使用预共享密钥配置WPA/WPA2:IOS 15.2JB及更高版本

目录

简介

本文档介绍使用预共享密钥(PSK)的无线保护访问(WPA)和WPA2的配置示例。

先决条件

要求

Cisco 建议您了解以下主题：

- 熟悉Cisco IOS®软件的GUI或命令行界面(CLI)。
- 熟悉PSK、WPA和WPA2的概念

使用的组件

本文档中的信息基于运行Cisco IOS软件版本15.2JB的Cisco Aironet 1260接入点(AP)。

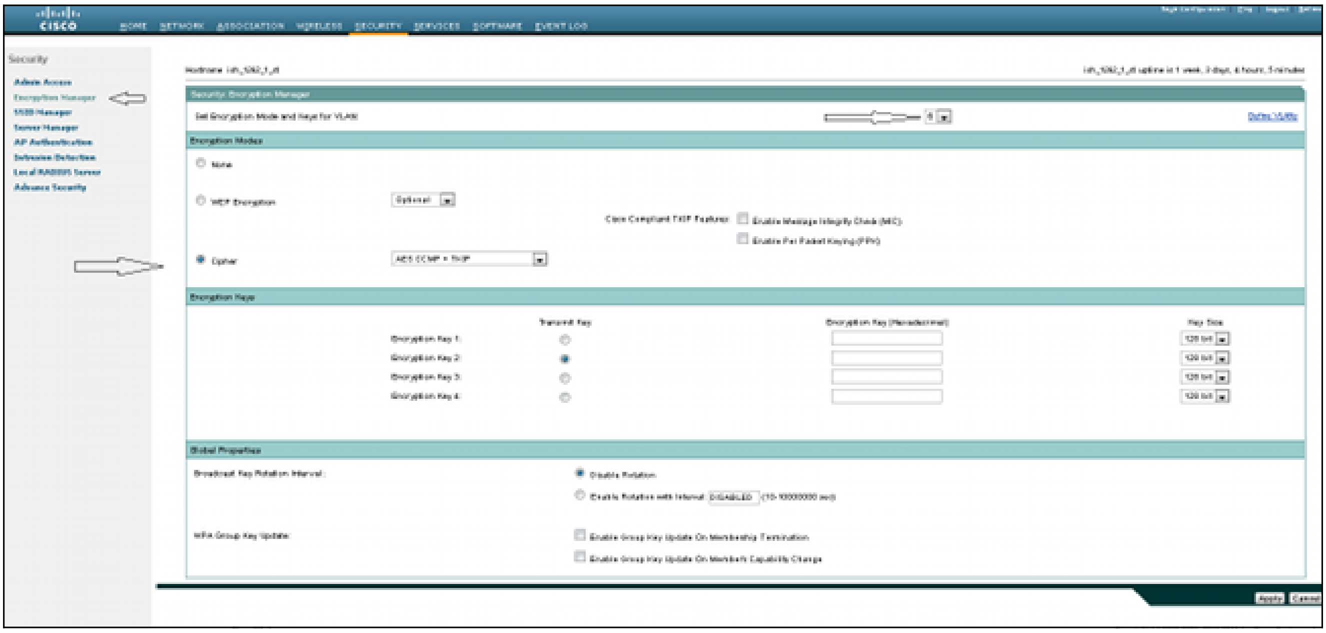
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

使用GUI进行配置

此程序介绍如何在Cisco IOS软件GUI中使用PSK配置WPA和WPA2:

1. 为为服务集标识符(SSID)定义的VLAN设置加密管理器。 导航至**Security** > **Encryption Manager**，确保已启用Cipher，并选择**AES CCMP + TKIP**作为要用于两个SSID的密码。



Hostname [illegible]

Security: Encryption Manager

Set Encryption Mode and Keys for VLAN: 6 | Define VLANs

Encryption Modes

○ None

○ WEP Encryption Optional

Cisco Compliant TKIP Features: □ Enable Message Integrity Check (MIC)
□ Enable Per Packet Keying (PPK)

● Cipher AES CCMP + TKIP

Encryption Keys

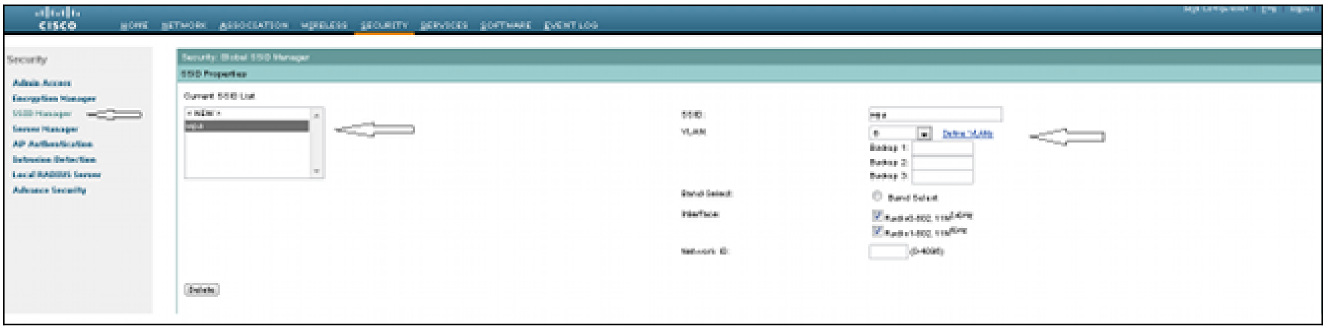
	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	○		128 bit
Encryption Key 2:	●		128 bit
Encryption Key 3:	○		128 bit
Encryption Key 4:	○		128 bit

Global Properties

Broadcast Key Rotation Interval: ● Disable Rotation
○ Enable Rotation with Interval: DISABLED (10-10000000 sec)

WPA Group Key Update: □ Enable Group Key Update On Membership Termination
□ Enable Group Key Update On Member's Capability Change

2. 使用步骤1中定义的加密参数启用正确的VLAN。导航至**Security** > **SSID Manager**，然后从Current SSID List中选择SSID。此步骤对WPA和WPA2配置都是常见的。



Security: Global SSID Manager

SSID Properties

Current SSID List
< NEW >
wpa

SSID: wpa

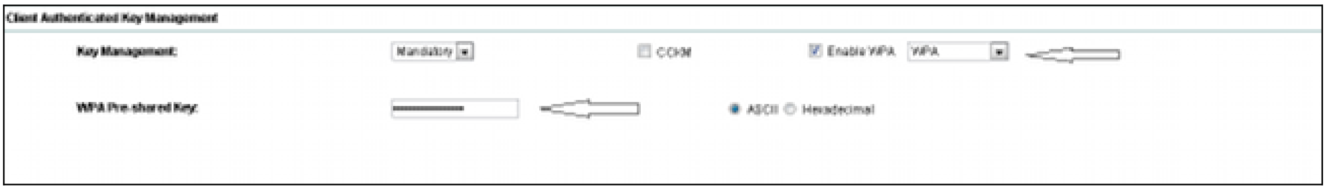
VLAN: 6 | Define VLANs
Backup 1:
Backup 2:
Backup 3:

Band Select: ○ Band Select

Interface: ☑ Radio0-802.11N 2.4GHz
☑ Radio1-802.11N 5GHz

Network ID: (0-4096)

3. 在SSID页中，将Key Management设置为**Mandatory**，然后选中**Enable WPA复**选框。从下拉列表中选择**WPA**以启用WPA。输入WPA预共享密钥。

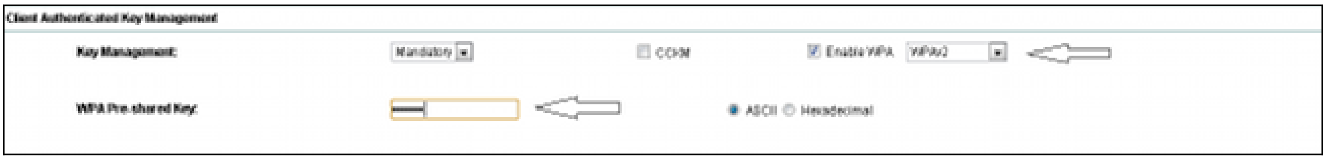


Client Authenticated Key Management

Key Management: Mandatory | □ CCKM | ☑ Enable WPA WPA

WPA Pre-shared Key: •••••••••••••• | ● ASCII ○ Hexadecimal

4. 从下**拉列**表中选择WPA2以启用WPA2。



Client Authenticated Key Management

Key Management: Mandatory ▾ □ CCKM ☑ Enable WPA WPAv2 ▾

WPA Pre-shared Key: ——— ● ASCII ○ Hexadecimal

使用CLI进行配置

注意：

使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

命令输出解释程序工具（仅限注册用户）支持某些 **show 命令。**使用输出解释器工具来查看 show 命令输出的分析。

这与在CLI中执行的配置相同：

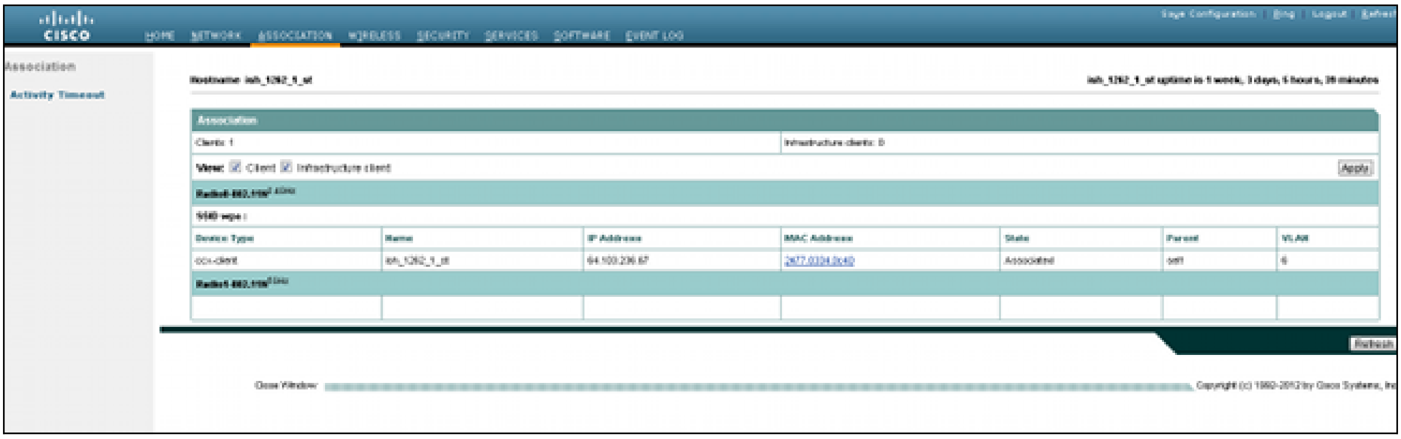
```
sh run
Building configuration...Current configuration : 5284 bytes
!
! Last configuration change at 04:40:45 UTC Thu Mar 11 1993
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ish_1262_1_st
!
!
logging 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
```

验证

要确认配置工作正常，请导航至**关联**，并验证客户端是否已连接：



Hostname ish_1262_1_st

ish_1262_1_st uptime is 1 week, 3 days, 5 hours, 39 minutes

Association

Clients: 1

Infrastructure clients: 0

View: ☑ Client ☑ Infrastructure client

Radio0-802.11N 2.4GHz

SSID wpa :

Device Type	Name	IP Address	MAC Address	State	Parent	VLAN
ccx-client	ish_1262_1_st	64.103.236.67	2477.0334.0c40	Associated	self	6

Radio1-802.11N 5GHz

Copyright (c) 1992-2012 by Cisco Systems, Inc

您还可以验证CLI中客户端与以下系统日志消息的关联：

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

故障排除

注意：使用 **debug 命令之前，请参阅**有关 Debug 命令的重要信息。

使用以下debug命令排除连接问题：

- **debug dot11 aaa manager keys** — 此调试显示AP和客户端之间在成对临时密钥(PTK)和组临时密钥(GTK)协商时发生的握手。
- **debug dot11 aaa authenticator state-machine** — 此调试显示客户端在关联和身份验证时通过的协商的各种状态。状态名称即可表示各种状态。
- **debug dot11 aaa authenticator process** — 此调试可帮助您诊断协商通信的问题。其详细信息显示了每个协商参与者所发送的内容，并显示了其他参与者的响应。您也可以将该 debug 命令与 **debug radius authentication 命令结合使用。**
- **debug dot11 station connection failure** — 此调试可帮助您确定客户端是否连接失败，并帮助您确定失败的原因。