WDS auf autonomen APs mit lokalem RADIUS-Server konfigurieren

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren **GUI-Konfigurationen** SSID erstellen Lokale RADIUS-Serverkonfiguration für WDS AP Lokale RADIUS-Serverkonfiguration auf dem WDS-Client-AP WDS für WDS AP aktivieren WDS auf dem WDS-Client-AP aktivieren **CLI-Konfigurationen** WDS-AP WDS-Client-AP Überprüfung CLI-Verifizierungs-Ausgabe auf WDS AP CLI-Verifizierungs-Ausgabe auf WDS-Client-AP Fehlerbehebung

Einleitung

In diesem Dokument wird beschrieben, wie Wireless Domain Services (WDS) in einer Konfiguration eines autonomen Access Points (AP) mit einem Iokalen RADIUS-Server konfiguriert werden. Das Dokument konzentriert sich auf Konfigurationen über die neue GUI, bietet aber auch CLI-Konfigurationen (Command Line Interface).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse der grundlegenden GUI- und CLI-Konfiguration auf autonomen APs verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Access Point der Serie 3602e auf der unabhängigen AP IOS[®] Software, Version 15.2(4)JA1; Dieses Gerät fungiert als WDS-AP und lokaler RADIUS-Server.
- Cisco Access Point der Serie 2602i auf der unabhängigen AP IOS-Software, Version 15.2(4)JA1; Dieses Gerät fungiert als WDS-Client-AP.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konfigurieren

Anmerkung: 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.

GUI-Konfigurationen

SSID erstellen

In diesem Verfahren wird beschrieben, wie Sie einen neuen Service Set Identifier (SSID) erstellen.

1. Navigieren Sie zu **Security > SSID Manager**, und klicken Sie auf **NEU**, um eine neue SSID zu erstellen.

ululu cisco	HOME NETWORK ASSOCIATION	WIRELESS SECURITY	SERVICES MANAGEMENT	SOFTWARE EVENT LOG	
Security	Hostname MAIB3602e				
Encryption Manager SSID Manager	Security: Global SSID Manager SSID Properties				
SSID Manager Server Manager AP Authentication Intrusion Detection Local RADIUS Server	Current SSD Liet	*		SSAD: VLAR:	VDS-EAP < NONE = w <u>Define VLANs</u> Bodap 1:
Harance security		w		Band-Select:	Bookup 2:
				Interface:	Resiled-602.11N ^{2.45He} Resiled-602.11N ^{55He}
				Helwark ID:	(0-4096)

2. Konfigurieren Sie die SSID für die EAP-Authentifizierung (Extensible Authentication Protocol).

Client Authentication Settings		
Methods Accepted:		
Øpen Authentication:	< NO ADDITION-	
Web Authentication	with MAC Authentication with EAP	
Shared Authentication:	with MAC Authentication and EAP with MAC Authentication or EAP	
Network EAP:	<pre>vith Optional EAP </pre> </th <th></th>	
Server Priorities:		
EAP Authentication Servers		MAC Authentication Servers
Use Defaults Define Defaults		Use Defaults Define Defaults
Customize		Customize
Priority 1: < NONE > w		Priority 1: < NONE >
Priority 2. < NONE > 💌		Priority 2. < NONE > 💌
Priority 3: <none> •</none>		Priority 3.

3. Legen Sie die gewünschte Verschlüsselungsstufe fest. Verwenden Sie in diesem Beispiel Wi-Fi Protected Access 2 (WPA2).

Client Authenticated Key Management			
Key Management:	Mandatory -	ССКМ	Enable WPA V4PAv2 V4PA
WPA Pre-shared Key:			ASCI Hexadecinal WPAv2 dot11r
11w Configuration:	Optional		
11w Association-comeback:	1000 (1000-20000)		
11w Saquery-retry:	100 (100-500)		

- 4. Klicken Sie auf Übernehmen, um die Einstellungen zu speichern.
- 5. Navigieren Sie zu **Security > Encryption Manager**, und wählen Sie die erforderliche Verschlüsselungsmethode aus.

Security	RADIO0-802.11N	2.4GHZ	RADIO1-802.11N5GHZ
Admin Access Encryption Manager	Hostname MAIB2602i		
SSID Manager Server Manager AP Authentication	Security: Encryption Mana Encryption Modes	ager - Radio0-802.11N ^{2.4GHz}	
Intrusion Detection	None		
Advance Security	WEP Encryption	Optional 👻	isco Compliant TKIP Features: 🔲 Enable
	Opher	WEP 128 bit WEP 128 bit	Enable
	Encryption Keys	WEP 40 bit TKIP CKIP CMIC	
		CKIP-CMIC TKIP + WEP 128 bit TKIP + WEP 40 bit AES CCMP AES CCMP + TKIP AES CCMP + TKIP + WEP 12 En AES CCMP + TKIP + WEP 12 En AES CCMP + TKIP + WEP 12	t Key 28 bit) bit
		Encryption Key 4:	0

Lokale RADIUS-Serverkonfiguration für WDS AP

In diesem Verfahren wird beschrieben, wie der lokale RADIUS-Server auf dem WDS AP konfiguriert wird:

 Navigieren Sie zu Security > Server Manager, fügen Sie die WDS AP Bridge Virtual Interface (BVI)-IP als lokalen RADIUS hinzu, und fügen Sie einen gemeinsamen geheimen Schlüssel hinzu.

Corporate Servers				
Current Server List				
RADIUS •				
C + Million -	IP Version:	₱ IPV4 © IPV6		
< NEW > Local-Fladks	Server Name:	Local-Radius		
	Server:	10.106.54.146	(Hostname or IP Address)	
	Shared Secret:	•••••		
Delete	Authentication Port (optional):	1812 (0-65536)		
	Accounting Port (optional):	1813 (0-65536)		
				Apply Cancel

 Navigieren Sie zu Sicherheit > Lokaler Radius-Server > Registerkarte General Set-Up (Allgemeine Einrichtung). Definieren Sie die EAP-Protokolle, die Sie verwenden möchten. Aktivieren Sie in diesem Beispiel die LEAP-Authentifizierung (Light Extensible Authentication Protocol).

ululu cisco	HOME NET	NORK ASSOCIATION	wpritess	SECURITY	SERVICES	BANAGEMENT	SOFTWARE	EVENT LOG		Says Configuration	E Pra I	Logout
Security	1	STATISTICS)i	GEN	IRAL SET-UP			EAP-FAST SET-UP			
Admin Access Encryption Manager	Hostnam	MAIB-WDS-AP							MAIB WDS AP uptime is 10 hos	ars, 42 minutes		
SSID Manager	Securi	Security: Local RADIUS Server - General Set-Up										
Server Manager AP Authentication	Local P	adius Server Authen	tication Settin	g1								
Intrusion Detection	Enabl	Authentication Prot	cols:		00	AP FAST						
Local RADIUS Server					R L	LAP						
Advance security					E M	AC						
											Apply	Cancel

3. Sie können auf derselben Seite auch Network Access Server (NAS)-IPs und Anmeldeinformationen für den Client-Benutzernamen/Kennwort hinzufügen. Die Konfiguration eines lokalen RADIUS auf einem WDS AP ist abgeschlossen.

Network Access Servers (AAA Clients)					
Current Network Access Servers < NEW > 10 106 54 846	Network Access	s Server:	10.106.54.146	(P Address)	
Delete	anared secret.			, 	Apply Cancel
Individual Users					
Current Users	Username: Password: Confirm Password: Group Name:	< NONE > •	* Text © NT Hest		
					Apply Concel

Lokale RADIUS-Serverkonfiguration auf dem WDS-Client-AP

In dieser Abbildung wird gezeigt, wie die IP-Adresse des WDS Access Points als RADIUS-Server konfiguriert wird:

Corporate Servers				
Current Server List RADIUS -				
	IP Version:	PV4 0 PV5		
< NEW > WDS-Rodius	Server Name:	WDS-Radius		
	Server:	10.106.54.146	(Hostname or IP Address)	
	Shared Secret:	•••••		
Delete	Authentication Port (optional):	1812 (0-65536)		
	Accounting Port (optional):	1813 (D-65536)		
				Apply Cancel

Beide APs sind jetzt mit SSIDs für die LEAP-Authentifizierung konfiguriert, und der WDS-Server fungiert als lokaler RADIUS. Verwenden Sie die gleichen Schritte für einen externen RADIUS. Nur die RADIUS-Server-IP wird geändert.

In diesem Verfahren wird beschrieben, wie WDS auf dem WDS AP aktiviert wird:

- Navigieren Sie zur Registerkarte Wireless > WDS > Allgemeine Einrichtung, und aktivieren Sie das Kontrollkästchen Diesen Access Point als Wireless-Domänendienste verwenden. Dadurch wird der WDS-Dienst am Access Point aktiviert.
- 2. Verwenden Sie in einem Netzwerk mit mehreren WDS-APs die Wireless Domain Services Priority-Option, um das primäre WDS und das Backup-WDS zu definieren. Der Wert liegt zwischen 1 und 255, wobei 255 die höchste Priorität darstellt.

cisco	BOME NETWORK ASSOCIATION WERLESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENTLOG	logout Befre
Wireless Services	WOS STATUS	
AP	Hostname MAIB.WDS.AP MAIB.WDS.AP uptime is 9 hours, 59 minutes	
	Wireless Services: WDS/WNM - General Set-Up	
	WDS - Wireless Domain Services - Global Properties	
	🗵 Use this AP as Wireless Domain Services	
	Wireless Domain Services Priority: 204 (1-255)	
a da in in a saba a	Use Local MAC List for Client Authentication	
	WNM - Wireless Network Manager - Global Configuration	
	Configure Wireless Network Manager	
thu this t	Wireless Network Manager Address: DRAIBLED (IP Address or Hostname)	
		Ar Cancel
	App	Ave. Cancel

3. Navigieren Sie zur Registerkarte Servergruppen auf derselben Seite. Erstellen Sie eine Liste der Infrastrukturserver-Gruppen, für die alle WDS-Client-APs authentifiziert werden. Zu diesem Zweck können Sie den lokalen RADIUS-Server auf dem WDS AP verwenden. Da sie bereits hinzugefügt wurde, wird sie in der Dropdown-Liste angezeigt.

li.ili. cisco	HOME NETWORK ASSOCIATION W	RLLISS SICURITY	SERVICES MANAGEMENT	SOFTWARE EV	VENT LOG	Saye Configuration Brig Legout B
Wireless Services	WDS STATUS	Ĭ.	GENERAL SET-UP	í.	SERVER GROUPS	
AP WDS	Hostname MAIB-WDS-AP				MAIB-WDS-AP uptin	ne is 10 hours, 3 minutes
	Wireless Services: WDS - Server (iroups				
	Server Group List		Server Group Name:	Infrastructure		
			Group Server Prioritie	s: Defre Seren		
		Deloto	Priority 1: Local-F	ladius •		
			Priority 2: <non Priority 3: <non< th=""><th>L> • E> •</th><th></th><th></th></non<></non 	L> • E> •		
	Use Group For: Intrastructure Authentication					

- 4. Aktivieren Sie das Optionsfeld **Gruppe verwenden für: Infrastrukturauthentifizierung**, und klicken Sie auf **Apply**, um die Einstellungen zu speichern.
- 5. Der WDS-AP-Benutzername und die Kennwörter können der lokalen RADIUS-Serverliste hinzugefügt werden.

WDS auf dem WDS-Client-AP aktivieren

In diesem Verfahren wird beschrieben, wie WDS auf dem WDS-Client-AP aktiviert wird:

1. Navigieren Sie zu **Wireless > AP**, und aktivieren Sie das Kontrollkästchen **An SWAN**-**Infrastruktur teilnehmen**. SWAN steht für Structured Wireless-Aware Network.

cisco	HOME NETWORK ASSOCIATION WIRELESS SECURITY SE	INVICES BANAGEMENT SOFTWARE EVENTLOG
Wireless Services	Hostname MAIB-WDS-Client	MAID WDS Client uptime is 10 hours, 50 minutes
WDS	Wireless Services: AP	
	Participate in SWAN Infrastructure:	Cnaole © Disable
	WD\$ Discovery:	Auto Discovery Specified Discovery: 10.106.54.146 (IP Address)
	Username: Password:	WD0Gket1
	Confirm Password: Authentication Methods Profile:	ONE > Define Authentication Methods Profiles
		Apply Gancel

 WDS-Client-APs können die WDS-APs automatisch erkennen. Alternativ können Sie im Textfeld Specified Discovery die IP-Adresse des WDS Access Points für die Client-Registrierung manuell eingeben.

Sie können auch den WDS-Client-Benutzernamen und das Kennwort für die Authentifizierung mithilfe des auf dem WDS-AP konfigurierten lokalen RADIUS-Servers hinzufügen.

CLI-Konfigurationen

WDS-AP

Dies ist eine Beispielkonfiguration für den WDS AP:

```
Current configuration : 2832 bytes
1
! Last configuration change at 05:54:08 UTC Fri Apr 26 2013
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
1
hostname MAIB-WDS-AP
1
1
logging rate-limit console 9
enable secret 5 $1$EdDD$dG47yIKn86GCqmKjFf1Sy0
1
aaa new-model
1
1
aaa group server radius rad_eap
server name Local-Radius
1
aaa group server radius Infrastructure
```

```
server name Local-Radius
1
aaa authentication login eap_methods group rad_eap
aaa authentication login method_Infrastructure group Infrastructure
aaa authorization exec default local
1
1
1
1
1
aaa session-id common
no ip routing
no ip cef
1
!
!
1
dot11 syslog
1
dot11 ssid WDS-EAP
authentication open eap eap_methods
authentication network-eap eap_methods
authentication key-management wpa version 2
guest-mode
1
!
dot11 guest
1
!
1
username Cisco password 7 13261E010803
username My3602 privilege 15 password 7 10430810111F00025D56797F65
!
1
bridge irb
1
!
1
interface Dot11Radio0
no ip address
no ip route-cache
1
encryption mode ciphers aes-ccm
!
ssid WDS-EAP
1
antenna gain 0
stbc
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
no ip address
no ip route-cache
1
encryption mode ciphers aes-ccm
!
ssid WDS-EAP
1
```

```
antenna gain 0
peakdetect
dfs band 3 block
stbc
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 GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
1
interface BVI1
ip address 10.106.54.146 255.255.255.192
no ip route-cache
ipv6 address dhcp
ipv6 address autoconfig
ipv6 enable
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
1
1
radius-server local
no authentication eapfast
no authentication mac
nas 10.106.54.146 key 7 045802150C2E1D1C5A
user WDSClient1 nthash 7
072E776E682F4D5D35345B5A227E78050D6413004A57452024017B0803712B224A
1
radius-server attribute 32 include-in-access-req format %h
radius-server vsa send accounting
1
radius server Local-Radius
address ipv4 10.106.54.146 auth-port 1812 acct-port 1813
key 7 060506324F41584B56
1
bridge 1 route ip
!
1
wlccp authentication-server infrastructure method_Infrastructure
wlccp wds priority 254 interface BVI1
line con 0
line vty 0 4
transport input all
1
end
```

WDS-Client-AP

Dies ist eine Beispielkonfiguration für den WDS-Client-AP:

```
Current configuration : 2512 bytes
1
! Last configuration change at 00:33:17 UTC Wed May 22 2013
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
1
hostname MAIB-WDS-Client
1
1
logging rate-limit console 9
enable secret 5 $1$vx/M$qP6DY30TGiXmjvUDvKKjk/
1
aaa new-model
1
1
aaa group server radius rad_eap
server name WDS-Radius
1
aaa authentication login eap_methods group rad_eap
aaa authorization exec default local
Ţ
1
1
1
1
aaa session-id common
no ip routing
no ip cef
1
1
1
1
dot11 syslog
1
dot11 ssid WDS-EAP
authentication open eap eap_methods
authentication network-eap eap_methods
authentication key-management wpa version 2
guest-mode
!
1
dot11 guest
1
eap profile WDS-AP
method leap
!
!
1
username Cisco password 7 062506324F41
username My2602 privilege 15 password 7 09414F000D0D051B5A5E577E6A
!
1
bridge irb
1
1
1
interface Dot11Radio0
```

```
no ip address
no ip route-cache
1
encryption mode ciphers aes-ccm
!
ssid WDS-EAP
1
antenna gain 0
stbc
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
no ip address
no ip route-cache
1
encryption mode ciphers aes-ccm
!
ssid WDS-EAP
1
antenna gain 0
peakdetect
dfs band 3 block
stbc
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 GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
1
interface BVI1
ip address 10.106.54.136 255.255.255.192
no ip route-cache
ipv6 address dhcp
ipv6 address autoconfig
ipv6 enable
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
1
1
radius-server attribute 32 include-in-access-reg format %h
radius-server vsa send accounting
!
```

```
radius server WDS-Radius
address ipv4 10.106.54.146 auth-port 1812 acct-port 1813
key 7 110A1016141D5A5E57
!
bridge 1 route ip
!
!
wlccp ap username WDSClient1 password 7 070C285F4D06485744
wlccp ap wds ip address 10.106.54.146
!
line con 0
line vty 0 4
transport input all
!
end
```

Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert. Nach Abschluss der Einrichtung sollte der WDS-Client-Access Point in der Lage sein, sich beim WDS-Access Point zu registrieren.

Auf dem WDS AP wird der WDS-Status als "Registriert" angezeigt.

WDS STATUS	l l	GENERAL S	HET-UP	ĬI.	SERVER GROUPS					
Hostname MAIB-WDS-AP					MAIB-WDS-AP	ptime is 10 hours,	16 minutes			
Wireless Services: WDS - Wire	Wireless Services: WDS - Wireless Domain Services - Status									
WDS Information										
MAC Address	IPv4 Address		IPv6 Address		Priority		State			
bc16.6516.62c4	10.106.04.146		=		254		Administratively St	andAkone - ACTIVE		
WDS Registration										
APs: 1			Mobile Nodes: 0							
AP Information										
Hostname	MAC Address		IPv4 Address		IPv6 Address		CDP Neighbor	State		
MAIB-WDS-Client	1872.ea24.40e6				2		BGL14-TACLAB	REGISTERED		
Mobile Node Information										
MAC Address	IP Address	State			SSID	VLAN ID	BSSID			
Wireless Network Manager In	Wireless Network Manager Information									
IP Address	Authentication Status	entication Status								

Auf dem WDS-Client-AP lautet der WDS-Status Infrastruktur.

	Hostname MAIBWDS Client			MAIB WDS Client uptime is 10 hours, 57 minutes	
	Wirelass Services Summary				
	WDS MAC Address	WDS IP Address	IN Authenticator	MN Authenticator	State
	bc16.6516.62c4	=	10.105.54.146	10.105.54.146	Infrastructure
	bc16.6516.62c4	=	10.106.54.146	10.106.54.146	Intrastructure

Anmerkung: 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.

CLI-Verifizierungs-Ausgabe auf WDS AP

Dieses Verfahren zeigt, wie Sie die WDS-AP-Konfiguration überprüfen:

MAIB-WDS-AP#sh wlccp wds ap

HOSTNAME MAC-ADDR IP-ADDR IPV6-ADDR STATE MAIB-WDS-Client f872.ea24.40e6 10.106.54.136 :: REGISTERED

MAIB-WDS-AP#**sh wlccp wds statistics**

WDS Statistics for last 10:34:13: Current AP count: 1 Current MN count: 0 AAA Auth Attempt count: 2 AAA Auth Success count: 2 AAA Auth Failure count: 0 MAC Spoofing Block count: 0 Roaming without AAA Auth count: 0 Roaming with full AAA Auth count: 0 Fast Secured Roaming count: 0 MSC Failure count: 0 MSC Failure count: 0 MIC Failure count: 0 RN Mismatch count: 0

CLI-Verifizierungs-Ausgabe auf WDS-Client-AP

Dieses Verfahren zeigt, wie die WDS-Client-AP-Konfiguration überprüft wird:

```
MAIB-WDS-Client#sh wlccp ap
WDS = bc16.6516.62c4, IP: 10.106.54.146 , IPV6: ::
state = wlccp_ap_st_registered
IN Authenticator = IP: 10.106.54.146 IPV6: ::
MN Authenticator = IP: 10.106.54.146 IPv6::
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.