Conectividad del Wireless LAN usando un ISR con el ejemplo de configuración de la encripción WEP y de la 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 de la serie de la Tecnología inalámbrica de Cisco ISR.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de cómo configurar los parámetros básicos de las Cisco 870 Series ISR.
- Conocimiento de cómo configurar el adaptador de red inalámbrica de cliente 802.11a/b/g usando utilidad Aironet Desktop (ADU).

Refiera a la guía de instalación y configuración de los adaptadores del cliente del Wireless LAN del Cisco Aironet 802.11a/b/g (CB21AG y PI21AG), libere 2.5 para la información sobre cómo configurar el adaptador del cliente 802.11a/b/g.

Componentes Utilizados

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

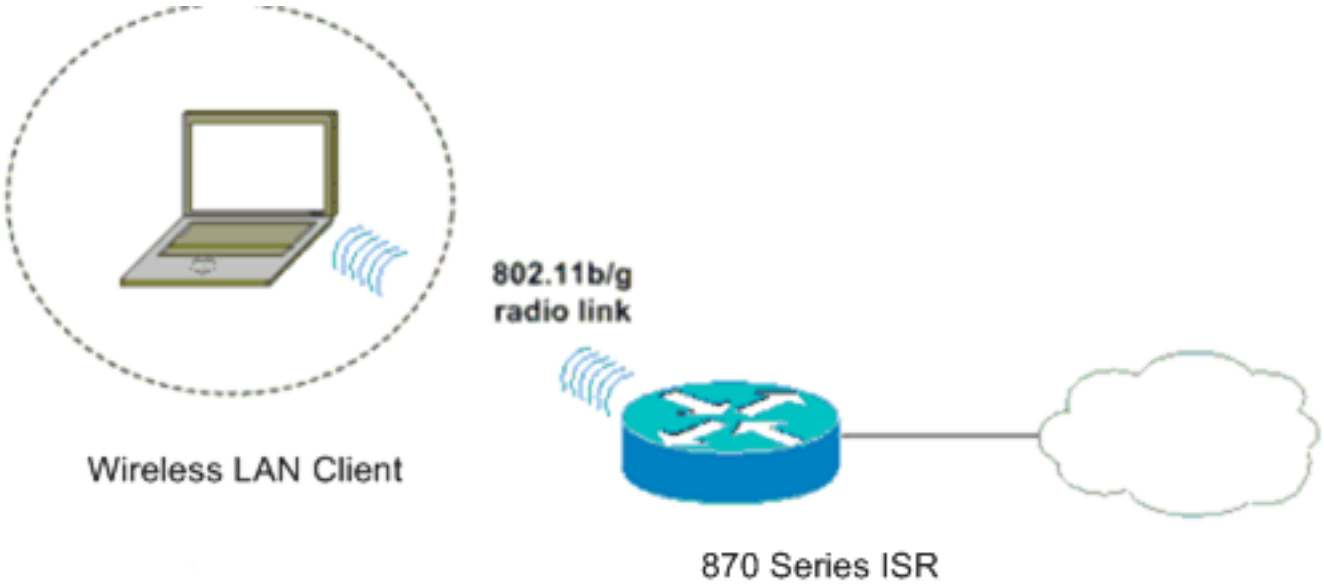
- Cisco 871W ISR que funciona con el Software Release 12.3(8)YI1 de Cisco IOS®
- Laptop con utilidad Aironet Desktop la versión 2.5
- adaptador del cliente del a/b/g del 802.11 que funciona con la versión de firmware 2.5

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Diagrama de la red

Este documento utiliza esta configuración de red:

En esta configuración, el cliente del Wireless LAN se asocia al 870 Router. El servidor interno del Protocolo de configuración dinámica de host (DHCP) en el 870 Router se utiliza para proporcionar una dirección IP a los clientes de red inalámbrica. La encripción WEP se habilita en los 870 ISR y el cliente WLAN. La autenticación LEAP se utiliza para autenticar a los usuarios de red inalámbrica y la característica local del servidor de RADIUS en el 870 Router se utiliza para validar las credenciales.



Convenciones

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

Configuración del 871W Router

Complete estos pasos para configurar el 871W ISR como Punto de acceso para validar las peticiones de la asociación de los clientes de red inalámbrica.

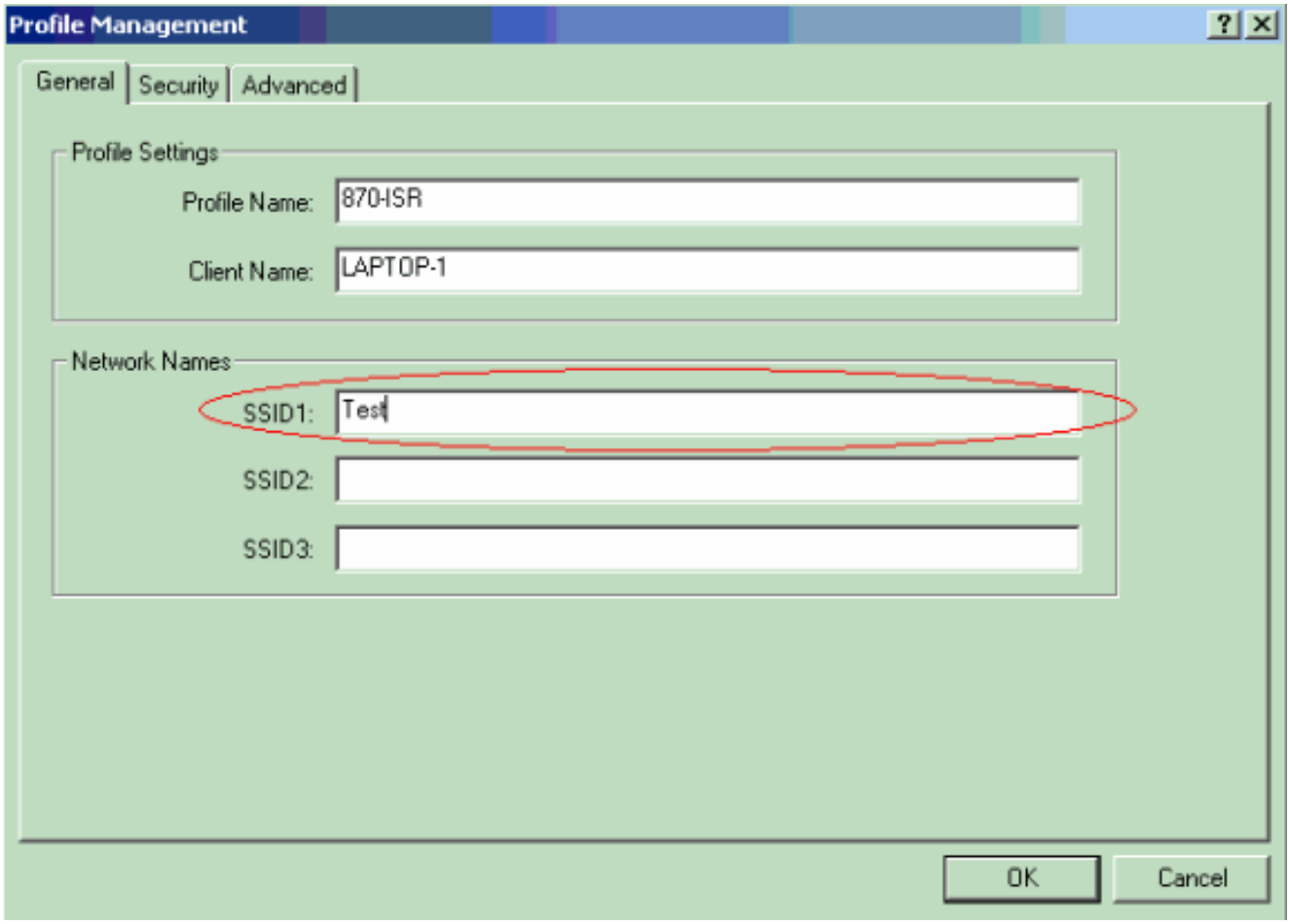
1. Configure el Integrated Routing and Bridging (IRB) y ponga al Grupo de Bridge.Teclee estos comandos del modo de configuración global para habilitar el IRB.`WirelessRouter<config>#bridge irb !--- Enables IRB. WirelessRouter<config>#bridge 1 protocol ieee !--- Defines the type of Spanning Tree Protocol as ieee. WirelessRouter<config>#bridge 1 route ip !--- Enables the routing of the specified protocol in a bridge group.`
2. Configure el (BVI) de la Interfaz Virtual Interconectada.Asigne una dirección IP al BVI. Teclee estos comandos del 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` Refiera a la *configuración del Grupo de Bridge en la* sección de los *Puntos de acceso y de los Bridges de* usar los VLA N con el equipo de red inalámbrica del Cisco Aironet para más información sobre las funciones de los Grupos de Bridge en los Puntos de acceso.
3. Configure la característica interna del servidor DHCP en el 871W ISR.La característica interna del servidor DHCP en el router se puede utilizar para asignar los IP Addresses a los clientes de red inalámbrica 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 se debe también configurar para validar los IP Addresses de un servidor DHCP.
4. Configure el 871W ISR como servidor de RADIUS local.En el modo de configuración global, teclee estos comandos de configurar el 871W ISR como servidor de 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 explicar al servidor de 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 radio.La configuración de la interfaz radio implica la configuración de los diversos parámetros de red inalámbrica en el router incluyendo el SSID, el modo de encripción, el tipo de autenticación, la velocidad, y el papel del router inalámbrico. Este ejemplo utiliza a la **Test** llamada SSID.Teclee estos comandos de configurar la interfaz 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 870 Router valida las peticiones de la asociación de los clientes de red inalámbrica una vez que se hace este procedimiento.Cuando usted configura el tipo de la autenticación EAP en el router, se recomienda para elegir el **Network EAP y para abrirse con el EAP** como tipos de autenticación para evitar cualquier problema de la 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 los clientes de la tecnología inalámbrica de Cisco.**Nota:** Use la herramienta Command Lookup Tool (clientes registrados solamente) para encontrar más información sobre los comandos usados en este documento.

Configuración del adaptador del cliente

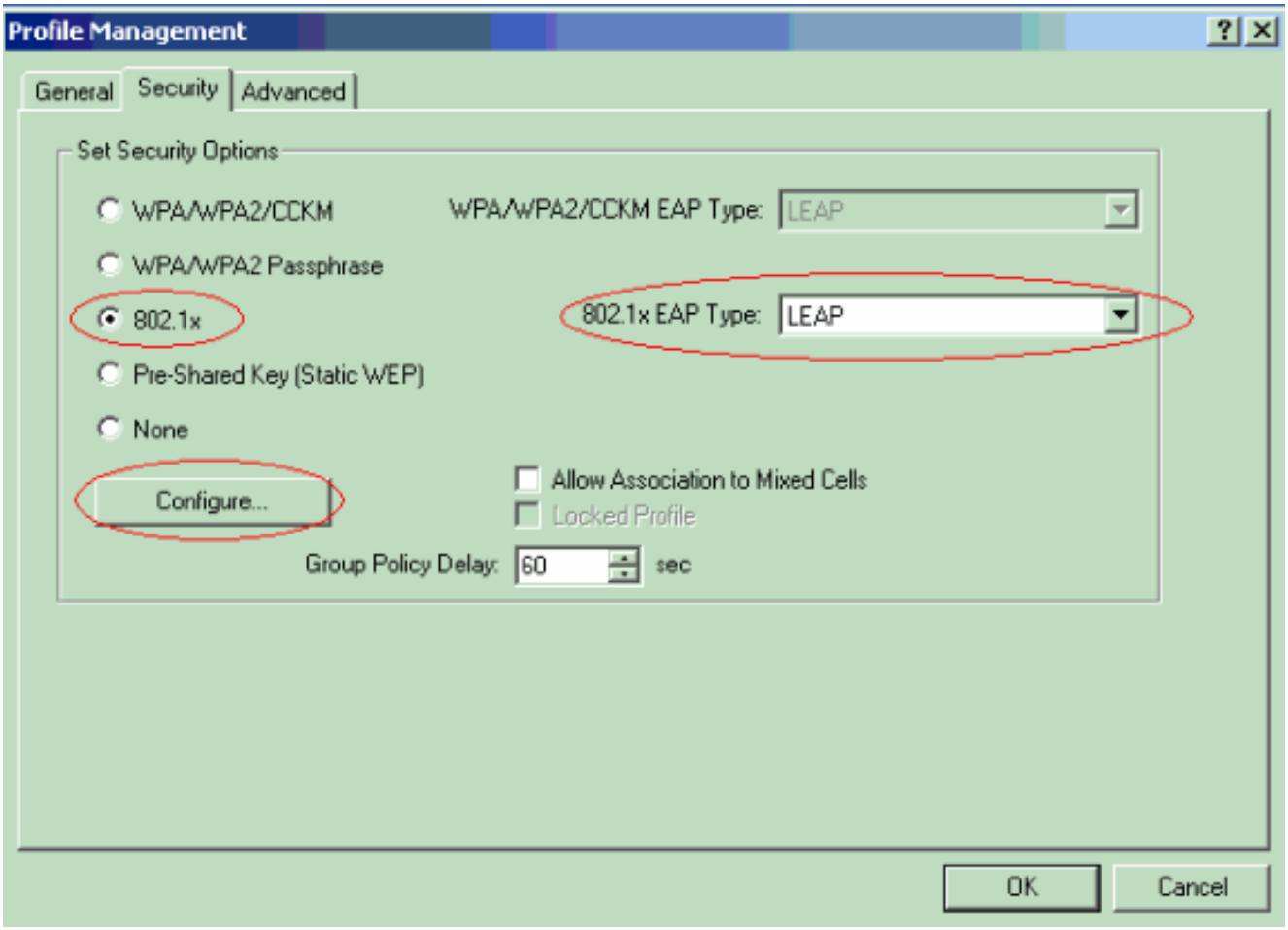
Complete estos pasos para configurar el adaptador del cliente. Este procedimiento crea un nuevo perfil llamado **870-ISR** en el ADU, como un ejemplo. Este procedimiento también utiliza la prueba como el SSID y habilita la autenticación LEAP en el adaptador del cliente.

1. Haga clic **nuevo** para crear un nuevo perfil en la ventana de administración del perfil en el ADU. Ingrese el nombre del perfil y el SSID que el adaptador del cliente utiliza conforme a la ficha general.En este ejemplo, el nombre del perfil es **870-ISR** y el SSID es **prueba**.**Nota:** El SSID debe hacer juego exactamente el SSID que usted configuró en el 871W ISR. El SSID es con diferenciación entre mayúsculas y minúsculas.

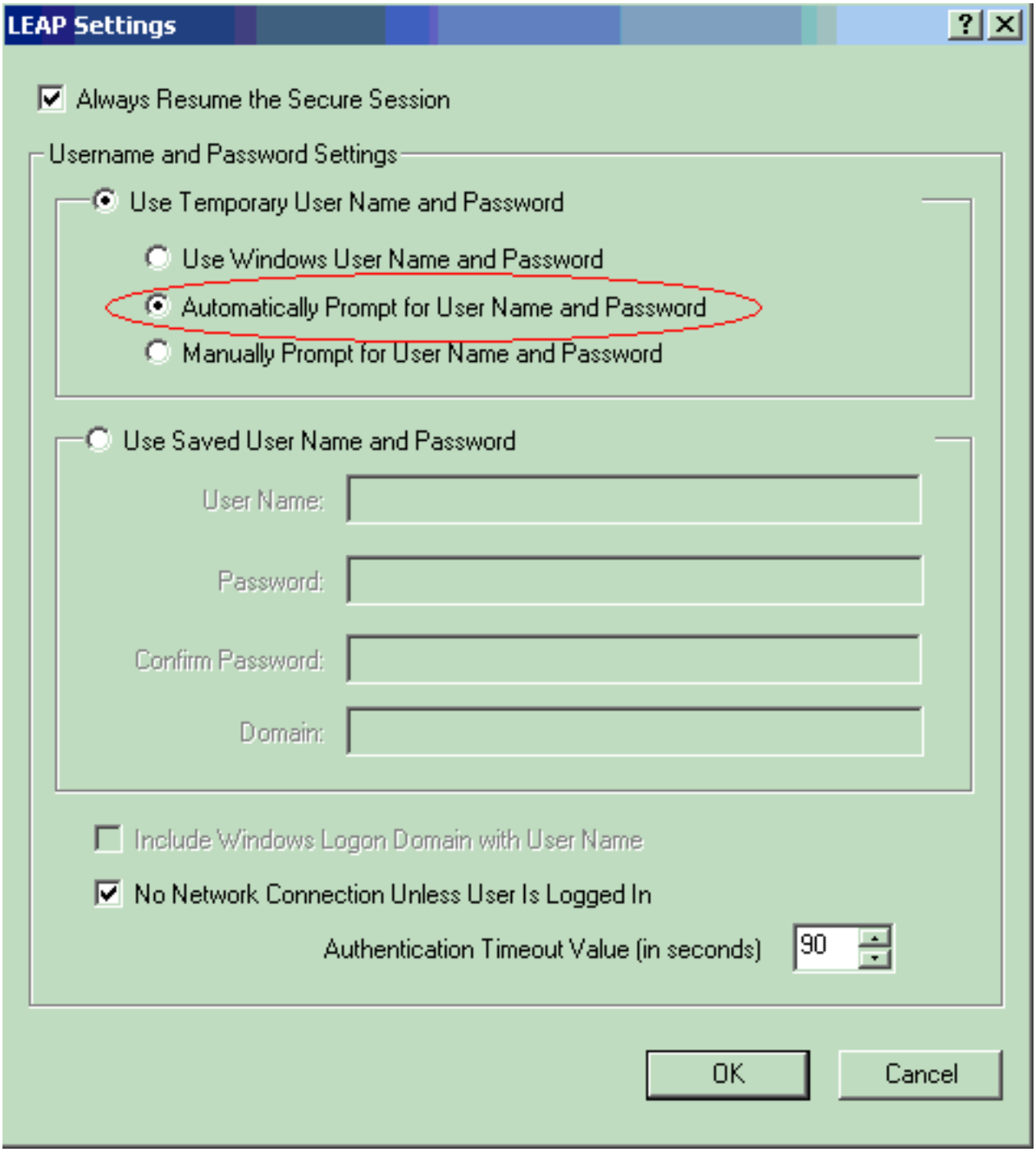


2. Vaya a la ficha de seguridad, seleccione el **802.1x** y elija el **SALTO del** menú EAP Type (Tipo EAP) del 802.1x.Esta acción habilita la autenticación LEAP en el adaptador del

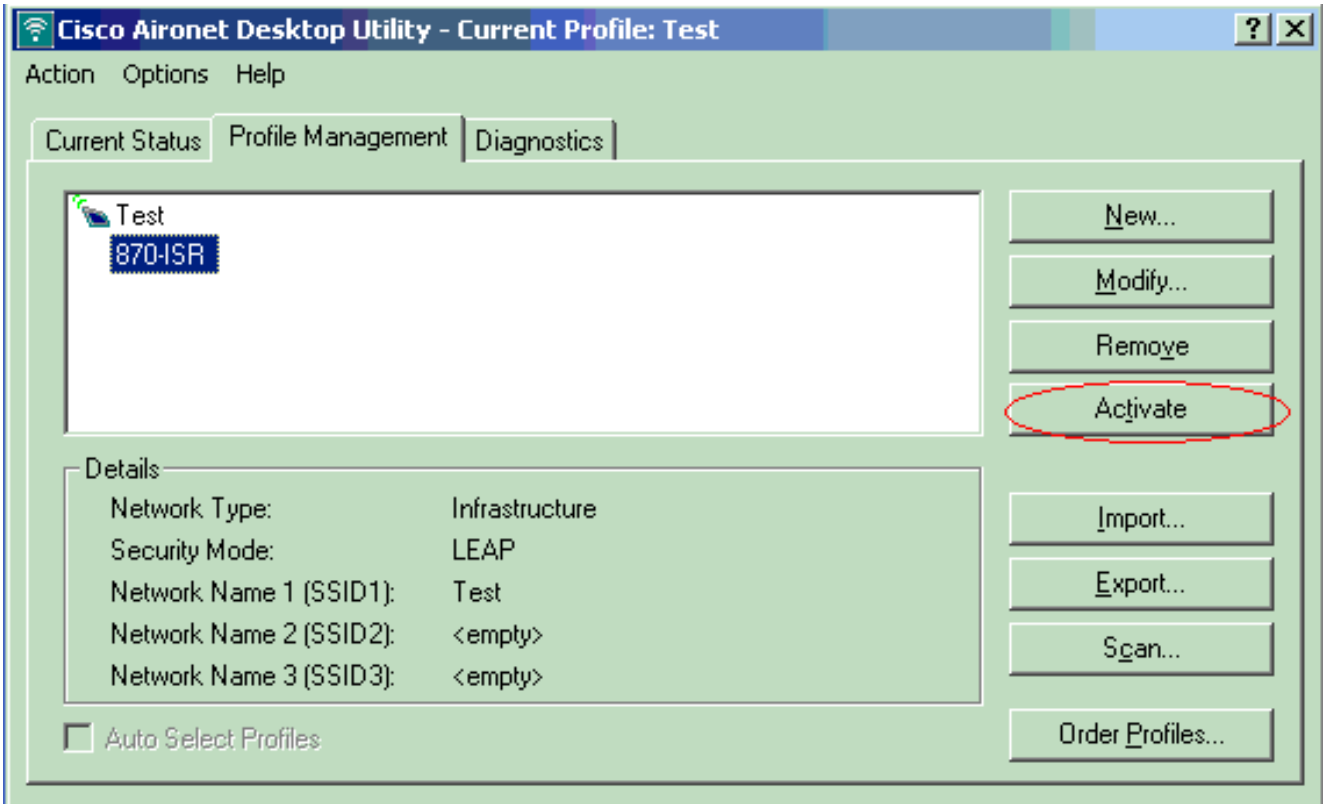
cliente.



3. **Configuración del** tecleo para definir las configuraciones del SALTO.Esta configuración elige la opción **indica automáticamente para el nombre de usuario y contraseña**. Esta opción le permite para ingresar manualmente el Nombre de usuario y la contraseña cuando ocurre la autenticación
LEAP.



4. Haga Click en OK para salir la ventana de administración del perfil.
5. El tecleo **activa** para habilitar este perfil en el adaptador del cliente.

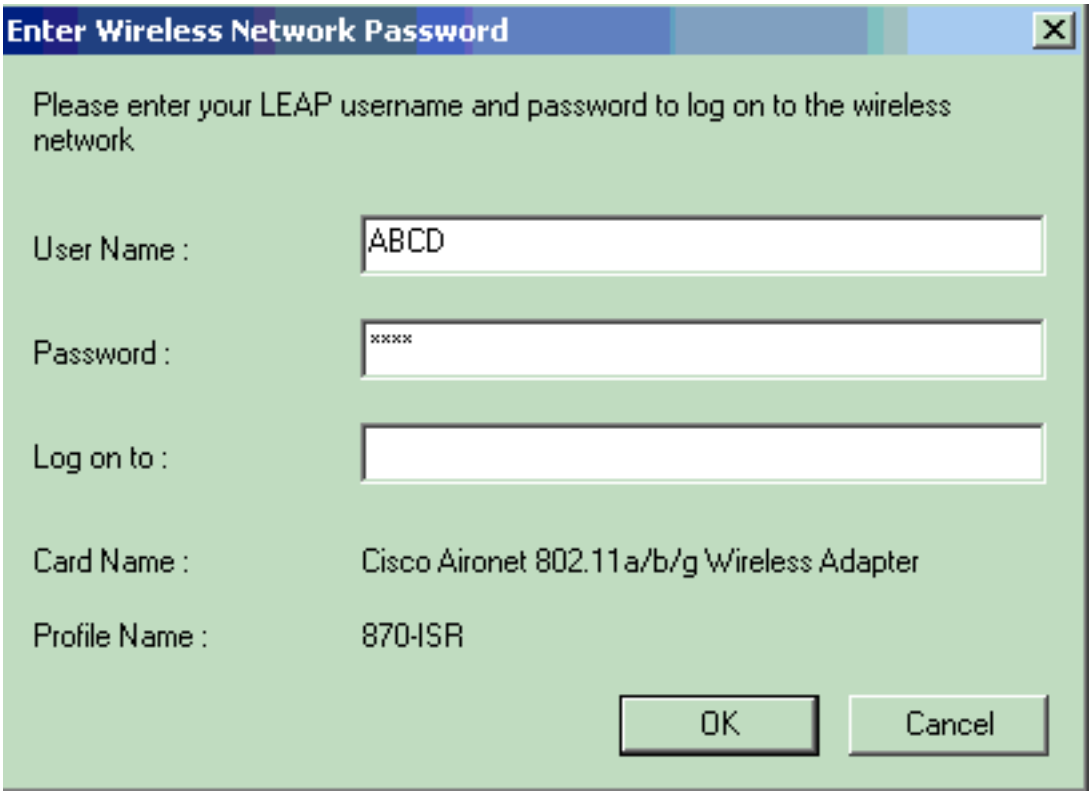


Verificación

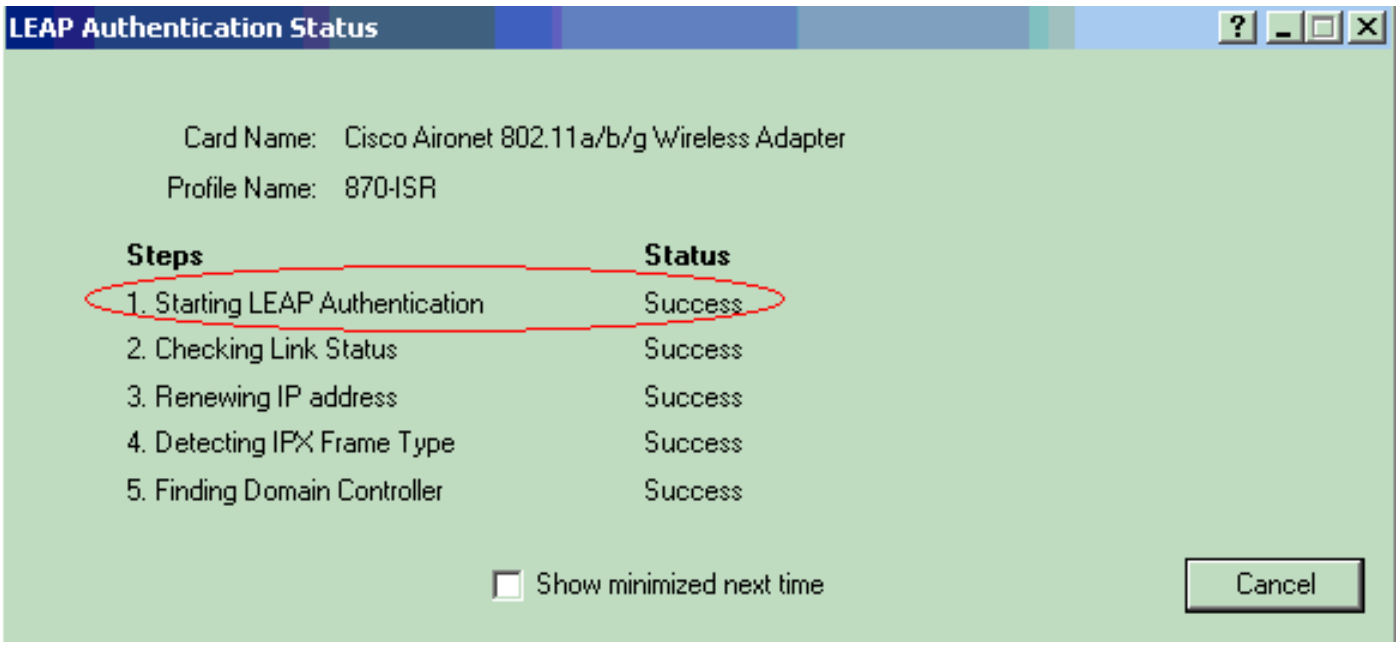
Use esta sección para confirmar que su configuración funciona correctamente.

Una vez configuran, activan el adaptador del cliente y al 870 Router el 870-ISR del perfil en el adaptador del cliente para verificar la configuración.

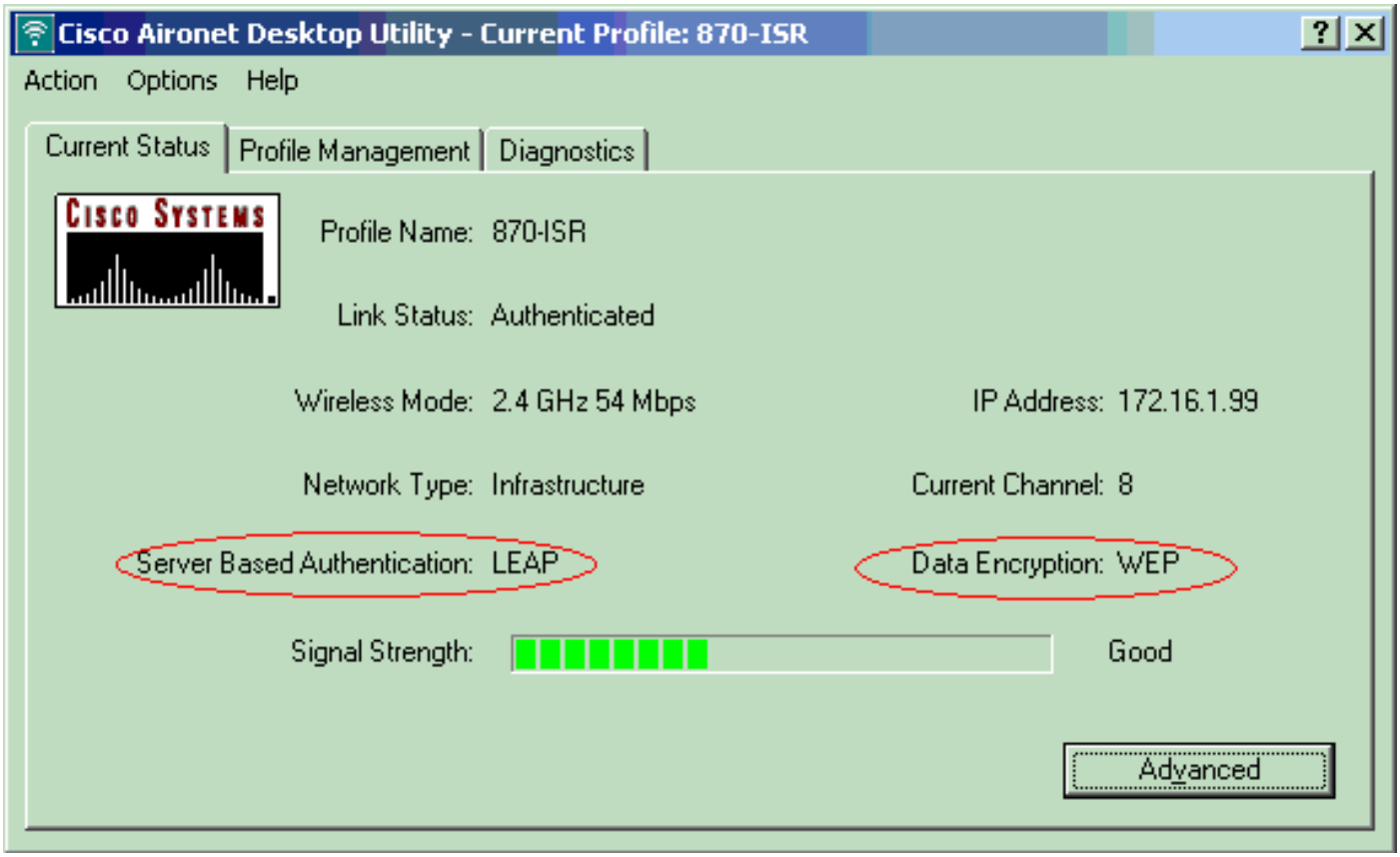
Ingrese el Nombre de usuario y la contraseña cuando las visualizaciones de la ventana de contraseña de la red inalámbrica del ingresar. Éstos deben corresponder a los que está configurados en el 871W ISR. Uno de los perfiles usados en este ejemplo es el Nombre de usuario **ABCD** y la contraseña **ABCD**.



La ventana de estado de la autenticación LEAP aparece. Esta ventana verifica los credenciales de usuario contra el servidor de RADIUS local.



Marque el estado actual ADU para verificar que el cliente utiliza la encripción 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.

- **muestre la asociación del dot11** — Verifica la configuración en el 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)`
- **muestre el atascamiento DHCP del IP** — 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`

Troubleshooting

Esta sección proporciona la información de Troubleshooting relevante a esta configuración.

1. Fije el método en el SSID **para abrirse** para inhabilitar temporalmente la autenticación.Esto elimina la posibilidad de los problemas del Radiofrecuencia (RF) que previenen la autenticación satisfactoria.Utilice los **comandos no authentication open eap eap_methods, no authentication network-eap eap_methods y authentication open del** CLI.Si el cliente se asocia con éxito, después el RF no contribuye al problema de asociación
2. Marque si el claves WEP configuradas en el router inalámbrico hacen juego con las claves WEP configuradas en los clientes.Si hay una discordancía en las claves WEP, los clientes no pueden comunicar con el router inalámbrico.
3. Verifique que las contraseñas del secreto compartido estén sincronizadas entre el router inalámbrico y el servidor de autenticación.

Usted puede también utilizar estos comandos debug de resolver problemas su configuración.

- **authenticator todo aaa del dot11 del debug** — Activa el debugging del MAC y de los paquetes de la autenticación EAP.
- **autenticación de RADIUS del debug** — Visualiza las negociaciones RADIUS entre el servidor y el cliente.
- **paquetes del servidor local del radio del debug** — Visualiza el contenido de los paquetes RADIUS se envían y se reciben que.
- **cliente del servidor local del radio del debug** — Visualiza los mensajes de error sobre las autenticaciones de cliente falladas.

Información Relacionada

- Algoritmos de encripción y tipos de autenticación
- Tipos de autenticación inalámbricos en el ISR fijo con el ejemplo de la configuración de SDM
- Tipos de autenticación inalámbricos en un ejemplo de configuración fijo ISR
- Guía de configuración de red inalámbrica del router de acceso de Cisco
- Router inalámbrico de 1800 ISR con el DHCP y el ejemplo de configuración internos de la autenticación abierta
- Página de Soporte de Red Inalámbrica
- Soporte Técnico y Documentación - Cisco Systems