Exemplo de configuração de WEP em um ponto de acesso autônomo

Contents

Introduction

Este documento descreve como usar e configurar a WEP (Wired Equivalent Privacy) em um ponto de acesso autônomo (AP) da Cisco.

Prerequisites

Requirements

Este documento pressupõe que você pode fazer uma conexão administrativa com os dispositivos WLAN e que os dispositivos funcionam normalmente em um ambiente não criptografado. Para configurar uma WEP de 40 bits padrão, você deve ter duas ou mais unidades de rádio que se comunicam entre si.

Componentes Utilizados

As informações neste documento são baseadas em um AP 1140 que executa o Cisco IOS® Release 15.2JB.

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.

Informações de Apoio

WEP é o algoritmo de criptografia integrado ao padrão 802.11 (Wi-Fi). O WEP usa a cifra de fluxo RC4 para confidencialidade e a soma de verificação da redundância cíclica-32 (CRC-32) para integridade .

A WEP padrão de 64 bits usa uma chave de 40 bits (também conhecida como WEP-40), que é concatenada com um vetor de inicialização de 24 bits (IV) para formar a chave RC4. Geralmente, uma chave WEP de 64 bits é inserida como uma string de 10 caracteres hexadecimais (base 16) (zero a nove e A-F). Cada caractere representa quatro bits e dez dígitos de quatro bits cada um é igual a 40 bits; se você adicionar o IV de 24 bits, ele produzirá a chave WEP completa de 64 bits.

Geralmente, uma chave WEP de 128 bits é inserida como uma string de 26 caracteres hexadecimais. Vinte e seis dígitos de quatro bits cada um equivale a 104 bits; se você adicionar o IV de 24 bits, ele produzirá a chave WEP completa de 128 bits. A maioria dos dispositivos permite que o usuário digite a chave como 13 caracteres ASCII.

Métodos de autenticação

Dois métodos de autenticação podem ser usados com WEP: Autenticação de Sistema Aberto e Autenticação de Chave Compartilhada.

Com a autenticação de sistema aberto, o cliente WLAN não precisa fornecer credenciais ao AP para autenticação. Qualquer cliente pode se autenticar com o AP e depois tentar se associar. Na verdade, não há autenticação. Subsequentemente, as chaves WEP podem ser usadas para criptografar quadros de dados. Neste ponto, o cliente deve ter as chaves corretas.

Com a Shared Key Authentication, a chave WEP é usada para autenticação em um handshake de resposta de desafio em quatro etapas:

1. O cliente envia uma solicitação de autenticação ao AP.
2. O AP responde com um desafio de texto claro.
3. O cliente criptografa o texto do desafio com a chave WEP configurada e responde com outra solicitação de autenticação.
4. O AP descriptografa a resposta. Se a resposta corresponder ao texto do desafio, o AP envia uma resposta positiva.

Após a autenticação e associação, a chave WEP pré-compartilhada também é usada para criptografar os quadros de dados com RC4.

Àprimeira vista, pode parecer que a Autenticação de Chave Compartilhada é mais segura do que a Autenticação de Sistema Aberto, uma vez que esta não oferece autenticação real. No entanto, o contrário é verdade. É possível derivar o fluxo de chaves usado para o handshake se você capturar os quadros de desafio na Shared Key Authentication. Portanto, é aconselhável usar a Autenticação de Sistema Aberto para autenticação WEP, em vez de Autenticação de Chave Compartilhada.

O Temporal Key Integrity Protocol (TKIP) foi criado para resolver esses problemas de WEP. Semelhante à WEP, o TKIP usa criptografia RC4. No entanto, o TKIP melhora a WEP com a adição de medidas como hashing de chave por pacote, Message Integrity Check (MIC) e rotação

de chave de broadcast para lidar com vulnerabilidades conhecidas da WEP. O TKIP usa a cifra de fluxo RC4 com chaves de 128 bits para criptografia e chaves de 64 bits para autenticação.

Configurar

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

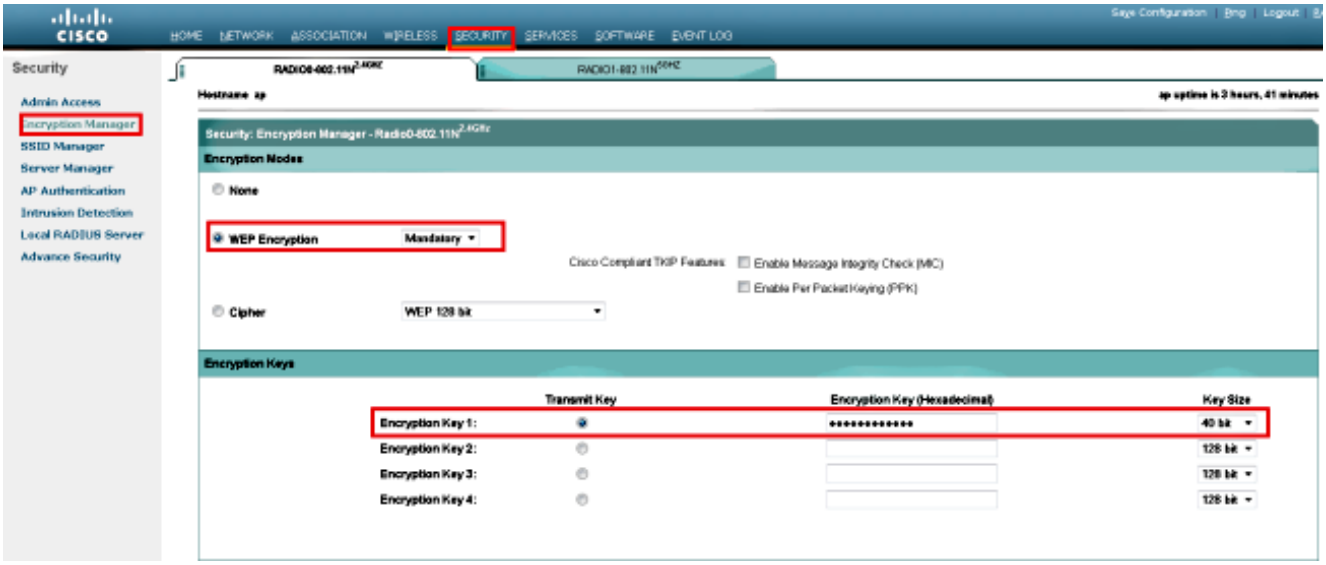
Configuração de GUI

Conclua estes passos para configurar a WEP com a GUI.

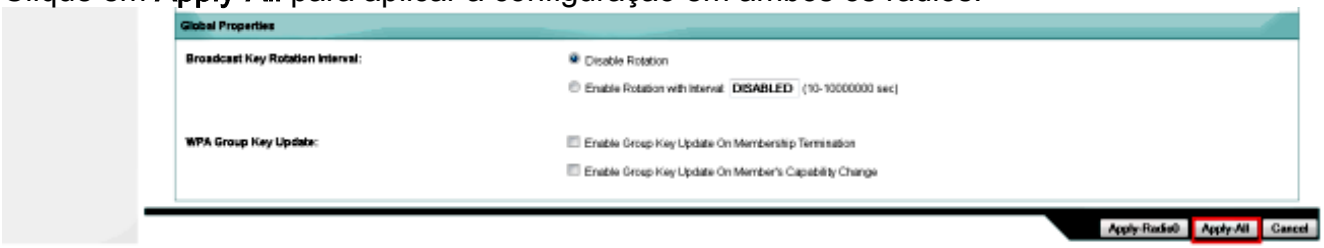
1. Conecte-se ao AP através da GUI.
2. No menu Segurança no lado esquerdo da janela, escolha **Gerenciador de criptografia** para a interface de rádio na qual deseja configurar suas chaves WEP estáticas.
3. Em Modos de criptografia, clique em **Criptografia WEP** e selecione **Obrigatório** no menu suspenso do cliente.

   Os Modos de Criptografia usados pela Estação são:
   Padrão (Sem criptografia) - Exige que os clientes se comuniquem com o AP sem qualquer criptografia de dados. Esta configuração não é recomendada.**Opcional** - Permite que os clientes se comuniquem com o AP com ou sem criptografia de dados. Normalmente, você usa essa opção quando tem dispositivos de cliente que não podem fazer uma conexão WEP, como clientes não-Cisco em um ambiente WEP de 128 bits.**Obrigatório (Criptografia Completa)** - Exige que os clientes usem criptografia de dados quando se comunicam com o AP. Clientes que não usam criptografia de dados não têm permissão para se comunicar. Essa opção é recomendada se você quiser maximizar a segurança da sua WLAN.
4. Em Chaves de criptografia, selecione o botão de opção **Chave de transmissão** e insira a chave hexadecimal de 10 dígitos. Verifique se Key Size (Tamanho da chave) está definido como **40 bit**.

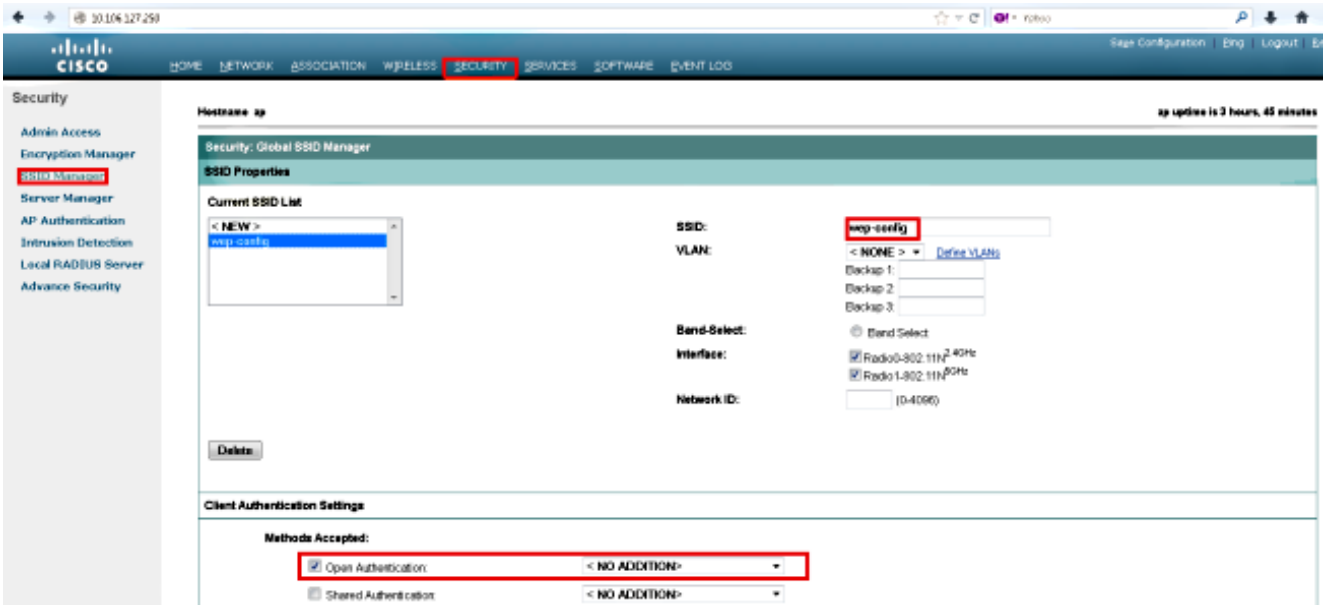
   Insira 10 dígitos hexadecimais para as chaves WEP de 40 bits ou 26 dígitos hexadecimais para as chaves WEP de 128 bits. As teclas podem ser qualquer combinação destes dígitos: 0 a 9a fA a
   F



5. Clique em **Apply-All** para aplicar a configuração em ambos os rádios.



6. Crie um SSID (Service Set Identifier) com **autenticação aberta** e clique em **Apply** para ativá-lo nos dois rádios.



7. Navegue até a rede e ative os rádios para **2,4 GHz** e **5 GHz** para que eles funcionem.

Configuração de CLI

Use esta seção para configurar o WEP com a 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

Insira este comando para confirmar se sua configuração funciona 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
```

Troubleshoot

Use esta seção para fazer o troubleshooting da sua configuração.

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

Esses comandos **debug** são úteis para solucionar problemas de configuração:

- **debug dot11 events** - Ativa a depuração para todos os eventos dot1x.
- **debug dot11 packets** - Ativa a depuração para todos os pacotes dot1x.

Aqui está um exemplo do registro exibido quando o cliente se associa com êxito à WLAN:

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

Quando o cliente inserir a chave errada, este erro será exibido:

```
*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
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.