Konfiguration von WPA/WPA2 mit vorinstalliertem Schlüssel: IOS 15.2JB und höher

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Konfiguration mit GUI Konfiguration mit CLI Überprüfen Fehlerbehebung

Einführung

In diesem Dokument wird eine Beispielkonfiguration für Wireless Protected Access (WPA) und WPA2 mit einem Pre-Shared Key (PSK) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Vertrautheit mit der GUI oder der Befehlszeilenschnittstelle (CLI) für die Cisco IOS[®] Software
- Vertrautheit mit den Konzepten von PSK, WPA und WPA2

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco Aironet 1260 Access Point (AP), der die Cisco IOS Software Release 15.2JB ausführt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Konfiguration mit GUI

In diesem Verfahren wird beschrieben, wie WPA und WPA2 in der Benutzeroberfläche der Cisco IOS-Software mit einem PSK konfiguriert werden:

 Richten Sie den Verschlüsselungsmanager für das für den Service Set Identifier (SSID) definierte VLAN ein. Navigieren Sie zu Security > Encryption Manager, stellen Sie sicher, dass Cipher aktiviert ist, und wählen Sie AES CCMP + TKIP als Verschlüsselung für beide SSIDs aus.

cisco gove ge	THORE ASSOCIATION WIRELESS	ECURITY SERVICES SOFT	HARE EVENTION		ante constraints - End Index - Dec	
Security	Notices (d)_002,5_d				ish_SN2_1_displice is 1 week, i-dopt, il hours, 5 nindes	
Encryption Nameper	Security Broryption Memoper					
1100 Hanaper	Set Encryption Mode and Neys for VLAS				Date: 34/0x	
AP Authoritoriton	Encryption Modes					
Soferanian Defection Local AABERS Server	© 1674					
Advance Security	O wer broughton	üpterst m				
			Citics Compliant Table	Feature: Erutin Message Integrity Chica (MIC)		
				Eratin Per Fadet Keyleg (PPr)		
	Dphw	AES COMP + THIP				
	Energetion Naya					
			Transmit Rep	Droryption Ray (Neradectine))	Hey from	
		Onorgation Ray 1	0		428.04	
		Enorgetion Key 2	•		420 647	
		Drotyption Ray 3	0		428.04	
		Enorgetion Key E	0		420.64 (m)	
	Bistel Properties					
	Browboard, Rep Rotation, History 1		· Dauble Relation			
			Caratha fourier with Interval (Individual) (05-10000000 ave)			
_	with Group Key lipitate		E Enable Group Hay Bodd	On Membership Termination		
			Enables Group May Special	On Minister's Capability Change		
					Acoty State	

2. Aktivieren Sie das richtige VLAN mit den in Schritt 1 definierten

Verschlüsselungsparametern. Navigieren Sie zu **Security > SSID Manager**, und wählen Sie die SSID aus der Liste Current SSID (Aktuelle SSID-Liste) aus. Dieser Schritt ist sowohl für die WPA- als auch die WPA2-Konfiguration üblich.

cisco gore	BETWORK BEFOREFOR MERLESS SECURITY SERVICES SOFTWAR	RE DANTIOS		place de la calera
Security Admin.Access	Security: Birtol 150 Managar 150 Progettee			
Encryption Manager SSID Hanager Server Manager AP Authentication Indexion Indextion Indexion Indextion Land ApDIDIS Server	Ourwet 558 Lat	550. VLAM	Real Contractions	
Advance Security		Rand Gelecit	C Band Select	
		Piefice	12 Rad at 400, 116 Are 12 Rad at 400, 116 Are	
		Network E:	(0-4004)	
	(Beinte)			

3. Legen Sie auf der Seite SSID Key Management (Schlüsselverwaltung) auf Obligatorisch fest, und aktivieren Sie das Kontrollkästchen Enable WPA (WPA aktivieren). Wählen Sie WPA aus der Dropdown-Liste aus, um WPA zu aktivieren. Geben Sie den WPA Pre-shared Key ein.

Client Authenticated Key Management				
Key Management;	Mandatory 💌	Ссня	Enable WPA WPA	
WPA Pre-shared Key.			NGCII 🗇 Hexadecimal	

4. Wählen Sie WPA2 aus der Dropdown-Liste aus, um WPA2 zu aktivieren.

Client Authenticated Key Management				
Key Management:	Mandatory 💌	🖾 ссня	🗷 Enable VPA 🛛 VPAQ	
WPA Pre-shared Key:		• •	SCII © Hexadecimal	

Konfiguration mit CLI

Hinweise:

Verwenden Sie das <u>Command Lookup Tool</u> (nur <u>registrierte</u> Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Das <u>Output Interpreter Tool</u> (nur <u>registrierte</u> Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter Tool, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Dies ist die gleiche Konfiguration wie in der CLI:

```
sh run
Building configuration...Current configuration : 5284 bytes
1
! 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
1
1
logging rate-limit console 9
enable secret 5 $1$Iykv$1tUkNYeB6omK41S181TbQ1
1
no aaa new-model
ip cef
ip domain name cisco.com
1
!
1
dot11 syslog
1
dot11 ssid wpa
vlan 6
authentication open
authentication key-management wpa
mbssid guest-mode
```

```
wpa-psk ascii 7 060506324F41584B56
1
dot11 ssid wpa2
vlan 7
authentication open
authentication key-management wpa version 2
wpa-psk ascii 7 110A1016141D5A5E57
1
bridge irb
1
1
1
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
1
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
1
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
1
encryption vlan 7 mode ciphers aes-ccm tkip
1
ssid wpa
!
```

```
ssid wpa2
1
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
1
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
1
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
1
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
1
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
```

Überprüfen

Um zu überprüfen, ob die Konfiguration ordnungsgemäß funktioniert, navigieren Sie zu **Zuordnung**, und überprüfen Sie, ob der Client verbunden ist:

cisco	HOME	METWORK ASSOCIATION V	QABLESS SECURITY SERVICES	E SOLLANE ENDALIOO			Sage Configuratio	in Bing Logout Batha		
Association Activity Timeout		Rostname ish_1282_1_st				iab_036	t_1_st uptime is 1 week,) days, 6 hours, 28 minutes		
		Association								
		Chertic 1			Wheelpachare-chemic D	Maxhutus dets: 0				
		Meet Z Clent Z Infactuative clent				Apple				
		Ratios-MO. 110 ^{2 Alley}								
540 wpe :										
		Device Type	Rame	IF Address	MAC Address	State	Parent	VLAR		
		cos-diet.	86,5282,5,8	64.103.236.67	2877.0304.0x40	Associated	047	4		
Radius 442.499 ⁴ Dec										
	-							fates		
		Occer Wittelow'					Capyright (r	() 1982-2012 by Gluco Systems, P		

Sie können mit der folgenden Syslog-Meldung auch die Clientzuordnung in der CLI überprüfen:

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

Fehlerbehebung

Hinweis: Weitere Informationen <u>zu Debug-Befehlen</u> vor der Verwendung von **Debug-**Befehlen finden Sie unter<u>Wichtige Informationen</u>.

Verwenden Sie diese Debugbefehle, um Verbindungsprobleme zu beheben:

- debug dot11 aaa manager keys Dieses Debuggen zeigt den Handshake zwischen dem Access Point und dem Client als paarweise transient key (PTK) und group transient key (GTK) negotiate (Gruppentransient Key) an.
- debug dot11 aaa authentifizierer state-machine Dieses Debuggen zeigt die verschiedenen Verhandlungszustände an, die ein Client durchläuft, während der Client verknüpft und authentifiziert. Diese Zustände werden durch die Zustandsnamen angegeben.
- debug dot1aaa authentifizierer prozess Dieser debug hilft Ihnen bei der diagnostizierung von problematischer kommunikation. Die detaillierten Informationen zeigen, was jeder Teilnehmer an der Aushandlung sendet, und zeigen die Antwort des anderen Teilnehmers an. Sie können dieses Debuggen auch zusammen mit dem Befehl debug radius authentication verwenden.
- debug dot1 station connection failure Mit diesem Debuggen können Sie feststellen, ob die Clients die Verbindung nicht herstellen können, und den Grund für Fehler ermitteln.