

# Wired Equivalent Privacy (WEP) en el ejemplo de la configuración de las puntas y de los puentes de acceso Aironet

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configure el WEP en las puntas de acceso Aironet](#)

[Puntas de acceso Aironet que se ejecutan sistema operativo VxWorks](#)

[Configuraciones de VxWorks](#)

[Aironet APs que funciona con el software del Cisco IOS](#)

[Configure los puentes de Aironet](#)

[Configuraciones de VxWorks](#)

[Configure los adaptadores del cliente](#)

[Fije las claves WEP](#)

[Active el WEP](#)

[Configure los puentes del grupo de trabajo](#)

[Configuración](#)

[Información Relacionada](#)

## Introducción

Este documento proporciona métodos para configurar Wired Equivalent Privacy (WEP) en componentes Cisco Aironet Wireless LAN (WLAN).

**Nota:** Refiera a la sección [estática de las claves de la red del capítulo 6 - configurar las redes inalámbricas \(WLAN\)](#) para más información sobre la configuración WEP en los reguladores inalámbricos LAN (WLCs).

El WEP es el algoritmo de encriptación incorporado al estándar del 802.11 (Wi-Fi). La encriptación WEP utiliza la cifra de secuencia del código 4 del Ron (RC4) con 40- o las claves del 104-bit y 24-bit un vector de inicialización (iv).

Mientras que el estándar especifica, el WEP utiliza el algoritmo RC4 con una clave 40-bit o del 104-bit y un 24-bit IV. RC4 es un algoritmo simétrico porque utiliza la misma clave para el cifrado y el desciframiento de los datos. Cuando se activa el WEP, cada "estación de radio" tiene una clave. La clave se utiliza para codificar los datos antes de la transmisión de estos a través de las ondas. Si una estación recibe un paquete que no se revuelva con la clave apropiada, el paquete

se desecha y nunca se entrega al host.

El WEP se puede utilizar sobre todo para una oficina en el hogar o una oficina pequeña que no requiera mismo la fuerte seguridad.

La implementación WEP de Aironet está en la dotación física. Por lo tanto, el efecto de rendimiento mínimo resulta cuando usted utiliza el WEP.

**Nota:** Hay algunos problemas conocidos con el WEP, que le hace no un método de encriptación fuerte. Los problemas son:

- Hay mucho consumo de recursos gasto administrativo para mantener una clave WEP compartida.
- El WEP tiene el mismo problema que todos los sistemas basados en las claves compartidas. Cualquier secreto dado a una persona llega a ser público después de un período de tiempo.
- El IV que siembra el algoritmo WEP se envía en el texto claro.
- La suma de comprobación WEP es Lineal y fiable.

El Temporal Key Integrity Protocol (TKIP) se ha creado para abordar estos problemas WEP. Similar al WEP, el TKIP utiliza el cifrado RC4. Sin embargo, el TKIP aumenta el WEP agregando las medidas tales como rotación dominante del Troceo clave del por-paquete, del control de la Integridad del mensaje (MIC), y de la difusión para dirigir las vulnerabilidades conocidas del WEP. El TKIP utiliza la cifra de secuencia RC4 con las claves del 128-bit para el cifrado y las claves 64-bit para la autenticación.

## prerrequisitos

### Requisitos

Este documento asume que usted puede hacer una conexión administrativa a los dispositivos de la red inalámbrica (WLAN) y que los dispositivos funcionan normalmente en un entorno sin encriptación.

Para configurar 40-bit estándar WEP, usted debe tener dos o más unidades de radio que comunican con uno a.

**Nota:** Los Productos de Aironet pueden establecer las conexiones WEP 40-bit con los Productos de IEEE 802.11b-compliant no-Cisco. Este documento no dirige la configuración de los otros dispositivos.

Para la creación de un link del 128-bit WEP, los Productos Cisco obran recíprocamente solamente con los otros productos de Cisco.

### Componentes Utilizados

Utilice estos componentes con este documento:

- Dos o más unidades de radio que comunican con uno a
- Una conexión administrativa al dispositivo de la red inalámbrica (WLAN)

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.

## [Convenciones](#)

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

## [Configure el WEP en las puntas de acceso Aironet](#)

### [Puntas de acceso Aironet que se ejecutan sistema operativo VxWorks](#)

Complete estos pasos:

1. Haga una conexión al punto de acceso.
2. Navegue al menú de encriptación de Radio AP. Utilice una de estas trayectorias: **Summary Status (Estado de resumen) > Setup (Configuración) > encriptación de datos del >Radio de la radio/de la dotación física AP (WEP) > encriptación de datos de radio AP> Security Setup (Configuración de seguridad) del > Security (Seguridad) del Summary Status (Estado de resumen) > Setup (Configuración): Encriptación de datos de radio (WEP) > encriptación de datos de la radio AP**  
**Nota:** Para realizar los cambios a esta página, usted debe ser administrador con la identidad y escribir las capacidades. **Opinión del buscador Web del menú de encriptación de datos de la radio AP**

AP340-258b25 **AP Radio Data Encryption**


Cisco AP340
Uptime: 00:44:41

Map Help

Use of Data Encryption by Stations is: No Encryption

Accept Authentication Types:  Open  Shared Key

	Transmit With Key	Encryption Key	Key Size
WEP Key 1:	<input checked="" type="radio"/>		40 bit
WEP Key 2:	-		not set
WEP Key 3:	<input type="radio"/>		40 bit
WEP Key 4:	<input type="radio"/>		128 bit

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).  
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).  
This radio supports Encryption for all Data Rates.

Apply
OK
Cancel
Restore Defaults

[Map][Login][Help]

Cisco AP340
© Copyright 2000 Cisco Systems, Inc.
credits

## Configuraciones de VxWorks

La página de la encriptación de datos de la radio AP presenta una variedad de opciones para utilizar. Algunas opciones son obligatorias para el WEP. Esta sección observa estas opciones obligatorias. Las otras opciones no son necesarias para que el WEP funcione, sino que se recomiendan.

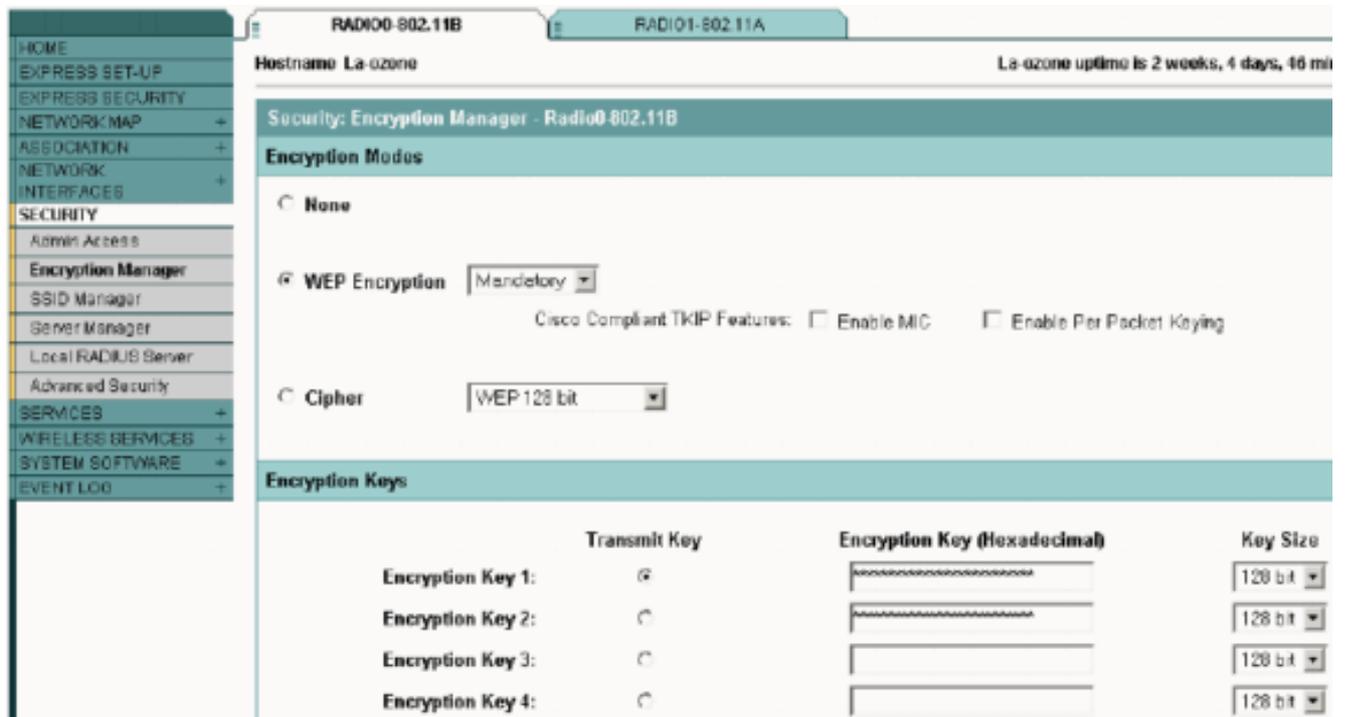
- El uso de la encriptación de datos por las estaciones es:** Utilice esta determinación para elegir si los clientes deben utilizar la encriptación de datos cuando comunican con el AP. El menú desplegable enumera tres opciones:
  - Ningún cifrado (valor por defecto)** — Requiere a los clientes comunicar con el AP sin ninguna encriptación de datos. Esta configuración no se recomienda.
  - Opcional** — Permite al cliente a comunicar con el AP cualquier con o sin la encriptación de datos. Típicamente, usted utiliza esta opción cuando usted tiene dispositivos cliente que no puedan hacer una conexión WEP, tal como clientes de no-Cisco en un entorno del 128-bit WEP.
  - Encriptación completa (RECOMENDADA)** — Requiere a los clientes utilizar la encriptación de datos cuando comunican con el AP. No se permite a los clientes que no utilizan la encriptación de datos comunicar. Se recomienda esta opción si usted desea maximizar la Seguridad de su red inalámbrica (WLAN).**Nota:** Usted debe fijar una clave WEP antes de que usted active el uso del cifrado. Vea la sección **(OBLIGATORIA) de la clave de encriptación de esta lista.**

- **Valide los tipos de la autenticación** Usted puede elegir abierto, la clave compartida, o ambas opciones para fijar las autenticaciones que el AP reconocerá. **Ábrase (RECOMENDADO)** — Esta configuración por defecto permite que cualquier dispositivo, sin importar sus claves WEP, autentique e intente asociarse. **Clave compartida** — Esta configuración dice el AP enviar un sólo texto, consulta de clave compartida a cualquier dispositivo que intente asociarse al AP. **Nota:** Esta interrogación puede salir del AP abierto a un ataque de texto conocido de los intrusos. Por lo tanto, esta configuración no es tan segura como la configuración abierta.
- **Transmita con la clave** Estos botones permiten que usted seleccione la clave que el AP utiliza durante la Transmisión de datos. Usted puede seleccionar solamente una clave al mismo tiempo. Cualquiera o todo el de las claves del conjunto puede ser utilizado para recibir los datos. Usted debe fijar la clave antes de que usted la especifique como la clave de transmitir.
- **Clave de encriptación (OBLIGATORIA)** Estos campos permiten que usted ingrese las claves WEP. Ingrese 10 dígitos hexadecimales para las claves WEP 40-bit o 26 dígitos hexadecimales para las claves WEP del 128-bit. Las claves pueden ser cualquier combinación de estos dígitos: 0 a 9a fA a F Para proteger la Seguridad de la clave WEP, las claves WEP existentes no aparecen en el sólo texto en los campos de entrada. En las versiones recientes de los APs, usted puede suprimir las claves existentes. Sin embargo, usted no puede corregir las claves existentes. **Nota:** Usted debe poner las claves WEP para su red, APs, y dispositivos cliente de la misma manera. Por ejemplo, si usted fija la clave WEP 3 en su AP a 0987654321 y selecciona esta clave como la clave activa, usted debe también fijar la clave WEP 3 en el dispositivo cliente al mismo valor.
- **Tamaño de clave (OBLIGATORIO)** Esta configuración fija las claves a 40-bit o al 128-bit WEP. Si el “no establecido” aparece para esta selección, la clave no se fija. **Nota:** Usted no puede suprimir una clave seleccionando el “no establecido”.
- **Botones de acción** Cuatro configuraciones del control de los botones de acción. Si el Javascript se activa en su buscador Web, una ventana de la ventana emergente de confirmación aparece después de que usted haga clic cualquier botón, excepto la cancelación. **Aplíquese** — Este botón activa las nuevas configuraciones del valor. Sigue habiendo el navegador en la página. **AUTORIZACIÓN** — Este botón aplica las nuevas configuraciones y mueve al navegador de nuevo a la página de configuración principal. **Cancelación** — Este botón cancela los cambios de la configuración y vuelve las configuraciones previamente a los valores almacenados. Usted entonces vuelve a la página de configuración principal. **Valores por defecto del Restore** — Este botón cambia todas las configuraciones en esta página de nuevo a las configuraciones por defecto de la fábrica.

**Nota:** En las versiones recientes de Cisco IOS® de los APs, del control solamente los botones de la **aplicación** y de la **cancelación** están disponibles para esta página.

**Vista del emulador de terminal del menú de encriptación de datos**





## [Configure los puentes de Aironet](#)

Si usted utiliza VxWorks, complete estos pasos:

1. Haga una conexión al puente.
2. Navegue al menú de la aislamiento. Elija el **>Radio del menú principal > de la configuración > el > Privacy (Privacidad) I80211**. Los controles menu de la aislamiento el uso del cifrado en el paquete de datos que es transmitido sobre el aire por las radios. El algoritmo RSA RC4 y el que está de hasta cuatro claves sabidas se utilizan para cifrar los paquetes. Cada nodo en la celda de radio debe conocer todas las claves funcionando, pero las claves unas de los se pueden seleccionar para transmitir los datos. **Vista del emulador de terminal del menú de la aislamiento**

```

Configuration Radio I80211 Privacy Menu
Option          Value      Description
1 - Encryption  [ off ]  - Encrypt radio packets
2 - Auth        [ open ] - Authentication mode
3 - Client      [ open ] - Client authentication modes allowed
4 - Key
5 - Transmit
Enter an option number or name, "=" main menu, <ESC> previous menu
>_

```

Refiera a [configurar las habitaciones de la cifra y el WEP - puente de las 1300 Series](#) y [configurar las características WEP y WEP - puente de las 1400 Series](#) para la información sobre cómo configurar el WEP en 1300 y los puentes de las 1400 Series a través del modo CLI.

Para utilizar el GUI para configurar los puentes de las 1300 y 1400 Series, complete el mismo procedimiento explicado en el [Aironet APs que funcionan con la sección del software del Cisco IOS de](#) este documento.

## [Configuraciones de VxWorks](#)

El menú de la aislamiento presenta un conjunto de opciones que usted deba configurar. Algunas opciones son obligatorias para el WEP. Esta sección observa estas opciones obligatorias. Las otras opciones no son necesarias para que el WEP funcione, sino que se recomiendan.

Esta sección presenta las opciones de menú en la orden que aparecen en la [vista del emulador de terminal del menú de la aislamiento](#). Sin embargo, configure las opciones en esta orden:

1. Clave
2. Transmita
3. Auténtico
4. Cliente
5. Cifrado

La configuración en esta orden se asegura de que las condiciones previas necesarias estén puestas mientras que usted configura cada configuración.

Éstas son las opciones:

- **Clave (OBLIGATORIA)** La opción de la clave programa las claves de encriptación en el puente. Le incitan fijar una de las cuatro claves. Le incitan dos veces ingresar la clave. Para definir la clave, usted debe ingresar 10 o 26 dígitos hexadecimales, que depende encendido si la configuración del puente está para las claves 40-bit o del 128-bit. Utilice cualquier combinación de estos dígitos: 0 a 9a fA a FLas claves deben corresponder con en **todos los** Nodos en la celda de radio, y usted debe ingresar las claves en la misma orden. Usted no necesita definir las cuatro claves, mientras el número de claves haga juego en cada dispositivo en la red inalámbrica (WLAN).
- **Transmita** La opción del transmitir dice a radio qué claves a utilizar para transmitir los paquetes. Cada radio puede descifrar los paquetes recibidos que se envían con las cuatro claves unas de los.
- **Auténtico** Usted utiliza opción Auth (Autenticación) encendido los puentes del repetidor para determinar qué modo de autenticación utiliza la unidad para conectar con su padre. Los valores permitidos son abiertos o clave compartida. El protocolo del 802.11 especifica un procedimiento en el cual un cliente deba autenticar con un padre antes de que el cliente pueda asociarse. **Ábrase (RECOMENDADO)** — Este modo de autenticación es esencialmente un funcionamiento nulo. Se permite a todos los clientes autenticar. **Clave compartida** — Este modo permite que el padre envíe el cliente un texto del desafío, que el cliente cifra y vuelve al padre. Si el padre descifra con éxito el texto del desafío, autentican al cliente. **Precaución:** No utilice el modo de la clave compartida. Cuando usted lo utiliza, un sólo texto y una versión cifrada de los mismos datos transmite en el aire. Esto no gana cualquier cosa. Si la clave del usuario es incorrecta, la unidad no descifra los paquetes, y los paquetes no pueden acceder a la red.
- **Cliente** La opción Cliente determina el modo de autenticación que los nodos del cliente utilizan para asociar a la unidad. Éstos son los valores se permiten que: **Ábrase (RECOMENDADO)** — Este modo de autenticación es esencialmente un funcionamiento nulo. Se permite a todos los clientes autenticar. **Clave compartida** — Este modo permite que el padre envíe el cliente un texto del desafío, que el cliente cifra y vuelve al padre. Si el padre descifra con éxito el texto del desafío, autentican al cliente. **Ambos** — Este modo permite que el cliente utilice cualquier modo.
- **Cifrado** De — Si usted fija la opción de encriptación a apagado, no se hace ningún cifrado. Los datos transmiten en el claro. **En (OBLIGATORIO)** — Si usted fija la opción de encriptación a

encendido, se cifran todos los paquetes de datos transmitidos y se desecha cualquier paquete recibido unencrypted. **Mezclado** — En el modo mezclado, un puente de la raíz o del repetidor valida la asociación de los clientes que tienen cifrado dado vuelta cualquiera con./desc. En este caso, solamente los paquetes de datos entre los Nodos que ambos utilizan se cifran. Los paquetes de multidifusión se envían en el claro. Todos los Nodos pueden considerar los paquetes. **Precaución:** No utilice el modo mezclado. Si un cliente que hace el cifrado activar envía un paquete de multidifusión a su padre, se cifra el paquete. El padre descifra el paquete y retransmite el paquete en el claro a la célula, y otros Nodos pueden considerar el paquete. La capacidad de ver un paquete en ambos forma encriptada o no encriptada puede contribuir a romper una clave. La inclusión del modo mezclado está solamente para la compatibilidad con los otros vendedores.

## Configure los adaptadores del cliente

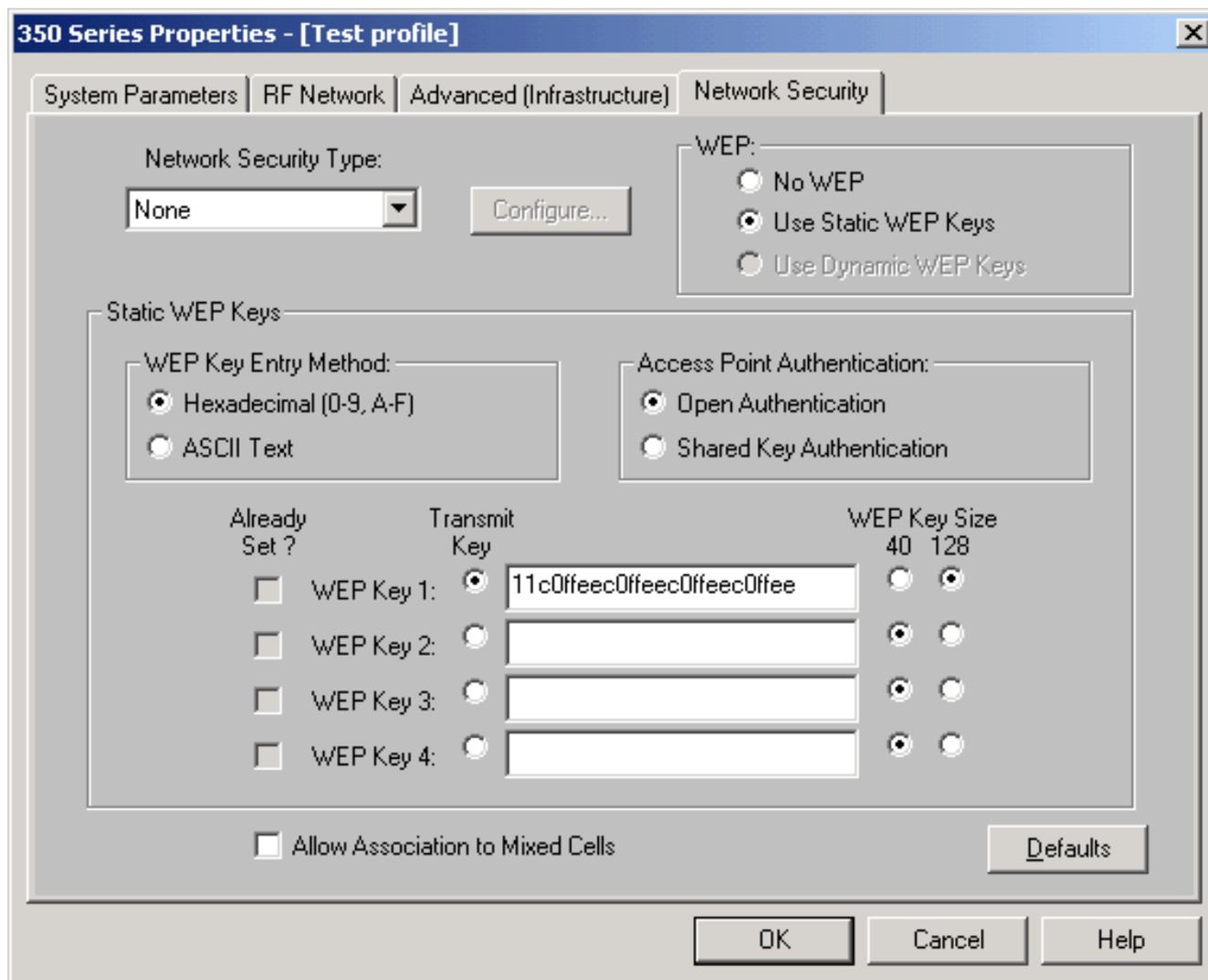
Usted debe completar dos pasos principales para poner el WEP en el adaptador del cliente de Aironet:

1. Configure la clave WEP/las claves en el encargado del cifrado del cliente.
2. Active el WEP en la utilidad de cliente de Aironet (ACU).

## Fije las claves WEP

Complete estos pasos para poner las claves WEP en los adaptadores del cliente:

1. Abra el ACU y elija al **encargado del perfil**.
2. Elija el perfil donde usted quiere activar el WEP y el tecleo **corrige**.
3. Haga clic la **ficha de seguridad de la red** para visualizar las opciones de seguridad, y haga clic las **claves del WEP estático del uso**. Esta acción activa las opciones de configuración WEP se amortiguan que cuando no se selecciona ningún WEP.



4. Para la clave WEP que usted quiere crear, elija **40** bits o **128** bajo el tamaño de la clave WEP a la derecha de la ventana. **Nota:** los adaptadores del cliente del 128-bit pueden utilizar las claves 40-bit o del 128-bit. Pero los adaptadores 40-bit pueden utilizar solamente las claves 40-bit. **Nota:** Su clave WEP del adaptador del cliente debe hacer juego la clave WEP que los otros componentes de la red inalámbrica (WLAN) con los cuales usted comunica el uso. Cuando usted fija más de una clave WEP, usted debe asignar las claves WEP a los mismos números de la clave WEP para todos los dispositivos. Las claves WEP se deben comprender de los caracteres hexadecimales y deben contener 10 caracteres para las claves WEP 40-bit o 26 caracteres para las claves WEP del 128-bit. Los caracteres hexadecimales pueden ser: 0 a 9a fA a F. **Nota:** Las claves WEP del texto ASCII no se utilizan en el Aironet APs. Por lo tanto, usted debe elegir (0-9, A-F) la opción hexadecimal si usted planea utilizar su adaptador del cliente con estos APs. **Nota:** Después de que usted cree la clave WEP, usted puede escribir sobre ella. Pero usted no puede corregirla o suprimirla. **Nota:** Si usted utiliza una versión posterior de utilidad Aironet Desktop (ADU) en vez del ACU como utilidad de cliente, usted puede también suprimir la clave WEP creada y sustituirla por un nuevo.
5. Haga clic el botón de la **clave de transmitir** que está al lado de una de las claves que usted creó. Con esta acción, usted indica que esta clave es la clave que usted quiere utilizar para transmitir los paquetes.
6. Tipo bajo **persistente de la clave WEP** del teclado. Esta acción permite que su adaptador del cliente conserve esta clave WEP, incluso cuando la potencia al adaptador se quita o en la reinicialización del ordenador en el cual la clave está instalada. Si usted elige temporal para

esta opción, se pierde la clave WEP cuando la potencia se quita de su adaptador del cliente.  
7. Click OK.

## Permiso WEP

Complete estos pasos:

1. Abra el ACU y elija **corrija las propiedades de la barra de menú**.
2. Haga clic la **ficha de seguridad de la red** para visualizar las opciones de seguridad.
3. Controle el **permiso Casilla de verificación WEP** para activar el WEP.

Refiera a [configurar el WEP en el ADU](#) para que los pasos configuren el WEP usando el ADU como utilidad de cliente.

## Configure los puentes del grupo de trabajo

Hay diferencias entre el puente del grupo de trabajo de las 340 Series de Aironet y el puente de las 340 Series de Aironet. Sin embargo, la configuración del puente del grupo de trabajo para utilizar el WEP es casi idéntica a la configuración del puente. Vea la sección de los [puentes de Aironet del configurar](#) para la configuración del puente.

1. Conecte con el puente del grupo de trabajo.
2. Navegue al menú de la aislamiento. Elija **Main > Configuration > Radio > el > Privacy (Privacidad) I80211** para tener acceso al menú de VxWorks de la aislamiento.

## Configuración

El menú de la aislamiento presenta a configuraciones las listas de esa esta sección. Configure las opciones en el puente del grupo de trabajo en esta orden:

1. Clave
2. Transmita
3. Auténtico
4. Cifrado

Éstas son las opciones:

- **Clave**La opción dominante establece la clave WEP que las aplicaciones del puente para recibir los paquetes. El valor debe hacer juego la clave que el AP o el otro dispositivo con los cuales el puente del grupo de trabajo comunica las aplicaciones. La clave consiste en hasta 10 caracteres hexadecimales para el cifrado 40-bit o 26 caracteres hexadecimales para el cifrado del 128-bit. Los caracteres hexadecimales pueden ser cualquier combinación de estos dígitos: 0 a 9a fA a F
- **Transmita**La opción del transmitir establece la clave WEP que las aplicaciones del puente para transmitir los paquetes. Usted puede elegir para utilizar la misma clave que usted utilizó para la opción dominante. Si usted elige una diversa clave, usted debe establecer una clave que corresponde con en el AP. Solamente una clave WEP se puede utilizar al mismo tiempo para las transmisiones. La clave WEP que usted utiliza para transmitir los datos se debe fijar al mismo valor en su puente y otros dispositivos del grupo de trabajo con los cuales comunique.

- **Autenticación (auténtica)** El parámetro Auth determina qué método de autenticación utiliza el sistema. Las opciones son: **Ábrase (RECOMENDADO)** — La configuración abierta del valor por defecto permite que cualquier AP, sin importar sus configuraciones de WEP, autentique y después intente comunicar con el puente. **Clave compartida** — Esta configuración da instrucciones al puente para enviar un sólo texto, consulta de clave compartida a los APs en un intento por comunicar con el puente. La configuración de clave compartida puede salir del puente abierto a un ataque de texto conocido de los intrusos. Por lo tanto, esta configuración no es tan segura como la configuración abierta.
- **Cifrado** La opción de encriptación fija los parámetros de encriptación en todos los paquetes de datos, excepto los paquetes de asociación y algunos paquetes de control. Hay cuatro opciones: **Nota:** El AP debe tener el cifrado activo y una clave fijada correctamente. **De** — Ésta es la configuración por defecto. Se apaga todo el cifrado. El puente del grupo de trabajo no comunica con un AP con el uso del WEP. **En (RECOMENDADO)** — Esta configuración requiere el cifrado de todas las Transferencias de datos. El puente del grupo de trabajo comunica solamente con los APs que utilizan el WEP. **Mezclado encendido** — Esta configuración significa que el puente utiliza siempre el WEP para comunicar con el AP. Sin embargo, el AP comunica con todos los dispositivos, si utilizan el WEP o no utilizan el WEP. **Mezclado apagado** — Esta configuración significa que el puente no utiliza el WEP para comunicar con el AP. Sin embargo, el AP comunica con todos los dispositivos, si utilizan el WEP o no utilizan el WEP. **Precaución:** Si usted selecciona encendido o mezclado encendido mientras que la categoría WEP y usted configuran el puente a través de su link de radio, la Conectividad al puente se pierde si usted fija la clave WEP incorrectamente. Asegúrese de que usted utilice exactamente las mismas configuraciones cuando usted fija la clave WEP en el puente del grupo de trabajo y la clave WEP en los otros dispositivos en su red inalámbrica (WLAN).

## Información Relacionada

- [Asociación de los estándares de IEEE](#)
- [Productos de Lan de la serie inalámbrica Aironet 340](#)
- [Recursos de Soporte de Red Inalámbrica](#)
- [Página de soporte de LAN inalámbrica](#)
- [Guía de configuración de software del Cisco IOS para las puntas de acceso Aironet de Cisco](#)
- [Guía de configuración de software del Cisco IOS para el Punto de acceso al aire libre/puente del Cisco Aironet de la serie 1300](#)
- [Guía de configuración de software de la punta de acceso Aironet de Cisco para VxWorks](#)
- [Guía de configuración de software del puente del Cisco Aironet de la serie 1400](#)
- [Guías de configuración del Cisco Aironet Wireless LAN Client Adapters](#)
- [Descripción inalámbrica de la Seguridad de LAN de Cisco](#)
- [Tecnología inalámbrica \(movilidad\) que asegura las redes inalámbricas](#)
- [Ejemplo de Configuración de Punto de Acceso como Bridge de Grupo de Trabajo](#)
- [Preguntas Frecuentes sobre el Bridge del Grupo de Trabajo Cisco Aironet](#)
- [Procedimiento de recuperación de contraseña para el equipo Aironet de Cisco](#)
- [FAQ de la punta de acceso Aironet de Cisco](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)