Configuração de WPA/WPA2 com chave pré-compartilhada: IO 15.2JB e mais tarde

Índice

Introdução

Este documento descreve uma configuração de exemplo para o acesso protegido Sem fio (WPA) e o WPA2 com uma chave pré-compartilhada (PSK).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Familiaridade com o GUI ou o comando line interface(cli) para o software do ® do Cisco IOS
- Familiaridade com os conceitos do PSK, do WPA, e do WPA2

Componentes Utilizados

A informação neste documento é baseada no Access Point (AP) do Cisco Aironet 1260 que executa o Cisco IOS Software Release 15.2JB.

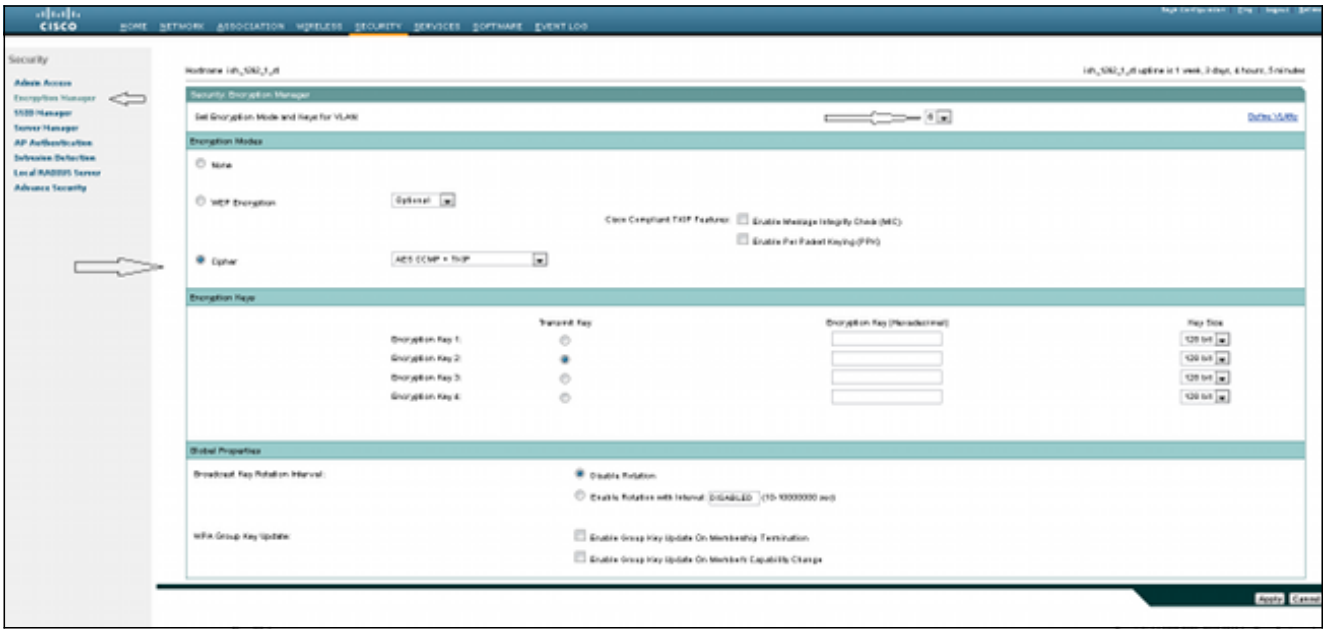
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer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

Configurar

Configuração com GUI

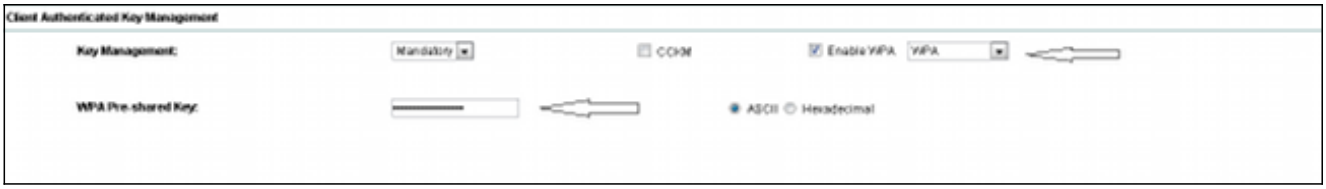
Este procedimento descreve como configurar o WPA e o WPA2 com um PSK no Cisco IOS Software GUI:

1. Estabelecer o gerenciador de criptografia para o VLAN definido para o Service Set Identifier (SSID). Navegue à **Segurança** > ao **gerenciador de criptografia**, assegure-se de que a cifra esteja permitida, e **AES** seleto **CCMP + TKIP** como a cifra a ser usada para ambos os SSID.



2. Permita o VLAN correto com os parâmetros de criptografia definidos em etapa 1. navegam à **Segurança** > ao **gerenciador de SSID**, e selecionam o SSID da lista atual SSID. Esta etapa é comum para a configuração WPA e WPA2.

3. Na página SSID, ajuste o gerenciamento chave a **imperativo**, e verifique a caixa de seleção da **possibilidade WPA**. Selecione o **WPA da** lista de drop-down a fim permitir o WPA. Incorpore a chave pré-compartilhada WPA.



4. Selecione o **WPA2 da** lista de drop-down a fim permitir o WPA2.

Configuração com CLI

> Notas:
>
> Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.
>
> A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

Esta é a mesma configuração feita dentro do CLI:

```
sh run
Building configuration...Current configuration : 5284 bytes
!
! Last configuration change at 04:40:45 UTC Thu Mar 11 1993
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ish_1262_1_st
!
!
logging rate-limit console 9
enable secret 5 $1$Iykv$1tUkNYeB6omK41S18lTbQ1
!
no aaa new-model
ip cef
ip domain name cisco.com
!
!
!
dot11 syslog
!
dot11 ssid wpa
vlan 6
authentication open
authentication key-management wpa
mbssid guest-mode
```

```
wpa-psk ascii 7 060506324F41584B56
!
dot11 ssid wpa2
vlan 7
authentication open
authentication key-management wpa version 2
wpa-psk ascii 7 110A1016141D5A5E57
!
bridge irb
!
!
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption vlan 6 mode ciphers aes-ccm tkip
!
encryption vlan 7 mode ciphers aes-ccm tkip
!
ssid wpa
!
ssid wpa2
!
antenna gain 0
mbssid
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 Dot11Radio0.6
encapsulation dot1Q 6
no ip route-cache
bridge-group 6
bridge-group 6 subscriber-loop-control
bridge-group 6 spanning-disabled
bridge-group 6 block-unknown-source
no bridge-group 6 source-learning
no bridge-group 6 unicast-flooding
!
interface Dot11Radio0.7
encapsulation dot1Q 7
no ip route-cache
bridge-group 7
bridge-group 7 subscriber-loop-control
bridge-group 7 spanning-disabled
bridge-group 7 block-unknown-source
no bridge-group 7 source-learning
no bridge-group 7 unicast-flooding
!
interface Dot11Radio1
no ip address
no ip route-cache
!
encryption vlan 6 mode ciphers aes-ccm tkip
!
encryption vlan 7 mode ciphers aes-ccm tkip
!
ssid wpa
!
```

```
ssid wpa2
!
antenna gain 0
no dfs band block
mbssid
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 Dot11Radio1.6
encapsulation dot1Q 6
no ip route-cache
bridge-group 6
bridge-group 6 subscriber-loop-control
bridge-group 6 spanning-disabled
bridge-group 6 block-unknown-source
no bridge-group 6 source-learning
no bridge-group 6 unicast-flooding
!
interface Dot11Radio1.7
encapsulation dot1Q 7
no ip route-cache
bridge-group 7
bridge-group 7 subscriber-loop-control
bridge-group 7 spanning-disabled
bridge-group 7 block-unknown-source
no bridge-group 7 source-learning
no bridge-group 7 unicast-flooding
!
interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
no keepalive
bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
!
interface GigabitEthernet0.6
encapsulation dot1Q 6
no ip route-cache
bridge-group 6
bridge-group 6 spanning-disabled
no bridge-group 6 source-learning
!
interface GigabitEthernet0.7
encapsulation dot1Q 7
no ip route-cache
bridge-group 7
bridge-group 7 spanning-disabled
no bridge-group 7 source-learning
!
interface BVI1
ip address 10.105.132.172 255.255.255.128
no ip route-cache
!
ip forward-protocol nd
ip http server
```

```
ip http secure-server
```

Verificar

A fim confirmar que a configuração trabalha corretamente, navegue à **associação**, e verifique que o cliente está conectado:

Você pode igualmente verificar a associação de cliente no CLI com este mensagem do syslog:

```
*Mar 11 05:39:11.962: %DOT11-6-ASSOC: Interface Dot11Radio0, Station
ish_1262_1_st 2477.0334.0c40 Associated KEY_MGMT[WPAv2 PSK]
```

Troubleshooting

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

Use estes comandos debug a fim pesquisar defeitos problemas de conectividade:

- **debugar chaves do gerente aaa do dot11** - Isto debuga mostras o aperto de mão que ocorre entre o AP e o cliente como a chave por pares transiente (PTK) e a chave transiente do grupo (GTK) negocia.
- **debugar a estado-máquina do autenticador aaa do dot11** - Isto debuga mostras os vários estados de negociações que um cliente passa completamente enquanto o cliente associa e autentica. Os nomes do estado indicam estes estados.
- **debugar o processo do autenticador aaa do dot11** - Isto debuga ajudas que você diagnostica problemas com comunicações negociadas. A informação detalhada mostra o que cada participante na negociação envia e mostra a resposta do outro participante. Você pode igualmente usar este debuga conjuntamente com o **comando debug radius authentication**.
- **debugar a falha de conexão da estação do dot11** - Isto debuga ajudas que você determina se os clientes estão falhando a conexão e o ajuda a determinar a razão para falhas.