事前共有鍵による WPA/WPA2 の設定： IOS 15.2JB 以降

目次

概要

このドキュメントでは、事前共有キー（PSK）を使用した Wireless Protected Access（WPA）および WPA2 の設定例を説明します。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco IOS® ソフトウェアの GUI またはコマンドライン インターフェイス（CLI）
- PSK、WPA、および WPA2 の概念

使用するコンポーネント

このドキュメントの情報は、Cisco IOS ソフトウェア リリース 15.2JB を実行する Cisco Aironet 1260 アクセス ポイント（AP）に基づくものです。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

GUI による設定

次の手順は、Cisco IOS ソフトウェア GUI で PSK を使用して WPA および WPA2 を設定する方法を説明しています。

1. Service Set Identifier（SSID）用に定義されている VLAN の Encryption Manager をセットアップします。 [Security] > [Encryption Manager] に移動し、[Cipher] が有効になっていることを確認し、両方の SSID に使用する暗号化として [AES CCMP + TKIP] を選択します。

2. ステップ 1 で定義した暗号化パラメータを使用して、正しい VLAN を有効にします。 [Security] > [SSID Manager] に移動し、[Current SSID Lis] から SSID を選択します。 このステップは、WPA と WPA2 の設定で共通です。

3. SSID ページで、[Key Management] を [Mandatory] に設定し、[Enable WPA] チェックボックスをオンにします。 ドロップダウン リストから [WPA] を選択し、WPA を有効にします。 WPA の事前共有キーを入力します。

4. ドロップダウン リストから [WPA2] を選択し、WPA2 を有効にします。

CLI による設定

> **注**：
>
> このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。
>
> 特定の show コマンドがアウトプット インタープリタ ツール（登録ユーザ専用）でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

これは CLI 内で行う設定と同じです。

```
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
```

確認

設定が適切に動作していることを確認するには、[Association] に移動し、クライアントが接続されていることを確認します。

次の syslog メッセージで、CLI でのクライアント関連付けを確認できます。

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

トラブルシューティング

> **注:** debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

接続に関する問題のトラブルシューティングを行うには、次の debug コマンドを使用します。

- **debug dot11 aaa manager keys**：pairwise transient key（PTK）と group transient key（GTK）がネゴシエートするときに AP とクライアント間で発生するハンドシェイクを表示します。
- **debug dot11 aaa authenticator state-machine**：クライアントが関連付けと認証を実行する際に遷移していくネゴシエーションのさまざまな状態を表示します。 状態名は、それぞれの状態を示します。
- **debug dot11 aaa authenticator process**：ネゴシエーション関連の通信に関する問題を診断する場合、この debug コマンドは非常に有効です。 このコマンドによって表示された詳細情報には、ネゴシエーションのそれぞれの側が送信した内容と、もう一方が応答した内容が表示されます。 この debug コマンドは、**debug radius authentication** コマンドと併用することも

できます。

- debug dot11 station connection failure：この debug コマンドは、クライアントが接続に失敗しているかどうかを判別したり、失敗した接続の原因を特定したりする場合に有用です。