Configuración de WEP en puntos de acceso y puentes Aironet

Contenido

Introducción

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

Nota: Refiérase a la sección Claves Web Estáticas del Capítulo 6 - Configuración de WLAN para obtener más información sobre la configuración WEP en los controladores de LAN inalámbrica (WLC).

WEP es el algoritmo de cifrado incorporado en el estándar 802.11 (Wi-Fi). La encriptación WEP utiliza el cifrado de flujo de código 4 (RC4) de Ron con claves de 40 o 104 bits y un vector de inicialización de 24 bits (IV).

Como especifica el estándar, WEP utiliza el algoritmo RC4 con una clave de 40 o 104 bits y una IV de 24 bits. RC4 es un algoritmo simétrico porque utiliza la misma clave para el cifrado y el descifrado de datos. Cuando se habilita 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 está codificado con la clave apropiada, el paquete se descarta y nunca se entrega al host.

WEP se puede utilizar principalmente para oficinas domésticas o pequeñas oficinas que no requieren una seguridad muy segura.

La implementación de Aironet WEP está en el hardware. Por lo tanto, el impacto de rendimiento mínimo se produce cuando se utiliza WEP.

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

- Hay una gran cantidad de gastos administrativos para mantener una clave WEP compartida.
- WEP tiene el mismo problema que todos los sistemas basados en claves compartidas. Cualquier secreto que se dé a una persona se hace público después de un período de tiempo.
- La IV que semilla el algoritmo WEP se envía en texto claro.
- La suma de comprobación WEP es lineal y predecible.

Se ha creado el protocolo de integridad de clave temporal (TKIP) para solucionar estos problemas WEP. Al igual que WEP, TKIP utiliza cifrado RC4. Sin embargo, TKIP mejora WEP al agregar medidas como el hash de clave por paquete, la verificación de integridad del mensaje (MIC) y la rotación de clave de difusión para abordar las vulnerabilidades conocidas de WEP. TKIP utiliza el cifrado de flujo RC4 con claves de 128 bits para el cifrado y claves de 64 bits para la autenticación.

Prerequisites

Requirements

Este documento asume que puede realizar una conexión administrativa a los dispositivos WLAN y que los dispositivos funcionan normalmente en un entorno no cifrado.

Para configurar el WEP estándar de 40 bits, debe tener dos o más unidades de radio que se comuniquen entre sí.

Nota: Los productos Aironet pueden establecer conexiones WEP de 40 bits con productos de Cisco no conformes con IEEE 802.11b. Este documento no aborda la configuración de otros dispositivos.

Para la creación de un enlace WEP de 128 bits, los productos de Cisco solo interactúan con otros productos de Cisco.

Componentes Utilizados

Utilice estos componentes con este documento:

- Dos o más unidades de radio que se comunican entre sí
- Una conexión administrativa al dispositivo WLAN

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

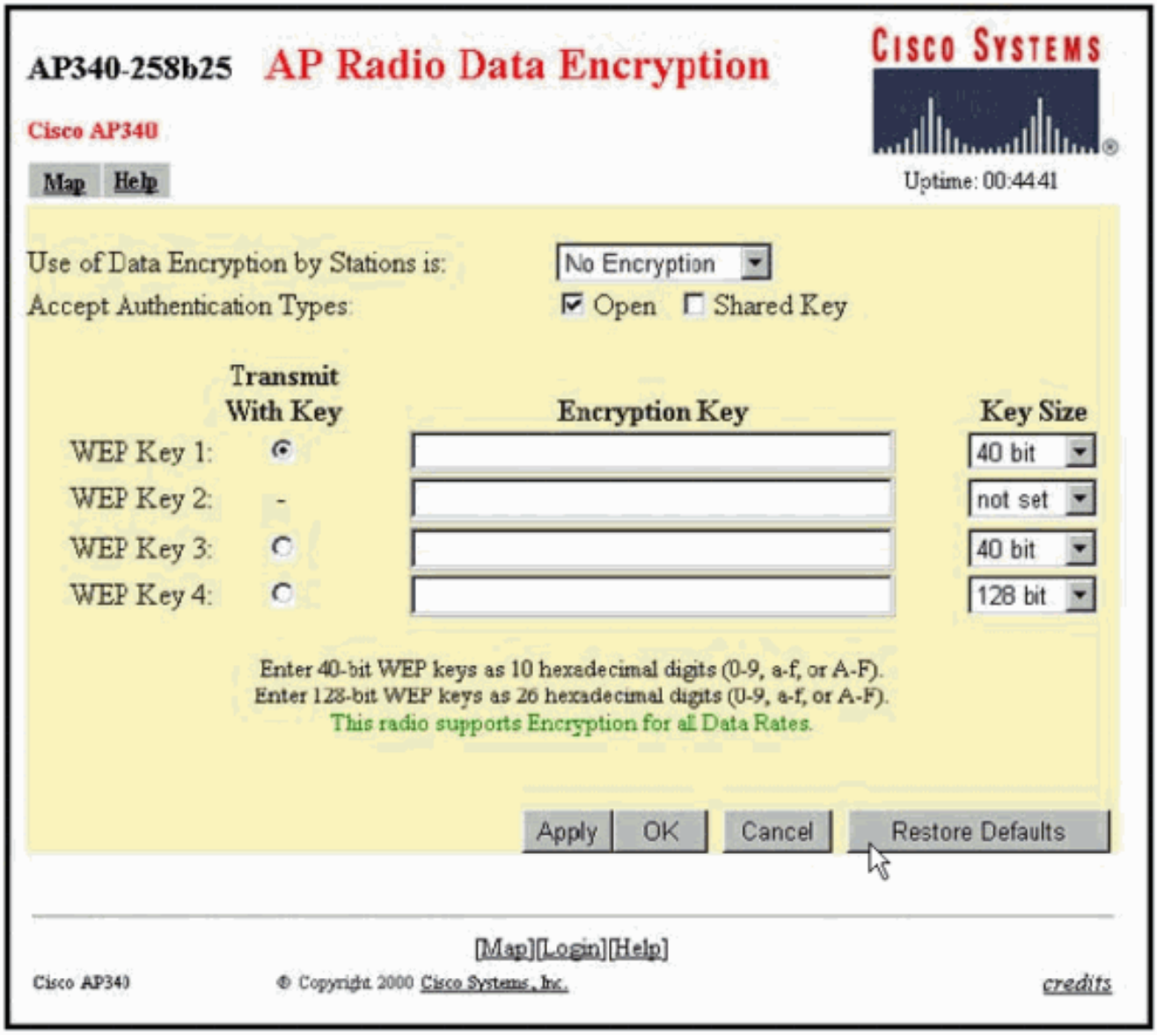
Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Configuración de WEP en puntos de acceso Aironet

Puntos De Acceso Aironet Que Ejecutan El Sistema Operativo VxWorks

Complete estos pasos:

1. Realice una conexión al punto de acceso (AP).
2. Navegue hasta el menú AP Radio Encryption .Utilice una de estas trayectorias:**Summary Status > Setup > AP Radio/Hardware > Radio Data Encryption (WEP) > AP Radio Data EncryptionSummary Status > Setup > Security > Security Setup: Cifrado de datos de radio (WEP) > Cifrado de datos de radio APNota:** Para realizar cambios en esta página, debe ser un administrador con funciones de identidad y escritura.**Vista del explorador de Internet del menú Data Encryption (Cifrado de datos)**



Configuración de VxWorks

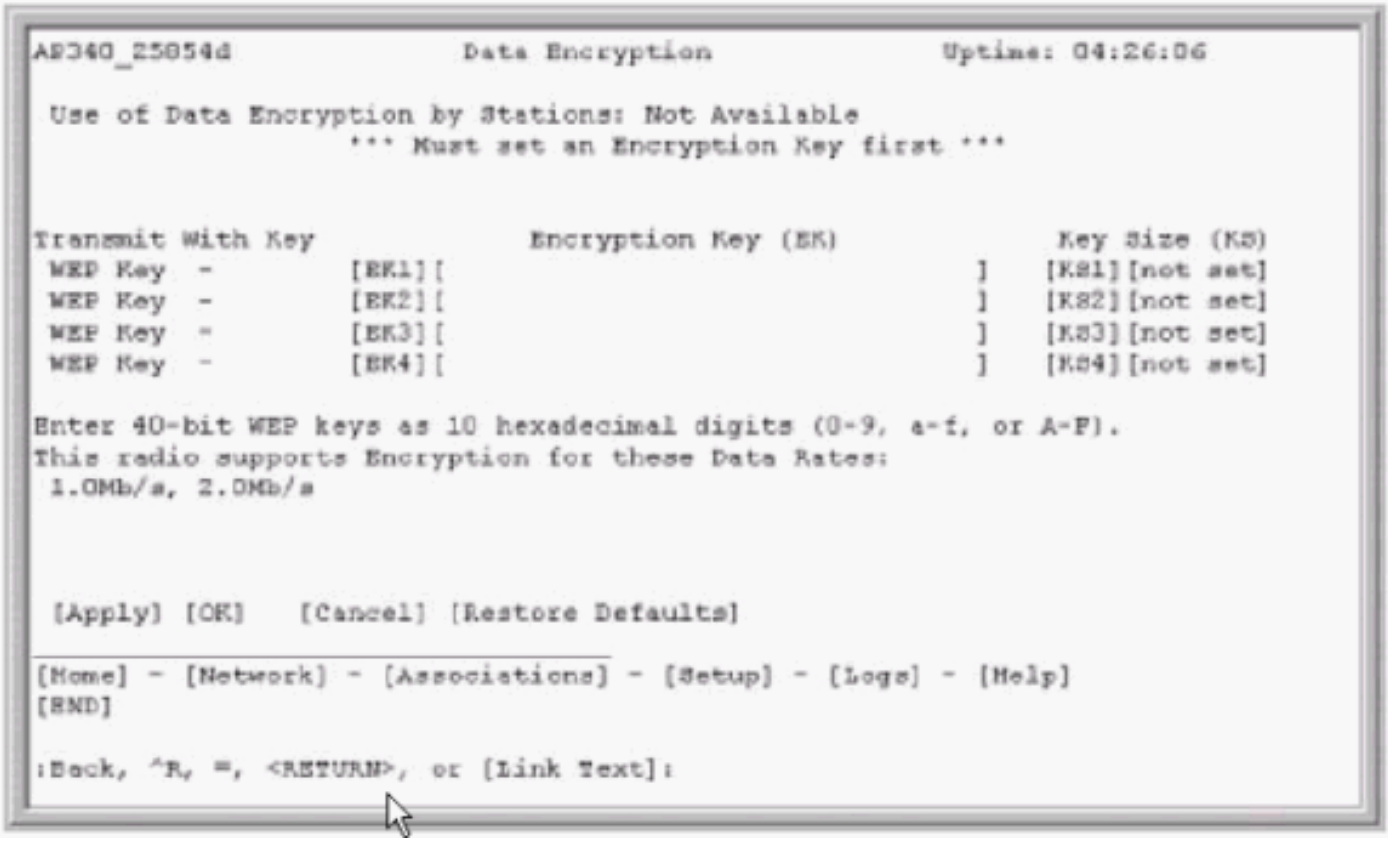
La página AP Radio Data Encryption (Encriptación de datos de radio AP) presenta una variedad de opciones para utilizar. Algunas opciones son obligatorias para WEP. En esta sección se señalan estas opciones obligatorias. No son necesarias otras opciones para que WEP funcione, pero se recomiendan.

- **El uso de encripción de información por estaciones es:**Utilice esta configuración para elegir si los clientes deben utilizar el cifrado de datos cuando se comunican con el AP. El menú desplegable muestra tres opciones:**Sin cifrado (valor predeterminado)**: requiere que los clientes se comuniquen con el AP sin ningún cifrado de datos. No se recomienda esta configuración.**Opcional**: permite a los clientes comunicarse con el AP con o sin el cifrado de datos. Normalmente, se utiliza esta opción cuando hay dispositivos cliente que no pueden realizar una conexión WEP, como los clientes que no son de Cisco en un entorno WEP de 128 bits.**Cifrado completo (RECOMENDADO)**: requiere que los clientes utilicen el cifrado de datos cuando se comunican con el AP. Los clientes que no utilizan el cifrado de datos no pueden comunicarse. Esta opción se recomienda si desea maximizar la seguridad de su WLAN.**Nota:** Debe establecer una clave WEP antes de habilitar el uso de cifrado. Consulte la sección **Clave de cifrado (OBLIGATORIA)** de esta lista.
- **Aceptación de los tipos de autenticación**Puede elegir Open (Abrir), Shared Key (Clave compartida) o ambas opciones para establecer las autenticaciones que el AP reconocerá.**Abrir (RECOMENDADO)**: esta configuración predeterminada permite que cualquier dispositivo, independientemente de sus claves WEP, se autentique e intente asociarse.**Clave compartida**: esta configuración indica al AP que envíe una consulta de clave compartida de texto sin formato a cualquier dispositivo que intente asociarse con el AP.**Nota:** Esta consulta puede dejar el AP abierto a un ataque de texto conocido de intrusos. Por lo tanto, esta configuración no es tan segura como la opción Abrir.
- **Transmitir con clave**Estos botones le permiten seleccionar la clave que el AP utiliza durante la transmisión de datos. Sólo puede seleccionar una clave a la vez. Se puede utilizar cualquiera o todas las teclas definidas para recibir datos. Debe establecer la clave antes de especificarla como la clave de transmisión.
- **Clave de encripción (OBLIGATORIA).**Estos campos permiten introducir las claves WEP. Introduzca 10 dígitos hexadecimales para las claves WEP de 40 bits o 26 dígitos hexadecimales para las claves WEP de 128 bits. Las teclas pueden ser cualquier combinación de estos dígitos:0 a 9a fA a FPara proteger la seguridad de la clave WEP, las claves WEP existentes no aparecen en texto sin formato en los campos de entrada. En las versiones recientes de los AP, puede eliminar las claves existentes. Sin embargo, no puede editar las claves existentes.**Nota:** Debe configurar las claves WEP para su red, AP y dispositivos cliente exactamente de la misma manera. Por ejemplo, si configura la clave WEP 3 en su AP a 0987654321 y selecciona esta clave como la clave activa, también debe establecer la clave WEP 3 en el dispositivo cliente al mismo valor.
- **Tamaño de clave (obligatorio)**Esta configuración establece las claves en WEP de 40 o 128 bits. Si aparece "not set" para esta selección, la clave no está establecida.**Nota:** No puede eliminar una clave seleccionando "no establecido".
- **botones Action (Acción)**Cuatro botones de acción controlan la configuración. Si JavaScript está activado en el explorador Web, aparecerá una ventana emergente de confirmación después de hacer clic en cualquier botón, excepto en Cancelar.**Aplicar**: este botón activa la nueva configuración de valor. El explorador permanece en la página.**Aceptar**: este botón aplica los nuevos parámetros y devuelve el explorador a la página principal de configuración.**Cancelar**: este botón cancela los cambios de configuración y devuelve la

configuración a los valores almacenados anteriormente. A continuación, volverá a la página de configuración principal.**Restaurar valores predeterminados**: este botón vuelve a cambiar todos los parámetros de esta página a los predeterminados de fábrica.

Nota: En las versiones recientes de Cisco IOS® de los AP, sólo los botones de control **Aplicar** y **Cancelar** están disponibles para esta página.

Vista del emulador de terminal del menú Data Encryption (Cifrado de datos)



Vista del emulador de terminal de la secuencia de configuración de clave WEP (Cisco IOS® Software)

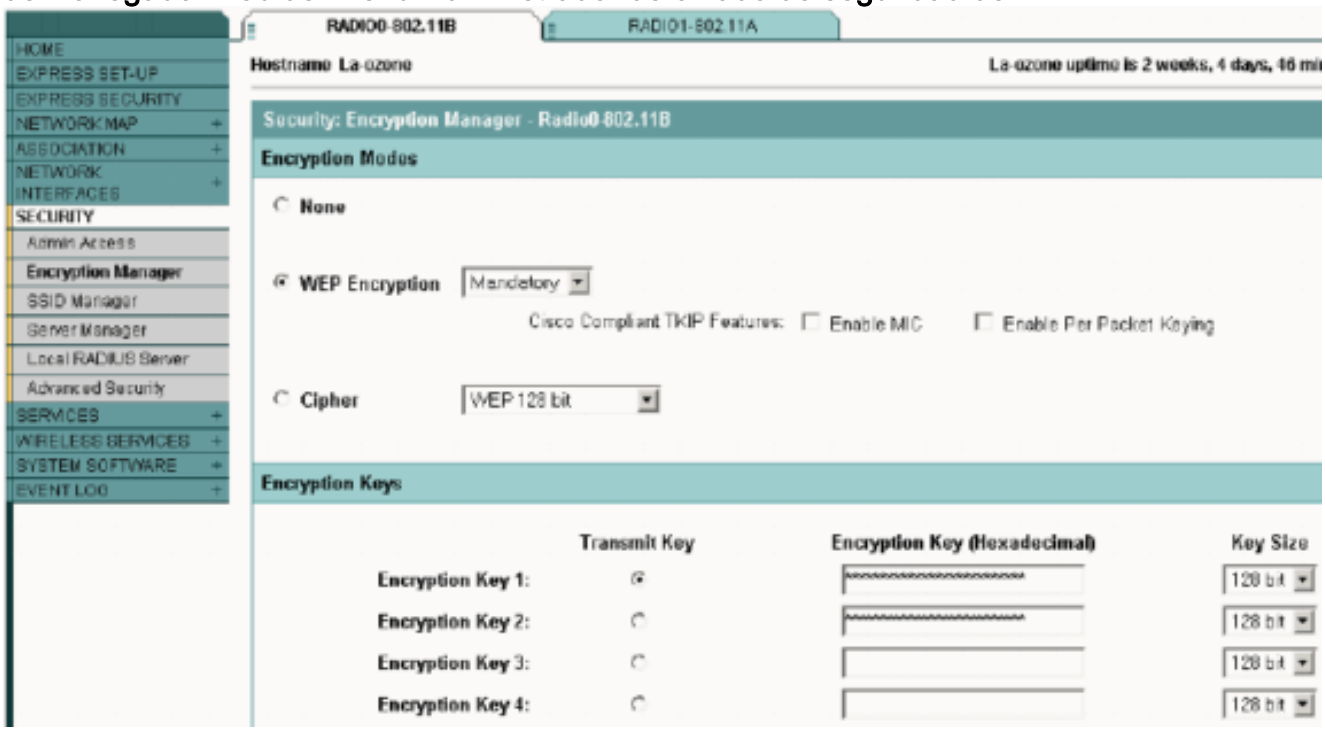
```
La-ozone>
La-ozone>
La-ozone>enable
Password:
La-ozone#
La-ozone#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
La-ozone(config)#interface dot
La-ozone(config)#interface dot11Radio 0
La-ozone(config-if)#encryption key 1 size 128bit 11c0ffeec0ffeec0ffeec0ffee ?
  transmit-key  Set the key as transmit key
  <cr>

La-ozone(config-if)#encryption key 1 size 128bit 11c0ffeec0ffeec0ffeec0ffee transmit-key
La-ozone(config-if)#end
La-ozone#
*Mar 19 00:42:13.893: %SYS-5-CONFIG_I: Configured from console by console
La-ozone#
La-ozone#
```

AP Aironet que Ejecutan Cisco IOS Software

Complete estos pasos:

1. Realice una conexión con el AP.
2. En la opción de menú SECURITY en el lado izquierdo de la ventana, elija **Encryption**

Manager para la interfaz de radio a la que desea configurar las claves WEP estáticas.**Vista del navegador web del menú Administrador de cifrado de seguridad de AP**



Configurar los puentes Aironet

Si utiliza VxWorks, siga estos pasos:

1. Establezca una conexión con el puente.
2. Vaya al menú Privacidad.Elija **Main Menu > Configuration > Radio > I80211 > Privacy**.El menú Privacidad controla el uso del cifrado en el paquete de datos que se transmite por el aire por las radios. El algoritmo RSA RC4 y una de hasta cuatro claves conocidas se utilizan para cifrar los paquetes. Cada nodo de la celda de radio debe conocer todas las claves en uso, pero se puede seleccionar cualquiera de las claves para transmitir los datos.**Vista del emulador de terminal del menú de privacidad**

```
        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                       - Set the keys
5 - Transmit                  - Key number for transmit
 Enter an option number or name, "=" main menu, <ESC> previous menu
>_
```

Consulte Configuración de Conjuntos Cipher y Puente WEP - Serie 1300 y Configuración de Funciones WEP y WEP - Puente Serie 1400 para obtener información sobre cómo configurar WEP en los Bridges Serie 1300 y 1400 a través del modo CLI.

Para utilizar la GUI para configurar los Bridges de las Series 1300 y 1400, complete el mismo procedimiento explicado en la sección Aironet APs que Ejecutan el Cisco IOS Software de este documento.

Configuración de VxWorks

El menú Privacidad presenta un conjunto de opciones que debe configurar. Algunas opciones son obligatorias para WEP. En esta sección se señalan estas opciones obligatorias. No son necesarias otras opciones para que WEP funcione, pero se recomiendan.

Esta sección presenta las opciones del menú en el orden en que aparecen en la Vista del emulador de terminal del menú de privacidad. Sin embargo, configure las opciones en este orden:

1. Clave
2. Transmitir
3. Autenticación
4. Cliente
5. Cifrado

La configuración en este orden garantiza que se configuran los requisitos previos necesarios a medida que se configura cada parámetro.

Estas son las opciones:

- **Clave (OBLIGATORIO)**La opción Key programa las claves de cifrado en el Bridge. Se le solicita que establezca una de las cuatro claves. Se le solicita dos veces que introduzca la clave. Para definir la clave, debe ingresar 10 ó 26 dígitos hexadecimales, lo que depende de si la configuración de Bridge es para claves de 40 ó 128 bits. Utilice cualquier combinación de estos dígitos:0 a 9a fA a FLas claves deben coincidir en ***todos*** los nodos de la celda de radio, y debe ingresar las claves en el mismo orden. No es necesario definir las cuatro claves, siempre y cuando el número de claves coincida en cada dispositivo de la WLAN.
- **Transmitir**La opción Transmit indica a la radio qué claves se deben utilizar para transmitir paquetes. Cada radio puede descifrar los paquetes recibidos que se envían con cualquiera de las cuatro claves.
- **Autenticación**Utilice la opción Auth en los bridges repetidores para determinar qué modo de autenticación utiliza la unidad para conectarse con su padre. Los valores permitidos son Open (Abrir) o Shared Key (Clave compartida). El protocolo 802.11 especifica un procedimiento en el que un cliente debe autenticarse con un padre antes de que el cliente pueda asociarse.**Abrir (RECOMENDADO)**: este modo de autenticación es esencialmente una operación nula. Todos los clientes pueden autenticarse.**Clave compartida**: este modo permite que el padre envíe al cliente un texto de desafío, que el cliente cifra y devuelve al padre. Si el padre descifra correctamente el texto del desafío, el cliente se autentica.**Precaución:** No utilice el modo de clave compartida. Cuando lo utiliza, una versión de texto sin formato y encriptada de los mismos datos transmite en el aire. Esto no gana nada. Si la clave de usuario es incorrecta, la unidad no descifra los paquetes y los paquetes no pueden obtener acceso a la red.
- **Cliente**La opción Cliente determina el modo de autenticación que los nodos del cliente utilizan para asociar a la unidad. Estos son los valores permitidos:**Abrir (RECOMENDADO)**: este modo de autenticación es esencialmente una operación nula. Todos los clientes pueden autenticarse.**Clave compartida**: este modo permite que el padre envíe al cliente un texto de desafío, que el cliente cifra y devuelve al padre. Si el padre descifra correctamente el texto del desafío, el cliente se autentica.**Both**: Este modo permite al cliente utilizar cualquiera de los dos modos.
- **CifradoDesactivado**: si establece la opción Cifrado en Desactivado, no se realiza ninguna

encriptación. Los datos se transmiten de forma clara.**On (OBLIGATORY)**: si establece la opción Encryption (Encriptación) en On (Encendido), todos los paquetes de datos transmitidos se cifran y se descartan todos los paquetes recibidos sin cifrar.**Mixto**: en el modo Mixto, un bridge raíz o repetidor acepta asociación de clientes que tienen el cifrado activado o desactivado. En este caso, sólo se cifran los paquetes de datos entre nodos que admiten ambos. Los paquetes de multidifusión se envían en el modo claro. Todos los nodos pueden ver los paquetes.**Precaución:** No utilice el modo Mixto. Si un cliente que tiene el cifrado habilitado envía un paquete multicast a su padre, el paquete se cifra. El padre descifra el paquete y retransmite el paquete en el clear a la celda, y otros nodos pueden ver el paquete. La capacidad de ver un paquete en forma encriptada y no encriptada puede contribuir a romper una clave. La inclusión del modo mixto es sólo para compatibilidad con otros proveedores.

Configurar adaptadores de cliente

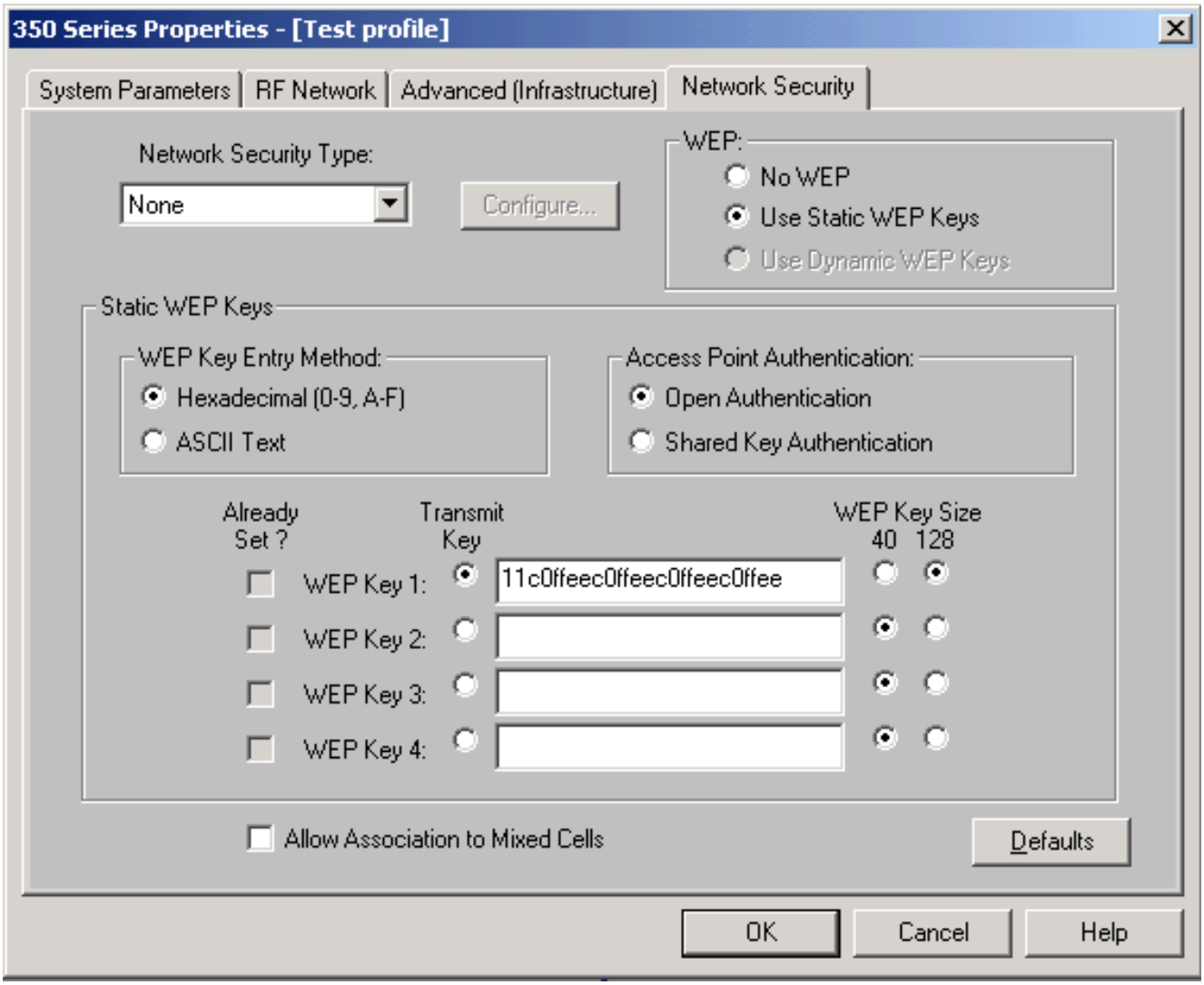
Debe completar dos pasos principales para configurar WEP en el Aironet Client Adapter:

1. Configure las claves WEP en Client Encryption Manager.
2. Active WEP en la utilidad Aironet Client (ACU).

Establecer las claves WEP

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

1. Abra ACU y elija **Profile Manager**.
2. Elija el perfil en el que desea habilitar WEP y haga clic en **Editar**.
3. Haga clic en la ficha **Seguridad de la red** para mostrar las opciones de seguridad y haga clic en **Usar claves WEP estáticas**.Esta acción activa las opciones de configuración WEP que se atenuan cuando no se selecciona ningún
WEP.



4. Para la clave WEP que desea crear, elija **40** bits o **128** bits bajo Tamaño de clave WEP en el lado derecho de la ventana.**Nota:** Los adaptadores de cliente de 128 bits pueden utilizar claves de 40 o 128 bits. Pero los adaptadores de 40 bits sólo pueden utilizar claves de 40 bits.**Nota:** La clave WEP del adaptador del cliente debe coincidir con la clave WEP que utilizan los otros componentes WLAN con los que se comunica.Al establecer más de una clave WEP, debe asignar las claves WEP a los mismos números de clave WEP para todos los dispositivos. Las claves WEP deben constar de caracteres hexadecimales y deben contener 10 caracteres para las claves WEP de 40 bits o 26 caracteres para las claves WEP de 128 bits. Los caracteres hexadecimales pueden ser:0 a 9a fA a F**Nota:** Las claves WEP de texto ASCII no se soportan en los AP Aironet. Por lo tanto, debe elegir la opción Hexadecimal (0-9, A-F) si planea utilizar su adaptador de cliente con estos AP.**Nota:** Después de crear la clave WEP, puede escribir sobre ella. Pero no puede editarlo ni eliminarlo.**Nota:** Si utiliza una versión posterior de Aironet Desktop Utility (ADU) en lugar de ACU como utilidad de cliente, también puede eliminar la clave WEP creada y reemplazarla por una nueva.
5. Haga clic en el botón **Transmit Key** que se encuentra junto a una de las claves que creó.Con esta acción, usted indica que esta clave es la clave que desea utilizar para transmitir paquetes.
6. Haga clic en **Persistent** en WEP Key Type (Tipo de clave WEP).Esta acción permite al adaptador del cliente conservar esta clave WEP, incluso cuando se quita la alimentación del adaptador o cuando se reinicia el equipo en el que se instala la clave. Si elige Temporal para esta opción, la clave WEP se pierde cuando se quita la alimentación del adaptador del

cliente.
7. Click OK.

Activar WEP

Complete estos pasos:

1. Abra ACU y elija **Editar propiedades** en la barra de menús.
2. Haga clic en la ficha **Seguridad de la red** para mostrar las opciones de seguridad.
3. Marque la casilla de verificación **Enable WEP** para activar WEP.

Consulte Configuración de WEP en ADU para ver los pasos para configurar WEP usando ADU como utilidad de cliente.

Configurar puentes de grupo de trabajo

Hay diferencias entre el puente de grupo de trabajo Aironet serie 340 y el puente Aironet serie 340. Sin embargo, la configuración del puente de grupo de trabajo para utilizar WEP es casi idéntica a la configuración del puente. Consulte la sección Configurar los puentes Aironet para ver la configuración del puente.

1. Conéctese al puente de grupo de trabajo.
2. Vaya al menú Privacidad.Elija **Main > Configuration > Radio > I80211 > Privacy** para acceder al menú Privacy VxWorks.

Configuración

El menú Privacidad presenta la configuración que se muestra en esta sección. Configure las opciones en el puente de grupo de trabajo en este orden:

1. Clave
2. Transmitir
3. Autenticación
4. Cifrado

Estas son las opciones:

- **Clave**La opción Key establece la clave WEP que el bridge utiliza para recibir paquetes. El valor debe coincidir con la clave que utiliza el AP u otro dispositivo con el que se comunica el puente de grupo de trabajo. La clave consta de hasta 10 caracteres hexadecimales para encriptación de 40 bits o 26 caracteres hexadecimales para encriptación de 128 bits. Los caracteres hexadecimales pueden ser cualquier combinación de estos dígitos:0 a 9a fA a F
- **Transmitir**La opción Transmit establece la clave WEP que utiliza el bridge para transmitir paquetes. Puede elegir utilizar la misma clave que utilizó para la opción Clave. Si elige una clave diferente, debe establecer una clave coincidente en el AP.Sólo se puede utilizar una clave WEP al mismo tiempo para las transmisiones. La clave WEP que se utiliza para transmitir datos se debe establecer en el mismo valor en el puente de grupo de trabajo y en otros dispositivos con los que se comunica.
- **Autenticación (Auth)**El parámetro Auth determina qué método de autenticación utiliza el sistema. Las opciones son:**Open (Abrir) (RECOMENDADO)**: la configuración predeterminada

Open (Abrir) permite que cualquier punto de acceso, independientemente de su configuración WEP, se autentique y, a continuación, intente comunicarse con el puente.**Clave compartida**: Esta configuración indica al puente que envíe una consulta de clave compartida de texto sin formato a los AP en un intento de comunicarse con el puente. La configuración de clave compartida puede dejar el puente abierto a un ataque de texto conocido de intrusos. Por lo tanto, esta configuración no es tan segura como la opción Abrir.

- **Cifrado**La opción Encryption (Encriptación) establece parámetros de encripción en todos los paquetes de datos, excepto en los paquetes de asociación y algunos paquetes de control. Hay cuatro opciones:**Nota:** El AP debe tener el cifrado activo y una clave configurada correctamente.**Off**: Esta es la configuración predeterminada. Toda la encriptación está desactivada. El puente de grupo de trabajo no se comunica con un AP con el uso de WEP.**On (RECOMENDADO)**: esta configuración requiere el cifrado de todas las transferencias de datos. El puente de grupo de trabajo sólo se comunica con los AP que utilizan WEP.**Mixto en**: Esta configuración significa que el puente siempre utiliza WEP para comunicarse con el AP. Sin embargo, el AP se comunica con todos los dispositivos, tanto si utilizan WEP como si no utilizan WEP.**Mixto off**: Esta configuración significa que el puente no utiliza WEP para comunicarse con el AP. Sin embargo, el AP se comunica con todos los dispositivos, tanto si utilizan WEP como si no utilizan WEP.**Precaución:** Si selecciona On o Mixed on como categoría WEP y configura el puente a través de su link de radio, la conectividad con el puente se pierde si configura la clave WEP incorrectamente. Asegúrese de utilizar exactamente la misma configuración cuando establezca la clave WEP en el puente de grupo de trabajo y la clave WEP en otros dispositivos de la WLAN.

Información Relacionada

- Asociación de Estándares IEEE
- Productos de Lan de la serie inalámbrica Airnet 340
- Recursos de Soporte de Red Inalámbrica
- Página de soporte de LAN inalámbrica
- Guía de configuración del software IOS de Cisco para puntos de acceso Aironet de Cisco
- Guía de Configuración del Software Cisco IOS para el Punto de Acceso/Puente para Exteriores Cisco Aironet serie 1300
- Guía de Configuración del Cisco Aironet Access Point Software para VxWorks
- Guía de Configuración de Cisco Aironet 1400 Series Bridge Software
- Guías de Configuración de Cisco Aironet Wireless LAN Client Adapters
- Descripción general de Cisco Wireless LAN Security
- Tecnología inalámbrica (movilidad) Protección de 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
- Preguntas frecuentes sobre los puntos de acceso Cisco Aironet.
- 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).