Wired Equivalent Privacy (WEP) en los puntos de acceso Aironet y el ejemplo de configuración de los Bridges

Contenido

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 los WLAN para más información sobre la configuración WEP en los reguladores del Wireless LAN (WLCs).

El WEP es el algoritmo de encripción incorporado al estándar del 802.11 (Wi-Fi). La encripción 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 descifrado de datos. Cuando se habilita 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 del Aironet está en el hardware. Por lo tanto, el efecto de rendimieento mínimo resulta cuando usted utiliza el WEP.

Nota: Hay algunos problemas conocidos con el WEP, que le hace no un método de encripción 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 Troceo clave por paquete, rotación dominante del Message Integrity Check (MIC), y del broadcast 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 WLAN y que los dispositivos funcionan normalmente en un entorno sin encripción.

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

Nota: Los productos Aironet pueden establecer las conexiones WEP 40-bit con los Productos del no Cisco de IEEE 802.11b-compliant. 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 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 los puntos de acceso Aironet

Puntos 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 encripción de Radio AP.Utilice una de estas trayectorias:**Encripción de datos del >Radio del Summary Status (Estado de resumen) > Setup (Configuración) > de la radio AP/del hardware (WEP) > encripción de datos de la radio AP> Security Setup (Configuración de seguridad) del > Security (Seguridad) del Summary Status (Estado de resumen) > Setup (Configuración): Radio Data Encryption (WEP) > encripción de datos de la radio APNota:** 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 encripción de datos de la radio AP**

Configuraciones de VxWorks

La página de la encripción 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 encripción de información por estaciones es:**Utilice esta determinación para elegir si los clientes deben utilizar la encripción de datos cuando comunican con el AP. El menú desplegable enumera tres opciones:**No encryption (valor por defecto)** — Requiere a los clientes comunicar con el AP sin ninguna encripción de datos. Esta configuración no se recomienda.**Opcional** — Permite al cliente a comunicar con el AP cualquier con o sin la encripción de datos. Típicamente, usted utiliza esta opción cuando usted tiene dispositivos del cliente que no puedan hacer una conexión WEP, tal como clientes del no Cisco en un entorno del 128-bit WEP.**Encripción completa (RECOMENDADA)** — Requiere a los clientes utilizar la encripción de datos cuando comunican con el AP. No se permite a los clientes que no utilizan la encripción 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 uso del Enable Encryption. Vea la sección de la **clave de encripción (MANDATORY) de** esta lista.
- **Aceptación de los tipos de autenticación**Usted puede elegir abierto, la clave compartida, o ambas opciones para fijar las autenticaciones que el AP reconocerá.**Ábrase (RECOMENDADO)** — Esta configuración predeterminada 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 un en un momento dominante. 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 encripción (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 FPara 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 AP, usted puede borrar las claves existentes. Sin embargo, usted no puede editar las claves existentes.**Nota:** Usted debe configurar las claves WEP para su red, AP, y dispositivos del 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 del cliente al mismo valor.
- **Tamaño de clave (MANDATORY)**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 borrar una clave seleccionando el “no establecido”.
- **botones Action (Acción)**Cuatro configuraciones del control de los botones de acción. Si el Javascript se habilita en su buscador Web, una ventana de la ventana emergente de confirmación aparece después de que usted haga clic cualquier botón, excepto la cancelación.**Apliqúese** — 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 predeterminadas de fábrica.

Nota: En las versiones recientes de Cisco IOS® de los AP, 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 encripción de datos Vista del emulador de terminal de la secuencia de configuración de la clave WEP (software de Cisco IOS®)

Aironet AP que funciona con el Cisco IOS Software

Complete estos pasos:

1. Haga una conexión al AP.
2. De la opción del menú de seguridad en el lado izquierdo de la ventana, elija al **administrador del cifrado** para la interfaz radio a la cual usted quiere configurar sus claves de WEP estático.**Opinión del buscador Web del menú del administrador de encripción segura AP**

Aironet Bridge de la configuración

Si usted utiliza VxWorks, complete estos pasos:

1. Haga una conexión al Bridge.

2. Navegue al menú de privacidad.Elija el **>Radio del menú principal > de la configuración > el > Privacy (Privacidad) I80211**.Los controles de menú de privacidad 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 privacidad**

Refiera a configurar las habitaciones de la cifra y el WEP - Bridge de las 1300 Series y configurar las características WEP y WEP - Bridge de las 1400 Series para la información sobre cómo configurar el WEP en 1300 y los Bridges de las 1400 Series a través del modo CLI.

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

Configuraciones de VxWorks

El menú de privacidad 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 privacidad. Sin embargo, configure las opciones en esta orden:

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

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

Éstas son las opciones:

- **Clave (OBLIGATORIO)**La opción de la clave programa las claves de encripción en el Bridge. A le indican que fije una de las cuatro claves. A le indican dos veces que ingrese la clave. Para definir la clave, usted debe ingresar 10 o 26 dígitos hexadecimales, que depende encendido si la configuración de Bridge 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).
- **Transmitir**La opción del transmitir dice a radio qué claves a utilizar para transmitir los paquetes. Cada radio puede desencriptar los paquetes recibidos que se envían con las cuatro claves unas de los.
- AutenticaciónUsted utiliza opción Auth (Autenticación) encendido los Repeater Bridge para determinar que el modo de autenticación la unidad utiliza 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 de impugnación, que el cliente cifra y devuelve al padre. Si el padre desencripta con éxito el texto de impugnación, 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 desencripta los paquetes, y los paquetes no pueden acceder a la red.

- **Cliente**La opción Cliente determina al 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 de impugnación, que el cliente cifra y devuelve al padre. Si el padre desencripta con éxito el texto de impugnación, autentican al cliente.**Ambos** — Este modo permite que el cliente utilice cualquier modo.
- **CifradoDe** — Si usted fija la opción de encripción a apagado, se hace el no encryption. Los datos transmiten en el claro.**En (MANDATORY)** — Si usted fija la opción de encripción a encendido, se cifran todos los paquetes de datos transmitidos y se desecha cualquier paquete recibido unencrypted.**Mezclado** — En el modo mezclado, una raíz o un Repeater Bridge 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 soportan 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 habilitar envía un paquete de multidifusión a su padre, se cifra el paquete. El padre desencripta 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 combinado está solamente para la compatibilidad con los otros vendedores.

Adaptadores del cliente de la configuración

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

1. Configure la clave WEP/las claves en el administrador de encripción de cliente.
2. Habilite el WEP en el Aironet Client Utility (ACU).

Fije las claves WEP

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

1. Abra el ACU y elija al **administrador del perfil**.
2. Elija el perfil donde usted quiere habilitar el WEP y el tecleo **edita**.
3. Haga clic la **ficha de seguridad de la red** para visualizar las opciones de seguridad, y haga clic las **claves de 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 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 WLAN con quienes 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 soportan en el Aironet AP. Por lo tanto, usted debe elegir (0-9, A-F) la opción hexadecimal si usted planea utilizar su adaptador del cliente con estos AP.**Nota:** Después de que usted cree la clave WEP, usted puede escribir sobre ella. Pero usted no puede editarla o borrar.**Nota:** Si usted utiliza una versión posterior de utilidad Aironet Desktop (ADU) en vez del ACU como utilidad de cliente, usted puede también borrar la clave WEP creada y substituirla 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 tecleo.Esta acción permite que su adaptador del cliente conserve esta clave WEP, incluso cuando el poder 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 el poder se quita de su adaptador del cliente.
7. Haga clic en OK.

Permiso WEP

Complete estos pasos:

1. Abra el ACU y elija **Edit Properties de la** barra de menú.
2. Haga clic la **ficha de seguridad de la red** para visualizar las opciones de seguridad.
3. Marque 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 Bridges

Hay diferencias entre el Workgroup Bridge de las 340 Series del Aironet y el Bridge de las 340 Series del Aironet. Sin embargo, la configuración del Workgroup Bridge para utilizar el WEP es casi idéntica a la configuración del Bridge. Vea la sección de los Aironet Bridge de la configuración para la configuración del Bridge.

1. Conecte con el Workgroup Bridge.
2. Navegue al menú de privacidad.Elija **Main > Configuration > Radio > el > Privacy (Privacidad) I80211** para acceder el menú de VxWorks de la aislamiento.

Configuración

El menú de privacidad presenta a configuraciones las listas de esa esta sección. Configure las opciones en el Workgroup Bridge en esta orden:

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

Éstas son las opciones:

- **Clave**La opción dominante establece la clave WEP que las aplicaciones del Bridge para recibir los paquetes. El valor debe hacer juego la clave que el AP o el otro dispositivo con los cuales el Workgroup Bridge 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
- **Transmitir**La opción del transmitir establece la clave WEP que las aplicaciones del Bridge 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 Workgroup Bridge y otros dispositivos con los cuales comunique.
- **Autenticación (auth)**El parámetro Auth determina que el método de autenticación el sistema utiliza. Las opciones son:**Ábrase (RECOMENDADO)** — La configuración abierta predeterminada permite que cualquier AP, sin importar sus configuraciones de WEP, autentique y después intente comunicar con el Bridge.**Clave compartida** — Esta configuración da instrucciones el Bridge para enviar un sólo texto, consulta de clave compartida a los AP en un intento por comunicar con el Bridge. La configuración de clave compartida puede salir del Bridge 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 encripción fija los parámetros de encripción 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 un conjunto de teclas correctamente.**De** — Ésta es la configuración predeterminada. Se apaga todo el cifrado. El Workgroup Bridge no comunica con un AP con el uso del WEP.**En (RECOMENDADO)** — Esta configuración requiere el cifrado de todas las Transferencias de datos. El Workgroup Bridge comunica solamente con los AP que utilizan el WEP.**Mezclado encendido** — Esta configuración significa que el Bridge 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 Bridge 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 Bridge a través de su link de radio, la Conectividad al Bridge se pierde si usted fija la clave WEP incorrectamente. Aseegurese que usted utiliza exactamente las mismas configuraciones cuando usted fija la clave WEP en el Workgroup Bridge y la clave WEP en los otros dispositivos en su red inalámbrica (WLAN).

Información Relacionada

- Asociación de las normas 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 Cisco IOS Software para el puente de/punto de acceso al aire libre del Cisco Aironet de la serie 1300
- Guía de Configuración del Cisco Aironet Access Point Software para VxWorks
- Guía de configuración del Software de Bridge del Cisco Aironet de la serie 1400
- Guías de configuración del Cisco Aironet Wireless LAN Client Adapters
- Descripción de la Seguridad de LAN de la tecnología inalámbrica 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
- Preguntas frecuentes sobre los puntos de acceso Cisco Aironet.
- Soporte Técnico y Documentación - Cisco Systems