

Ejemplo de Configuración de Remote-Edge AP (REAP) con Lightweight AP y Wireless LAN Controllers (WLC)

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración del WLC para Funcionamiento Básico y Configuración de WLANs](#)

[Prime el AP para la instalación en el sitio remoto](#)

[Configure los 2800 Routers para Establecer el Link WAN](#)

[Implementar el AP REAP en el sitio remoto](#)

[Verificación](#)

[Troubleshoot](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

Introducción

Las funciones de punto de acceso de extremo remoto (REAP) introducidas con Cisco Unified Wireless Network permiten la implementación remota de los puntos de acceso ligeros (LAP) de Cisco desde el controlador de LAN inalámbrica (WLAN) (WLC). Esto los hace ideales para sucursales y pequeñas ubicaciones minoristas. Este documento explica cómo implementar una red WLAN basada en REAP mediante Cisco 1030 Series LAP y 4400 WLC.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de los WLC y cómo configurar los parámetros básicos del WLC
- Conocimiento del modo de operación REAP en un LAP 1030 de Cisco
- Conocimiento de la configuración de un servidor DHCP externo y/o servidor DNS

- Conocimiento de los conceptos de acceso Wi-Fi protegido (WPA)

Componentes Utilizados

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

- WLC de la serie Cisco 4400 que ejecuta la versión de firmware 4.2
- LAP de Cisco 1030
- Dos routers Cisco serie 2800 que ejecutan Cisco IOS® Software Release 12.2(13)T13
- Cisco Aironet 802.11a/b/g Client Adapter que ejecuta la versión de firmware 3.0
- Cisco Aironet Desktop Utility versión 3.0

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.

Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco para obtener más información sobre las convenciones del documento.](#)

Antecedentes

El modo REAP permite que un LAP resida a través de un link WAN, y aun así poder comunicarse con el WLC y proporcionar la funcionalidad de un LAP normal. El modo REAP se soporta solamente en los 1030 LAPs en este punto.

Para proporcionar esta funcionalidad, el REAP 1030 separa el plano de control del protocolo de punto de acceso ligero (LWAPP) del plano de datos inalámbricos. Los WLC de Cisco todavía se utilizan para el control y la gestión centralizados de la misma manera que se utilizan los puntos de acceso (AP) basados en LWAPP normales, mientras que todos los datos de usuario se puentean localmente en el AP. El acceso a los recursos de red locales se mantiene durante las interrupciones de la WAN.

Los AP REAP admiten dos modos de funcionamiento:

- modo REAP normal
- Modo autónomo

El LAP se configura en el modo REAP normal cuando el link WAN entre el REAP AP y el WLC está activo. Cuando los LAP funcionan en el modo REAP normal, pueden soportar hasta 16 WLAN.

Cuando el link WAN entre el WLC y el LAP se desactiva, el LAP habilitado para REAP cambia al modo autónomo. Durante el modo independiente, los LAP de REAP pueden soportar solamente una WLAN independientemente sin el WLC, si la WLAN se configura con privacidad equivalente a conexión con cables (WEP) o con cualquier método de autenticación local. En este caso, la WLAN que soporta el REAP AP es la primera WLAN que se configura en el AP, WLAN 1. Esto se debe a que la mayoría de los otros métodos de autenticación necesitan pasar información hacia y desde el controlador y, cuando el link WAN está inactivo, esta operación no es posible. En el modo autónomo, los LAP soportan un conjunto mínimo de funciones. Esta tabla muestra el

conjunto de funciones que soporta un LAP REAP cuando está en modo autónomo en comparación con las funciones que soporta un LAP REAP en modo normal (cuando el link WAN está activo y la comunicación al WLC está activa):

Características que un LAP REAP soporta en el modo REAP normal y en el modo autónomo

		REAP (normal mode)	REAP (standalone mode)
Protocols	IPv4	Yes	Yes
	IPv6	Yes	Yes
	All other protocols	Yes (only if client is also IP enabled)	Yes (only if client is also IP enabled)
	IP Proxy ARP	No	No
WLAN	Number of SSIDs	16	1 (the first one)
	Dynamic channel assignment	Yes	No
	Dynamic power control	Yes	No
	Dynamic load balancing	Yes	No
VLAN	Multiple interfaces	No	No
	802.1Q Support	No	No
WLAN Security	Rogue AP detection	Yes	No
	Exclusion list	Yes	Yes (existing members only)
	Peer-to-Peer blocking	No	No
	Intrusion Detection System	Yes	No
Layer 2 Security	MAC authentication	Yes	No
	802.1X	Yes	No
	WEP (64/128/152bits)	Yes	Yes
	WPA-PSK	Yes	Yes
	WPA2-PSK	No	No
	WPA-EAP	Yes	No
	WPA2-EAP	Yes	No
Layer 3 Security	Web Authentication	No	No
	IPsec	No	No
	L2TP	No	No
	VPN Pass-through	No	No
	Access Control Lists	No	No
QoS	QoS Profiles	Yes	Yes
	Downlink QoS (weighted round-robin queues)	Yes	Yes
	802.1p support	No	No
	Per-user bandwidth contracts	No	No
	WMM	No	No
	802.11e (future)	No	No
	AAA QoS Profile override	Yes	No
Mobility	Intra-subnet	Yes	Yes
	Inter-subnet	No	No
DHCP	Internal DHCP Server	No	No
	External DHCP Server	Yes	Yes
Topology	Direct connect (2006)	No	No

La tabla muestra que las VLAN múltiples no son soportadas en los LAPs REAP en ambos modos. No se admiten varias VLAN porque los LAP de REAP sólo pueden residir en una única subred porque no pueden realizar el etiquetado de VLAN IEEE 802.1Q. Por lo tanto, el tráfico en cada uno de los identificadores de conjunto de servicios (SSID) termina en la misma subred que la red con cables. Como resultado, el tráfico de datos no se separa en el lado cableado aunque el tráfico inalámbrico pueda segmentarse por el aire entre los SSID.

Consulte [Guía de implementación de REAP en la sucursal](#) para obtener más información sobre la implementación de REAP y cómo administrar REAP y sus limitaciones.

Configurar

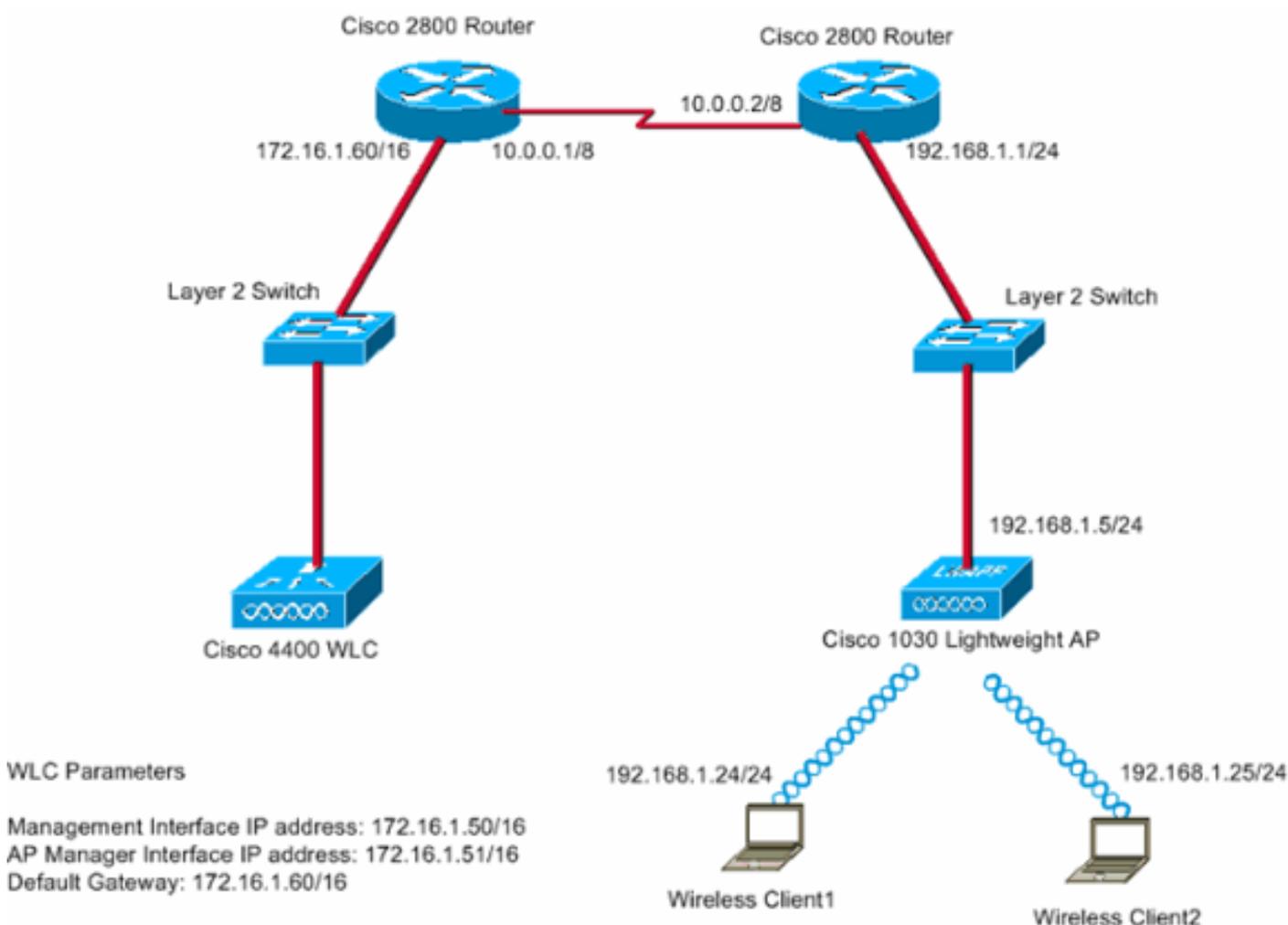
En esta sección encontrará la información para configurar las funciones descritas en este documento.

Para configurar los dispositivos para implementar la configuración de la red, complete estos pasos:

1. [Configure el WLC para el funcionamiento básico y configure las WLAN.](#)
2. [Prime el AP para la instalación en el sitio remoto.](#)
3. [Configure los 2800 routers para establecer el link WAN.](#)
4. [Implemente el LAP REAP en el sitio remoto.](#)

Diagrama de la red

En este documento, se utiliza esta configuración de red:



La oficina principal se conecta a la sucursal mediante una línea arrendada. La línea arrendada termina en los routers de la serie 2800 en cada extremo. Este ejemplo utiliza el protocolo Open Shortest Path First (OSPF) para rutear los datos en el enlace WAN con la encapsulación PPP. El WLC 4400 está en la oficina principal y el LAP 1030 debe desplegarse en la oficina remota. El

LAP 1030 debe soportar dos WLAN. Estos son los parámetros para las WLAN:

- **WLAN 1** SSID: **SSID1** Autenticación: **Abierta** Encriptación: **protocolo de integridad de clave temporal (TKIP) (clave precompartida WPA [WPA-PSK])**
- **WLAN 2** SSID: **SSID2** Autenticación: **protocolo de autenticación ampliable (EAP)** Cifrado: **TKIP** Nota: Para WLAN 2, la configuración en este documento utiliza WPA (autenticación 802.1x y TKIP para el cifrado).

Debe configurar los dispositivos para esta configuración.

[Configuración del WLC para Funcionamiento Básico y Configuración de WLANs](#)

Puede utilizar el asistente de configuración de inicio en la interfaz de línea de comandos (CLI) para configurar el WLC para el funcionamiento básico. Alternativamente, también puede utilizar la GUI para configurar el WLC. Este documento explica la configuración en el WLC con el uso del asistente de configuración de inicio en la CLI.

Después de que el WLC se inicie por primera vez, ingresa directamente al asistente de configuración de inicio. Utilice el asistente de configuración para configurar los parámetros básicos. Puede ejecutar el asistente en la CLI o en la GUI. Este es un ejemplo del asistente de configuración de inicio:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: WLC_MainOffice
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 172.16.1.50
Management Interface Netmask: 255.255.0.0
Management Interface Default Router: 172.16.1.60
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 172.16.1.1
AP Manager Interface IP Address: 172.16.1.51
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (172.16.1.1):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Main
Network Name (SSID): SSID1
Allow Static IP Addresses [YES][no]: Yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: Yes
Enable 802.11a Network [YES][no]: Yes
Enable 802.11g Network [YES][no]: Yes
Enable Auto-RF [YES][no]: Yes

Configuration saved!
Resetting system with new configuration...
```

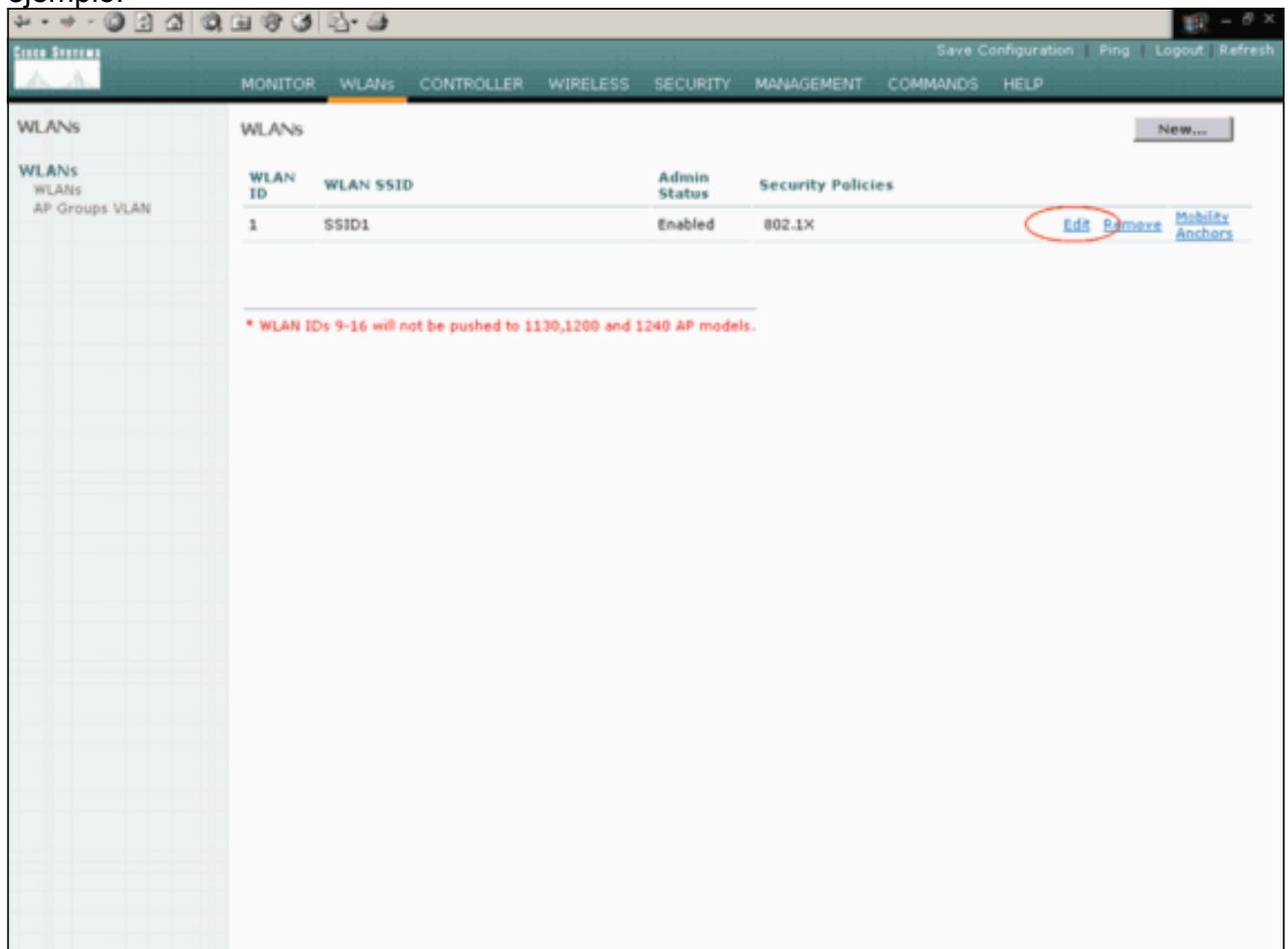
Este ejemplo configura estos parámetros en el WLC:

- Nombre del sistema
- Dirección IP de la interfaz de administración
- Dirección IP de la interfaz del administrador de AP

- Número de puerto de interfaz de administración
- Identificador de VLAN de la interfaz de administración
- Nombre del grupo de movilidad
- SSID
- Muchos otros parámetros

Estos parámetros se utilizan para configurar el WLC para el funcionamiento básico. Como muestra el resultado del WLC en esta sección, el WLC utiliza 172.16.1.50 como la dirección IP de la interfaz de administración y 172.16.1.51 como la dirección IP de la interfaz del administrador de AP. Para configurar las dos WLAN para su red, complete estos pasos en el WLC:

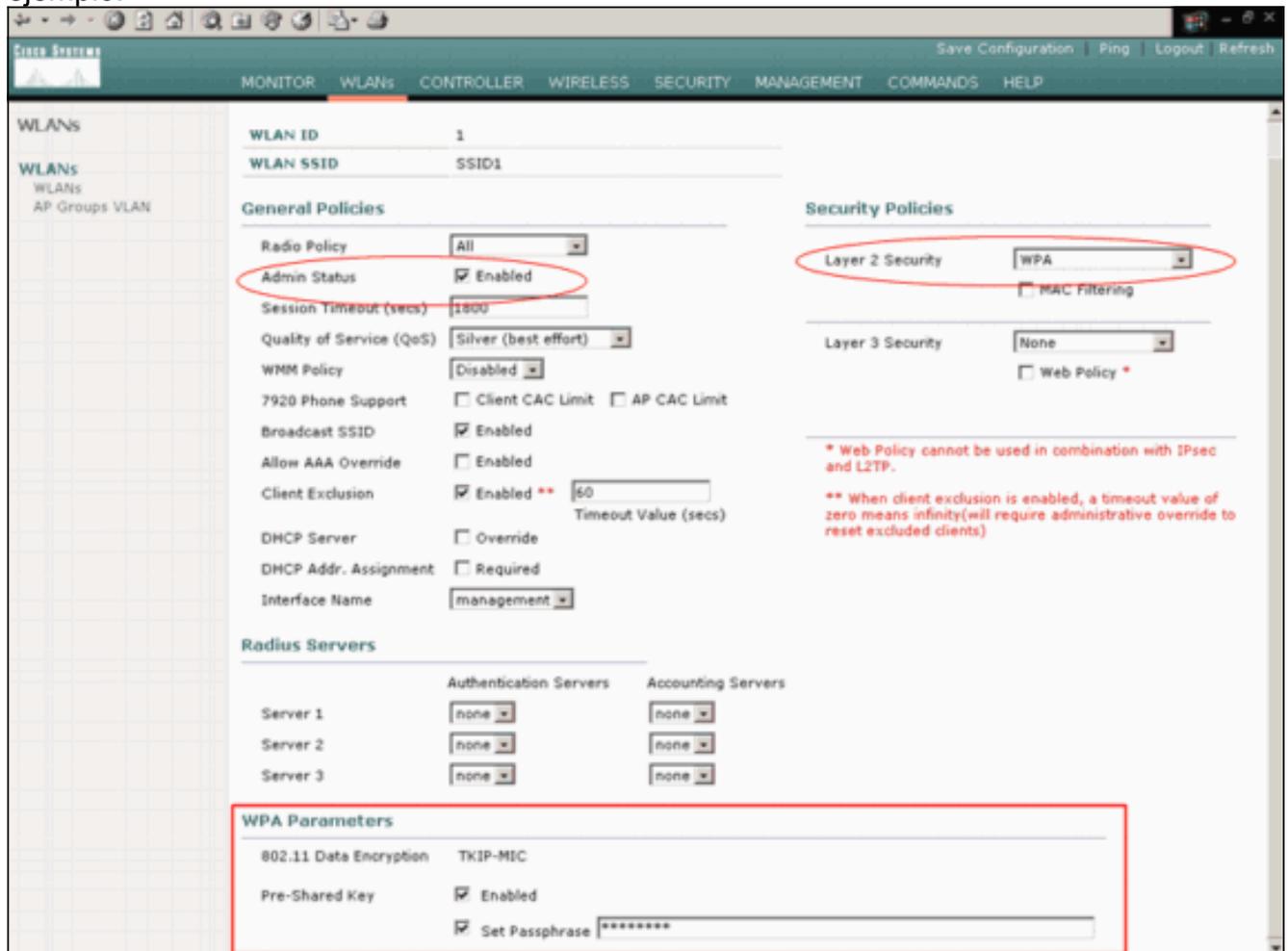
1. Desde la GUI del WLC, haga clic en **WLANs** en el menú en la parte superior de la ventana. Aparece la ventana WLAN. Esta ventana enumera las WLANs configuradas en el WLC. Debido a que configuré una WLAN con el uso del asistente de configuración de inicio, debe configurar los otros parámetros para esta WLAN.
2. Haga clic en **Editar** para el WLAN SSID1. Aquí tiene un ejemplo:



Aparece la ventana WLAN > Editar. En esta ventana, puede configurar los parámetros que son específicos de la WLAN, que incluye las Políticas generales, las Políticas de seguridad, el servidor RADIUS y otros.

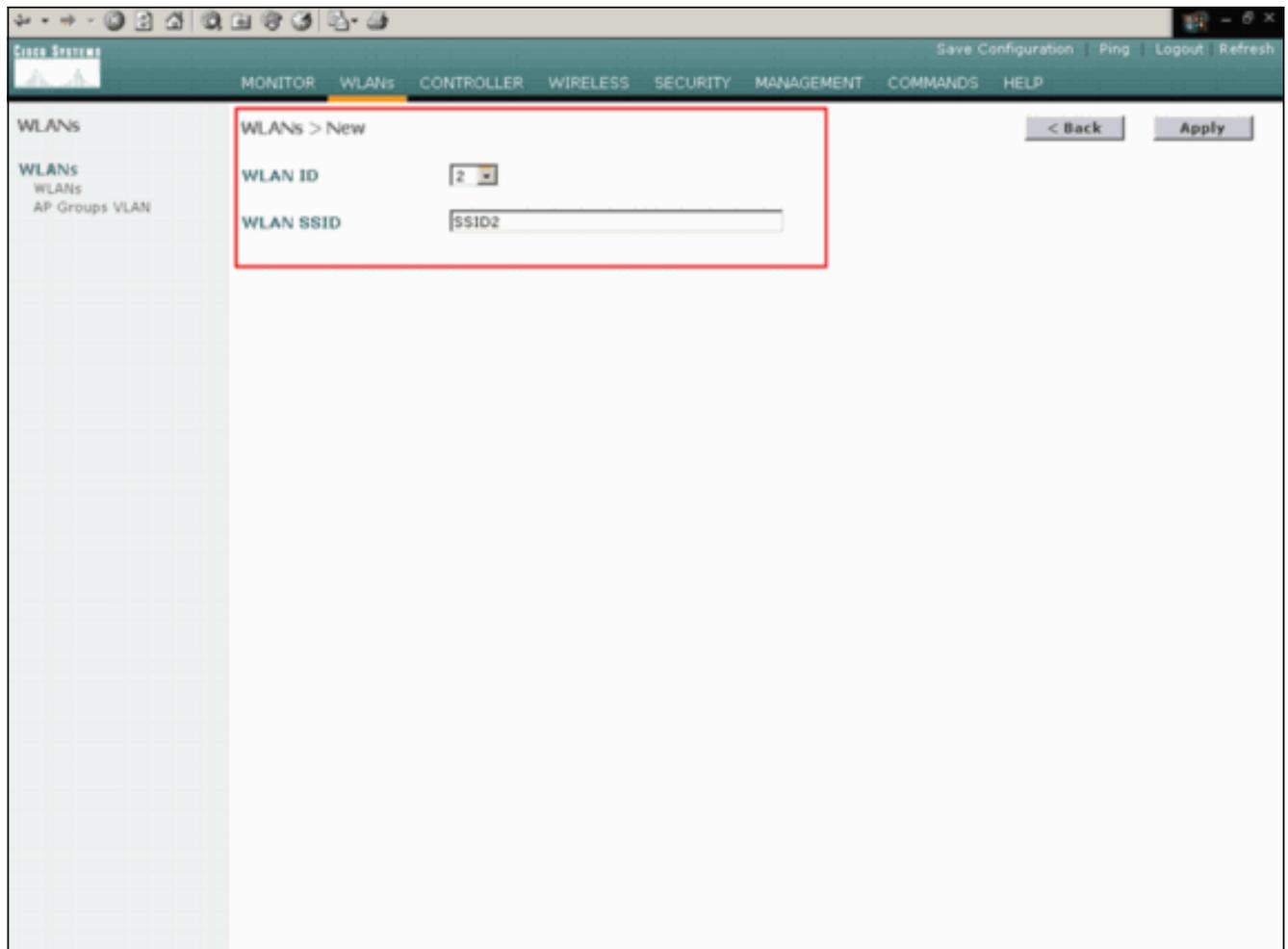
3. Realice estas selecciones en la ventana WLAN > Edit: En el área Políticas generales, marque la casilla de verificación **Enabled** junto a Admin Status para habilitar esta WLAN. Elija **WPA** en el menú desplegable Layer 2 Security para utilizar WPA para WLAN 1. Defina los parámetros WPA en la parte inferior de la ventana. Para utilizar WPA-PSK en WLAN 1, marque la casilla de verificación **Enabled** junto a Pre-Shared Key en el área WPA Parameters e ingrese la frase de paso para WPA-PSK. WPA-PSK utilizará TKIP para la

encriptación. **Nota:** La frase de paso WPA-PSK debe coincidir con la frase de paso configurada en el adaptador del cliente para que WPA-PSK funcione. Haga clic en Apply (Aplicar). Aquí tiene un ejemplo:



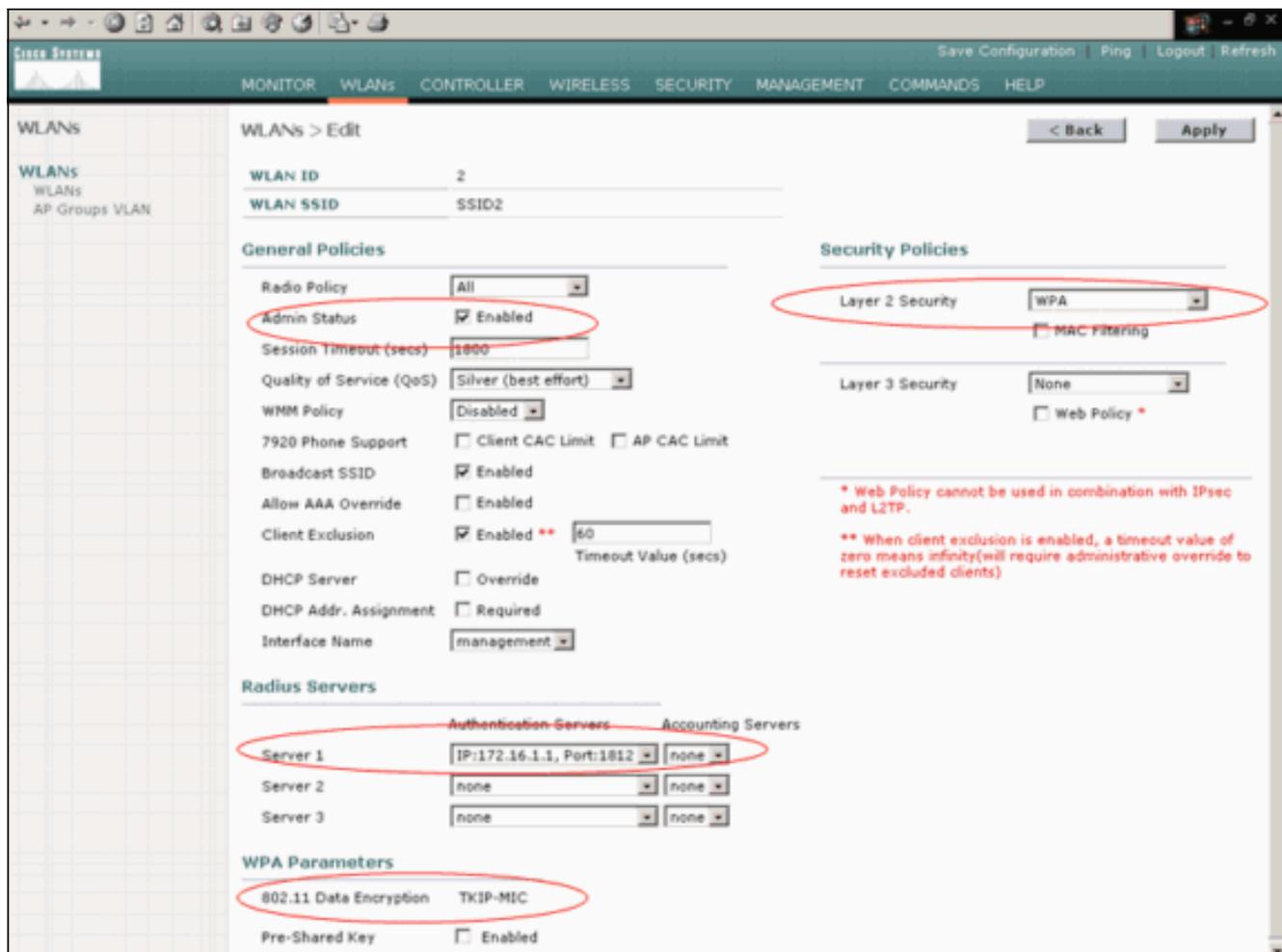
Ha configurado WLAN 1 para la encriptación WPA-PSK.

- Para definir WLAN 2, haga clic en **New** en la ventana WLANs. Aparece la ventana WLAN > New .
- En la ventana WLAN > New, defina el ID de WLAN y el SSID de WLAN, y haga clic en **Apply**. Aquí tiene un ejemplo:



Aparece la ventana WLAN > Edit para la segunda WLAN.

6. Realice estas selecciones en la ventana WLAN > Edit: En el área Políticas generales, marque la casilla de verificación **Enabled** junto a Admin Status para habilitar esta WLAN. Elija **WPA** en el menú desplegable Layer 2 Security para configurar WPA para esta WLAN. En el área Servidores RADIUS, elija el servidor RADIUS apropiado para usar para la autenticación de los clientes. Haga clic en Apply (Aplicar). Aquí tiene un ejemplo:



Nota: Este documento no explica cómo configurar los servidores RADIUS y la autenticación EAP. Para obtener información sobre cómo configurar la autenticación EAP con WLC, refiérase a [Ejemplo de Configuración de Autenticación EAP con Controladores WLAN \(WLC\)](#).

[Prime el AP para la instalación en el sitio remoto](#)

Priming es un proceso mediante el cual los LAP obtienen una lista de controladores a los que pueden conectarse. Los LAP son informados de todos los controladores del grupo de movilidad tan pronto como se conectan a un único controlador. De esta manera, los LAPs aprenden toda la información que necesitan para unirse a cualquier controlador en el grupo.

Para priorizar un AP compatible con REAP, conecte el AP a la red cableada en la oficina principal. Esta conexión permite que el AP detecte un único controlador. Después de que el LAP se une al controlador en la oficina principal, el AP descarga la versión del sistema operativo AP (OS) que corresponde con la infraestructura WLAN y la configuración. Las direcciones IP de todos los controladores del grupo de movilidad se transfieren al AP. Cuando el AP tiene toda la información que necesita, el AP se puede conectar en la ubicación remota. El AP puede entonces detectar y unirse al controlador menos utilizado de la lista, si la conectividad IP está disponible.

Nota: Asegúrese de configurar los AP en el modo "REAP" antes de apagarlos para enviarlos a los sitios remotos. Puede establecer el modo en el nivel de punto de acceso a través de la CLI o la GUI del controlador, o con el uso de plantillas de Wireless Control System (WCS). Los AP se configuran para realizar la funcionalidad "local" regular de forma predeterminada.

Los LAP pueden utilizar cualquiera de estos métodos para detectar el controlador:

- **Detección de capa 2**

- **Detección de capa 3** Con el uso de una difusión de subred local
 - Con el uso de la opción DHCP 43
 - Con el uso de un servidor DNS
 - Con el uso del aprovisionamiento aéreo (OTAP)
 - Con el uso de un servidor DHCP interno
- Nota:** Para utilizar un servidor DHCP interno, el LAP debe conectarse directamente al WLC.

Este documento asume que el LAP se registra al WLC con el uso del mecanismo de detección de la opción DHCP 43. Para obtener más información sobre el uso de la opción DHCP 43 para registrar el LAP en el controlador, así como otros mecanismos de detección, refiérase a [Registro de Lightweight AP \(LAP\) en un Wireless LAN Controller \(WLC\)](#).

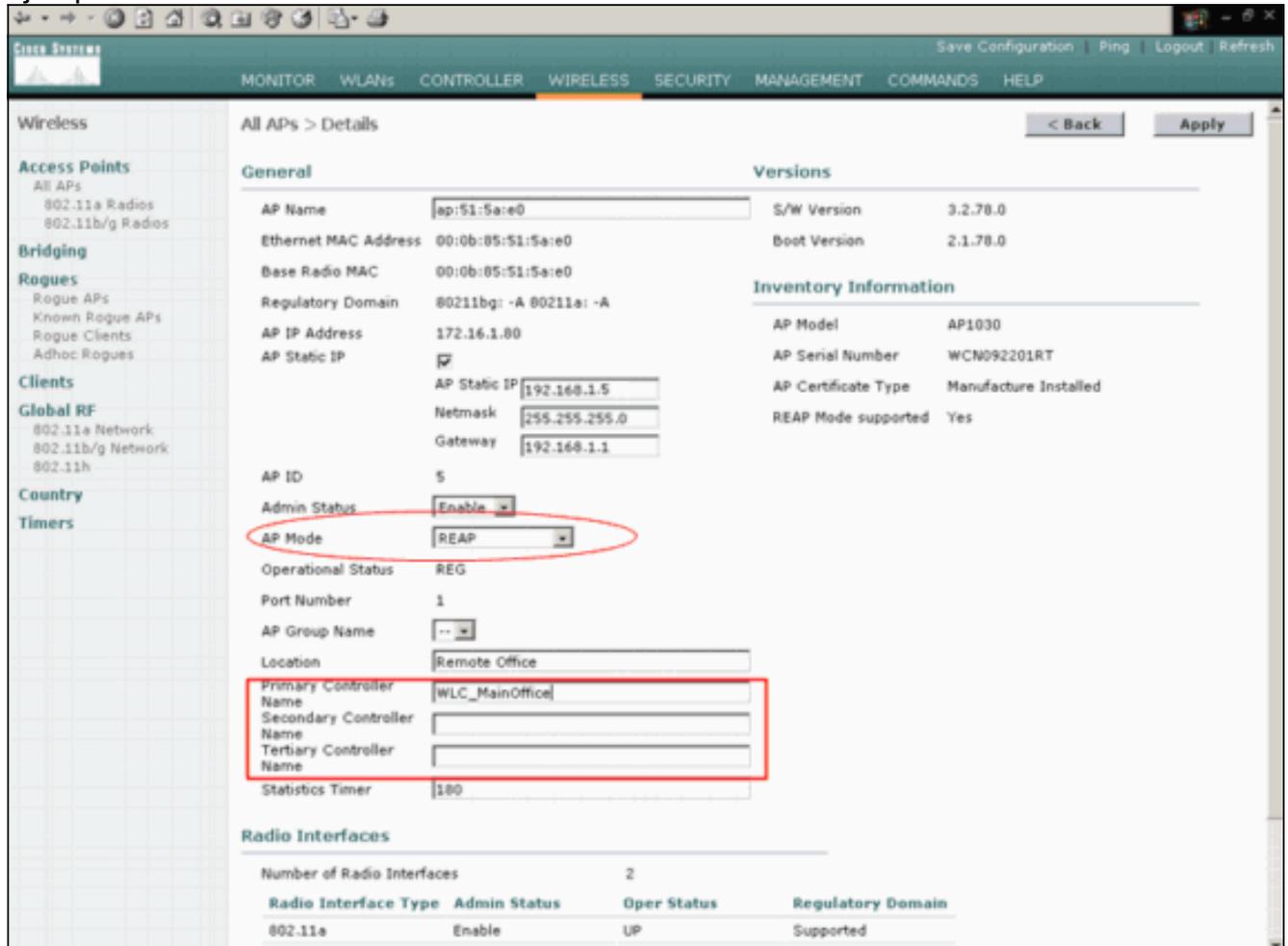
Después de que el LAP descubre el controlador, puede ver que el AP está registrado al controlador en la ventana Inalámbrica del WLC. Aquí tiene un ejemplo:

AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port	
ap:51:5a:e0	5	00:0b:05:51:5a:e0	Enable	REG	1	Detail

Complete estos pasos para configurar el LAP para el modo REAP normal:

1. Desde WLC GUI, haga clic en **Wireless**. Aparece la ventana All APs . Esta ventana enumera los APs que están registrados en el WLC.
2. Seleccione el AP que debe configurar para el modo REAP y haga clic en **Detail**. Aparece la ventana All APs > Detail para el AP específico. En esta ventana, puede configurar los diversos parámetros del AP, que incluyen: nombre AP Dirección IP (que puede cambiar a estática) Estado del administrador Parámetros de seguridad modo AP Lista de WLC a los que el AP puede conectarse Otros parámetros
3. Elija **REAP** en el menú desplegable AP Mode .Este modo sólo está disponible en los AP con capacidad REAP.
4. Defina los nombres de controlador que los AP utilizarán para registrarse y haga clic en

Aplicar. Puede definir hasta tres nombres de controlador (primario, secundario y terciario). Los AP buscan el controlador en el mismo orden que usted provee en esta ventana. Debido a que este ejemplo utiliza sólo un controlador, el ejemplo define el controlador como el controlador principal. Aquí tiene un ejemplo:



Ha configurado el AP para el modo REAP y puede implementarlo en el sitio remoto.

Nota: En esta ventana de ejemplo, puede ver que la dirección IP del AP se cambia a estática y se asigna una dirección IP estática 192.168.1.5. Esta asignación se produce porque ésta es la subred que se utilizará en la oficina remota. Por lo tanto, usted utiliza la dirección IP del servidor DHCP, 172.16.1.80, sólo durante la etapa de inicialización. Después de registrar el AP en el controlador, usted cambia la dirección a una dirección IP estática.

[Configure los 2800 Routers para Establecer el Link WAN](#)

Para establecer el link WAN, este ejemplo utiliza dos routers serie 2800 con OSPF para rutear la información entre las redes. Esta es la configuración de ambos routers para el escenario de ejemplo en este documento:

```

Oficina principal

MainOffice#show run
Building configuration...

Current configuration : 728 bytes
!
version 12.2
  
```

```

service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname MainOffice
!
!
ip subnet-zero
!
!
!
!
interface Ethernet0
 ip address 172.16.1.60 255.255.0.0
 !--- This is the interface which acts as the default
 gateway to the WLC. ! interface Virtual-Templat1 no ip
 address ! interface Serial0 no ip address ! interface
 Serial1 !--- This is the interface for the WAN link. ip
 address 10.0.0.1 255.0.0.0 encapsulation ppp !--- This
 example uses PPP. Use the appropriate !--- encapsulation
 for the WAN connection. ! router ospf 50 !--- Use OSPF
 to route data between the different networks. log-
 adjacency-changes network 10.0.0.0 0.255.255.255 area 0
 network 172.16.0.0 0.0.255.255 area 0 ! ! ip classless
 ip http server ! ! ! line con 0 line aux 0 line vty 0 4
 ! end

```

Sucursal

```

BranchOffice#show run
Building configuration...

Current configuration : 596 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BranchOffice
!
!
ip subnet-zero
!
!
!
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 !--- This is the interface which acts as the default
 gateway to the LAP. ! interface Serial0 no ip address !
 interface Serial1 !--- This is the interface for the WAN
 link. ip address 10.0.0.2 255.0.0.0 encapsulation ppp
 clockrate 56000 ! router ospf 50 !--- Use OSPF to route
 data between the different networks. log-adjacency-
 changes network 10.0.0.0 0.255.255.255 area 0 network
 192.168.1.0 0.0.0.255 area 0 ! ip classless ip http
 server ! ! ! ! line con 0 line aux 0 line vty 0 4 login
 autocommand access enable-timeout 2 ! end

```

[Implementar el AP REAP en el sitio remoto](#)

Ahora que ha configurado las WLAN en los WLC, ha preparado el LAP y establecido el link WAN entre la oficina principal y la oficina remota, está listo para implementar el AP en el sitio remoto.

Después de encender el AP en el sitio remoto, el AP busca el controlador en el orden que configuró en la etapa de inicialización. Después de que el AP encuentra el controlador, el AP se registra con el controlador. Aquí está un ejemplo. Desde el WLC, puede ver que el AP se ha unido al controlador en el puerto 1:

AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port
ap:51:5ae0	5	00:0b:05:51:5ae0	Enable	REG	1

Los clientes que tienen el SSID **SSID1**, y para los que WPA-PSK está habilitado, se asocian al AP en la WLAN 1. Los clientes que tienen el SSID **SSID2** y que tienen la autenticación 802.1x habilitada, se asocian al AP en la WLAN 2. Este es un ejemplo que muestra dos clientes. Un cliente está conectado a la WLAN 1 y el otro cliente está conectado a la WLAN 2:

The screenshot shows the Cisco Wireless LAN Controller (WLC) GUI. The main content area displays a table of clients. The table has the following columns: Client MAC Addr, AP Name, AP MAC Addr, WLAN, Type, Status, Auth, Port, and a set of action links (Detail, Link, Test, Disable, Remove). Two clients are listed, both with a status of 'Associated'.

Client MAC Addr	AP Name	AP MAC Addr	WLAN	Type	Status	Auth	Port	
00:40:96:ac:dd:05	ap:51:5a:e0	00:0b:85:51:5a:e0	SSID1	802.11a	Associated	Yes	1	Detail Link Test Disable Remove
00:40:96:ac:e6:57	ap:51:5a:e0	00:0b:85:51:5a:e0	SSID2	802.11a	Associated	Yes	1	Detail Link Test Disable Remove

Verificación

Utilice esta sección para confirmar que su configuración REAP funciona correctamente.

Nota: Consulte [Información Importante sobre Comandos Debug](#) antes de utilizar los comandos debug.

Apague el enlace WAN. Cuando el link WAN está inactivo, el AP pierde la conectividad con el WLC. El WLC luego desregistra el AP de su lista. Aquí tiene un ejemplo:

```
(Cisco Controller) >debug lwapp events enable
Wed May 17 15:04:22 2006: Did not receive heartbeat reply from AP 00:0B:85:51:5A:E0
Wed May 17 15:04:22 2006: Max retransmissions reached on AP 00:0B:85:51:5A:E0
(CONFIGURE_COMMAND, 1)
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Down LWAPP event for
AP 00:0b:85:51:5a:e0 slot 0
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event
for AP 00:0b:85:51:5a:e0 slot 0
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Down LWAPP event for
AP 00:0b:85:51:5a:e0 slot 1
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event
for AP 00:0b:85:51:5a:e0 slot 1
Wed May 17 15:04:22 2006: spamDeleteLCB: stats timer not initialized for AP
00:0b:85:51:5a:e0
Wed May 17 15:04:22 2006: Received LWAPP Down event for AP 00:0b:85:51:5a:e0 slot 0!
Wed May 17 15:04:22 2006: Deregister LWAPP event for AP 00:0b:85:51:5a:e0 slot 0
```

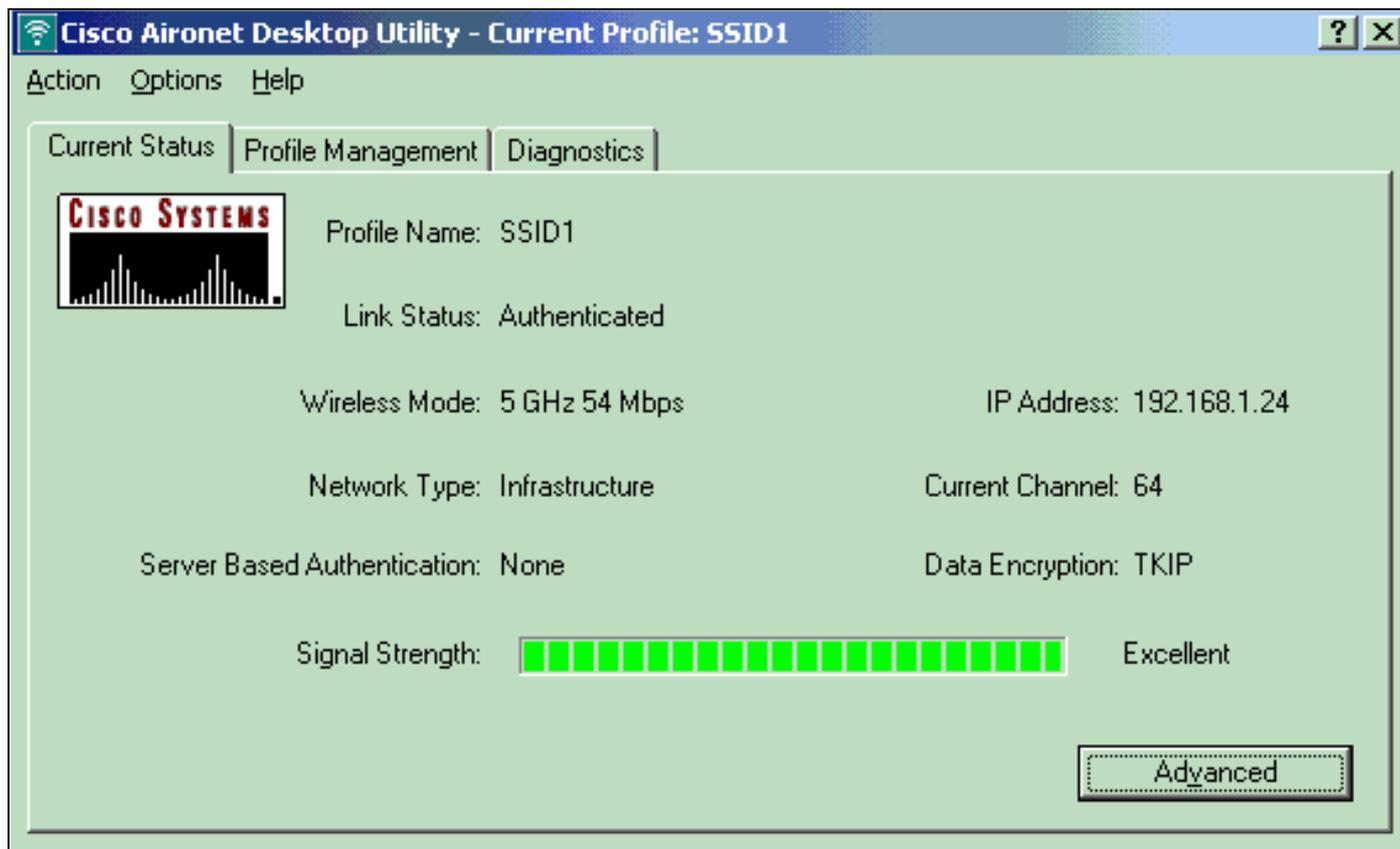
Wed May 17 15:04:22 2006: Received LWAPP Down event for AP 00:0b:85:51:5a:e0 slot 1!

Wed May 17 15:04:22 2006: Deregister LWAPP event for AP 00:0b:85:51:5a:e0 slot 1

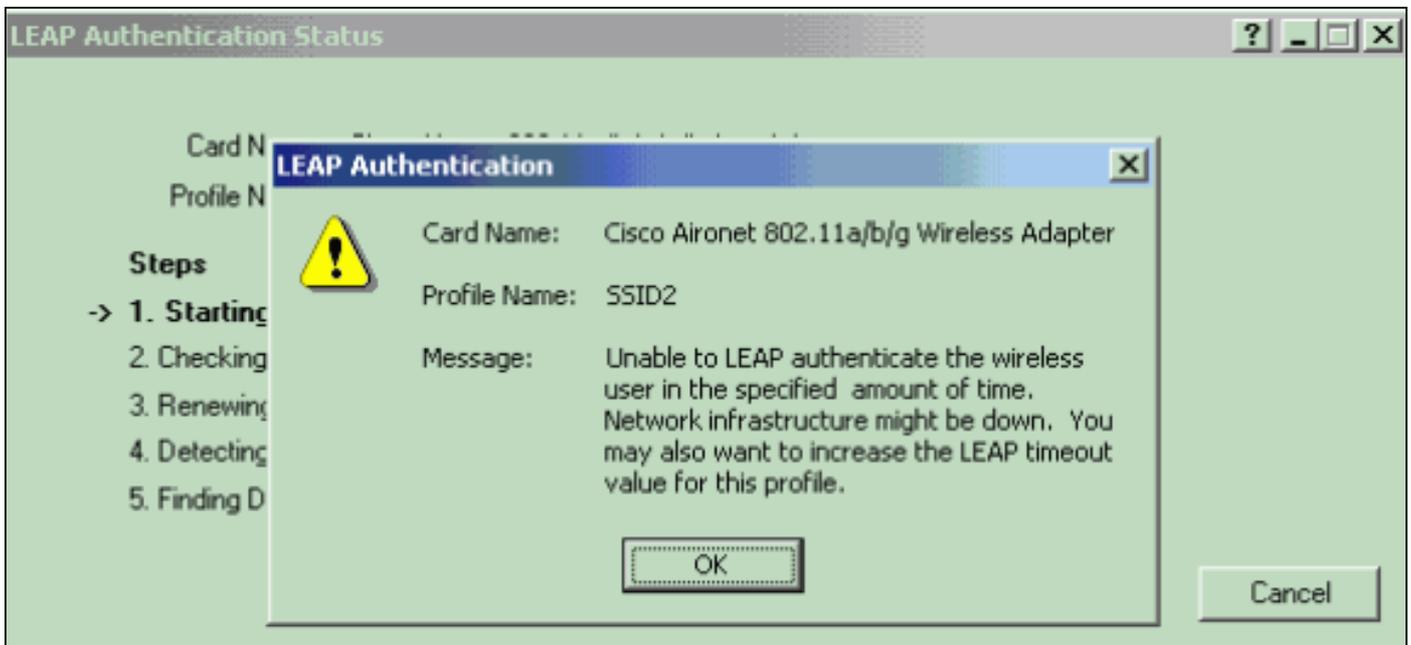
Desde la salida del comando **debug lwapp events enable**, puede ver que el WLC desregistra el AP porque el WLC no recibió una respuesta de latido del AP. Una respuesta de latido es similar a los mensajes de señal de mantenimiento. El controlador prueba cinco latidos consecutivos, con una separación de 1 segundo. Si el WLC no recibe una respuesta, el WLC desregistra el AP.

Cuando el AP está en modo autónomo, la luz de alimentación del AP parpadea. Los clientes que se asocian a la primera WLAN (WLAN 1) todavía están asociados al AP porque los clientes de la primera WLAN están configurados sólo para la encriptación WPA-PSK. El LAP maneja el cifrado en sí mismo en modo independiente. Este es un ejemplo que muestra el estado (cuando el link WAN está inactivo) de un cliente que está conectado a la WLAN 1 con SSID1 y WPA-PSK:

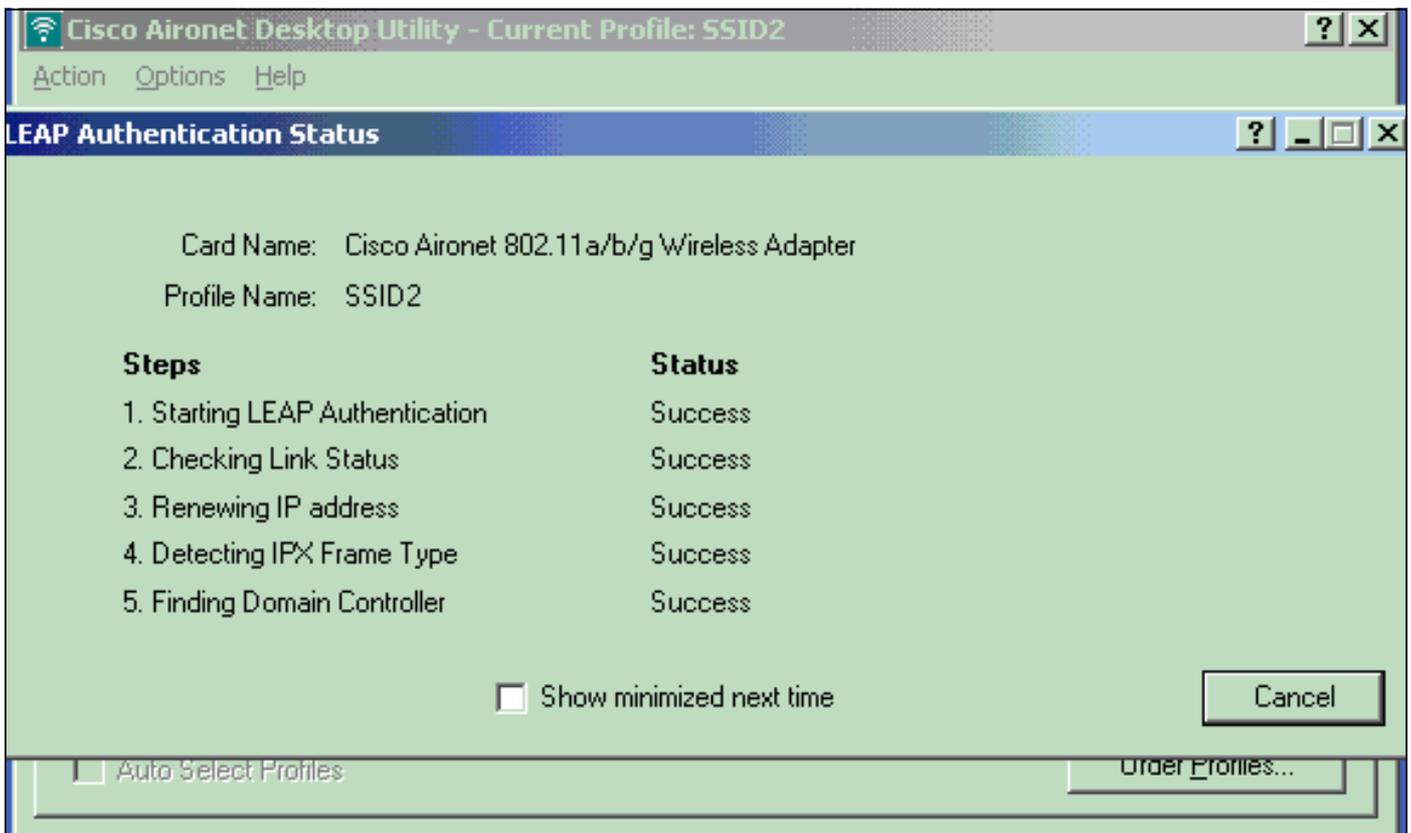
Nota: TKIP es el cifrado que se utiliza con WPA-PSK.



Los clientes que están conectados a WLAN 2 están desconectados porque WLAN 2 utiliza autenticación EAP. Esta desconexión ocurre porque los clientes que utilizan la autenticación EAP necesitan comunicarse con el WLC. Esta es una ventana de ejemplo que muestra que la autenticación EAP falla cuando el link WAN está inactivo:



Después de que el link WAN esté activo, el AP vuelve al modo REAP normal y se registra con el controlador. El cliente que utiliza la autenticación EAP también aparece. Aquí tiene un ejemplo:



Este ejemplo de salida del comando **debug lwapp events enable** en el controlador muestra estos resultados:

```
(Cisco Controller) >debug lwapp events enable
Wed May 17 15:06:40 2006: Successful transmission of LWAPP Discovery-Response
to AP 00:0b:85:51:5a:e0 on Port 1
Wed May 17 15:06:52 2006: Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0to
00:0b:85:33:84:a0 on port '1'
Wed May 17 15:06:52 2006: LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0is 1500,
remote debug mode is 0
```

```
Wed May 17 15:06:52 2006: Successfully added NPU Entry for AP 00:0b:85:51:5a:e0(index 51)
Switch IP: 172.16.1.51, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 192.168.1.5, AP
Port: 5550, next hop MAC: 00:d0:58:ad:ae:cb
Wed May 17 15:06:52 2006: Successfully transmission of LWAPP Join-Reply to AP
00:0b:85:51:5a:e0
Wed May 17 15:06:52 2006: Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 0
Wed May 17 15:06:52 2006: Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 1
Wed May 17 15:06:54 2006: Received LWAPP CONFIGURE REQUEST from AP 00:0b:85:51:5a:e0 to
00:0b:85:33:84:a0
Wed May 17 15:06:54 2006: Updating IP info for AP 00:0b:85:51:5a:e0 -- static 1,
192.168.1.5/255.255.255.0, gtw 192.168.1.1
```

Troubleshoot

Use esta sección para resolver problemas de configuración.

Comandos para resolución de problemas

Puede utilizar estos comandos **debug** para resolver problemas de la configuración.

Nota: Consulte [Información Importante sobre Comandos Debug](#) antes de utilizar los comandos **debug**.

- **debug lwapp events enable**—Muestra la secuencia de eventos que ocurren entre el LAP y el WLC.
- **debug lwapp errors enable**—Muestra los errores que ocurren en la comunicación LWAPP.
- **debug lwapp packet enable**—Muestra el debug de un seguimiento de paquetes LWAPP.
- **debug mac addr:** habilita la depuración MAC para el cliente que se especifica.

Información Relacionada

- [Guía de implementación de REAP en la sucursal](#)
- [Ejemplo de Configuración de Autenticación de EAP con Controladores de WLAN \(WLC\)](#)
- [Ejemplo de la configuración básica del controlador y del Lightweight Access Point del Wireless LAN](#)
- [Ejemplo de Configuración de Failover del Controlador WLAN para Puntos de Acceso Ligeros](#)
- [Página de Soporte de Red Inalámbrica](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).