

Configuración de WDS en AP autónomos con servidor RADIUS local

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuraciones GUI](#)

[Crear el SSID](#)

[Configuración del servidor RADIUS local en WDS AP](#)

[Configuración del Servidor RADIUS Local en el AP del Cliente WDS](#)

[Activar WDS en WDS AP](#)

[Activar WDS en WDS Client AP](#)

[Configuraciones CLI](#)

[AP WDS](#)

[AP cliente WDS](#)

[Verificación](#)

[Salida de verificación CLI en WDS AP](#)

[Salida de verificación CLI en el AP cliente WDS](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo configurar Wireless Domain Services (WDS) en una configuración de punto de acceso autónomo (AP) con un servidor RADIUS local. El documento se centra en las configuraciones a través de la nueva GUI, pero también proporciona configuraciones de interfaz de línea de comandos (CLI).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de la configuración básica de GUI y CLI en los AP autónomos.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Punto de acceso Cisco serie 3602e en el software autónomo AP IOS®, versión 15.2(4)JA1; este dispositivo actuará como un WDS AP y un servidor RADIUS local.
- Punto de acceso de la serie Cisco 2602i en software autónomo AP IOS, versión 15.2(4)JA1; este dispositivo actuará como un AP cliente WDS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

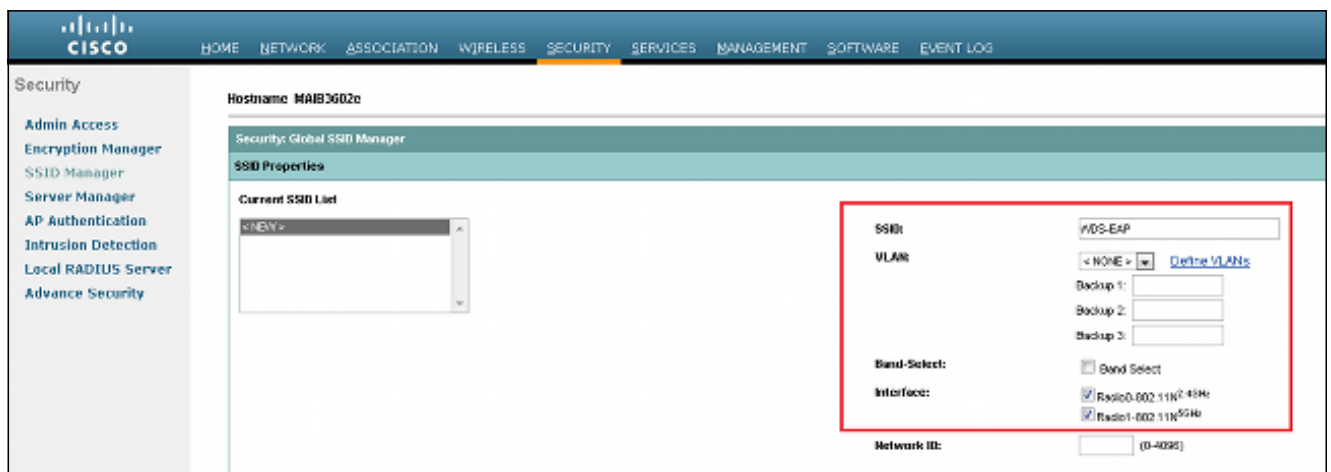
Nota: Use la [Command Lookup Tool \(clientes registrados solamente\)](#) para obtener más información sobre los comandos usados en esta sección.

Configuraciones GUI

Crear el SSID

Este procedimiento describe cómo crear un nuevo identificador de conjunto de servicios (SSID).

1. Navegue hasta **Seguridad > Administrador SSID**, y haga clic en **NUEVO** para crear un nuevo SSID.



2. Configure el SSID para la autenticación de protocolo de autenticación extensible (EAP).

Client Authentication Settings

Methods Accepted:

Open Authentication:

Web Authentication

Shared Authentication:

Network EAP:

< NO ADDITION >

< NO ADDITION >

with MAC Authentication

with EAP

with MAC Authentication and EAP

with MAC Authentication or EAP

with Optional EAP

< NO ADDITION >

Server Priorities:

EAP Authentication Servers

Use Defaults [Define Defaults](#)

Customize

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

MAC Authentication Servers

Use Defaults [Define Defaults](#)

Customize

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

3. Establezca el nivel de cifrado deseado. En este ejemplo, utilice el acceso Wi-Fi protegido 2 (WPA2).

Client Authenticated Key Management

Key Management: CKM Enable WPA

WPA Pre-shared Key:

ASCII Hexadecimal

11w Configuration: Optional Required

11w Association-comeback: (1000-20000)

11w Saquery-retry: (100-500)

WPAv2

WPA

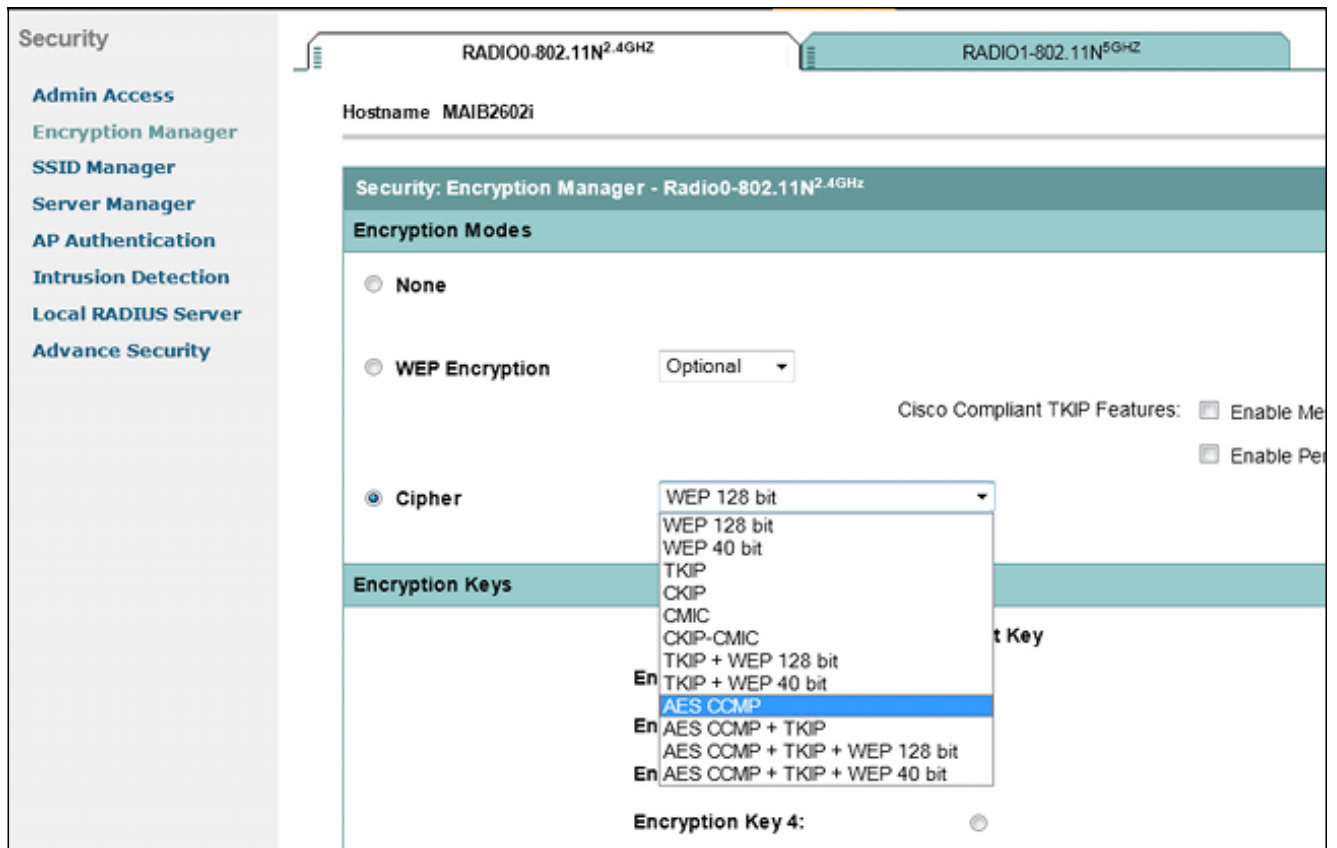
WPAv1

WPAv2

WPAv2 dot11r

4. Haga clic en **Aplicar** para guardar las configuraciones.

5. Navegue hasta **Seguridad > Administrador de cifrado** y elija el método de cifrado necesario.



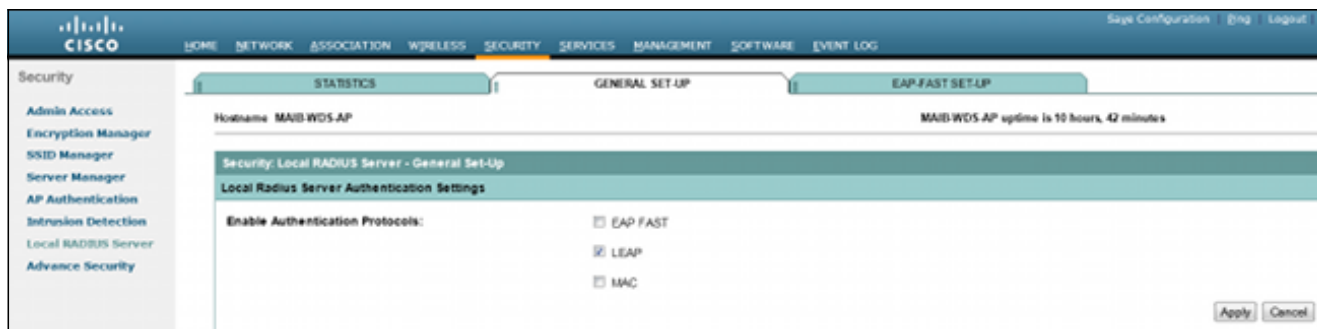
Configuración del servidor RADIUS local en WDS AP

Este procedimiento describe cómo configurar el servidor RADIUS local en el AP WDS:

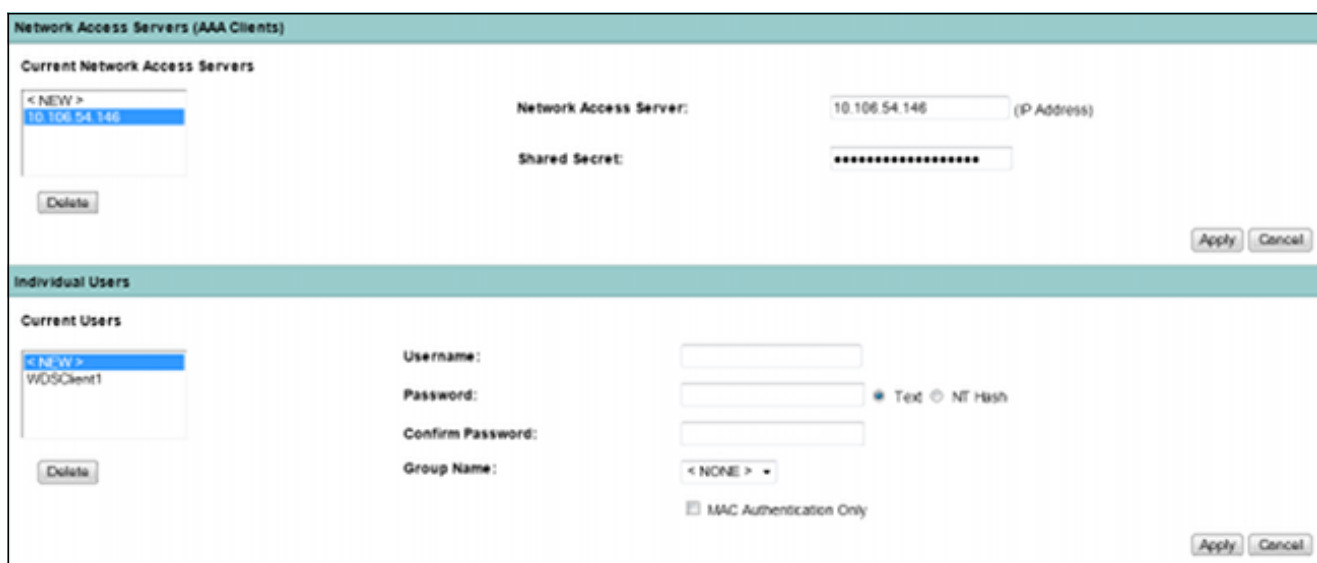
1. Vaya a **Security > Server Manager**, agregue la IP de la interfaz virtual del puente WDS AP (BVI) como RADIUS local y agregue un secreto compartido.



2. Vaya a **Seguridad > Servidor RADIUS Local > pestaña Configuración General**. Defina los protocolos EAP que desea utilizar. En este ejemplo, active la autenticación de protocolo de autenticación ampliable ligero (LEAP).

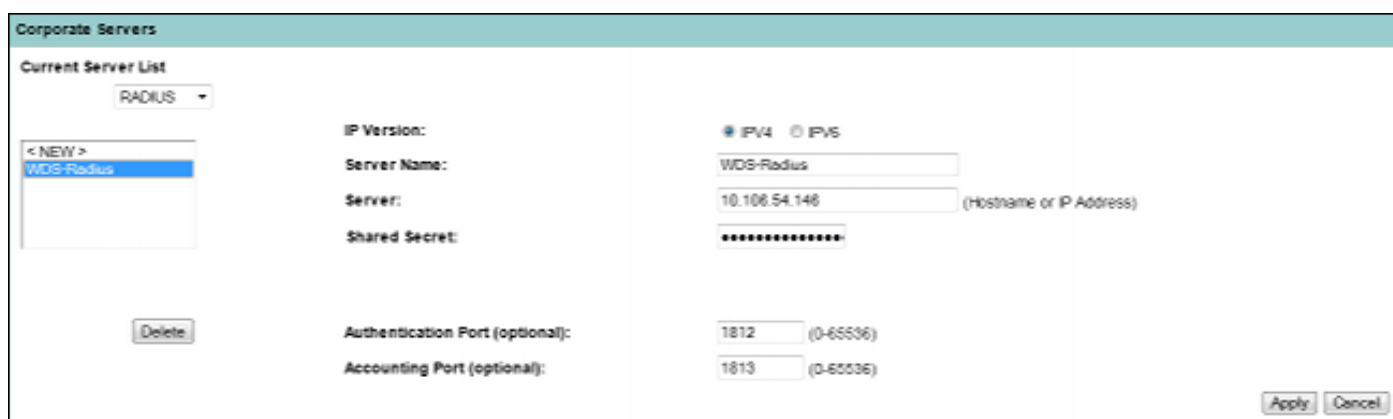


3. También puede agregar IP de servidor de acceso a la red (NAS) y credenciales de nombre de usuario/contraseña del cliente en la misma página. La configuración de un RADIUS local en un AP WDS está completa.



Configuración del Servidor RADIUS Local en el AP del Cliente WDS

Esta figura muestra cómo configurar la dirección IP del WDS AP como el servidor RADIUS:

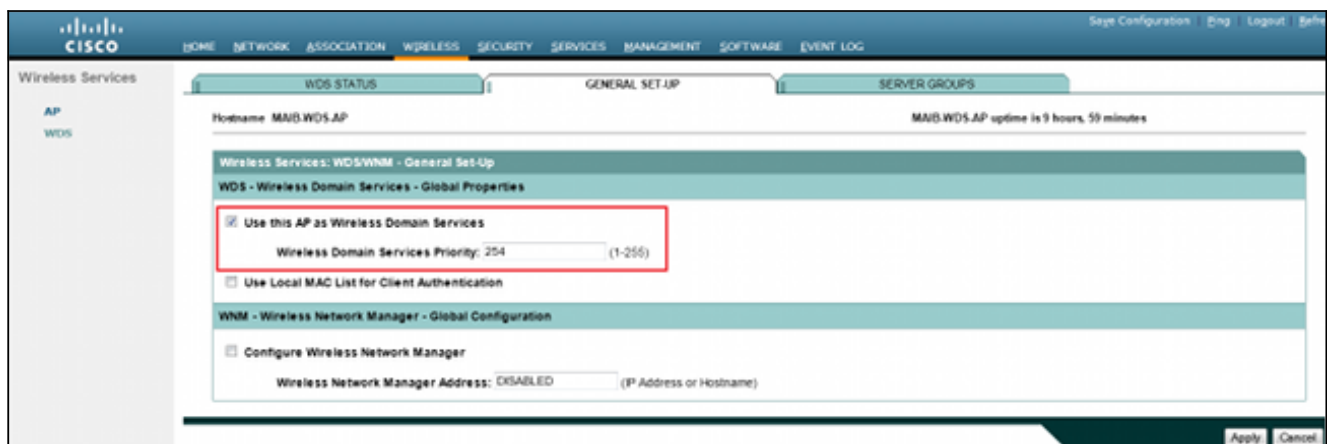


Ambos AP se configuran ahora con SSID para la autenticación LEAP, y el servidor WDS actúa como RADIUS local. Utilice los mismos pasos para un RADIUS externo; solo cambiará la IP del servidor RADIUS.

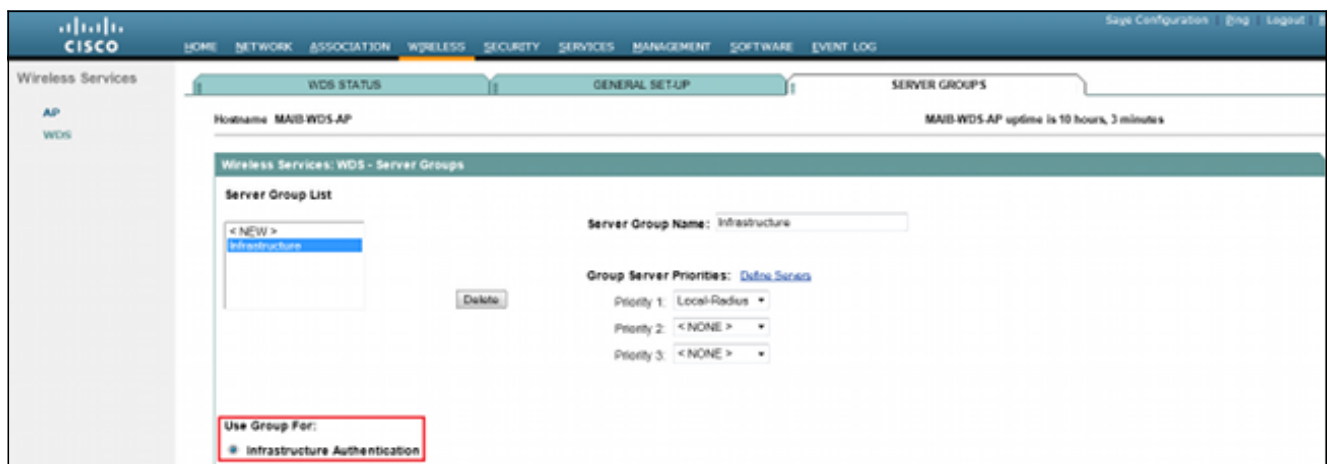
Activar WDS en WDS AP

Este procedimiento describe cómo habilitar WDS en el WDS AP:

1. Navegue hasta la pestaña **Wireless > WDS > General Set-Up** y active la casilla de verificación **Use este AP como Wireless Domain Services**. Esto habilita el servicio WDS en el AP.
2. En una red con varios WDS AP, use la opción **Wireless Domain Services Priority** para definir el WDS primario y el WDS de respaldo. El valor oscila entre 1 y 255, donde 255 es la prioridad más alta.



3. Vaya a la pestaña **Grupos de servidores** en la misma página. Cree una lista de grupos de servidores de infraestructura, a la cual se autenticarán todos los AP del cliente WDS. Puede utilizar el servidor RADIUS local en el AP WDS para este propósito. Puesto que ya se ha agregado, aparece en la lista desplegable.

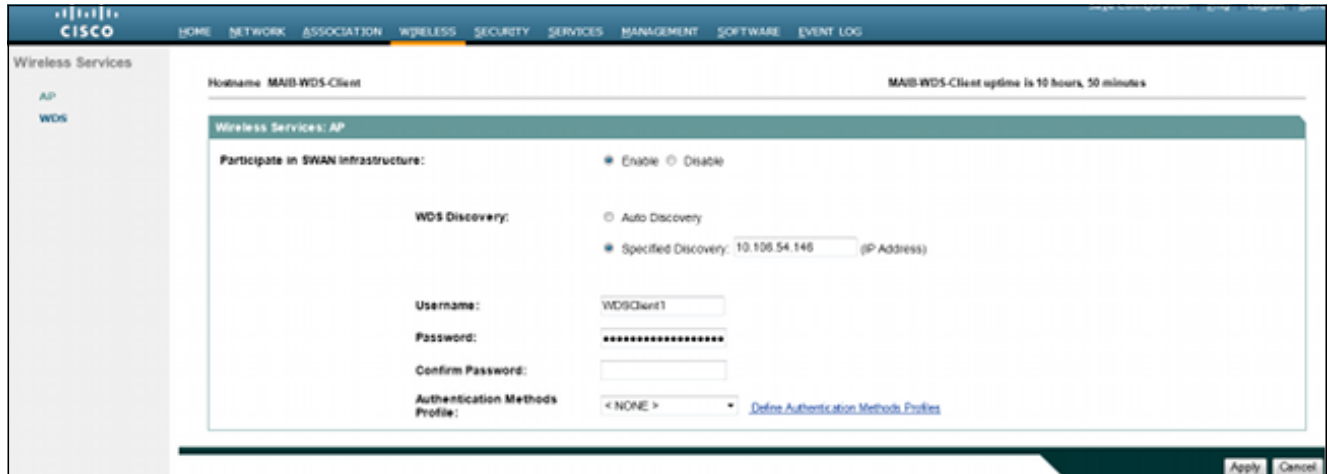


4. Activar el botón de opción **Usar grupo para: Autenticación de infraestructura**, y haga clic en **Aplicar** para guardar la configuración.
5. El nombre de usuario y las contraseñas de WDS AP se pueden agregar a la lista de servidores RADIUS local.

Activar WDS en WDS Client AP

Este procedimiento describe cómo habilitar WDS en el WDS client AP:

1. Vaya a **Wireless > AP** y active la casilla de verificación **Participar en la infraestructura SWAN**. SWAN significa red inalámbrica estructurada.



2. Los AP del cliente WDS pueden detectar automáticamente los AP WDS. O bien, puede ingresar manualmente la dirección IP del WDS AP para el registro del cliente en el cuadro de texto **Specified Discovery**.

También puede agregar el nombre de usuario y la contraseña del cliente WDS para la autenticación contra el servidor RADIUS local configurado en el AP WDS.

Configuraciones CLI

AP WDS

Esta es una configuración de ejemplo para el AP WDS:

```
Current configuration : 2832 bytes
!
! 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
!
hostname MAIB-WDS-AP
!
!
logging rate-limit console 9
enable secret 5 $1$EdDD$dG47yIKn86GCqmKjFf1Sy0
!
aaa new-model
!
!
aaa group server radius rad_eap
server name Local-Radius
!
aaa group server radius Infrastructure
server name Local-Radius
```

```
!  
aaa authentication login eap_methods group rad_eap  
aaa authentication login method_Infrastructure group Infrastructure  
aaa authorization exec default local  
!  
!  
!  
!  
aaa session-id common  
no ip routing  
no ip cef  
!  
!  
!  
dot11 syslog  
!  
dot11 ssid WDS-EAP  
authentication open eap eap_methods  
authentication network-eap eap_methods  
authentication key-management wpa version 2  
guest-mode  
!  
!  
dot11 guest  
!  
!  
!  
username Cisco password 7 13261E010803  
username My3602 privilege 15 password 7 10430810111F00025D56797F65  
!  
!  
bridge irb  
!  
!  
!  
interface Dot11Radio0  
no ip address  
no ip route-cache  
!  
encryption mode ciphers aes-ccm  
!  
ssid WDS-EAP  
!  
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  
!  
interface Dot11Radio1  
no ip address  
no ip route-cache  
!  
encryption mode ciphers aes-ccm  
!  
ssid WDS-EAP  
!  
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
!
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
!
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
!
!
radius-server local
no authentication eapfast
no authentication mac
nas 10.106.54.146 key 7 045802150C2E1D1C5A
user WDSClient1 ntnash 7
072E776E682F4D5D35345B5A227E78050D6413004A57452024017B0803712B224A
!
radius-server attribute 32 include-in-access-req format %h
radius-server vsa send accounting
!
radius server Local-Radius
address ipv4 10.106.54.146 auth-port 1812 acct-port 1813
key 7 060506324F41584B56
!
bridge 1 route ip
!
!
wlccp authentication-server infrastructure method_Infrastructure
wlccp wds priority 254 interface BVI1
!
line con 0
line vty 0 4
transport input all
!
end

```

AP cliente WDS

Esta es una configuración de ejemplo para el AP del cliente WDS:

```
Current configuration : 2512 bytes
!
! 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
!
hostname MAIB-WDS-Client
!
!
logging rate-limit console 9
enable secret 5 $1$vx/M$qP6DY30TGiXmjvUDvKKjk/
!
aaa new-model
!
!
aaa group server radius rad_eap
server name WDS-Radius
!
aaa authentication login eap_methods group rad_eap
aaa authorization exec default local
!
!
!
!
!
aaa session-id common
no ip routing
no ip cef
!
!
!
!
dot11 syslog
!
dot11 ssid WDS-EAP
authentication open eap eap_methods
authentication network-eap eap_methods
authentication key-management wpa version 2
guest-mode
!
!
dot11 guest
!
eap profile WDS-AP
method leap
!
!
!
username Cisco password 7 062506324F41
username My2602 privilege 15 password 7 09414F000D0D051B5A5E577E6A
!
!
!
bridge irb
!
!
!
interface Dot11Radio0
```

```
no ip address
no ip route-cache
!
encryption mode ciphers aes-ccm
!
ssid WDS-EAP
!
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
!
interface Dot11Radio1
no ip address
no ip route-cache
!
encryption mode ciphers aes-ccm
!
ssid WDS-EAP
!
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
!
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
!
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
!
!
radius-server attribute 32 include-in-access-req 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

```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente. Una vez que se complete la configuración, el AP del cliente WDS debería poder registrarse en el AP WDS.

En el WDS AP, el estado de WDS se muestra como Registrado.

WDS STATUS		GENERAL SET-UP		SERVER GROUPS	
Hostname: MAIB-WDS-AP			MAIB-WDS-AP uptime is 10 hours, 16 minutes		
Wireless Services: WDS - Wireless Domain Services - Status					
WDS Information					
MAC Address	IPv4 Address	IPv6 Address	Priority	State	
bc16.6516.62c4	10.106.54.146	::	254	Administratively StandAlone - ACTIVE	
WDS Registration					
APs: 1		Mobile Nodes: 0			
AP Information					
Hostname	MAC Address	IPv4 Address	IPv6 Address	CDP Neighbor	State
MAIB-WDS-Client	f872.ea24.4de6		::	BGL14-TACLAB	REGISTERED
Mobile Node Information					
MAC Address	IP Address	State	SSID	VLAN ID	BSSID
Wireless Network Manager Information					
IP Address	Authentication Status				

En el WDS Client AP, el estado de WDS es Infrastructure.

WDS STATUS		GENERAL SET-UP		SERVER GROUPS	
Hostname: MAIB-WDS-Client			MAIB-WDS-Client uptime is 10 hours, 57 minutes		
Wireless Services Summary					
AP					
WDS MAC Address	WDS IP Address	IN Authenticator	MN Authenticator	State	
bc16.6516.62c4	::	10.106.54.146	10.106.54.146	Infrastructure	

Nota: La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver un análisis de información de salida del comando show.

Salida de verificación CLI en WDS AP

Este procedimiento muestra cómo verificar la configuración de WDS AP:

```
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  
KSC Failure count: 0  
MIC Failure count: 0  
RN Mismatch count: 0
```

Salida de verificación CLI en el AP cliente WDS

Este procedimiento muestra cómo verificar la configuración AP del cliente WDS:

```
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::
```

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.