Configurer WDS sur des AP autonomes avec le serveur RADIUS local

Contenu

Introduction

Ce document décrit comment configurer les services de domaine sans fil (WDS) sur une configuration de point d'accès autonome (AP) avec un serveur RADIUS local. Le document se concentre sur les configurations via la nouvelle interface utilisateur graphique, mais fournit également des configurations d'interface de ligne de commande (CLI).

Conditions préalables

Conditions requises

Cisco recommande que vous connaissiez la configuration de base de l'interface utilisateur graphique et de l'interface de ligne de commande sur les points d'accès autonomes.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Point d'accès de la gamme Cisco 3602e sur le logiciel IOS® AP autonome, version 15.2(4)JA1 ; ce périphérique agira en tant que point d'accès WDS et serveur RADIUS local.
- Point d'accès de la gamme Cisco 2602i sur le logiciel IOS AP autonome, version 15.2(4)JA1 ; ce périphérique agira en tant qu'AP client 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.

Configuration

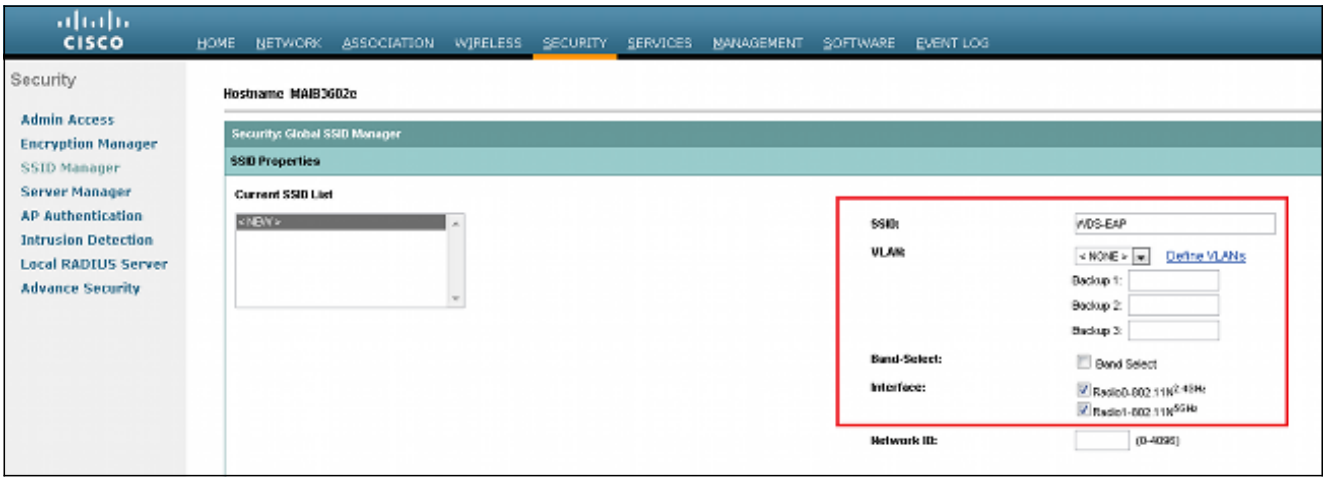
> **Note**: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Configurations de l'interface utilisateur graphique

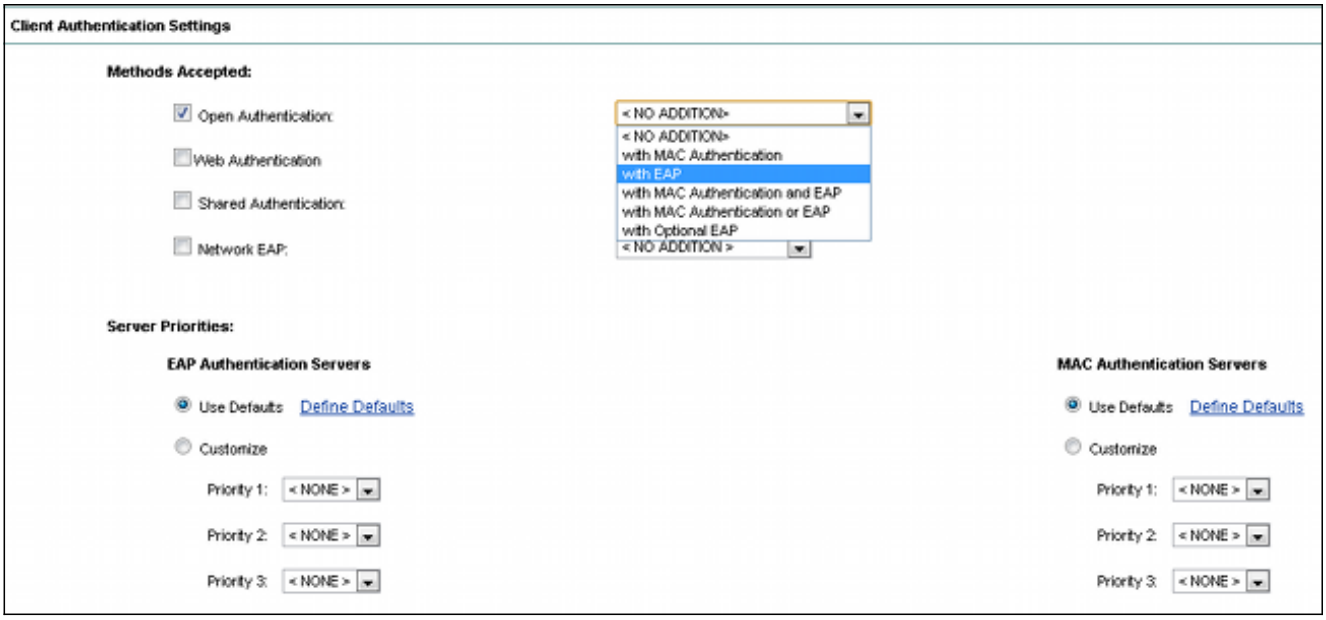
Créer le SSID

Cette procédure décrit comment créer un SSID (Service Set Identifier).

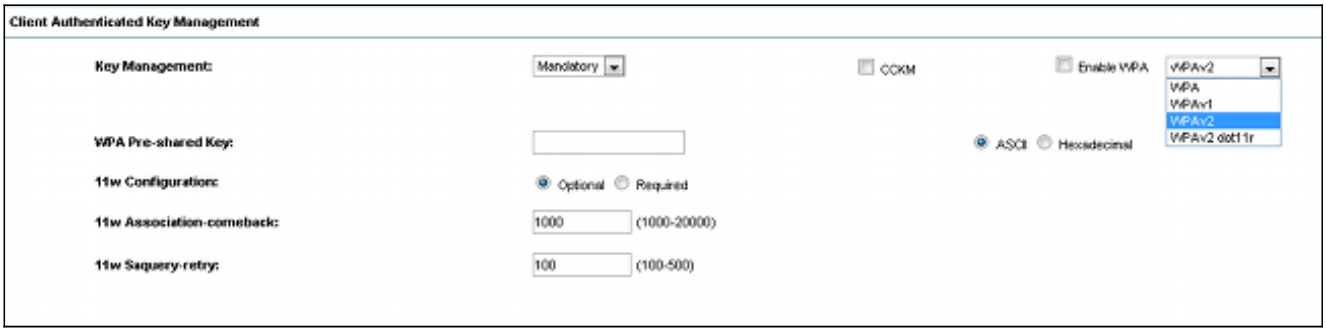
1. Accédez à **Security > SSID Manager**, puis cliquez sur **NEW** afin de créer un nouveau SSID.



2. Configurez le SSID pour l'authentification EAP (Extensible Authentication Protocol).

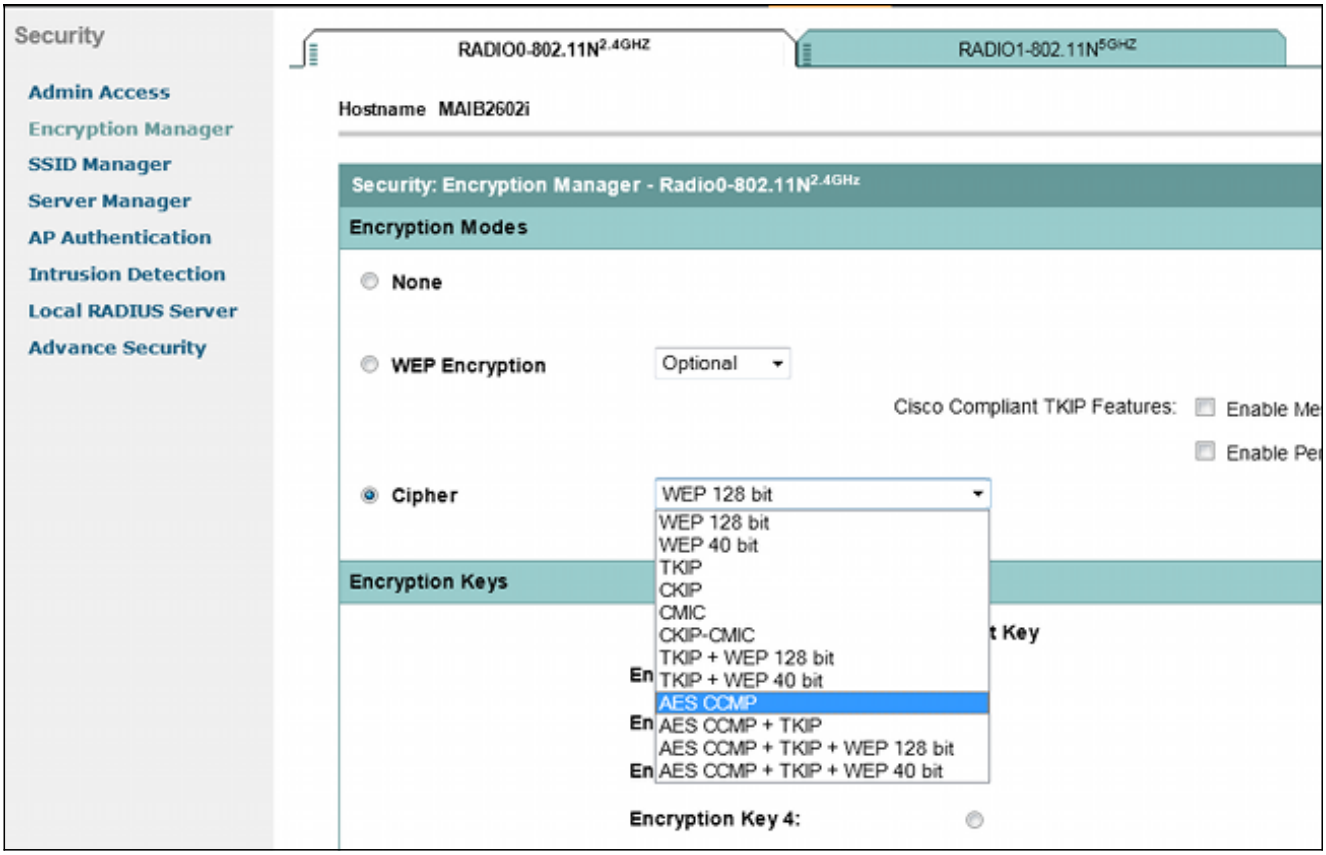


3. Définissez le niveau de chiffrement souhaité. Dans cet exemple, utilisez Wi-Fi Protected Access 2 (WPA2).



4. Cliquez sur **Apply afin de sauvegarder les paramètres.**

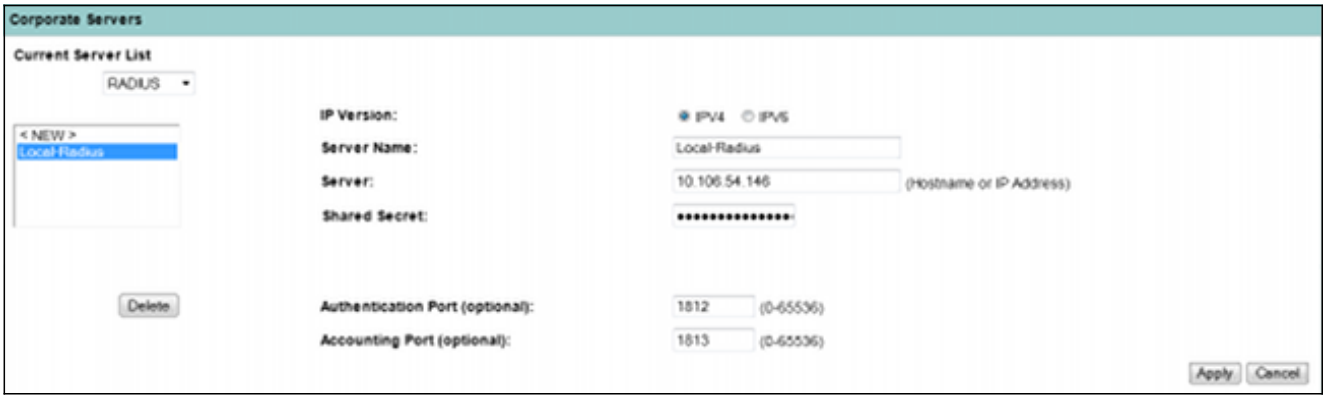
5. Accédez à **Security > Encryption Manager**, puis choisissez la méthode de chiffrement requise.



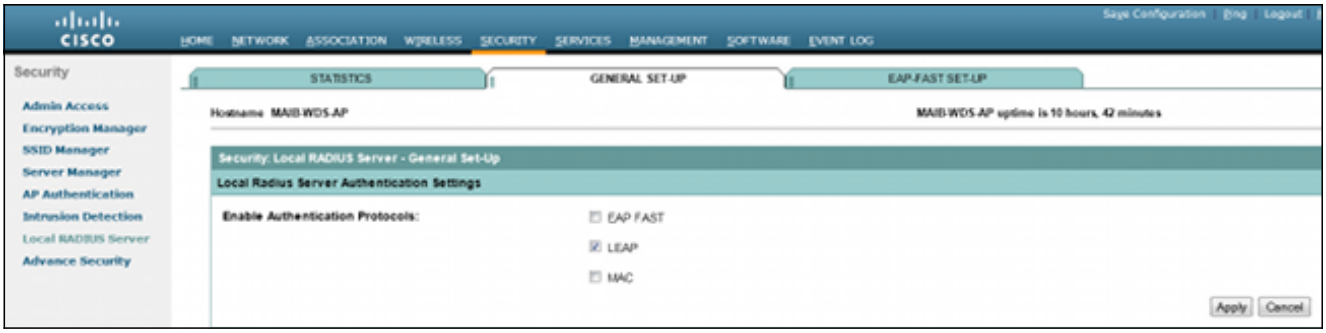
Configuration du serveur RADIUS local sur le point d'accès WDS

Cette procédure décrit comment configurer le serveur RADIUS local sur l'AP WDS :

1. Accédez à **Security > Server Manager**, ajoutez l'IP BVI (WDS AP Bridge Virtual Interface) du WDS en tant que RADIUS local et ajoutez un secret partagé.



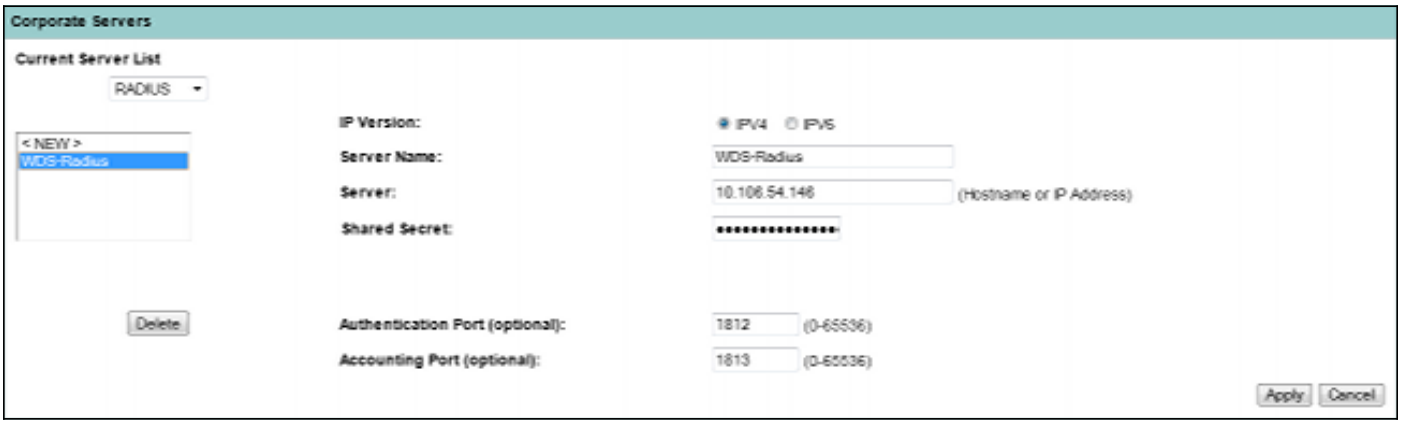
2. Accédez à **Security > Local Radius Server > General Set-Up** tab. Définissez les protocoles EAP que vous souhaitez utiliser. Dans cet exemple, activez l'authentification LEAP (Light Extensible Authentication Protocol).



3. Vous pouvez également ajouter des adresses IP de serveur d'accès réseau (NAS) et des informations d'identification de nom d'utilisateur/mot de passe client sur la même page. La configuration d'un RADIUS local sur un point d'accès WDS est terminée.

Configuration du serveur RADIUS local sur l'AP du client WDS

Cette figure montre comment configurer l'adresse IP du point d'accès WDS en tant que serveur RADIUS :



Les deux points d'accès sont maintenant configurés avec des SSID pour l'authentification LEAP, et le serveur WDS agit en tant que RADIUS local. Utilisez les mêmes étapes pour un RADIUS externe ; seule l'adresse IP du serveur RADIUS change.

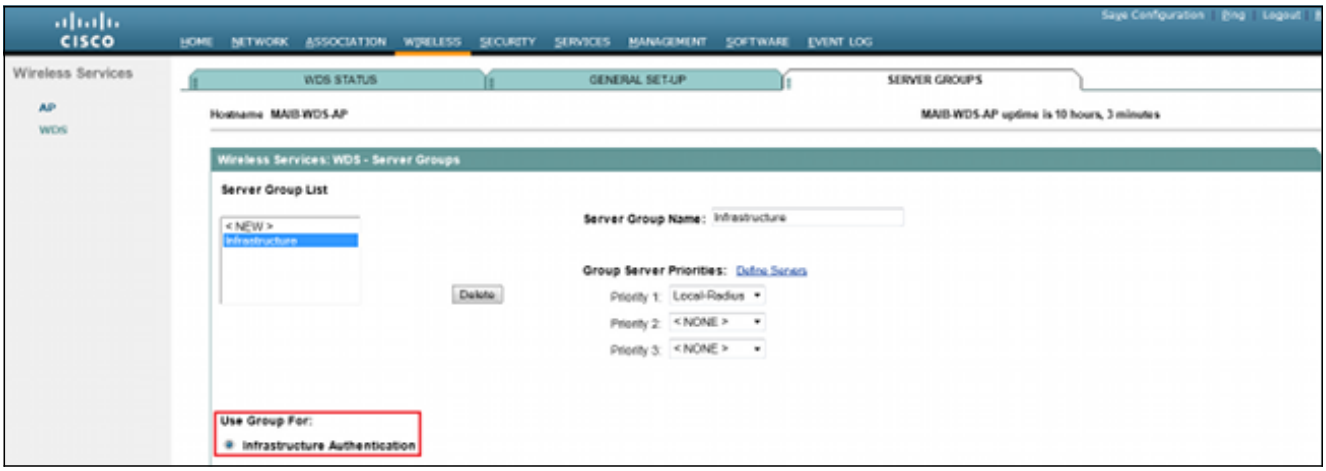
Activer WDS sur WDS AP

Cette procédure décrit comment activer WDS sur l'AP WDS :

1. Accédez à l'onglet **Wireless > WDS > General Set-Up** et activez la case à cocher **Use this AP as Wireless Domain Services**. Ceci active le service WDS sur l'AP.

2. Dans un réseau avec plusieurs points d'accès WDS, utilisez l'option Wireless Domain Services Priority afin de définir le WDS principal et le WDS de sauvegarde. La valeur est comprise entre 1 et 255, où 255 est la priorité la plus élevée.

3. Accédez à l'onglet **Groupes de serveurs** de la même page. Créez une liste de groupes de serveurs d'infrastructure, à laquelle tous les AP clients WDS s'authentifieront. Vous pouvez utiliser le serveur RADIUS local sur l'AP WDS à cette fin. Comme il a déjà été ajouté, il apparaît dans la liste déroulante.



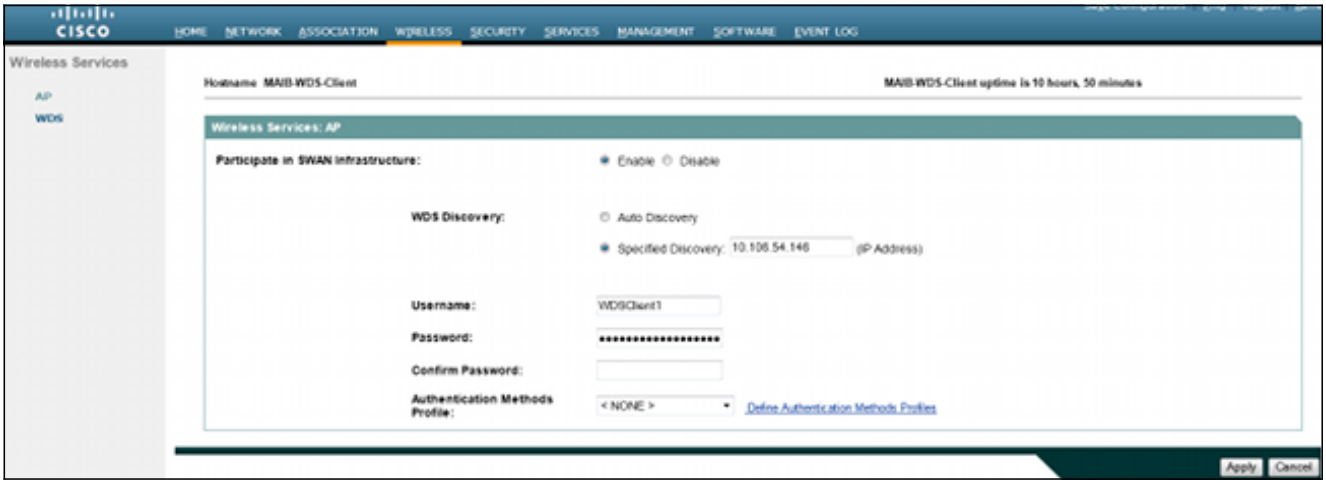
4. Activez la case d'option **Utiliser le groupe pour : Authentification de l'infrastructure**, puis cliquez sur **Apply** afin d'enregistrer les paramètres.

5. Le nom d'utilisateur et les mots de passe du point d'accès WDS peuvent être ajoutés à la liste des serveurs RADIUS locaux.

Activer WDS sur l'AP client WDS

Cette procédure décrit comment activer WDS sur l'AP client WDS :

1. Accédez à **Wireless > AP** et activez la case à cocher **Participate in SWAN Infrastructure**. SWAN signifie réseau sans fil structuré.



2. Les points d'accès clients WDS peuvent détecter automatiquement les points d'accès WDS. Vous pouvez également saisir manuellement l'adresse IP de l'AP WDS pour l'enregistrement du client dans la zone de texte **Découverte spécifiée**.

   Vous pouvez également ajouter le nom d'utilisateur et le mot de passe du client WDS pour l'authentification sur le serveur RADIUS local configuré sur l'AP WDS.

Configurations CLI

Point d'accès WDS

Voici un exemple de configuration pour l'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 nthash 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 client WDS

Voici un exemple de configuration pour l'AP client 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
```

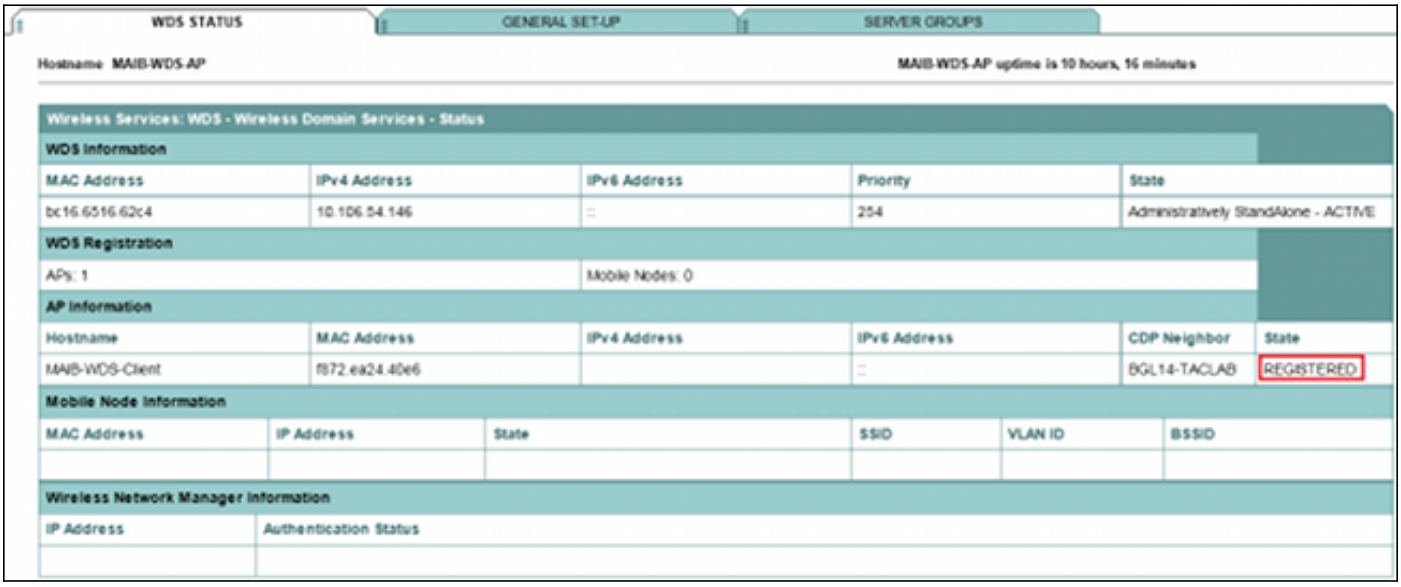
```
no ip address
no ip route-cache
!
encryption mode ciphers aes-ccm
!
ssid WDS-EAP
!
antenna gain 0
stbc
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
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
```

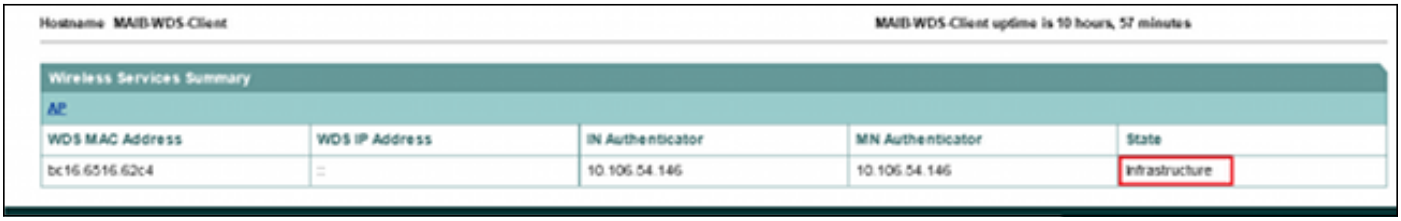
Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration. Une fois la configuration terminée, le point d'accès client WDS doit pouvoir s'enregistrer sur le point d'accès WDS.

Sur le point d'accès WDS, l'état WDS est indiqué comme enregistré.



Sur le point d'accès client WDS, l'état WDS est Infrastructure.



Note: L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Sortie de vérification CLI sur l'AP WDS

Cette procédure montre comment vérifier la configuration de l'AP WDS :

```
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
```

Sortie de vérification CLI sur l'AP client WDS

Cette procédure montre comment vérifier la configuration de l'AP client 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::
```

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.