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

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren Configuratie met GUI Configuratie met CLI Verifiëren Problemen oplossen

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 $\mathsf{IOS}^{\circledast}$ -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 IOSsoftware GUI:

 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.

nen Annen reprösen Nanneper Billenaper Anthenfeurlen Anthenfeurlen di ANDERS Server nanne Security	ofmane (H)_552,1,4 Instantio, Discussion Memogram End Encorpetion Mode and Reys for VLXX Installation Modes	_			ish_SB2,5,d spline in tweek, indept, & hours, 5 mind
reptine Viscoper D Nanager Net Nanager Anthenite utilize Anthenite United all RADIOS Server reace Scrattly	leastly Groupdon Mode and Neye for VLAX beingtion Mode and Neye for VLAX beingtion Modes				
Binkenspor Ver Nanspor Aufbenföcklice af RADDO's Server venes Societlig	Sel Encryption Wede and Neys for VLAX Promption Modes				
Anthenticution reason Detection al IRADERS Server reason Security	Promption Modes				Dates. 15.00a
reation Defaction of MADDIS Server searce Security	0.844				
same security	0.000				
	0 wer breaten	üptiengt m			
			Clock Compliant T	KIP Features: 🔝 Erabin Message Islagily Cheb (MC)	
				Evalue Per Padert Keying (PPv)	
	Epher	Act COP + THP			
	horgition Neye				
			Turand fay	Droryption Ray (Neraductine))	They Side
		Drorppton Ray 1	0		120.04
		Encryption Key 2	•		120.04
		Dronypition Ray 3	0		120.04
		Shorypton Ray E	0		General M
	Sobel Properties				
	Broadcast Rep Rotation Interval:		· Caudia Relation		
			C Exable Polatics with (New 10 (144) 10 (15 1000000 av)	
	with Group Key Update:		Enable Group Key lips	late On Ministentria Termination	
			Enables Group Hay light	Sate On Merchant Expatrilly Change	

 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.

cisco gore	NETWORK ASSOCIATION MURLESS SECURITY SERVICES SOFTWAR	e partico		Ministratives and effort
Security Admin.Access Encounties Namour	Secondy Binkel (550 Manager 550 Properties Correct 550 Ltat			
Still Hanaper Server Hanaper AP Artheolication Infoncion Detection Local RABIES Server Advance Security		550. VLAN	e e bita Mate Basay 1 Basay 2 Basay 2	
		Bard Salar: Partica	David Solvet Elaudi 40-002, 114/4016 Elaudi 4-002, 114/6016	
	(Seine)	Network C:	(0-404)	

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.

Client Authenticated Key Management					
Key Management;	Mandatory m	🖂 ссни	Enable WPA WPA	•	
WPA Pre-shared Key:	<		ICII O Hevadecimal		

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

Client Authenticated Key Management					
Key Management:	Mandatory 💌	Псски	Enable VPA VPA/2	• <>>	
WPA Pre-shared Key.	=<		SCII © Hexadecimal		

Configuratie met CLI

Opmerkingen:

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

De <u>Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde</u> <u>opdrachten met show.</u> 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
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
1
encryption vlan 6 mode ciphers aes-ccm tkip
1
encryption vlan 7 mode ciphers aes-ccm tkip
1
ssid wpa
1
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
1
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
!
ssid wpa
1
```

```
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
```

Verifiëren

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

cisco	HOME	SETWORK ASSOCIATION	WIRRLESS SECURITY SERVED	ES SOFTWARE EVENTION			Saya Contigoration	. Brd Color Tour		
Association Activity Timeout		Rothanie inh JSR2.5.4 inh JSR2.5.4						days, 5 hours, 36 minutes		
		Association								
		Chertic 1			Wheelvachure-chertic D					
		West 🗷 Client 🗷 Infractives	ute client					Apple		
		Radios-862, 110 ² Alley								
		\$140 wpe :	566 mpe i							
		Device Type	Rame	IP Address	MAC Address	State	Parent	VLAX		
		ocs-diett	86,5082,5,8	64.500.236.67	2677.0304.0x40	Associated	941	4		
		Radio 6 482, 110 ^{1 (H)}								
								fishes		
		Occas Witnesser					Capyright (c)	1982-2012 by Casos Systems,		

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 <u>Important Information on Debug Commands (Belangrijke informatie</u> <u>over opdrachten met debug) voordat u opdrachten met debug opgeeft.</u>

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.