Configuratie van WAP/WAP2 met Vooraf gedeelde sleutel: IOS 15.2JB en hoger

Inhoud

Inleiding

Dit document beschrijft een voorbeeldconfiguratie voor Wireless Protected Access (WAP) en WAP2 met een vooraf gedeelde toets (PSK).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Bekendheid met de GUI of de opdrachtregel interface (CLI) voor de Cisco IOS®-software
- Bekendheid met de concepten PSK, WAP en WAP2

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Aironet 1260 access point (AP) dat Cisco IOS-softwarerelease 15.2JB draait.

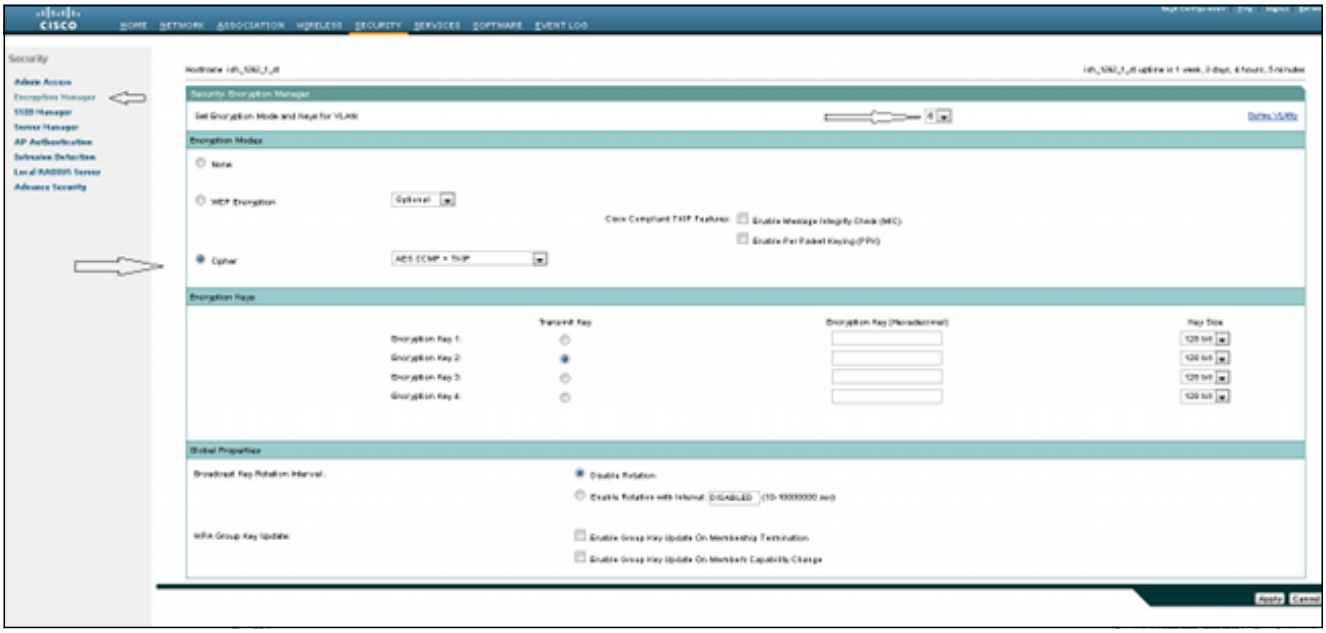
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Configuratie met GUI

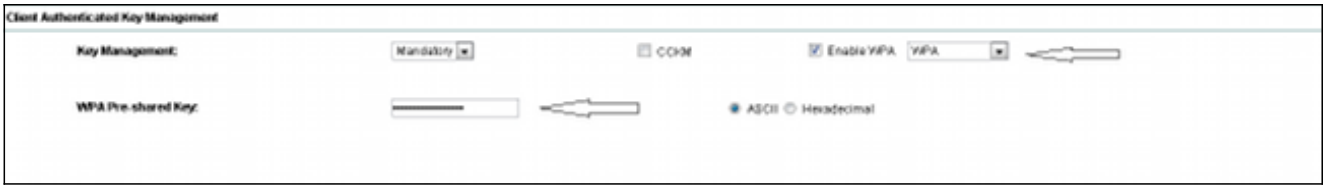
Deze procedure beschrijft hoe u WAP en WAP2 met een PSK kunt configureren in de Cisco IOS-software GUI:

1. Stel de Encryption Manager voor het VLAN in dat voor de Service Set-id (SSID) is gedefinieerd. Navigeer naar **Security > Encryption Manager**, controleer of Cijfer is ingeschakeld en selecteer **AES CCMP + TKIP** als het algoritme dat voor beide SSID's moet worden gebruikt.



2. Schakel het juiste VLAN in met de encryptieparameters die in Stap 1 zijn gedefinieerd. Navigeer naar **Security > SSID Manager** en selecteer SSID in de huidige SSID-lijst. Deze stap is gebruikelijk voor zowel de WAP- als de WAP2-configuratie.

3. Stel in de SSID pagina Key Management in op **Verplicht** en controleer het selectieteken **WAP inschakelen**. Selecteer **WAP** uit de vervolgkeuzelijst om WAP in te schakelen. Voer de vooraf gedeelde sleutel in.



4. Selecteer **WAP2** uit de vervolgkeuzelijst om WAP2 in te schakelen.

Configuratie met CLI

Opmerkingen:

Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met show. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

Dit is dezelfde configuratie gedaan binnen de 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
```

Verifiëren

Om te bevestigen dat de configuratie correct werkt, navigeer naar **Associatie** en controleer of de client is aangesloten:

U kunt de client-associatie in de CLI ook met dit syslogbericht controleren:

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

Problemen oplossen

> **Opmerking:** Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met **debug opgeeft.**

Gebruik deze debug-opdrachten om problemen met de connectiviteit op te lossen:

- **debug dot11 aaa Manager keys** - Dit debug toont de handdruk die optreedt tussen AP en de client tijdens onderhandelingen over de parwise transient key (PTK) en group transient key (GTK).
- **debug dot11 a.u.b.** een **authenticator state-machine** - Dit debug toont de verschillende onderhandelingsstaten die een client doorgeeft als associeert en authentiek verklaart. De staatsnamen geven deze staten aan.
- **debug dot11 a authenticator proces** - Dit debug helpt u problemen bij het diagnosticeren van communicatie via onderhandelingen. De gedetailleerde informatie laat zien wat elke deelnemer aan de onderhandelingen stuurt en toont de reactie van de andere deelnemer. U kunt dit debug ook gebruiken in combinatie met de opdracht **Straalverificatie** uitvoeren.
- **defect van de dot11-stationverbinding** debug - Dit debug helpt u om te bepalen of de klanten de verbinding niet aangaan en helpt u de reden voor mislukkingen te bepalen.