Ejemplo de Configuración de WEP en un Punto de Acceso Autónomo

Contenido

Introducción

Este documento describe cómo utilizar y configurar Wired Equivalent Privacy (WEP) en un punto de acceso autónomo (AP) de Cisco.

Prerequisites

Requirements

Este documento asume que usted puede hacer una conexión administrativa a los dispositivos WLAN, y que los dispositivos funcionan normalmente en un entorno no cifrado. Para configurar un WEP estándar de 40 bits, debe tener dos o más unidades de radio que se comuniquen entre sí.

Componentes Utilizados

La información de este documento se basa en un AP 1140 que ejecuta Cisco IOS® Release15.2JB.

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). If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

WEP es el algoritmo de encriptación incorporado en el estándar 802.11 (Wi-Fi). WEP utiliza el cifrado de flujo RC4 para la confidencialidad y la suma de comprobación Cyclic Redundancy Check-32 (CRC-32) para la integridad .

El WEP estándar de 64 bits utiliza una clave de 40 bits (también conocida como WEP-40), que se concatena con un vector de inicialización (IV) de 24 bits para formar la clave RC4. Una clave WEP de 64 bits se suele introducir como una cadena de 10 caracteres hexadecimales (base 16) (de cero a nueve y de A a F). Cada carácter representa cuatro bits, y diez dígitos de cuatro bits cada uno equivale a 40 bits; si agrega el IV de 24 bits, produce la clave WEP completa de 64 bits.

Una clave WEP de 128 bits se suele introducir como una cadena de 26 caracteres hexadecimales. Veintiséis dígitos de cuatro bits cada uno equivalen a 104 bits; si agrega el IV de 24 bits, producirá la clave WEP completa de 128 bits. La mayoría de los dispositivos permiten al usuario introducir la clave en 13 caracteres ASCII.

Métodos de autenticación

Se pueden utilizar dos métodos de autenticación con WEP: la autenticación de sistema abierto y la autenticación de clave compartida.

Con la autenticación de sistema abierto, el cliente WLAN no necesita proporcionar credenciales al AP para la autenticación. Cualquier cliente puede autenticarse con el AP y luego intentar asociarse. En efecto, no se produce ninguna autenticación. Posteriormente, las claves WEP se pueden utilizar para cifrar tramas de datos. En este momento, el cliente debe tener las claves correctas.

Con la autenticación de clave compartida, la clave WEP se utiliza para la autenticación en un protocolo de enlace de respuesta ante desafíos de cuatro pasos:

1. El cliente envía una solicitud de autenticación al AP.
2. El AP responde con un desafío de texto claro .
3. El cliente cifra el texto de desafío con la clave WEP configurada y responde con otra solicitud de autenticación.
4. El AP descifra la respuesta. Si la respuesta coincide con el texto de desafío, el AP envía una respuesta positiva.

Después de la autenticación y la asociación, la clave WEP previamente compartida también se utiliza para cifrar las tramas de datos con RC4.

A primera vista, puede parecer que la autenticación de clave compartida es más segura que la autenticación de sistema abierto, ya que esta última no ofrece autenticación real. Sin embargo, ocurre lo contrario. Es posible derivar la secuencia de claves utilizada para el intercambio de señales si captura las tramas de desafío en la autenticación de clave compartida. Por lo tanto, se recomienda utilizar la autenticación de sistema abierto para la autenticación WEP, en lugar de la autenticación de clave compartida.

Se creó el protocolo de integridad de clave temporal (TKIP) para abordar estos problemas WEP.

Al igual que WEP, TKIP utiliza encriptación RC4. Sin embargo, TKIP mejora WEP con la adición de medidas como hashing de claves por paquete, comprobación de integridad del mensaje (MIC) y rotación de claves de difusión para abordar vulnerabilidades WEP conocidas. TKIP utiliza el cifrado de flujo RC4 con claves de 128 bits para el cifrado y claves de 64 bits para la autenticación.

Configurar

Esta sección proporciona las configuraciones GUI y CLI para WEP.

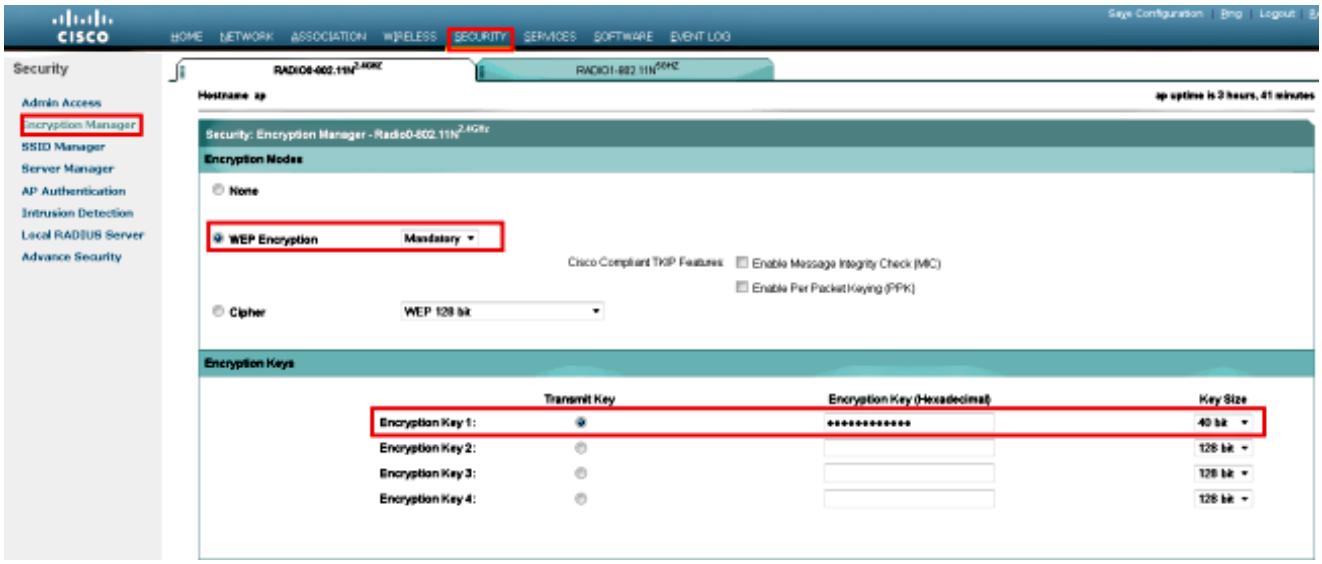
Configuración de la interfaz gráfica para el usuario

Complete estos pasos para configurar WEP con la GUI.

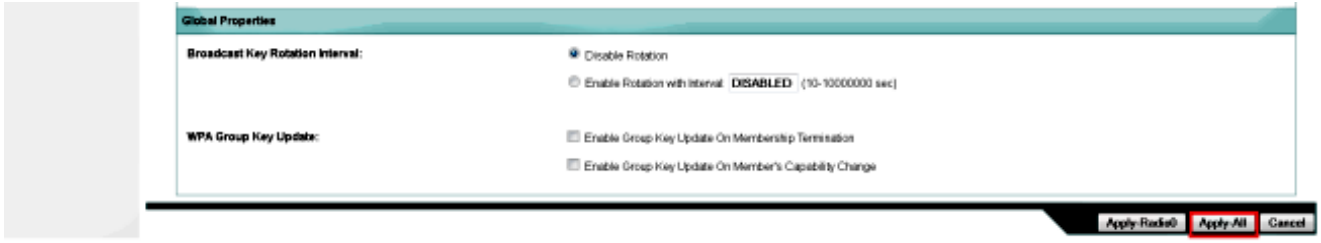
1. Conéctese al AP a través de la GUI.
2. En el menú Security de la parte izquierda de la ventana, elija Encryption Manager para la interfaz de radio en la que desea configurar las claves WEP estáticas.
3. En Encryption Modes (Modos de encriptación), haga clic en WEP Encryption (Encriptación WEP) y seleccione Obligatorio en el menú desplegable del cliente.

   Los modos de cifrado utilizados por la estación son:
   - Predeterminado (sin cifrado): requiere que los clientes se comuniquen con el AP sin cifrado de datos. No se recomienda esta configuración.
   - Opcional: permite a los clientes comunicarse con el AP con o sin encripción de datos. Normalmente, esta opción se utiliza cuando hay dispositivos cliente que no pueden establecer una conexión WEP, como los clientes que no son de Cisco en un entorno WEP de 128 bits.
   - Obligatorio (cifrado completo): requiere que los clientes utilicen el cifrado de datos cuando se comunican con el AP. Los clientes que no utilizan cifrado de datos no pueden comunicarse. Esta opción se recomienda si desea maximizar la seguridad de su WLAN.
4. En Encryption Keys (Claves de cifrado), seleccione el botón de opción Transmit Key e introduzca la clave hexadecimal de 10 dígitos. Asegúrese de que Key Size (Tamaño de clave) esté configurado en 40 bit.

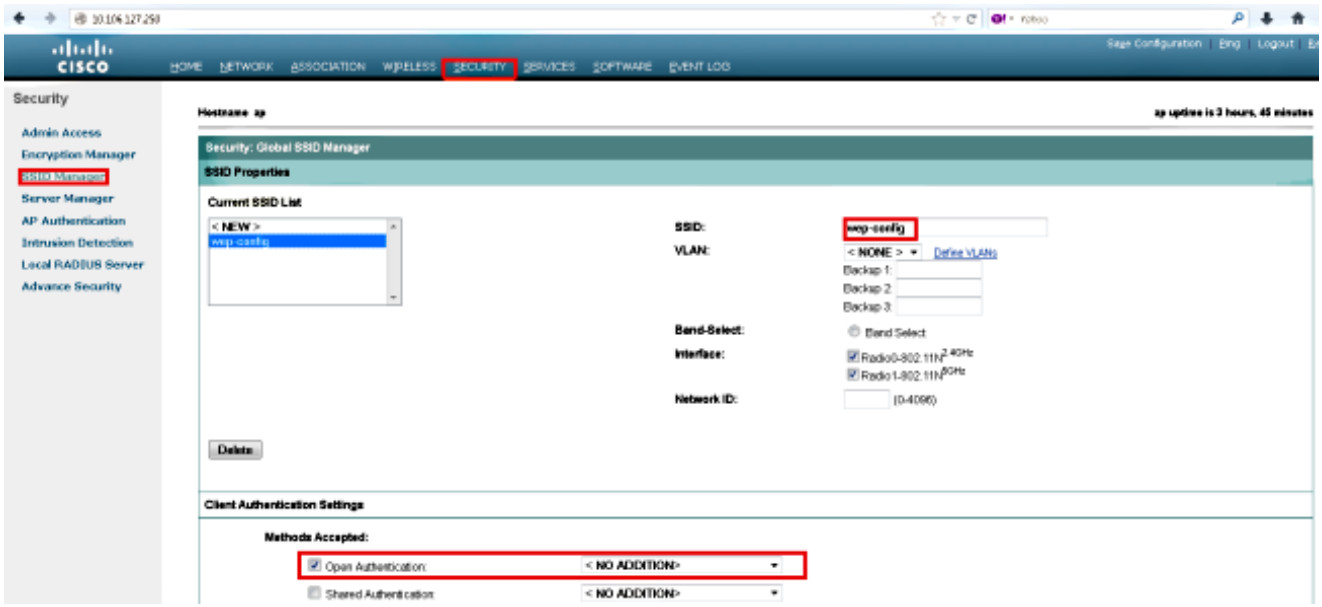
   Introduzca 10 dígitos hexadecimales para las claves WEP de 40 bits o 26 dígitos hexadecimales para las claves WEP de 128 bits. Las claves pueden ser cualquier combinación de estos dígitos:
   - 0 a 9
   - a a f
   - De A a F



5. Haga clic en Apply-All para aplicar la configuración en ambas radios.



6. Cree un identificador de conjunto de servicios (SSID) con Open Authentication, y haga clic en Apply para habilitarlo en ambas radios.



7. Navegue hasta la red y habilite las radios para 2,4 GHz y 5 GHz para que se puedan ejecutar.

Configuración de CLI

Utilice esta sección para configurar WEP con la CLI.

<#root>

ap#

show run

```
Building configuration...

Current configuration : 1794 bytes
!
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
logging rate-limit console 9
enable secret 5 $1$kxBl$OhRR4QtTUVDUA9GakGDFs1
!
no aaa new-model
ip cef
!
!
!
dot11 syslog
!
  dot11 ssid wep-config
  authentication open
  guest-mode
!
!
crypto pki token default removal timeout 0
!
!
```

```
username Cisco password 7 0802455D0A16
!
!
bridge irb
!
!
!
interface Dot11Radio0
 no ip address
 !
 encryption key 1 size 40bit 7 447B6D514EB7 transmit-key
 encryption mode wep mandatory
 !
 ssid wep-config
 !
 antenna gain 0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1

 no ip address
 !
 encryption key 1 size 40bit 7 447B6D514EB7 transmit-key
 encryption mode wep mandatory
 !
 ssid wep-config
 !
 antenna gain 0
 dfs band 3 block
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
 no keepalive
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface BVI1
 ip address dhcp
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip route 0.0.0.0 0.0.0.0 10.106.127.4
!
```

```
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
login local
transport input all
!
end
```

Verificación

Ingrese este comando para confirmar que su configuración funciona correctamente:

<#root>

ap#

show dot11 associations

```
802.11 Client Stations on Dot11Radio0:
SSID [wep-config] :
MAC Address    IP address      Device        Name           Parent         State
1cb0.94a2.f64c 10.106.127.251  unknown       -              self           Assoc
```

Troubleshoot

Use esta sección para resolver problemas su configuración.

> Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos debug.

Estos comandos debug son útiles para resolver problemas de configuración:

- debug dot11 events - Habilita la depuración para todos los eventos dot1x.
- debug dot11 packets - Habilita la depuración para todos los paquetes dot1x.

A continuación se muestra un ejemplo del registro que se muestra cuando el cliente se asocia con éxito a la WLAN:

```
*Mar  1 02:24:46.246: %DOT11-6-ASSOC: Interface Dot11Radio0, Station
1cb0.94a2.f64c Associated KEY_MGMT[NONE]
```

Cuando el cliente ingresa la clave incorrecta, se muestra este error:

```
*Mar  1 02:26:00.741: %DOT11-4-ENCRYPT_MISMATCH: Possible encryption key
mismatch between interface Dot11Radio0 and station 1cb0.94a2.f64c
*Mar  1 02:26:21.312: %DOT11-6-DISASSOC: Interface Dot11Radio0, Deauthenticating
Station 1cb0.94a2.f64c Reason: Sending station has left the BSS
*Mar  1 02:26:21.312: *** Deleting client 1cb0.94a2.f64c
```

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).