WEP en un ejemplo autónomo de la Configuración de punto de acceso

Contenido

Introducción

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

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

Componentes Utilizados

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

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.

Antecedentes

El WEP es el algoritmo de encripción incorporado al estándar del 802.11 (Wi-Fi). El WEP utiliza la cifra de secuencia RC4 para la confidencialidad, y la suma de comprobación de la redundancia cíclica Check-32 (CRC-32) para la integridad.

El WEP 64-bit estándar utiliza un bit 40 dominante (también conocido como WEP-40), que se concatena con 24-bit un vector de inicialización (iv) para formar la clave RC4. Una clave WEP 64-bit se ingresa generalmente como cadena de 10 (base 16) caracteres hexadecimales (cero a nueve y A-F). Cada carácter representa cuatro bits, y los diez dígitos de cuatro bits cada uno igualan 40 bits; si usted agrega el 24-bit IV, presenta la clave WEP 64-bit completa.

Una clave WEP del 128-bit se ingresa generalmente como cadena de 26 caracteres hexadecimales. Veintiséis dígitos de cuatro bits bits cada equals104; si usted agrega el 24-bit IV, presenta la clave WEP completa del 128-bit. La mayoría de los dispositivos permiten que el usuario ingrese la clave como 13 caracteres ASCII.

Métodos de autentificación

Dos métodos de autenticación se pueden utilizar con el WEP: Autenticación y clave de autenticación compartida del sistema operativo.

Con la autenticación del sistema operativo, el cliente WLAN no necesita proporcionar las credenciales al AP para la autenticación. Cualquier cliente puede autenticar con el AP, y después intenta asociarse. En efecto, ninguna autenticación ocurre. Posteriormente, las claves WEP se pueden utilizar para cifrar los marcos de datos. En este momento, el cliente debe tener las claves correctas.

Con la clave de autenticación compartida, la clave WEP se utiliza para la autenticación en un cuatro-paso, apretón de manos de la respuesta de seguridad:

1. El cliente envía un pedido de autenticación al AP.
2. El AP contesta con un desafío del texto claro.
3. El cliente cifra el texto de impugnación con la clave WEP configurada, y responde con otro pedido de autenticación.
4. El AP desencripta la respuesta. Si la respuesta hace juego el texto de impugnación, el AP envía una respuesta positiva.

Después de la autenticación y de la asociación, la clave WEP PRE-compartida también se utiliza para cifrar los marcos de datos con el RC4.

En el primer vistazo, puede ser que parezca como si la clave de autenticación compartida es más segura que autenticación del sistema operativo, puesto que este último no ofrece ninguna autenticación real. Sin embargo, el revés es verdad. Es posible derivar el keystream usado para el apretón de manos si usted captura las tramas de desafío en la clave de autenticación compartida. Por lo tanto, es recomendable utilizar la autenticación del sistema operativo para la autenticación WEP, bastante que la clave de autenticación compartida.

El Temporal Key Integrity Protocol (TKIP) fue creado para abordar estos problemas WEP. Similar al WEP, el TKIP utiliza el cifrado RC4. Sin embargo, el TKIP aumenta el WEP con la adición de las medidas tales como Troceo clave por paquete, rotación dominante del Message Integrity Check (MIC), y del broadcast para dirigir las vulnerabilidades sabidas 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.

Configurar

Esta sección proporciona el GUI y las configuraciones CLI para el WEP.

Configuración de la interfaz gráfica para el usuario

Complete estos pasos para configurar el WEP con el GUI.

1. Conecte con el AP con el GUI.
2. 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.
3. Bajo modos de encripción, haga clic la **encripción WEP**, y seleccione **obligatorio del** menú desplegable para el cliente.

   Los modos de encripción usados por la estación son:
   Valor por defecto (no encryption) - 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.**Obligatorio (encripción completa)** - 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).
4. Bajo las claves de encripción, seleccione el botón de radio de la **clave de transmitir**, y ingrese la clave del hexadecimal 10-digit. Asegúrese de que el tamaño de clave esté fijado al **bit 40**.

   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
5. El tecleo **Aplicó a todos** para aplicar la configuración en ambas radios.
6. Cree un Service Set Identifier (SSID) con la **autenticación abierta**, y el tecleo **se aplica** para habilitarla en ambas las radios.

7. Navegue a la red, y permita a las radios para **2.4 gigahertz** y **5 gigahertz** para conseguirlos que se ejecutan.

Configuración de CLI

Utilice esta sección para configurar el WEP con el CLI.

```
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 trabaja correctamente:

```
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
```

Troubleshooting

Use esta sección para resolver problemas su configuración.

> Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

Estos **comandos debug** son útiles para resolver problemas la configuración:

- **eventos del dot11 del debug** - Habilita el debug para todos los eventos del dot1x.
- **paquetes del dot11 del debug** - Habilita el debug para todos los paquetes del dot1x.

Aquí está un ejemplo del registro que visualiza cuando el cliente se asocia con éxito a la red inalámbrica (WLAN):

```
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
```

Cuando el cliente ingresa la clave incorrecta, esta los errores apareces:

```
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
```