el modo de configuración global para habilitar IRB.

```
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. Configure la interfaz virtual puenteada (BVI).Asigne una dirección IP a la BVI. Escriba estos comandos desde el modo de configuración global.

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

   Refiérase a la sección *Configuración de Bridge Group en Puntos de Acceso y Puentes de Uso de VLAN con Equipo Inalámbrico Cisco Aironet* para obtener más información sobre la funcionalidad de los Grupos de Bridge en los puntos de acceso.
3. Configure la función de servidor DHCP interno en el ISR 871W.La función de servidor DHCP interno del router se puede utilizar para asignar direcciones IP a clientes inalámbricos que se asocian al router. Complete estos comandos en el modo de configuración global.

```
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
```

   Nota: El adaptador del cliente también debe configurarse para aceptar direcciones IP de un servidor DHCP.
4. Configure el ISR 871W como un servidor RADIUS local.En el modo de configuración global, escriba estos comandos para configurar el ISR 871W como un servidor RADIUS local.

```
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.
```

   Nota: Utilice los puertos 1812 y 1813 para la autenticación y la contabilización del servidor RADIUS local.

```
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. Configure la interfaz de radio.La configuración de la interfaz de radio implica la configuración de varios parámetros inalámbricos en el router, incluidos el SSID, el modo de cifrado, el tipo de autenticación, la velocidad y la función del router inalámbrico. Este ejemplo utiliza el SSID llamado **Test**.Escriba estos comandos para configurar la interfaz de radio en el modo de configuración global.

```
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.
```

El router 870 acepta solicitudes de asociación de los clientes inalámbricos una vez que se realiza este procedimiento.Cuando configura el tipo de autenticación EAP en el router, se recomienda elegir **Red-EAP y Abierto con EAP** como tipos de autenticación para evitar cualquier problema de autenticación.

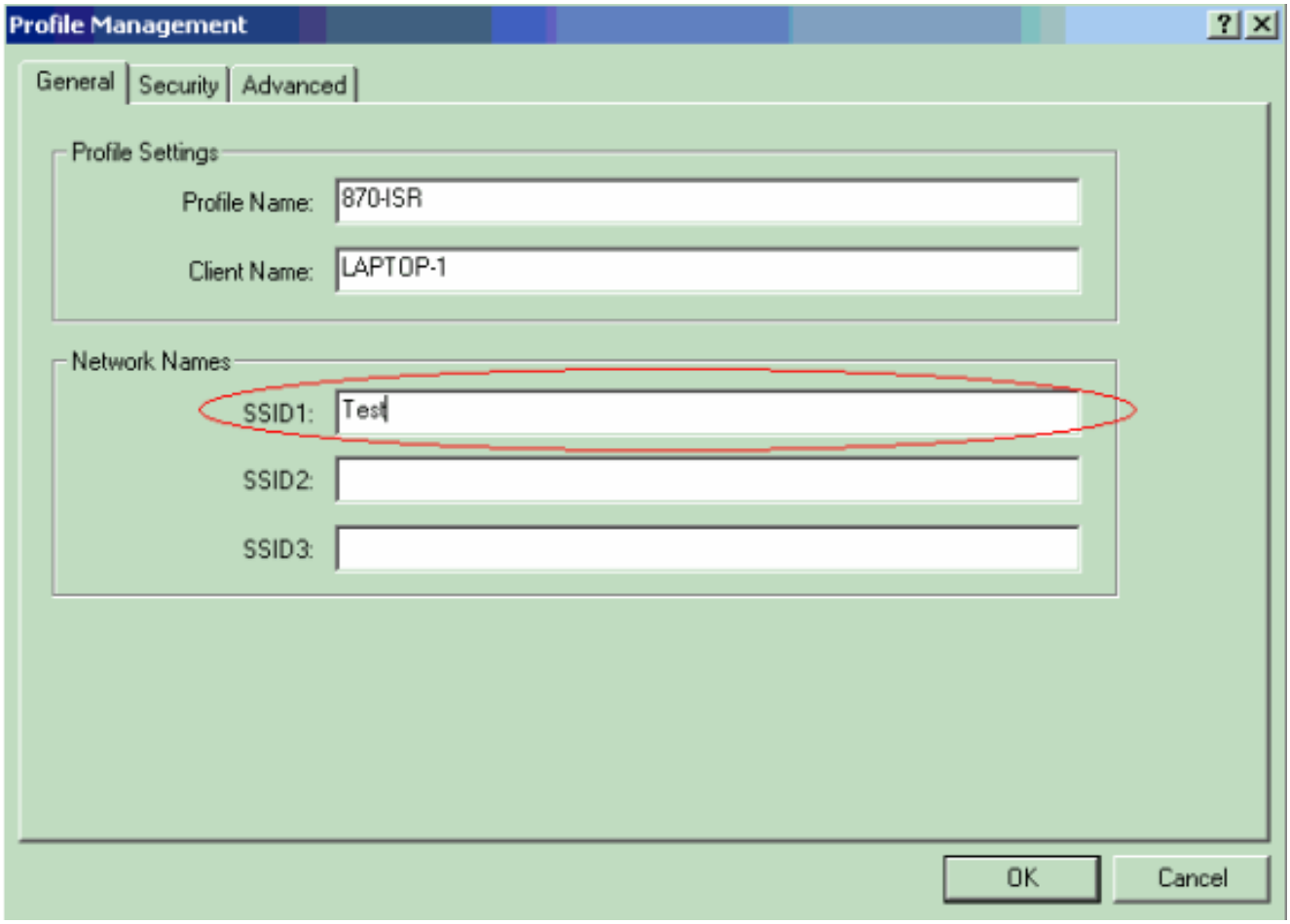
```
WirelessRouter<config-ssid>#authentication network-eap eap_methods
WirelessRouter<config-ssid>#authentication open eap eap_methods
```

Nota: Este documento asume que la red tiene solamente clientes Cisco Wireless.**Nota:** Use la Command Lookup Tool (sólo clientes registrados) para obtener más información sobre los comandos utilizados en este documento.

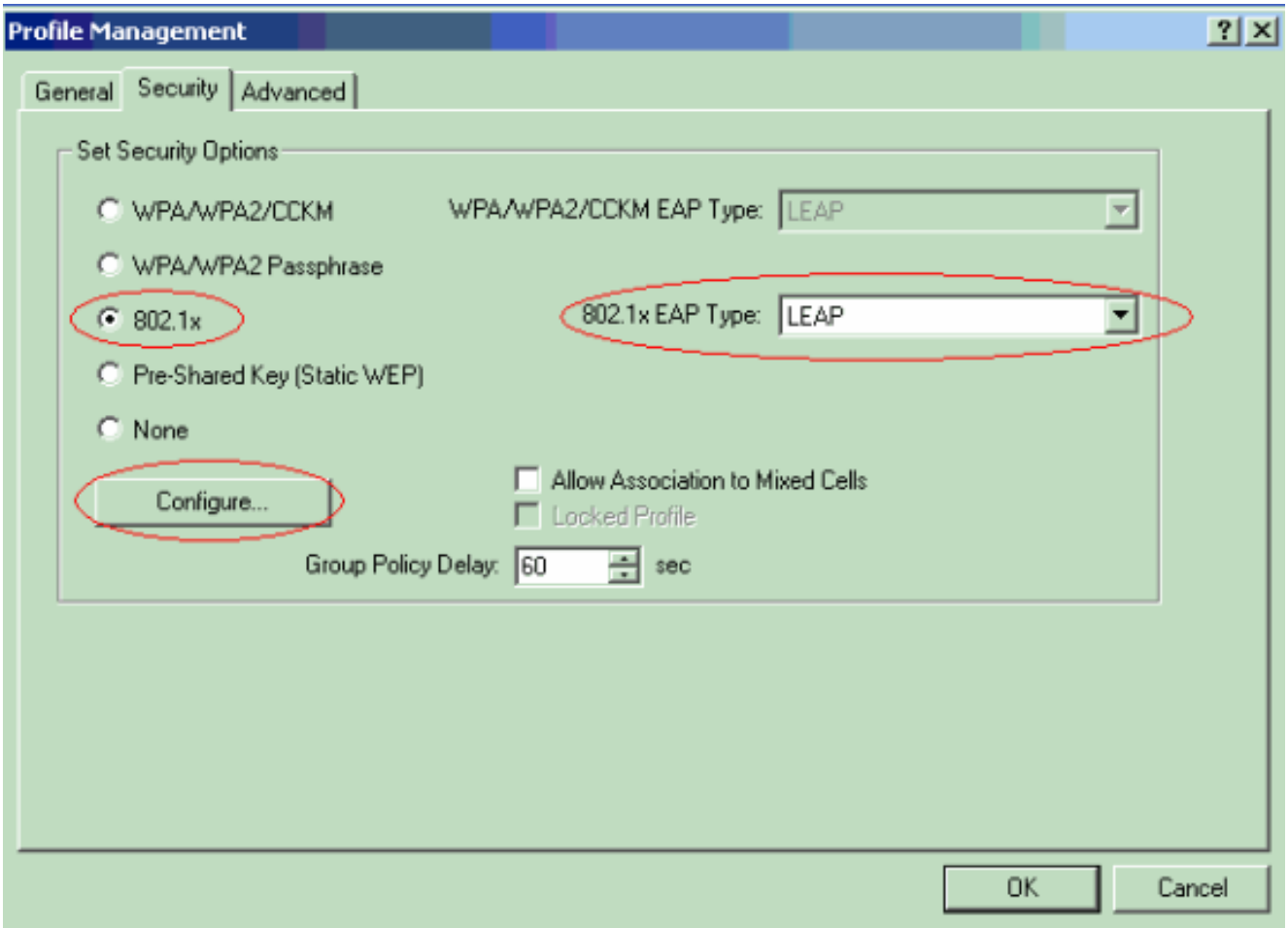
Configuración del adaptador del cliente

Complete estos pasos para configurar el adaptador del cliente. Este procedimiento crea un nuevo perfil llamado **870-ISR** en la ADU, como ejemplo. Este procedimiento también utiliza Test como SSID y habilita la autenticación LEAP en el adaptador del cliente.

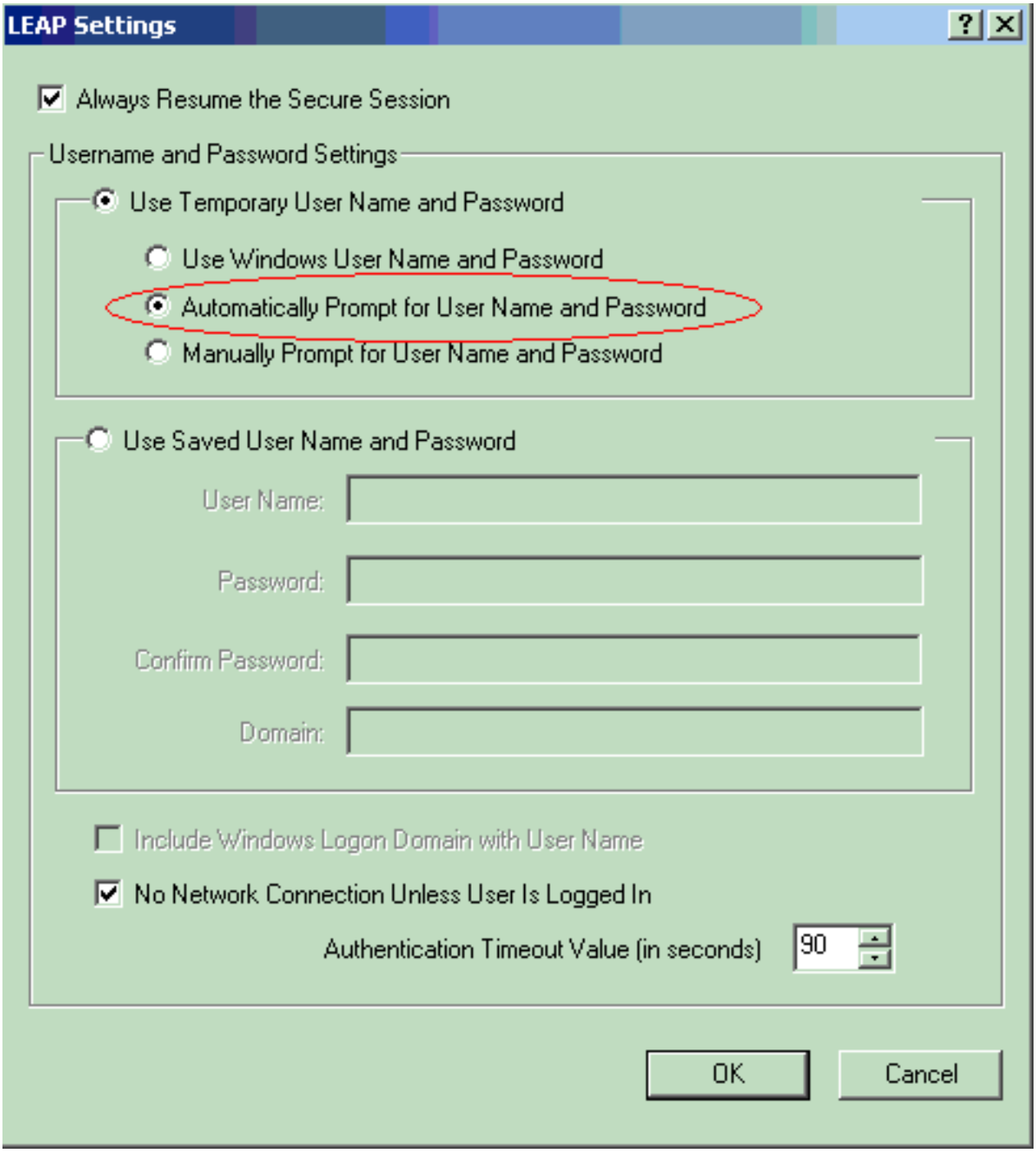
1. Haga clic en **Nuevo** para crear un nuevo perfil en la ventana Administración de perfiles en la ADU. Introduzca el nombre del perfil y el SSID que utiliza el adaptador del cliente en la ficha General.En este ejemplo, el nombre del perfil es **870-ISR** y el SSID es **Test**.**Nota:** El SSID debe coincidir exactamente con el SSID que configuró en el ISR 871W. SSID distingue entre mayúsculas y
minúsculas.



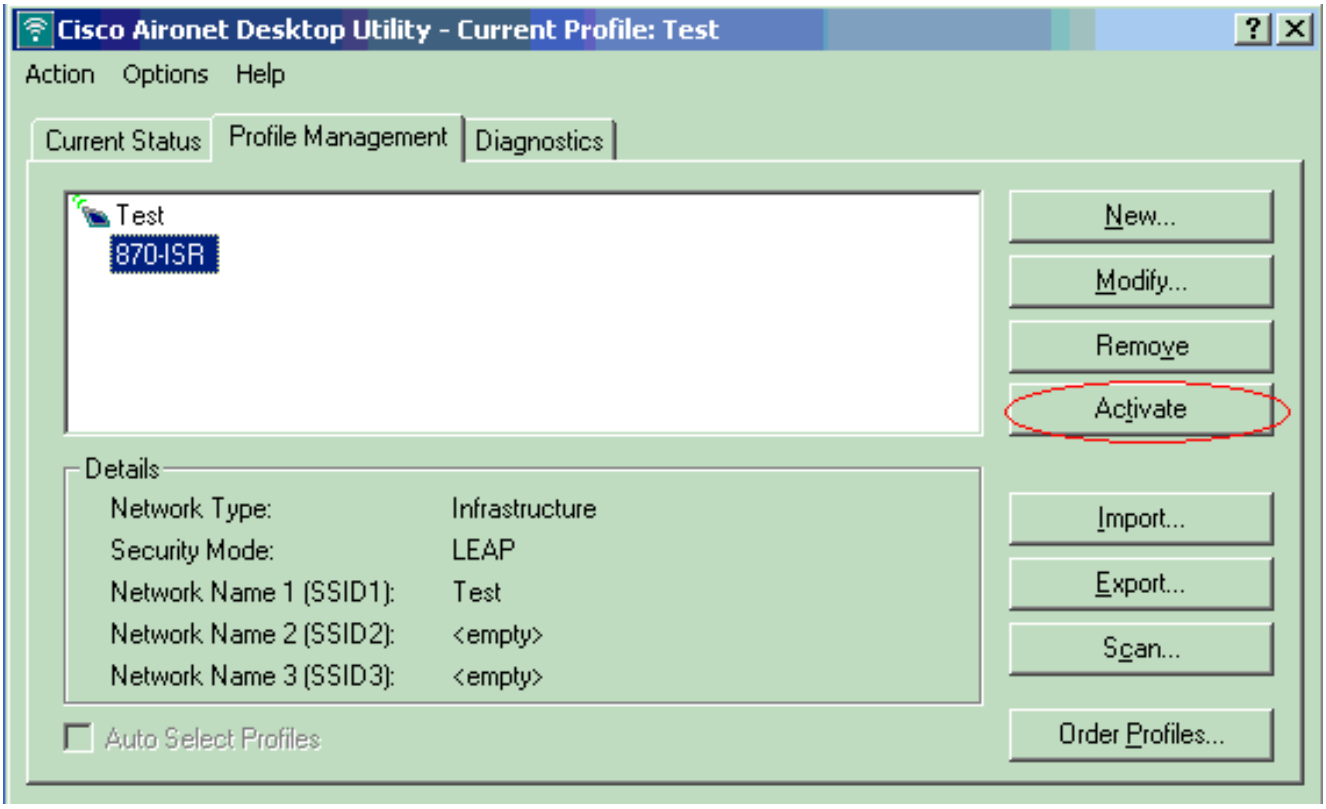
2. Vaya a la ficha Security , seleccione **802.1x** y elija **LEAP** en el menú 802.1x EAP Type .Esta acción habilita la autenticación LEAP en el adaptador del cliente.



3. Haga clic en **Configurar** para definir la configuración de LEAP.Esta configuración elige la opción **Solicitar automáticamente nombre de usuario y contraseña**. Esta opción permite introducir manualmente el nombre de usuario y la contraseña cuando se realiza la autenticación
LEAP.



4. Haga clic en **Aceptar** para salir de la ventana Administración de perfiles.
5. Haga clic en **Activar** para habilitar este perfil en el adaptador del cliente.

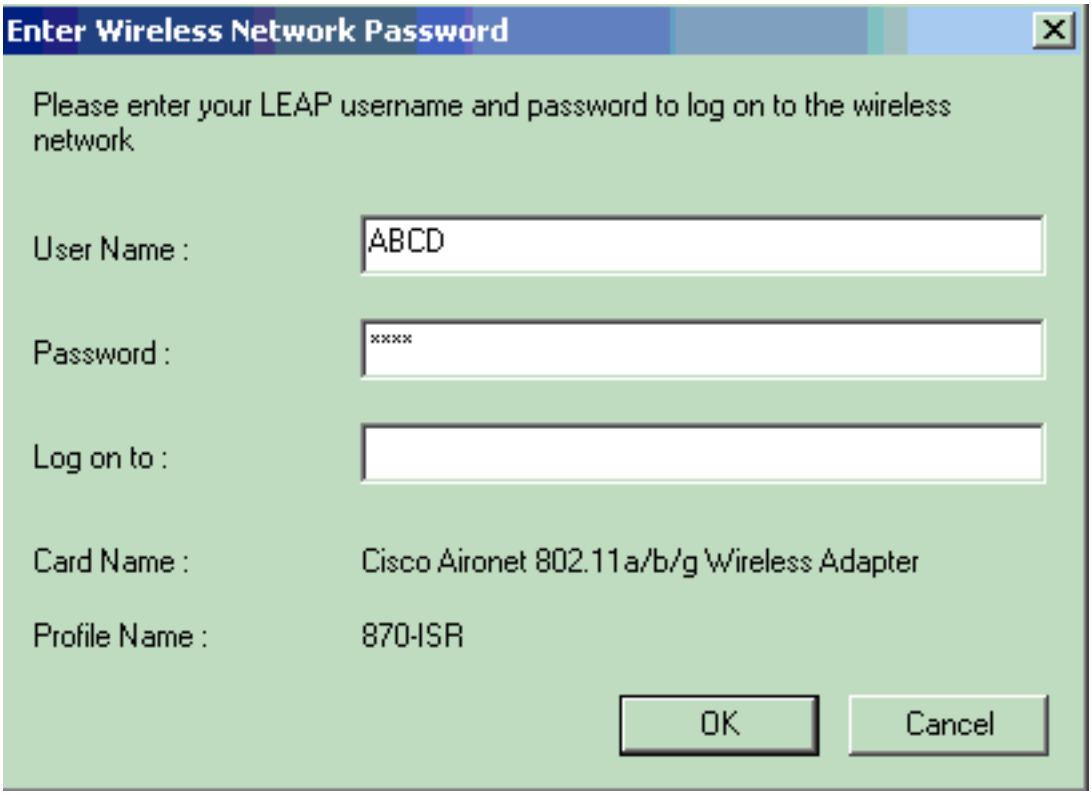


Verificación

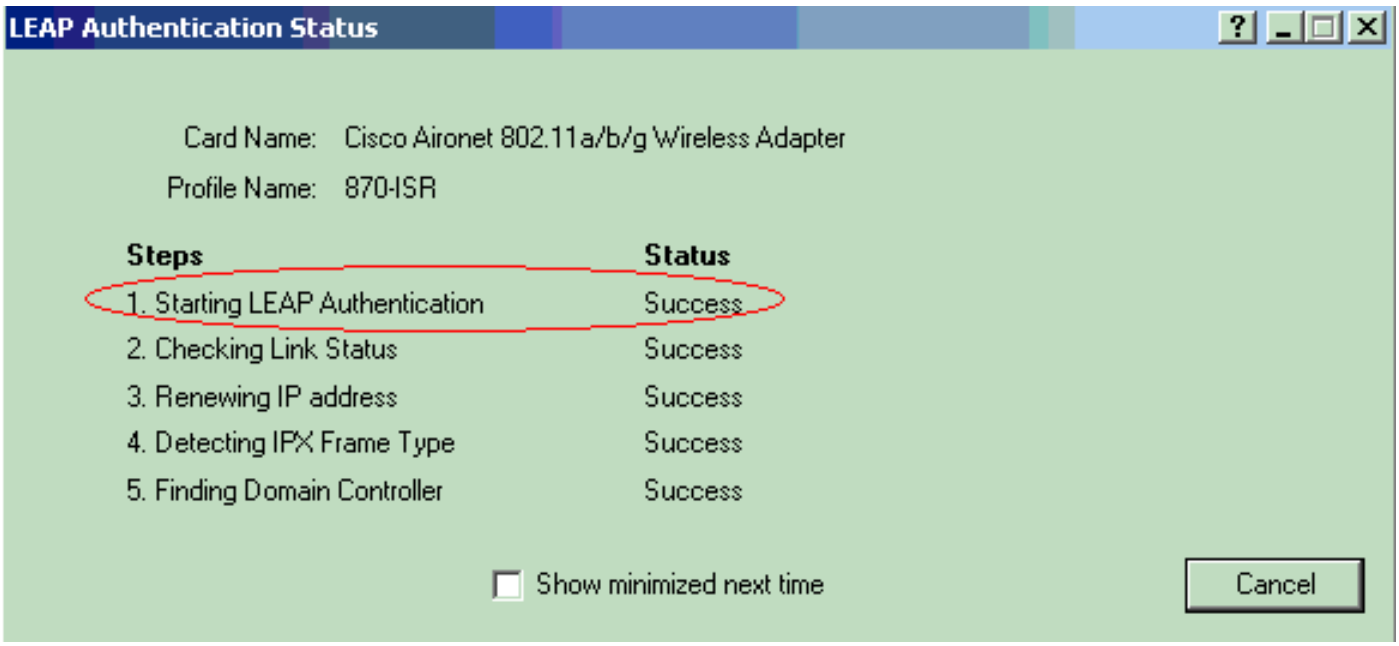
Use esta sección para confirmar que su configuración funciona correctamente.

Una vez configurado el adaptador del cliente y el router 870, active el perfil 870-ISR en el adaptador del cliente para verificar la configuración.

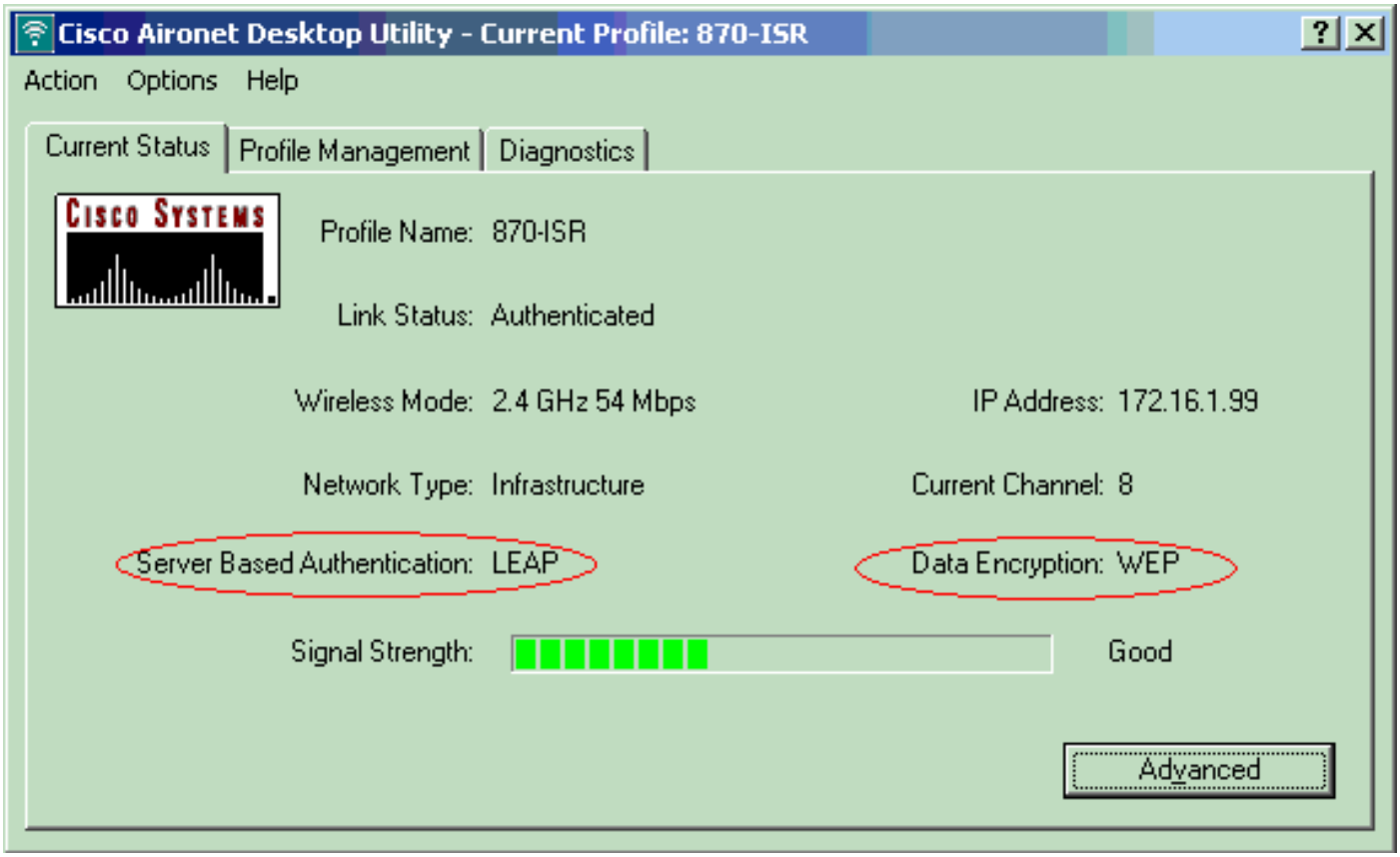
Introduzca el nombre de usuario y la contraseña cuando aparezca la ventana Introducir contraseña de red inalámbrica. Estos deben corresponder a los configurados en el ISR 871W. Uno de los perfiles utilizados en este ejemplo es User Name **ABCD** y Password **ABCD**.



Aparece la ventana LEAP Authentication Status . Esta ventana verifica las credenciales del usuario con el servidor RADIUS local.



Verifique el estado actual de ADU para verificar que el cliente utiliza la encriptación WEP y la autenticación LEAP.



La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **show dot11 association**: verifica la configuración en el router 870.

```
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**: verifica que el cliente tenga una dirección IP a través del servidor DHCP.

```
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
```

Troubleshoot

Esta sección proporciona información de troubleshooting relevante para esta configuración.

1. Establezca el método en SSID en **Open** para inhabilitar temporalmente la autenticación.Esto elimina la posibilidad de problemas de radiofrecuencia (RF) que impiden una autenticación correcta.Utilice los comandos **no authentication open eap_method**, **no authentication network-eap eap_method** y **authentication open** de la CLI.Si el cliente se asocia

correctamente, RF no contribuye al problema de asociación
2. Compruebe si las claves WEP configuradas en el router inalámbrico coinciden con las claves WEP configuradas en los clientes.Si hay una discordancia en las claves WEP, los clientes no pueden comunicarse con el router inalámbrico.
3. Verifique que las contraseñas secretas compartidas estén sincronizadas entre el router inalámbrico y el servidor de autenticación.

También puede utilizar estos comandos debug para resolver problemas de su configuración.

- **debug dot11 aaa authenticator all: Activa la depuración de los paquetes de autenticación MAC y EAP.**
- **debug radius authentication**: Muestra las negociaciones de RADIUS entre el servidor y el cliente.
- **debug radius local-server packets**: Muestra el contenido de los paquetes RADIUS que se envían y se reciben.
- **debug radius local-server client**: Muestra los mensajes de error de las autenticaciones fallidas del cliente.

Información Relacionada

- Algoritmos de cifrado y tipos de autenticación
- Ejemplo de Configuración de Tipos de Autenticación Inalámbrica en ISR Fijo a través de SDM
- Ejemplo de Configuración de Tipos de Autenticación Inalámbrica en un ISR Fijo
- Guía de configuración inalámbrica del router de acceso de Cisco
- Ejemplo de configuración de router inalámbrico ISR 1800 con DHCP interno y autenticación abierta
- Página de Soporte de Red Inalámbrica
- Soporte Técnico y Documentación - Cisco Systems