

使用本地RADIUS服务器在自治AP上配置WDS

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[GUI配置](#)

[创建SSID](#)

[WDS AP上的本地RADIUS服务器配置](#)

[WDS客户端AP上的本地RADIUS服务器配置](#)

[在WDS AP上启用WDS](#)

[在WDS客户端AP上启用WDS](#)

[CLI配置](#)

[WDS AP](#)

[WDS客户端AP](#)

[验证](#)

[WDS AP上的CLI验证输出](#)

[WDS客户端AP上的CLI验证输出](#)

[故障排除](#)

简介

本文档介绍如何使用本地RADIUS服务器在自主接入点(AP)设置上配置无线域服务(WDS)。本文档重点介绍通过新GUI进行的配置，同时提供命令行界面(CLI)配置。

先决条件

要求

思科建议您了解自治AP上的基本GUI和CLI配置。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 自治AP IOS®软件版本15.2(4)^{JA1}上的Cisco 3602e系列接入点；此设备将用作WDS AP和本地

RADIUS服务器。

- 自治AP IOS软件版本15.2(4)JA1上的思科2602i系列接入点；此设备将充当WDS客户端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

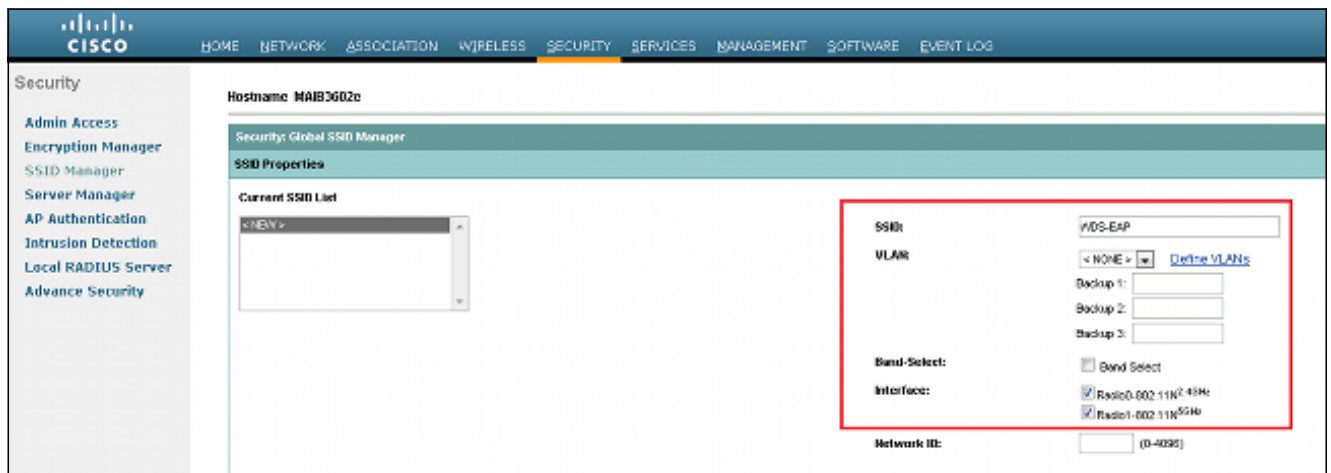
注意：使用[命令查找工具（仅限注册用户）](#)可获取有关本部分所使用命令的详细信息。

GUI配置

创建SSID

此过程介绍如何创建新的服务集标识符(SSID)。

1. 导航至Security > SSID Manager，然后单击NEW以创建新的SSID。



2. 配置SSID以进行可扩展身份验证协议(EAP)身份验证。

Client Authentication Settings

Methods Accepted:

Open Authentication:

Web Authentication

Shared Authentication:

Network EAP:

Server Priorities:

EAP Authentication Servers

Use Defaults [Define Defaults](#)

Customize

Priority 1:

Priority 2:

Priority 3:

MAC Authentication Servers

Use Defaults [Define Defaults](#)

Customize

Priority 1:

Priority 2:

Priority 3:

3. 设置所需的加密级别。在本示例中，使用Wi-Fi保护访问2(WPA2)。

Client Authenticated Key Management

Key Management: CCKM Enable WPA

WPA Pre-shared Key:

ASCII Hexadecimal

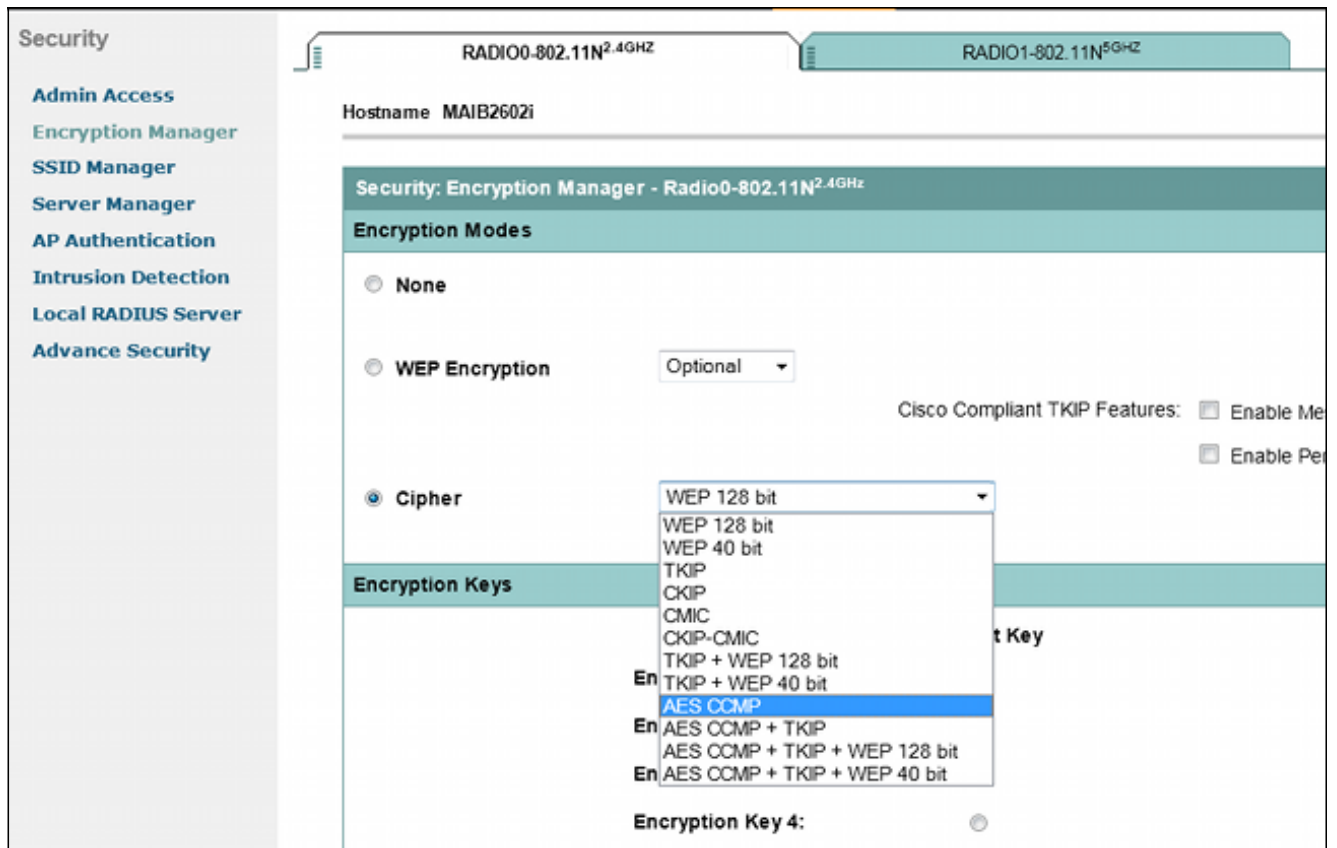
11w Configuration: Optional Required

11w Association-comeback: (1000-20000)

11w Seqquery-retry: (100-500)

4. 单击 **Apply** 以保存设置。

5. 导航至**Security > Encryption Manager**，然后选择所需的加密密码方法。



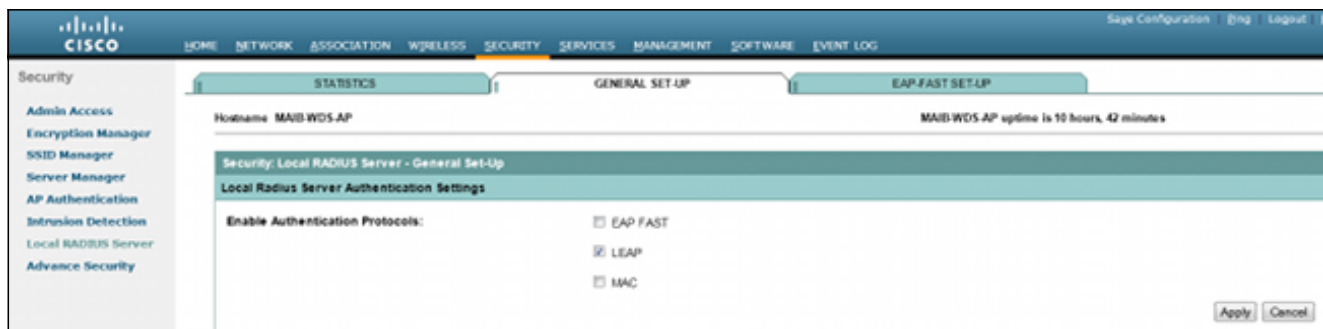
WDS AP上的本地RADIUS服务器配置

此过程介绍如何在WDS AP上配置本地RADIUS服务器：

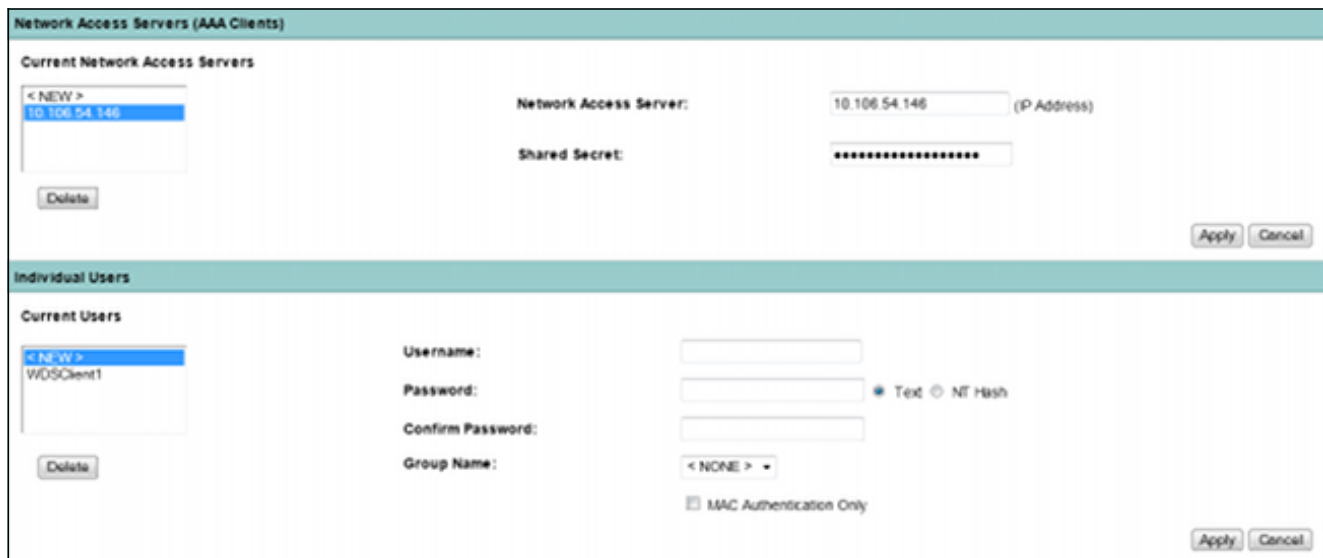
1. 导航至**Security > Server Manager**，添加WDS AP网桥虚拟接口(BVI)IP作为本地RADIUS，并添加共享密钥。



2. 导航至**Security > Local Radius Server > General Set-Up** 选项卡。定义要使用的EAP协议。在本示例中，启用轻量级可扩展身份验证协议(LEAP)身份验证。

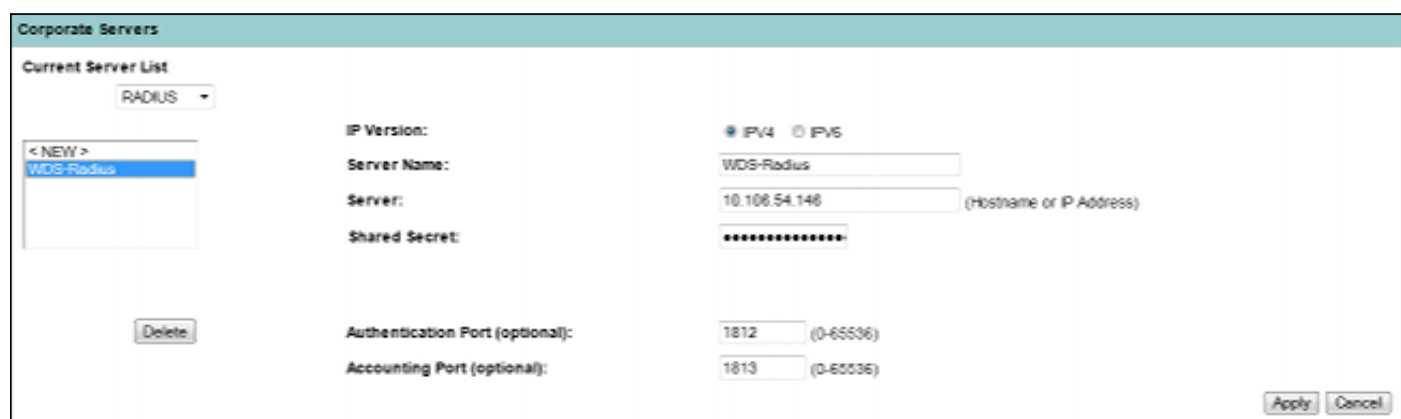


3. 您还可以在同一页面上添加网络接入服务器(NAS)IP和客户端用户名/密码凭证。在WDS AP上配置本地RADIUS已完成。



WDS客户端AP上的本地RADIUS服务器配置

此图显示如何将WDS AP的IP地址配置为RADIUS服务器：

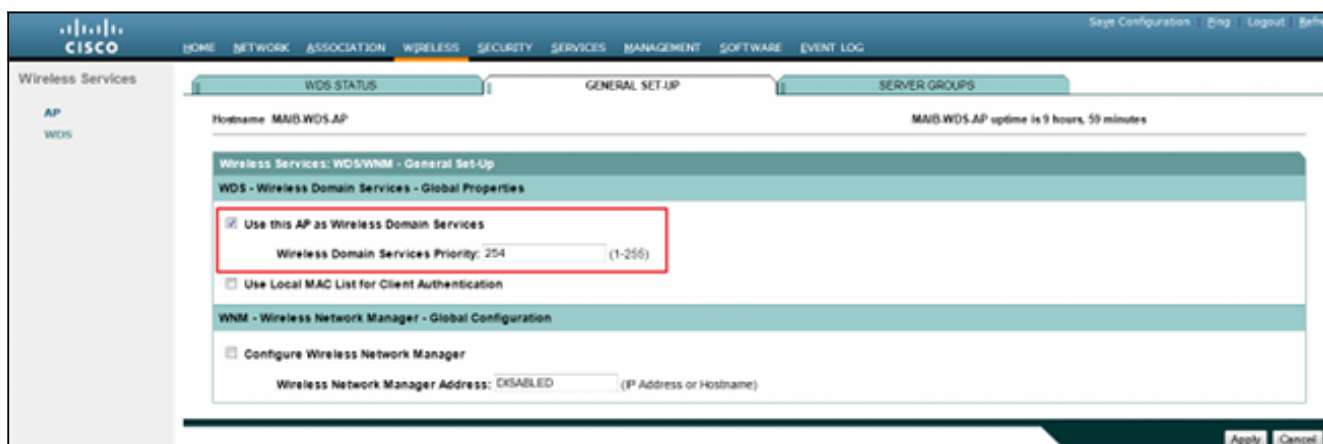


两个AP现在都配置了SSID以进行LEAP身份验证，而WDS服务器充当本地RADIUS。对外部RADIUS使用相同的步骤；仅RADIUS服务器IP将更改。

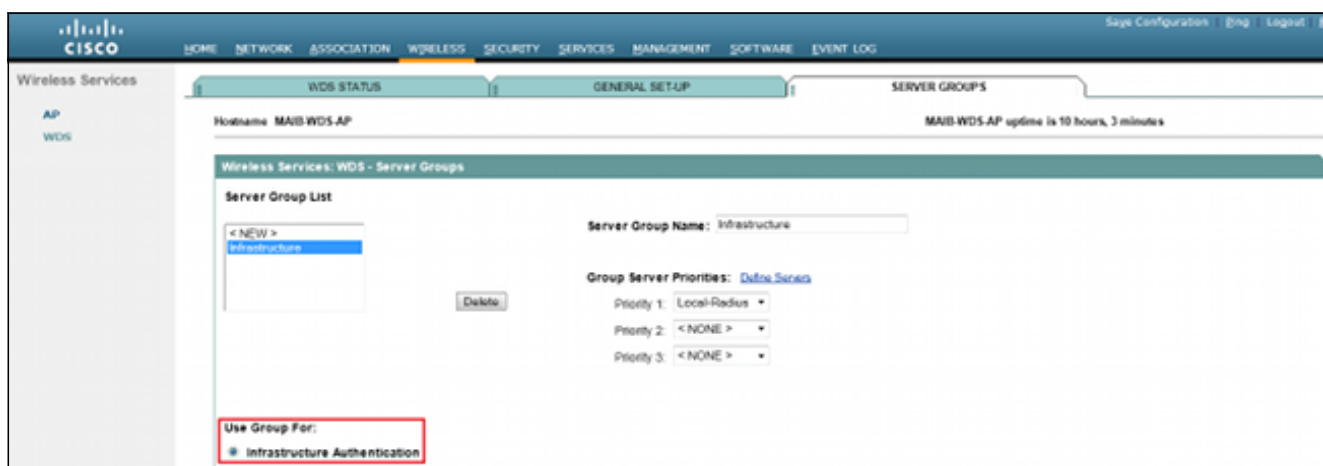
在WDS AP上启用WDS

此程序描述如何在WDS AP上启用WDS:

1. 导航至Wireless > WDS > General Set-Up 选项卡，并启用Use this AP as Wireless Domain Services复选框。这将在AP上启用WDS服务。
2. 在具有多个WDS AP的网络中，使用Wireless Domain Services Priority选项以定义主WDS和备份WDS。值范围为1到255，其中255是最高优先级。



3. 导航至同一页上的“服务器组”选项卡。创建基础设施服务器组列表，所有WDS客户端AP将验证该列表。您可以在WDS AP上使用本地RADIUS服务器来实现此目的。由于已添加，因此它会显示在下拉列表中。

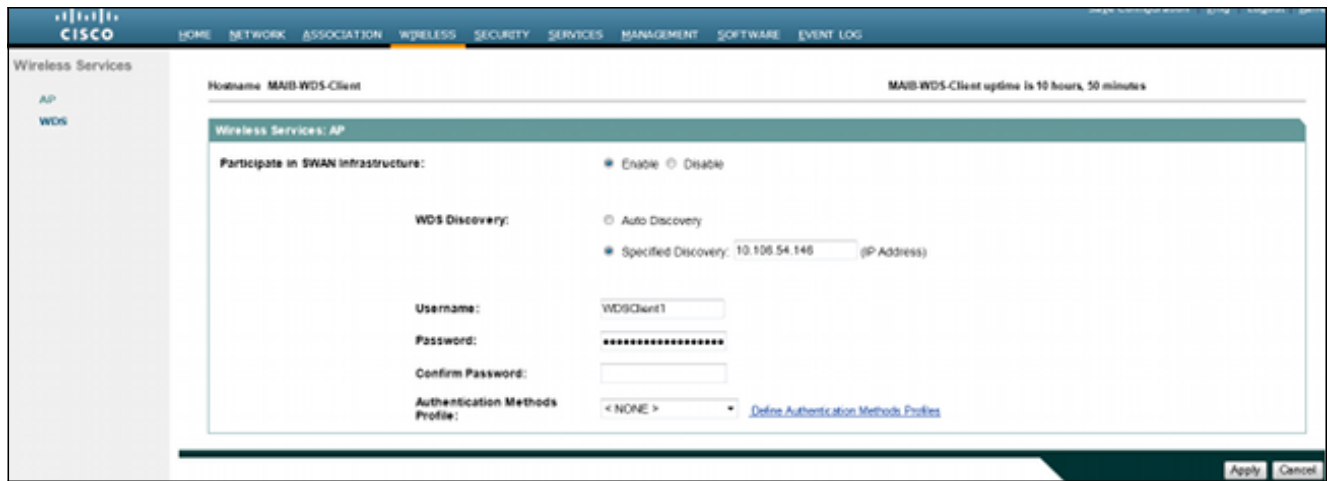


4. 启用单选按钮“使用组：Infrastructure Authentication”，然后单击Apply以保存设置。
5. WDS AP用户名和密码可以添加到本地RADIUS服务器列表。

在WDS客户端AP上启用WDS

此过程描述如何在WDS客户端AP上启用WDS:

1. 导航到Wireless > AP，并启用Participate in SWAN Infrastructure复选框。SWAN代表结构化无线感知网络。



2. WDS客户端AP可以自动发现WDS AP。或者，您可以在“指定发现”文本框中手动输入WDS AP的IP地址以进行客户端注册。

您还可以添加WDS客户端用户名和密码，以针对WDS AP上配置的本地RADIUS服务器进行身份验证。

CLI配置

WDS AP

以下是WDS AP的示例配置：

```

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 nhash 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

```

WDS客户端AP

以下是WDS客户端AP的示例配置：

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

```

验证

使用本部分可确认配置能否正常运行。设置完成后，WDS客户端AP应能注册到WDS AP。

在WDS AP上，WDS状态显示为Registered。

WDS Information		IPv4 Address	IPv6 Address	Priority	State
MAC Address	bc16.6516.62c4	10.106.54.146	::	254	Administratively StandAlone - ACTIVE

AP Information		MAC Address	IPv4 Address	IPv6 Address	CDP Neighbor	State
Hostname	MAIB-WDS-Client	f872.ea24.40e6		::	BGL14-TACLAB	REGISTERED

在WDS客户端AP上，WDS状态为Infrastructure。

WDS MAC Address	WDS IP Address	IN Authenticator	MN Authenticator	State
bc16.6516.62c4	::	10.106.54.146	10.106.54.146	Infrastructure

注意： [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。

WDS AP上的CLI验证输出

此过程显示如何验证WDS AP配置：

```
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
```

WDS客户端AP上的CLI验证输出

此过程显示如何验证WDS客户端AP配置：

```
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::
```

故障排除

目前没有针对此配置的故障排除信息。