사전 공유 키를 사용하여 WPA/WPA2 구성: IOS 15.2JB 이상

목차

소개

이 문서에서는 PSK(Pre-Shared Key)가 있는 WPA(Wireless Protected Access) 및 WPA2의 샘플 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco IOS® 소프트웨어의 GUI 또는 CLI(Command-Line Interface)에 대한 지식
- PSK, WPA 및 WPA2의 개념 숙지

사용되는 구성 요소

이 문서의 정보는 Cisco IOS Software 릴리스 15.2JB를 실행하는 Cisco Aironet 1260 Access Point(AP)를 기반으로 합니다.

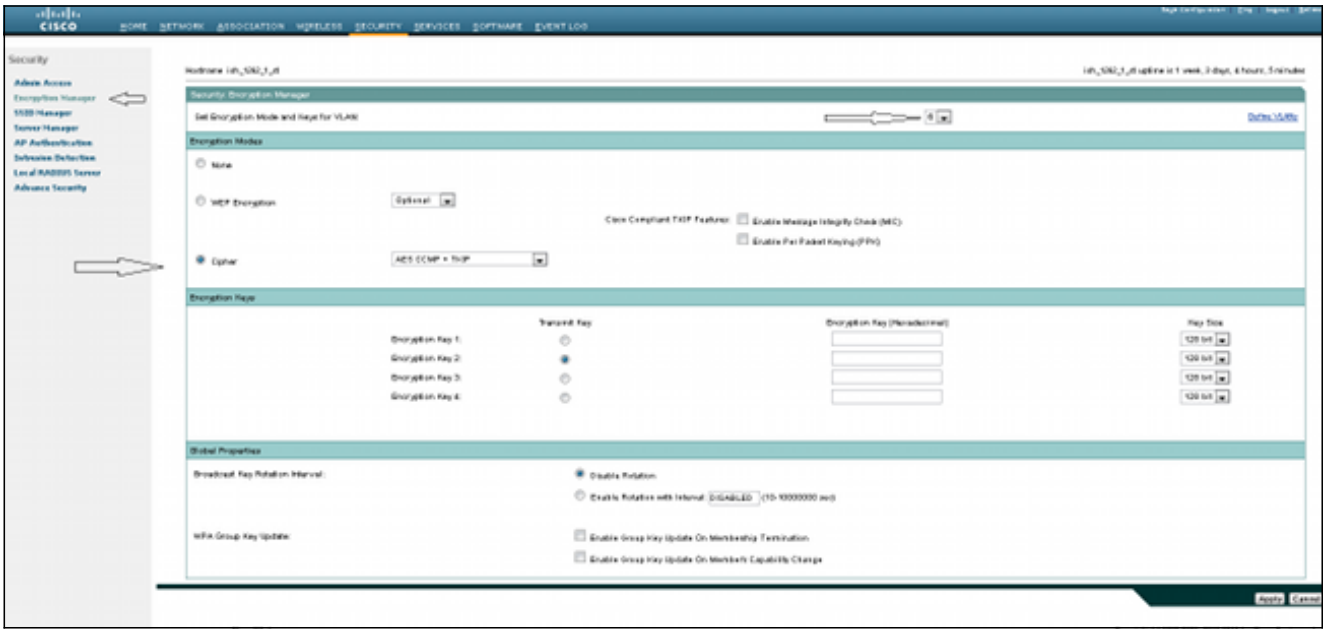
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

GUI를 통한 구성

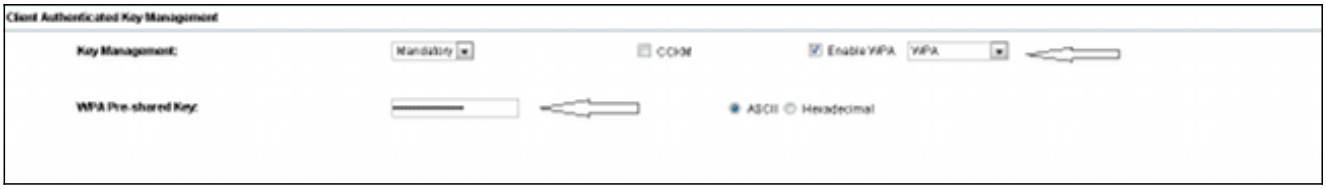
다음 절차에서는 Cisco IOS 소프트웨어 GUI에서 PSK를 사용하여 WPA 및 WPA2를 구성하는 방법에 대해 설명합니다.

1. SSID(Service Set Identifier)에 대해 정의된 VLAN에 대해 암호화 관리자를 설정합니다. Security(**보안**) > **Encryption Manager(암호화 관리자**)로 이동하여 Cipher(암호)가 활성화되었는지 확인한 다음 AES CCMP + TKIP를 두 SSID에 모두 사용할 암호로 선택합니다.



2. 1단계에서 정의된 암호화 매개변수를 사용하여 올바른 VLAN을 활성화합니다. **Security(보안)** > **SSID Manager(SSID 관리자**)로 이동하고 Current SSID List(현재 SSID 목록)에서 SSID를 선택합니다. 이 단계는 WPA 및 WPA2 컨피그레이션에 공통적으로 적용됩니다.

3. SSID 페이지에서 Key Management(키 관리)를 **Mandatory(필수)**로 설정하고 Enable WPA(**WPA 활성화)** 확인란을 선택합니다. WPA**를** 활성화하려면 드롭다운 목록에서 WPA를 선택합니다. WPA 사전 공유 키를 입력합니다.



4. WPA2를 활성화하려면 드롭다운 목록에서 **WPA2**를 선택합니다.

CLI를 사용한 구성

참고:

이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다. **show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

이는 CLI 내에서 수행되는 것과 동일한 컨피그레이션입니다.

```
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
```

다음을 확인합니다.

컨피그레이션이 제대로 작동하는지 확인하려면 **Association(연결)**으로 이동하고 클라이언트가 연결되었는지 확인합니다.

CLI에서 다음 syslog 메시지와 클라이언트 연결을 확인할 수도 있습니다.

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

문제 해결

> **참고: debug** 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

연결 문제를 해결하려면 다음 debug 명령을 사용합니다.

- **debug dot11 aaa manager keys** - 이 디버그는 AP와 클라이언트 사이에 PTK(pairwise transient key) 및 GTK(group transient key) 협상 중 발생하는 핸드셰이크를 표시합니다.
- **debug dot11 aaa authenticator state-machine** - 이 디버그는 클라이언트가 연결하고 인증하면서 통과하는 협상의 다양한 상태를 표시합니다. 상태 이름은 이러한 상태를 나타냅니다.
- **debug dot11 aaa authenticator process** - 이 디버그는 협상된 통신 문제를 진단하는 데 도움이 됩니다. 세부 정보는 협상의 각 참가자가 보내는 내용을 표시하고 다른 참가자의 응답을 표시합니다. 이 디버그를 debug radius **authentication** 명령과 함께 사용할 수도 있습니다.
- **debug dot11 station connection failure** - 이 디버그는 클라이언트가 연결에 실패하는지 확인하고 실패 원인을 확인하는 데 도움이 됩니다.