Configuración de WPA/WPA2 con la clave previamente compartida: IOS 15.2JB y posterior

Contenido

Introducción

Este documento describe una configuración de muestra para el acceso protegido Tecnología inalámbrica (WPA) y el WPA2 con una clave previamente compartida (PSK).

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Familiaridad con el GUI o el comando line interface(cli) para el software del ® del Cisco IOS
- Familiaridad con los conceptos de PSK, de WPA, y de WPA2

Componentes Utilizados

La información en este documento se basa en el Cisco Aironet 1260 puntos de acceso que funcione con el Cisco IOS Software Release 15.2JB.

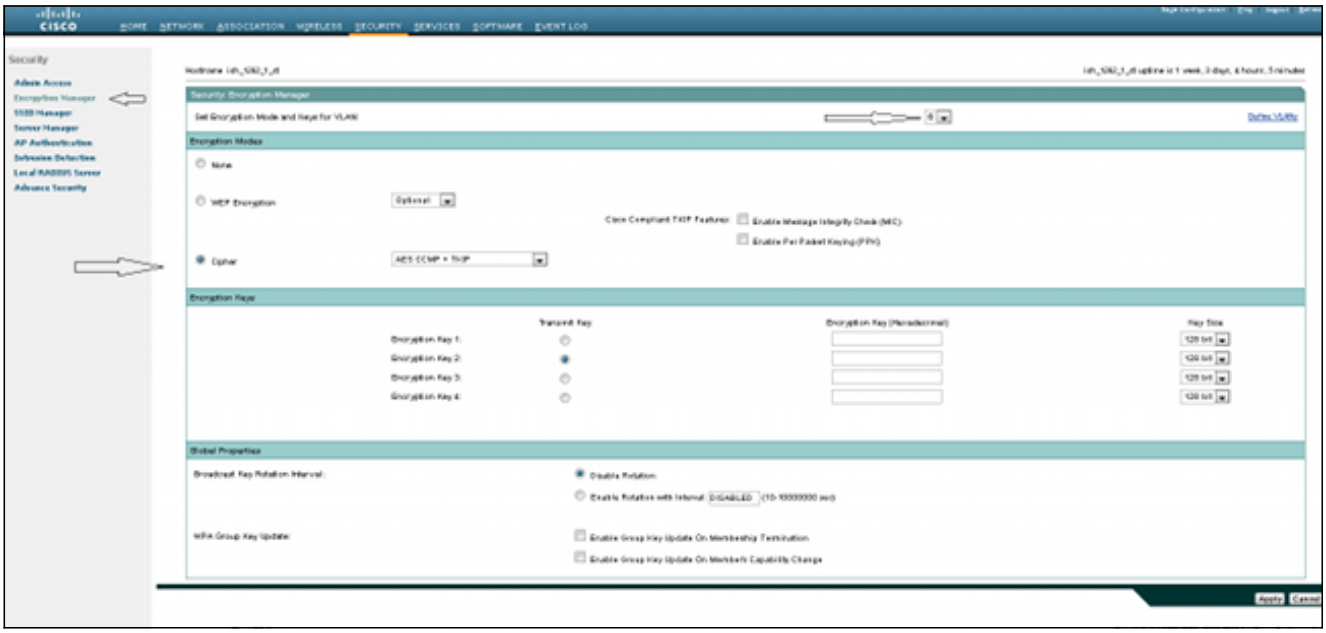
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Configuración con el GUI

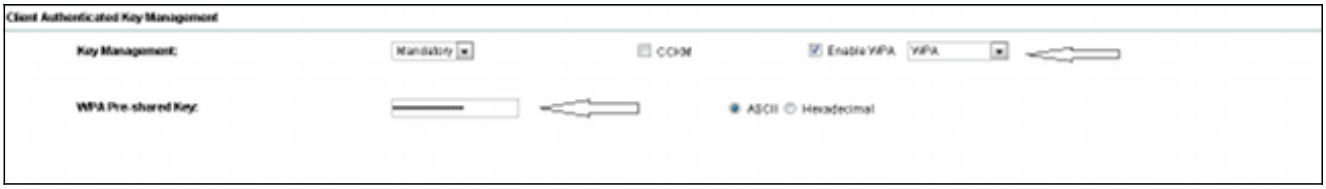
Este procedimiento describe cómo configurar el WPA y el WPA2 con un PSK en el Cisco IOS Software GUI:

1. Configure al administrador del cifrado para el VLA N definido para el Service Set Identifier (SSID). Navegue al **administrador de la Seguridad >** del **cifrado**, asegúrese que la cifra está habilitada, y **CCMP** selecto **AES + TKIP** como la cifra que se utilizará para ambos SSID.



2. Habilite el VLA N correcto con los parámetros de encripción definidos en el paso 1. navegan a la **Seguridad >** al **administrador SSID**, y seleccionan el SSID de la lista actual SSID. Este paso es común para la configuración WPA y WPA2.

3. En la página SSID, fije la administración de claves a **obligatorio**, y marque la **casilla de verificación WPA del permiso**. Seleccione el **WPA de la** lista desplegable para habilitar el WPA. Ingrese la clave previamente compartida WPA.



4. Seleccione el **WPA2 de la** lista desplegable para habilitar el WPA2.

Configuración con el CLI

> Notas:
>
> Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.
>
> La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

Ésta es la misma configuración hecha dentro del 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
```

Verificación

Para confirmar que la configuración trabaja correctamente, navegue a la **asociación**, y verifique que el cliente está conectado:

Usted puede también verificar la asociación del cliente en el CLI con este mensaje de 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 Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

Utilice estos comandos debug para resolver problemas los problemas de conectividad:

- **haga el debug de las claves del administrador aaa del dot11** - Este debug muestra que el apretón de manos que ocurre entre el AP y el cliente como la clave en parejas transitoria (PTK) y la clave transitoria del grupo (GTK) negocian.
- **estado-máquina del authenticator aaa del dot11 del debug** - Este debug muestra los diversos estados de las negociaciones que un cliente pasa a través mientras que el cliente se asocia y autentica. Los nombres del estado indican estos estados.
- **proceso del authenticator aaa del dot11 del debug** - Este debug le ayuda a diagnosticar los problemas con las comunicaciones negociadas. La información detallada muestra lo que envía cada participante en la negociación y muestra la respuesta del otro participante. Usted puede también utilizar este debug conjuntamente con el **comando debug radius authentication**.
- **falla de conexión de la estación del dot11 del debug** - Este debug le ayuda a determinar si los clientes están fallando la conexión y le ayuda a determinar la razón de los incidentes.