WEP em um exemplo autônomo da configuração do ponto de acesso

Índice

Introdução

Este documento descreve como usar e configurar o Wired Equivalent Privacy (WEP) em um Access Point (AP) autônomo de Cisco.

Pré-requisitos

Requisitos

Este documento supõe que você pode fazer uma conexão administrativa aos dispositivos de WLAN, e que os dispositivos funcionam normalmente em um ambiente não criptografado. A fim configurar um padrão 40-bit WEP, você deve ter dois ou mais unidades de rádio que se comunicam um com o otro.

Componentes Utilizados

A informação neste documento é baseada em uns 1140 AP que executem o ® Release15.2JB do Cisco IOS.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto

potencial de qualquer comando.

Informações de Apoio

O WEP é o algoritmo de criptografia construído no padrão do 802.11 (Wi-fi). O WEP usa a cifra de córrego RC4 para a confidencialidade, e a soma de verificação da redundância cíclica Check-32 (CRC-32) para a integridade.

O WEP 64-bit padrão usa um bit 40 chave (igualmente sabido como WEP-40), que seja concatenado com 24-bit um vetor de inicialização (iv) a fim formar a chave RC4. Uma chave de WEP 64-bit é incorporada geralmente como uma corda (base 16) dos caráteres 10 hexadecimais (zero a nove e A-F). Cada caráter representa quatro bit, e os dez dígitos de quatro bit cada um igualam 40 bit; se você adiciona o 24-bit IV, produz a chave de WEP 64-bit completa.

Uma chave de WEP do 128-bit é incorporada geralmente como uma corda de 26 caracteres hexadecimais. Vinte e seis dígitos de quatro bit bit cada equals104; se você adiciona o 24-bit IV, produz a chave de WEP completa do 128-bit. A maioria de dispositivos permitem que o usuário incorpore a chave como 13 caracteres ASCII.

Métodos de autenticação

Dois métodos de autenticação podem ser usados com WEP: Autenticação e autenticação de chave compartilhada do sistema aberto.

Com autenticação do sistema aberto, o cliente de WLAN não precisa de fornecer credenciais ao AP para a autenticação. Todo o cliente pode autenticar com o AP, e tenta então associar. De fato, nenhuma autenticação ocorre. Subseqüentemente, as chaves de WEP podem ser usadas a fim cifrar frames de dados. Neste momento, o cliente deve ter as chaves corretas.

Com autenticação de chave compartilhada, a chave de WEP é usada para a autenticação em uma quatro-etapa, aperto de mão da resposta de desafio:

1. O cliente envia um pedido de autenticação ao AP.
2. O AP responde com um desafio da minuta.
3. O cliente cifra o texto de desafio com a chave de WEP configurada, e responde com um outro pedido de autenticação.
4. O AP decifra a resposta. Se a resposta combina o texto de desafio, o AP envia uma resposta positiva.

Após a autenticação e a associação, a chave de WEP PRE-compartilhada é usada igualmente a fim cifrar os frames de dados com RC4.

Àprimeira vista, pôde parecer como se a autenticação de chave compartilhada é mais segura do que autenticação do sistema aberto, desde que o último não oferece nenhuma autenticação real. Contudo, o reverso é verdadeiro. É possível derivar a sequência de chave usada para o aperto de mão se você captura os challenge frame na autenticação de chave compartilhada. Daqui, é aconselhável usar a autenticação do sistema aberto para a autenticação WEP, um pouco do que a autenticação de chave compartilhada.

O Temporal Key Integrity Protocol (TKIP) foi criado a fim endereçar estas edições WEP. Similar

ao WEP, o TKIP usa a criptografia RC4. Contudo, o TKIP aumenta o WEP com a adição de medidas tais como o pacote per. hashing-chave, a rotação chave do Message Integrity Check (MIC), e da transmissão a fim endereçar vulnerabilidades conhecidas WEP. O TKIP usa a cifra de córrego RC4 com chaves do 128-bit para a criptografia e chaves 64-bit para a autenticação.

Configurar

Esta seção fornece o GUI e as configurações de CLI para o WEP.

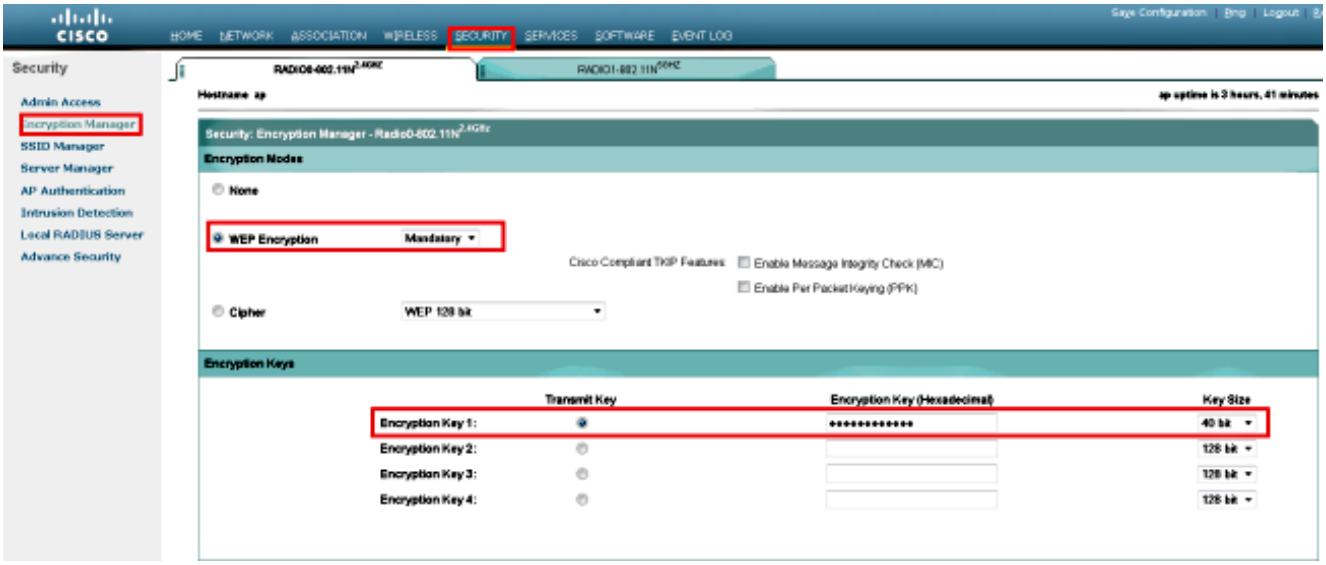
Configuração de GUI

Termine estas etapas a fim configurar o WEP com o GUI.

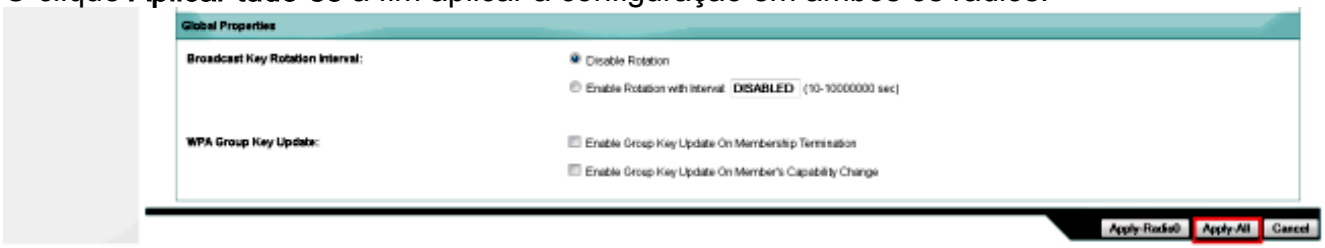
1. Conecte ao AP com o GUI.
2. Do menu Segurança no à esquerda do indicador, escolha o **gerenciador de criptografia** para a interface de rádio a que você quer configurar suas chaves de WEP estático.
3. Sob modos de criptografia, clique a **criptografia de WEP**, e selecione **imperativo do** menu suspenso para o cliente.

   Os modos de criptografia usados pela estação são:
   Padrão (no encryption) - Requer cliente a comunicar-se com o AP sem alguma criptografia de dados. Este ajuste não é recomendado.**Opcional** - Permite cliente a comunicar-se com o AP um ou outro com ou sem a criptografia de dados. Tipicamente, você usa esta opção quando você tem os dispositivos do cliente que não podem fazer uma conexão WEP, tal como clientes não-Cisco em um ambiente do 128-bit WEP.**Imperativo (criptografia total)** - Requer cliente para usar a criptografia de dados quando se comunicarem com o AP. Não são permitidos aos clientes que não usam a criptografia de dados comunicar-se. Esta opção é recomendada se você deseja maximizar a Segurança de seu WLAN.
4. Sob chaves de criptografia, selecione o botão de rádio da **chave transmissora**, e incorpore a chave do hexadecimal 10-digit. Assegure-se de que o tamanho chave esteja ajustado ao **bit 40**.

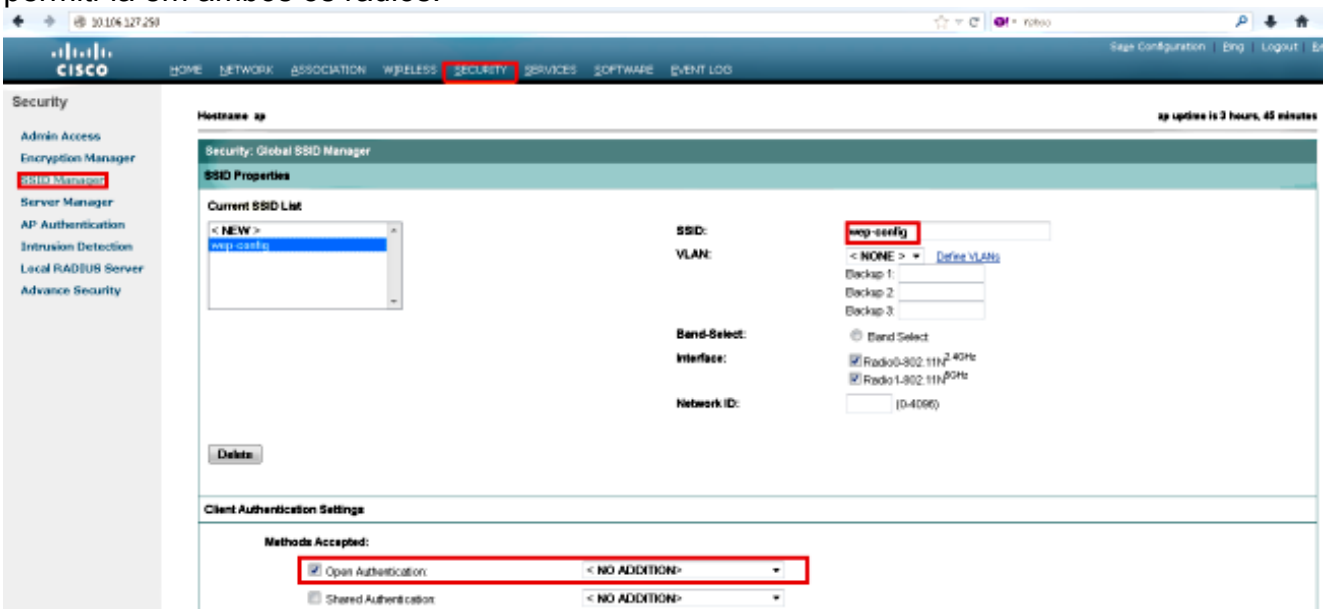
   Incorpore os dígitos hexadecimais 10 para as chaves de WEP 40-bit, ou os 26 dígitos hexadecimais para chaves de WEP do 128-bit. As chaves podem ser toda a combinação destes dígitos:
   0 a
   9àfàF



5. O clique **Aplicar tudo-se** a fim aplicar a configuração em ambos os rádios.



6. Crie um Service Set Identifier (SSID) com a **autenticação aberta**, e o clique **aplica-se** a fim permiti-la em ambos os rádios.



7. Navegue à rede, e permita os rádios para **2.4 gigahertz gigahertz** e **5** a fim obtê-los que são executado.

Configuração de CLI

Use esta seção a fim configurar o WEP com o 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
```

Verificar

Incorpore este comando a fim confirmar que sua configuração trabalha corretamente:

```
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 seção para fazer o troubleshooting da sua configuração.

> **Note**: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

Estes **comandos debug** são úteis a fim pesquisar defeitos a configuração:

- **debugar eventos do dot11** - Permite debugar para todos os eventos do dot1x.
- **debugar pacotes do dot11** - Permite debugar para todos os pacotes do dot1x.

Está aqui um exemplo do log que indica quando o cliente associa com sucesso ao 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
```

Quando o cliente incorporar a chave errada, esta exibições de erros:

```
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
```