

Exemple de configuration d'un point d'accès Remote-Edge (REAP) avec des points d'accès légers et des contrôleurs de réseau local sans fil

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurer le WLC pour le fonctionnement de base et configurer les WLAN](#)

[Prime du point d'accès pour l'installation sur le site distant](#)

[Configurer les routeurs 2800 pour établir la liaison WAN](#)

[Déployer le point d'accès REAP sur le site distant](#)

[Vérification](#)

[Dépannage](#)

[Dépannage des commandes](#)

[Informations connexes](#)

[Introduction](#)

Les fonctionnalités REAP (Remote Edge Access Point) introduites avec Cisco Unified Wireless Network permettent le déploiement à distance des LAP (Lightweight Access Points) Cisco à partir du contrôleur WLC (LAN sans fil). Elles sont donc idéales pour les succursales et les petits commerces. Ce document explique comment déployer un réseau local sans fil basé sur l'architecture REAP à l'aide des contrôleurs de réseau local sans fil de la série Cisco 4400 et des points d'accès allégés de la série Cisco 1030.

[Conditions préalables](#)

[Conditions requises](#)

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Connaissance des WLC et configuration de leurs paramètres de base
- Connaissance du mode de fonctionnement REAP dans un LAP Cisco 1030
- Connaissance de la configuration d'un serveur DHCP externe et/ou d'un serveur DNS

(Domain Name System)

- Connaissance des concepts du WPA (Wi-Fi Protected Access)

Components Used

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

- WLC de la gamme Cisco 4400 qui exécute la version 4.2 du micrologiciel
- LAP Cisco 1030
- Deux routeurs de la gamme Cisco 2800 qui exécutent le logiciel Cisco IOS® version 12.2(13)T13
- Adaptateur client Cisco Aironet 802.11a/b/g qui exécute la version 3.0 du micrologiciel
- Utilitaire de bureau Cisco Aironet version 3.0

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Informations générales

Le mode REAP permet à un LAP de résider sur une liaison WAN, tout en étant capable de communiquer avec le WLC et de fournir la fonctionnalité d'un LAP normal. Le mode REAP est pris en charge uniquement sur les LAP 1030 à ce stade.

Afin de fournir cette fonctionnalité, le 1030 REAP sépare le plan de contrôle LWAPP (Lightweight Access Point Protocol) du plan de données sans fil. Les WLC Cisco sont toujours utilisés pour le contrôle et la gestion centralisés de la même manière que les points d'accès LWAPP ordinaires, tandis que toutes les données utilisateur sont pontées localement sur le point d'accès. L'accès aux ressources du réseau local est maintenu pendant les pannes de réseau étendu.

Les points d'accès REAP prennent en charge deux modes de fonctionnement :

- Mode REAP normal
- Mode autonome

Le LAP est défini en mode REAP normal lorsque la liaison WAN entre le point d'accès REAP et le WLC est active. Lorsque les LAP fonctionnent en mode REAP normal, ils peuvent prendre en charge jusqu'à 16 WLAN.

Lorsque la liaison WAN entre le WLC et le LAP est interrompue, le LAP activé par REAP passe en mode autonome. En mode autonome, les LAP REAP peuvent prendre en charge un seul WLAN indépendamment sans le WLC, si le WLAN est configuré avec le WEP (Wired Equivalent Privacy) ou une méthode d'authentification locale. Dans ce cas, le WLAN pris en charge par le point d'accès REAP est le premier WLAN configuré sur le point d'accès, WLAN 1. En effet, la plupart des autres méthodes d'authentification doivent transmettre des informations au contrôleur et à

partir de celui-ci et, lorsque la liaison WAN est arrêtée, cette opération n'est pas possible. En mode autonome, les LAP prennent en charge un ensemble minimal de fonctionnalités. Ce tableau présente l'ensemble des fonctionnalités prises en charge par un LAP REAP lorsqu'il est en mode autonome par rapport aux fonctionnalités prises en charge par un LAP REAP en mode normal (lorsque la liaison WAN est active et que la communication avec le WLC est active) :

Fonctionnalités prises en charge par un LAP REAP en mode REAP normal et en mode autonome

		REAP (normal mode)	REAP (standalone mode)
Protocols	IPv4	Yes	Yes
	IPv6	Yes	Yes
	All other protocols	Yes (only if client is also IP enabled)	Yes (only if client is also IP enabled)
	IP Proxy ARP	No	No
WLAN	Number of SSIDs	16	1 (the first one)
	Dynamic channel assignment	Yes	No
	Dynamic power control	Yes	No
	Dynamic load balancing	Yes	No
VLAN	Multiple interfaces	No	No
	802.1Q Support	No	No
WLAN Security	Rogue AP detection	Yes	No
	Exclusion list	Yes	Yes (existing members only)
	Peer-to-Peer blocking	No	No
	Intrusion Detection System	Yes	No
Layer 2 Security	MAC authentication	Yes	No
	802.1X	Yes	No
	WEP (64/128/152bits)	Yes	Yes
	WPA-PSK	Yes	Yes
	WPA2-PSK	No	No
	WPA-EAP	Yes	No
	WPA2-EAP	Yes	No
Layer 3 Security	Web Authentication	No	No
	IPsec	No	No
	L2TP	No	No
	VPN Pass-through	No	No
	Access Control Lists	No	No
QoS	QoS Profiles	Yes	Yes
	Downlink QoS (weighted round-robin queues)	Yes	Yes
	802.1p support	No	No
	Per-user bandwidth contracts	No	No
	WMM	No	No
	802.11e (future)	No	No
	AAA QoS Profile override	Yes	No
Mobility	Intra-subnet	Yes	Yes
	Inter-subnet	No	No
DHCP	Internal DHCP Server	No	No
	External DHCP Server	Yes	Yes
Topology	Direct connect (2006)	No	No

Le tableau montre que plusieurs VLAN ne sont pas pris en charge sur les LAP REAP dans les deux modes. Plusieurs VLAN ne sont pas pris en charge, car les LAP REAP ne peuvent résider que sur un seul sous-réseau, car ils ne peuvent pas effectuer d'étiquetage VLAN IEEE 802.1Q. Par conséquent, le trafic sur chacun des identificateurs de série de services (SSID) se termine sur

le même sous-réseau que le réseau câblé. Par conséquent, le trafic de données n'est pas séparé du côté câblé, même si le trafic sans fil peut être segmenté entre les SSID.

Reportez-vous au [Guide de déploiement REAP de la succursale](#) pour plus d'informations sur le déploiement REAP, et comment gérer REAP et ses limites.

Configuration

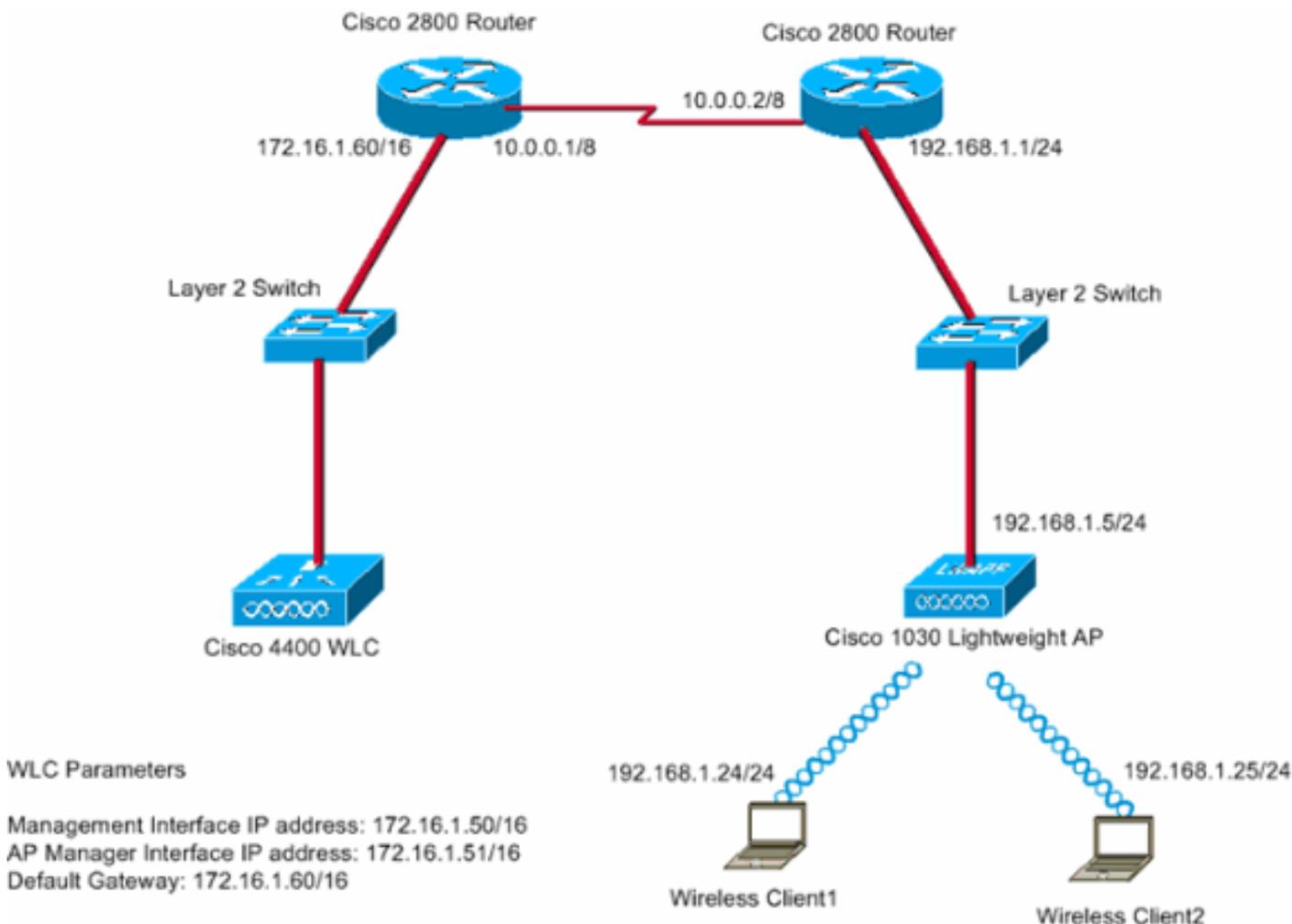
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Afin de configurer les périphériques pour mettre en oeuvre la configuration du réseau, procédez comme suit :

1. [Configurez le WLC pour le fonctionnement de base et configurez les WLAN.](#)
2. [Prime le point d'accès pour l'installation sur le site distant.](#)
3. [Configurez les routeurs 2800 pour établir la liaison WAN.](#)
4. [Déployez le LAP REAP sur le site distant.](#)

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Le bureau central se connecte à la succursale à l'aide d'une ligne louée. La ligne louée se termine

sur les routeurs de la gamme 2800 à chaque extrémité. Cet exemple utilise le protocole OSPF (Open Shortest Path First) pour acheminer les données sur la liaison WAN avec encapsulation PPP. Le WLC 4400 se trouve au bureau central et le LAP 1030 doit être déployé au bureau distant. Le LAP 1030 doit prendre en charge deux WLAN. Voici les paramètres des WLAN :

- **WLAN 1** SSID : **SSID1** Authentification - Ouvrir Cryptage : **Protocole TKIP (Temporal Key Integrity Protocol) (Clé prépartagée WPA [WPA-PSK])**
- **WLAN 2** SSID : **SSID2** Authentification : **protocole EAP (Extensible Authentication Protocol)** Chiffrement : **TKIP** Remarque : pour WLAN 2, la configuration de ce document utilise WPA (authentification 802.1x et TKIP pour le chiffrement).

Vous devez configurer les périphériques pour cette configuration.

[Configurer le WLC pour le fonctionnement de base et configurer les WLAN](#)

Vous pouvez utiliser l'assistant de configuration initiale sur l'interface de ligne de commande (CLI) afin de configurer le WLC pour le fonctionnement de base. Pour configurer le WLC, vous pouvez également utiliser l'interface graphique (GUI). Ce document explique la configuration sur le WLC avec l'utilisation de l'assistant de configuration de démarrage sur l'interface de ligne de commande.

Lors du premier démarrage du WLC, celui-ci ouvre directement l'assistant de configuration de démarrage. Vous utilisez l'assistant de configuration pour configurer les paramètres de base. Vous pouvez exécuter l'assistant sur le CLI ou l'interface graphique (GUI). Voici un exemple de l'assistant de configuration initiale :

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: WLC_MainOffice
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 172.16.1.50
Management Interface Netmask: 255.255.0.0
Management Interface Default Router: 172.16.1.60
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 172.16.1.1
AP Manager Interface IP Address: 172.16.1.51
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (172.16.1.1):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Main
Network Name (SSID): SSID1
Allow Static IP Addresses [YES][no]: Yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: Yes
Enable 802.11a Network [YES][no]: Yes
Enable 802.11g Network [YES][no]: Yes
Enable Auto-RF [YES][no]: Yes
```

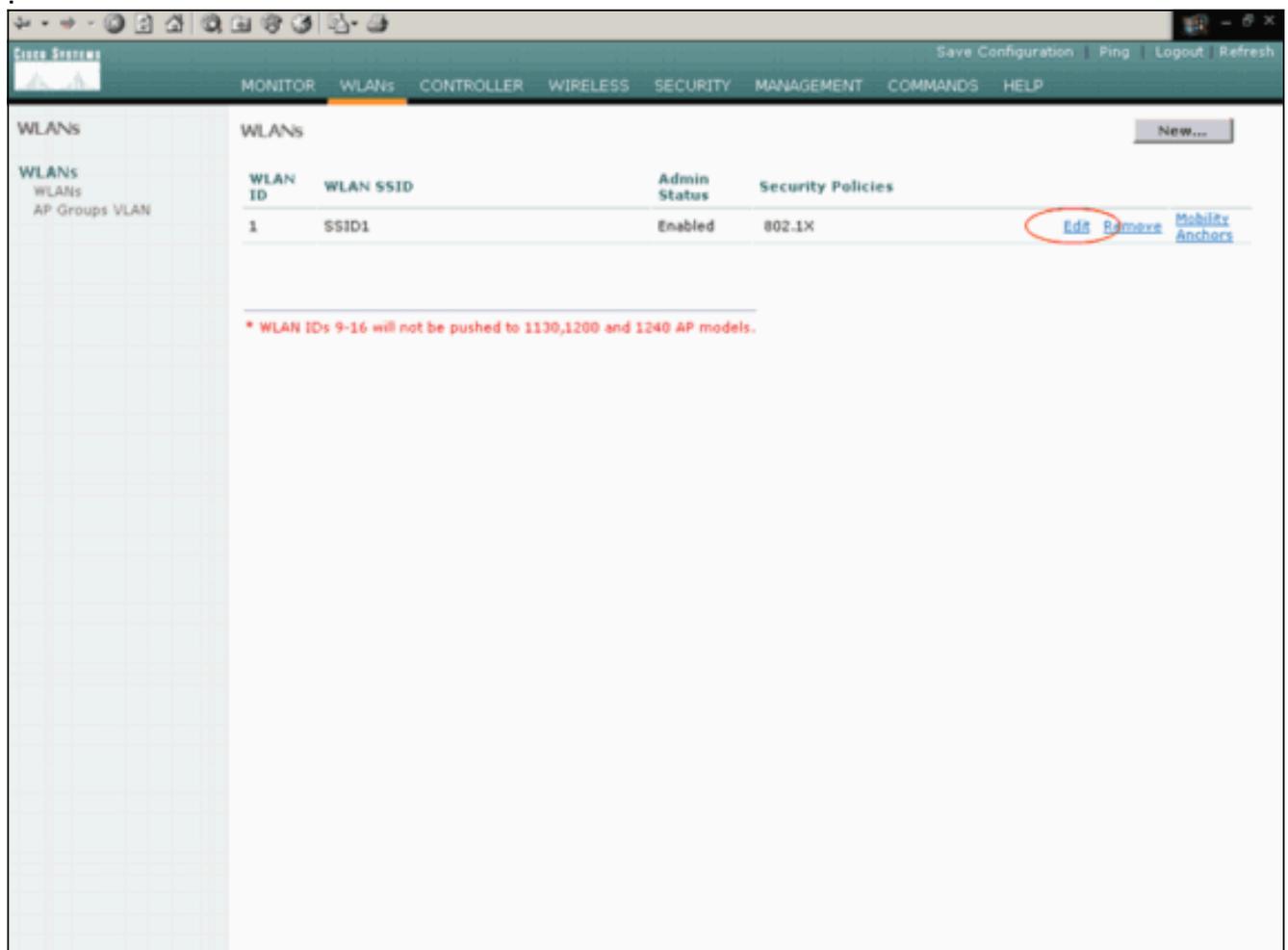
```
Configuration saved!
Resetting system with new configuration...
```

Cet exemple configure ces paramètres sur le WLC :

- Nom du système
- Interface de gestion des adresses IP
- Adresse IP de l'interface du gestionnaire d'AP
- Numéro de port d'interface de gestion
- Identificateur VLAN de l'interface de gestion
- Nom du groupe de mobilité
- SSID
- Beaucoup d'autres paramètres

Ces paramètres sont utilisés pour configurer le WLC pour le fonctionnement de base. Comme le montre le résultat du WLC dans cette section, le WLC utilise 172.16.1.50 comme adresse IP de l'interface de gestion et 172.16.1.51 comme adresse IP de l'interface du gestionnaire AP. Afin de configurer les deux WLAN pour votre réseau, complétez ces étapes sur le WLC :

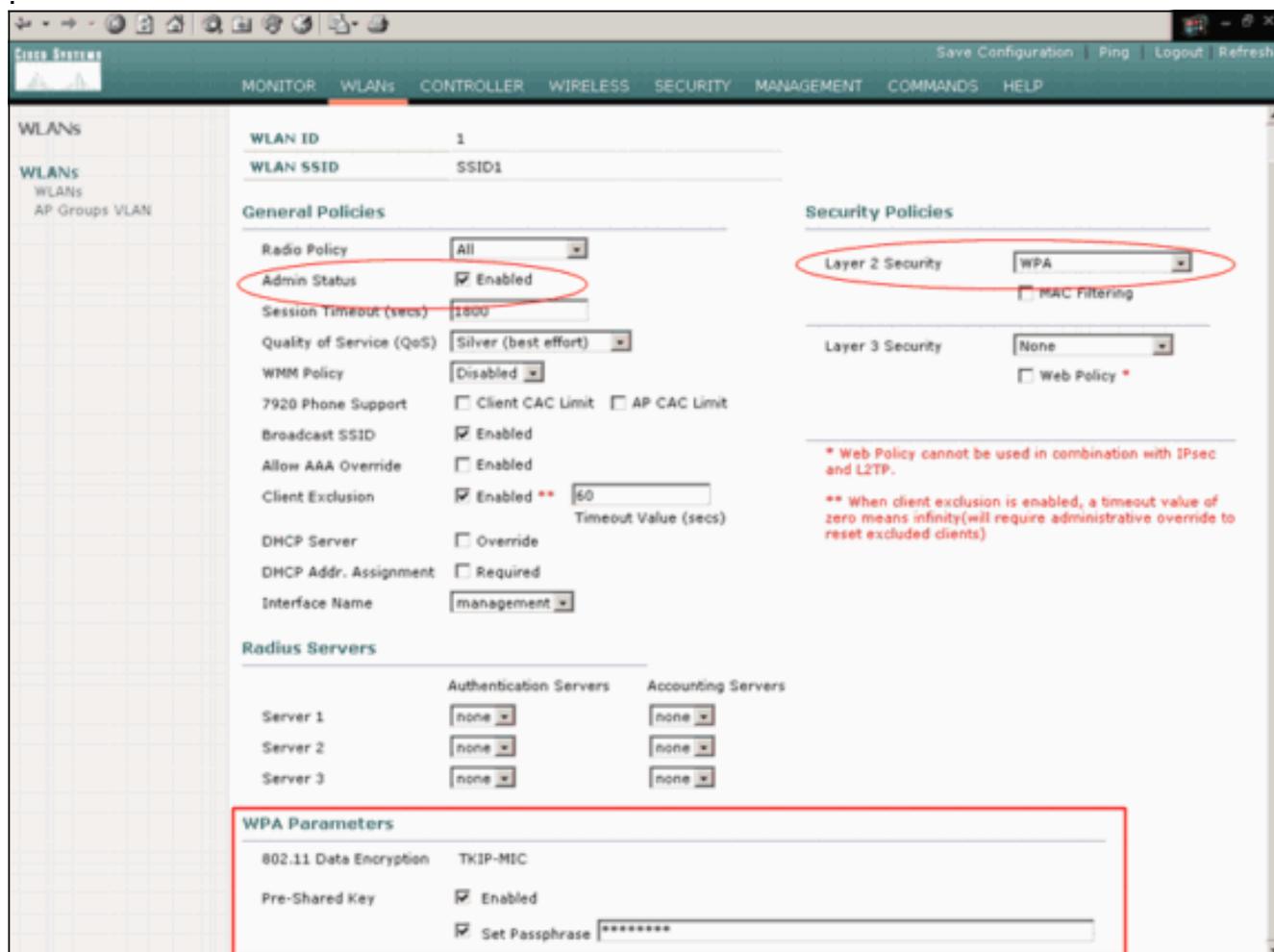
1. Dans l'interface utilisateur graphique du WLC, cliquez sur **WLAN** dans le menu en haut de la fenêtre. La fenêtre de WLAN s'affiche. Cette fenêtre répertorie les WLAN configurés sur le WLC. Étant donné que vous avez configuré un WLAN à l'aide de l'assistant de configuration initiale, vous devez configurer les autres paramètres de ce WLAN.
2. Cliquez sur **Edit** pour le SSID 1 WLAN. Voici un exemple



La fenêtre WLAN > Edit [WLAN > Modifier] s'affiche. Dans cette fenêtre, vous pouvez configurer les paramètres spécifiques au WLAN, qui incluent les stratégies générales, les stratégies de sécurité, le serveur RADIUS et d'autres.

3. Effectuez ces sélections dans la fenêtre WLANs > Edit : Dans la zone Stratégies générales, activez la case à cocher **Activé** en regard de Statut Admin afin d'activer ce WLAN. Choisissez **WPA** dans le menu déroulant Layer 2 Security afin d'utiliser WPA pour WLAN 1. Définissez

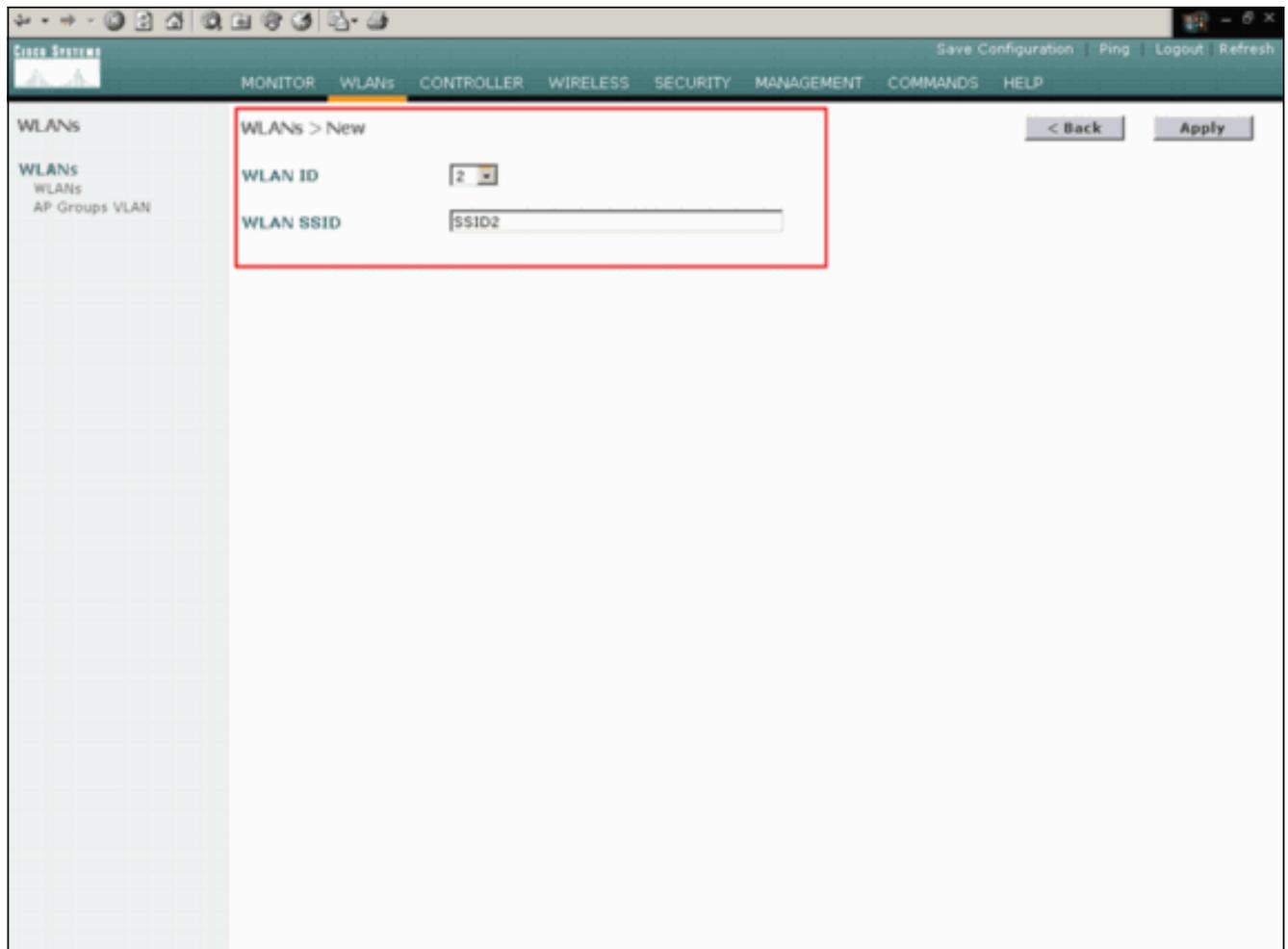
les paramètres WPA en bas de la fenêtre. Afin d'utiliser WPA-PSK sur WLAN 1, cochez la case **Enabled** en regard de Pre-Shared Key dans la zone WPA Parameters et saisissez la phrase de passe pour WPA-PSK. WPA-PSK utilisera TKIP pour le chiffrement. **Remarque** : la phrase de passe WPA-PSK doit correspondre à la phrase de passe configurée sur l'adaptateur client pour que WPA-PSK fonctionne. Cliquez sur Apply. Voici un exemple :



Vous avez configuré le WLAN 1 pour le cryptage WPA-PSK.

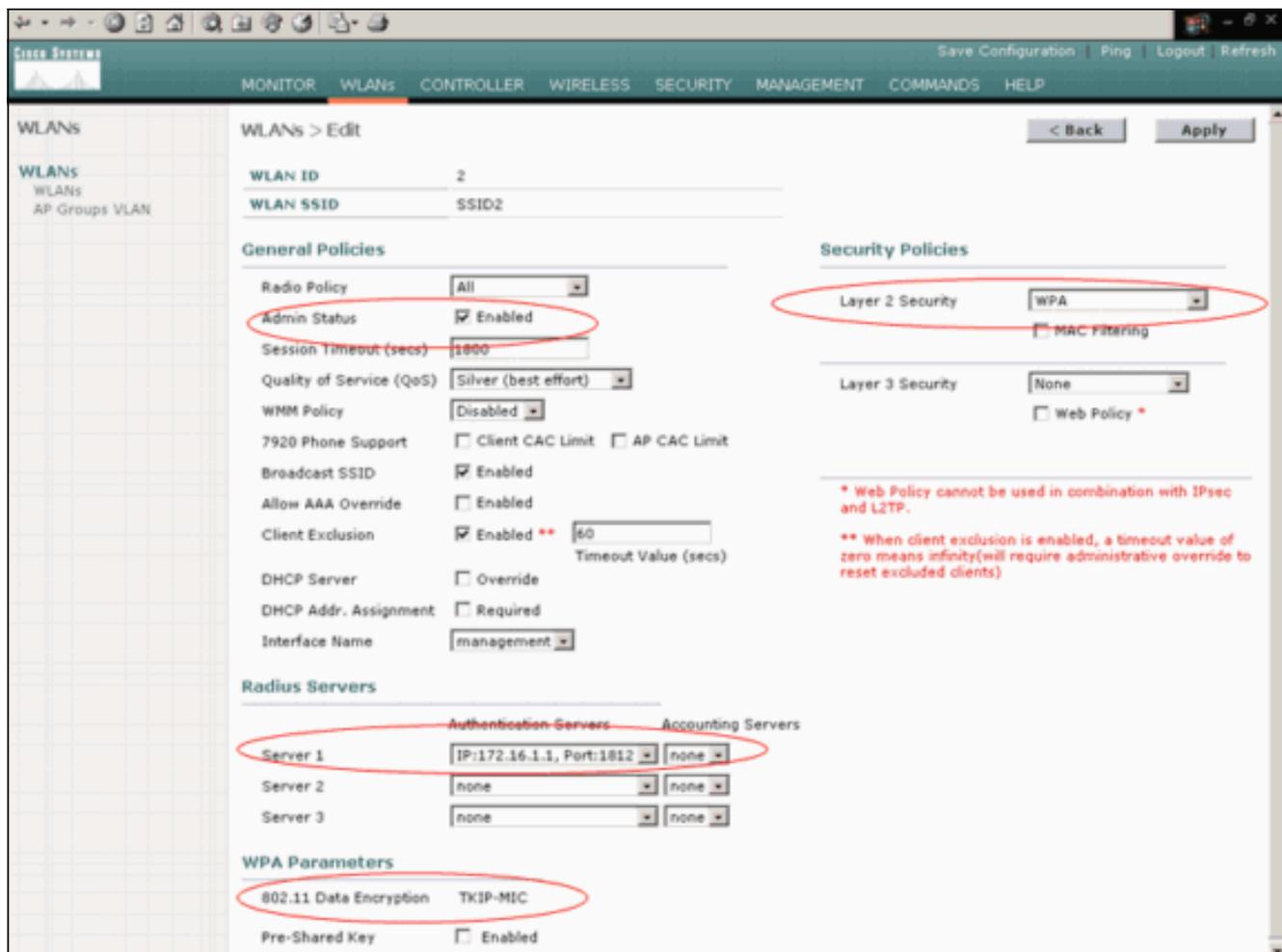
4. Afin de définir WLAN 2, cliquez sur **New** dans la fenêtre WLANs. La fenêtre WLAN > New apparaît.
5. Dans la fenêtre WLAN > New, définissez l'ID WLAN et le SSID WLAN, puis cliquez sur **Apply**. Voici un exemple

:



La fenêtre WLAN > Edit pour le deuxième WLAN apparaît.

6. Effectuez ces sélections dans la fenêtre WLANs > Edit : Dans la zone Stratégies générales, activez la case à cocher **Activé** en regard de Statut Admin afin d'activer ce WLAN. Choisissez **WPA** dans le menu déroulant Layer 2 Security afin de configurer WPA pour ce WLAN. Dans la zone Serveurs Radius, sélectionnez le serveur RADIUS approprié à utiliser pour l'authentification des clients. Cliquez sur Apply. Voici un exemple :



Remarque : Ce document n'explique pas comment configurer les serveurs RADIUS et l'authentification EAP. Pour plus d'informations sur la façon de configurer l'authentification EAP avec les WLC, référez-vous à [Exemple de configuration de l'authentification EAP avec les contrôleurs WLAN \(WLC\)](#).

[Prime du point d'accès pour l'installation sur le site distant](#)

L'établissement de connexion est un processus par lequel les LAP obtiennent une liste de contrôleurs auxquels ils peuvent se connecter. Les LAP sont informés de tous les contrôleurs du groupe de mobilité dès qu'ils se connectent à un contrôleur unique. De cette manière, les LAP apprennent toutes les informations dont ils ont besoin pour rejoindre n'importe quel contrôleur du groupe.

Afin de créer un point d'accès compatible REAP, connectez le point d'accès au réseau câblé du bureau central. Cette connexion permet au point d'accès de découvrir un contrôleur unique. Une fois que le LAP se connecte au contrôleur au bureau central, le point d'accès télécharge la version du système d'exploitation AP qui correspond à l'infrastructure WLAN et à la configuration. Les adresses IP de tous les contrôleurs du groupe de mobilité sont transférées au point d'accès. Lorsque le point d'accès dispose de toutes les informations dont il a besoin, il peut être connecté à l'emplacement distant. Le point d'accès peut ensuite détecter et joindre le contrôleur le moins utilisé de la liste, si la connectivité IP est disponible.

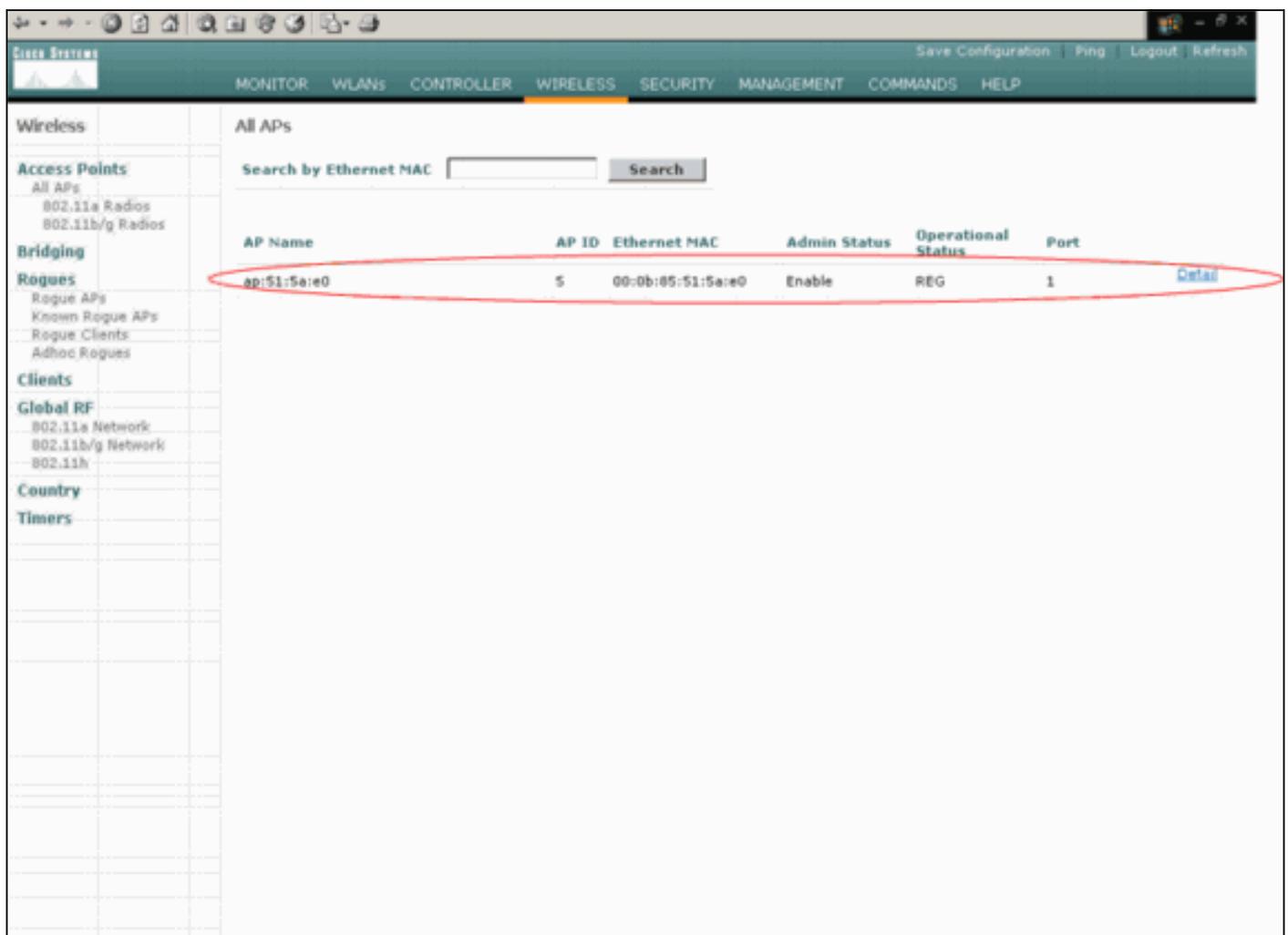
Remarque : Assurez-vous de définir les points d'accès en mode REAP avant de les désactiver afin de les expédier aux sites distants. Vous pouvez définir le mode au niveau du point d'accès via l'interface de ligne de commande ou l'interface utilisateur graphique du contrôleur, ou à l'aide de modèles de système de contrôle sans fil (WCS). Les points d'accès sont configurés pour exécuter une fonctionnalité locale régulière par défaut.

Les LAP peuvent utiliser l'une de ces méthodes afin de détecter le contrôleur :

- **Détection de couche 2**
 - **Détection de couche 3** Avec l'utilisation d'une diffusion de sous-réseau local
Avec l'utilisation de l'option DHCP 43
Avec l'utilisation d'un serveur DNS
Avec l'utilisation du provisionnement en vol (OTAP)
Avec l'utilisation d'un serveur DHCP interne
- Remarque :** Pour utiliser un serveur DHCP interne, le LAP doit se connecter directement au WLC.

Ce document suppose que le LAP s'enregistre auprès du WLC avec l'utilisation du mécanisme de détection de l'option DHCP 43. Pour plus d'informations sur l'utilisation de l'option DHCP 43 pour enregistrer le LAP au contrôleur, ainsi que sur les autres mécanismes de détection, référez-vous à [Enregistrement d'AP léger \(LAP\) à un contrôleur LAN sans fil \(WLC\)](#).

Une fois que le LAP a détecté le contrôleur, vous pouvez voir que l'AP est enregistré au contrôleur dans la fenêtre Wireless du WLC. Voici un exemple :

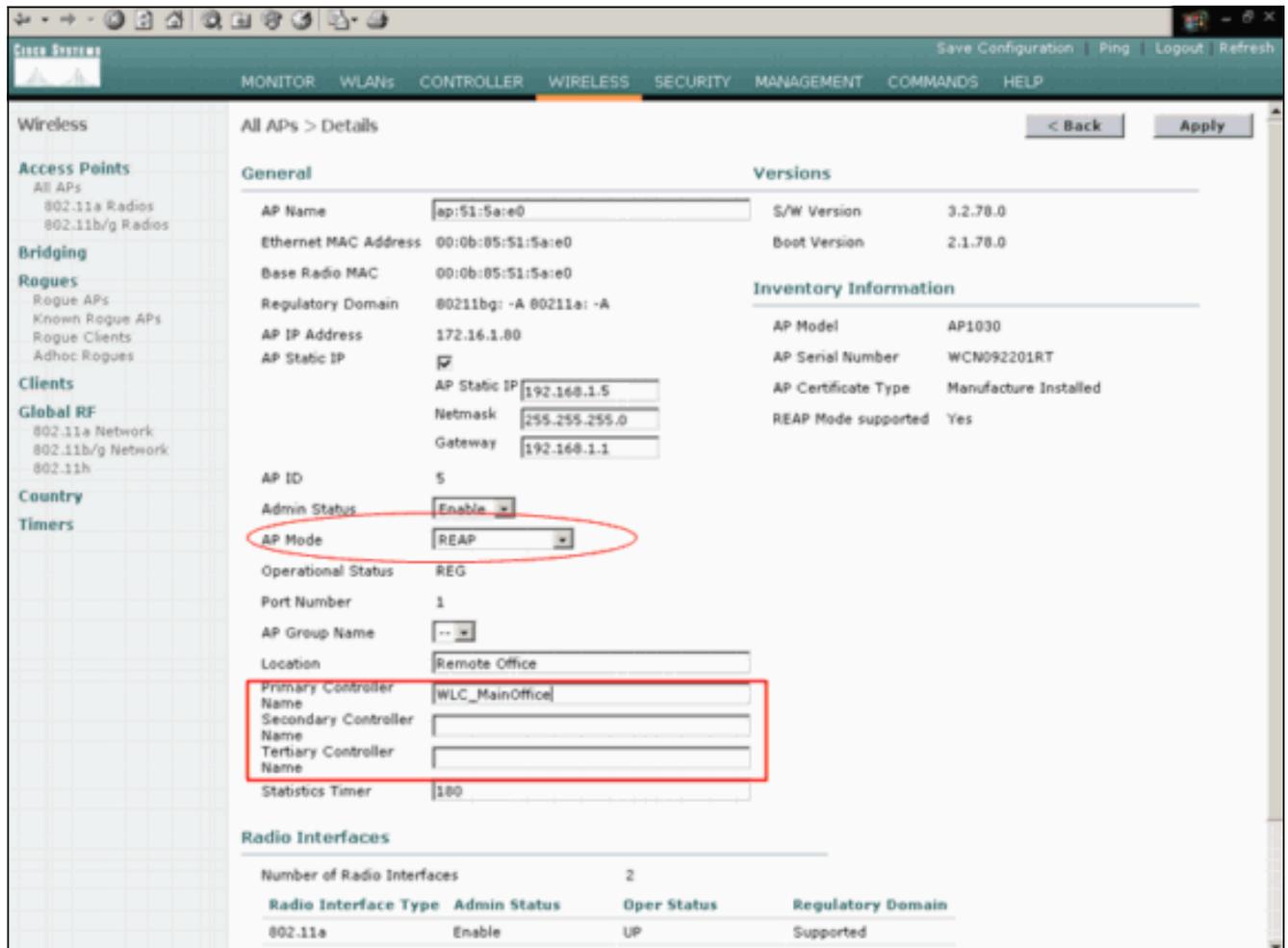


Complétez ces étapes afin de configurer le LAP pour le mode REAP normal :

1. Depuis la GUI du WLC, cliquez sur **Wireless**. La fenêtre Tous les AP s'affiche. Cette fenêtre répertorie les points d'accès enregistrés auprès du WLC.
2. Sélectionnez l'AP que vous devez configurer pour le mode REAP et cliquez sur **Detail**. La fenêtre All APs > Detail de l'AP spécifique s'affiche. Dans cette fenêtre, vous pouvez configurer les différents paramètres de l'AP, qui incluent :
Nom du point d'accès
Adresse IP (que vous pouvez changer en adresse statique)
État de l'administrateur
Paramètres de sécurité
Mode AP
Liste des WLC auxquels le point d'accès peut se connecter
Autres

paramètres

3. Choisissez **REAP** dans le menu déroulant Mode AP. Ce mode est uniquement disponible sur les AP compatibles REAP.
4. Définissez les noms de contrôleur que les AP utiliseront pour s'enregistrer et cliquez sur **Apply**. Vous pouvez définir jusqu'à trois noms de contrôleur (principal, secondaire et tertiaire). Les AP recherchent le contrôleur dans le même ordre que celui que vous fournissez dans cette fenêtre. Comme cet exemple n'utilise qu'un seul contrôleur, il définit le contrôleur comme contrôleur principal. Voici un exemple



Vous avez configuré l'AP pour le mode REAP et vous pouvez le déployer sur le site distant.

Remarque : Dans cette fenêtre d'exemple, vous pouvez voir que l'adresse IP du point d'accès est modifiée en statique et qu'une adresse IP statique 192.168.1.5 est attribuée. Cette affectation se produit car il s'agit du sous-réseau à utiliser au bureau distant. Ainsi, vous utilisez l'adresse IP du serveur DHCP, 172.16.1.80, uniquement pendant l'amorçage. Une fois l'AP enregistré sur le contrôleur, vous modifiez l'adresse en adresse IP statique.

[Configurer les routeurs 2800 pour établir la liaison WAN](#)

Afin d'établir la liaison WAN, cet exemple utilise deux routeurs de la gamme 2800 avec OSPF pour acheminer les informations entre les réseaux. Voici la configuration des deux routeurs pour l'exemple de scénario dans ce document :

Bureau principal

```
MainOffice#show run
Building configuration...

Current configuration : 728 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname MainOffice
!
!
ip subnet-zero
!
!
!
!
interface Ethernet0
 ip address 172.16.1.60 255.255.0.0
 !--- This is the interface which acts as the default
 gateway to the WLC. ! interface Virtual-Templat1 no ip
 address ! interface Serial0 no ip address ! interface
 Serial11 !--- This is the interface for the WAN link. ip
 address 10.0.0.1 255.0.0.0 encapsulation ppp !--- This
 example uses PPP. Use the appropriate !--- encapsulation
 for the WAN connection. ! router ospf 50 !--- Use OSPF
 to route data between the different networks. log-
 adjacency-changes network 10.0.0.0 0.255.255.255 area 0
 network 172.16.0.0 0.0.255.255 area 0 ! ! ip classless
 ip http server ! ! ! line con 0 line aux 0 line vty 0 4
 ! end
```

Succursale

```
BranchOffice#show run
Building configuration...

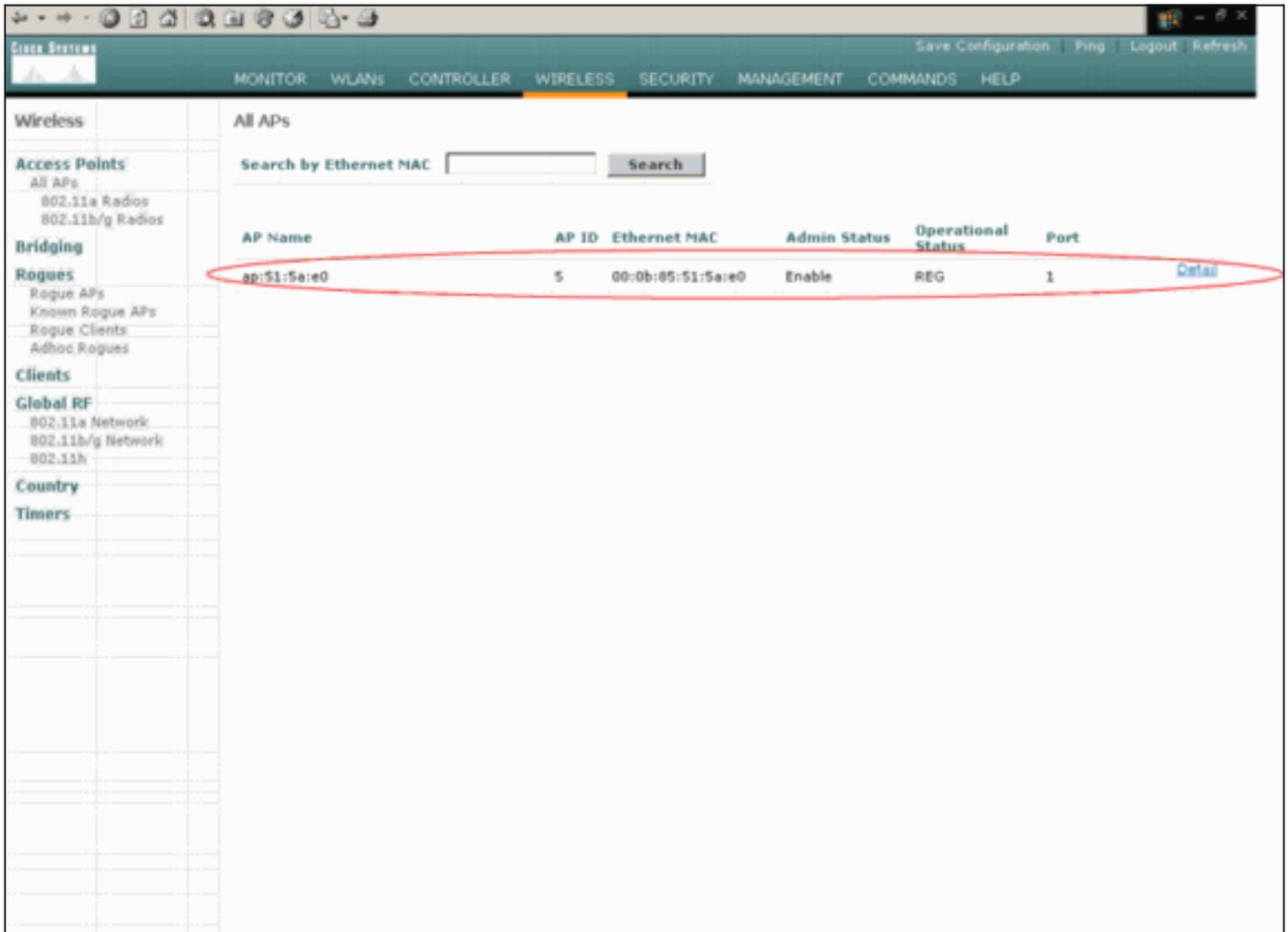
Current configuration : 596 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BranchOffice
!
!
ip subnet-zero
!
!
!
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 !--- This is the interface which acts as the default
 gateway to the LAP. ! interface Serial0 no ip address !
 interface Serial11 !--- This is the interface for the WAN
 link. ip address 10.0.0.2 255.0.0.0 encapsulation ppp
 clockrate 56000 ! router ospf 50 !--- Use OSPF to route
 data between the different networks. log-adjacency-
 changes network 10.0.0.0 0.255.255.255 area 0 network
 192.168.1.0 0.0.0.255 area 0 ! ip classless ip http
```

```
server ! ! ! line con 0 line aux 0 line vty 0 4 login
autocommand access enable-timeout 2 ! end
```

Déployer le point d'accès REAP sur le site distant

Maintenant que vous avez configuré des WLAN sur les WLC, amorcé le LAP et établi la liaison WAN entre le bureau central et le bureau distant, vous êtes prêt à déployer l'AP sur le site distant.

Une fois que vous avez mis le point d'accès sur le site distant, le point d'accès recherche le contrôleur dans l'ordre que vous avez configuré à l'étape d'amorçage. Une fois que le point d'accès a trouvé le contrôleur, le point d'accès s'enregistre auprès du contrôleur. Voici un exemple. À partir du WLC, vous pouvez voir que l'AP a rejoint le contrôleur sur le port 1 :



The screenshot shows the Cisco Wireless LAN Controller (WLC) GUI. The 'All APs' section is active, displaying a table of APs. The table has the following columns: AP Name, AP ID, Ethernet MAC, Admin Status, Operational Status, and Port. A single AP is listed with the following details:

AP Name	AP ID	Ethernet MAC	Admin Status	Operational Status	Port
ap:51:5a:e0	5	00:0b:05:51:5a:e0	Enable	REG	1

Les clients qui ont le SSID **SSID1**, et pour lesquels WPA-PSK est activé, s'associent au point d'accès sur le WLAN 1. Les clients qui ont le SSID **SSID2**, et qui ont l'authentification 802.1x activée, s'associent au point d'accès sur WLAN 2. Voici un exemple qui montre deux clients. Un client est connecté au WLAN 1 et l'autre au WLAN 2 :

Save Configuration Ping Logout Ref Close

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Monitor Clients Items 1 to 2 of 2

Search by MAC address Search

Client MAC Addr	AP Name	AP MAC Addr	WLAN	Type	Status	Auth	Port	
00:40:96:ac:dd:05	ap:51:5a:e0	00:0b:85:51:5a:e0	SSID1	802.11a	Associated	Yes	1	Detail Link Test Disable Remove
00:40:96:ac:e6:57	ap:51:5a:e0	00:0b:85:51:5a:e0	SSID2	802.11a	Associated	Yes	1	Detail Link Test Disable Remove

Summary
Statistics
Controller Ports
Wireless
Rogue APs
Known Rogue APs
Rogue Clients
Adhoc Rogues
802.11a Radios
802.11b/g Radios
Clients
RADIUS Servers

Vérification

Utilisez cette section pour confirmer que votre configuration REAP fonctionne correctement.

Remarque : Consulter les [renseignements importants sur les commandes de débogage](#) avant d'utiliser les commandes de débogage.

Désactivez la liaison WAN. Lorsque la liaison WAN est interrompue, le point d'accès perd la connectivité avec le WLC. Le WLC désinscrit ensuite l'AP de sa liste. Voici un exemple :

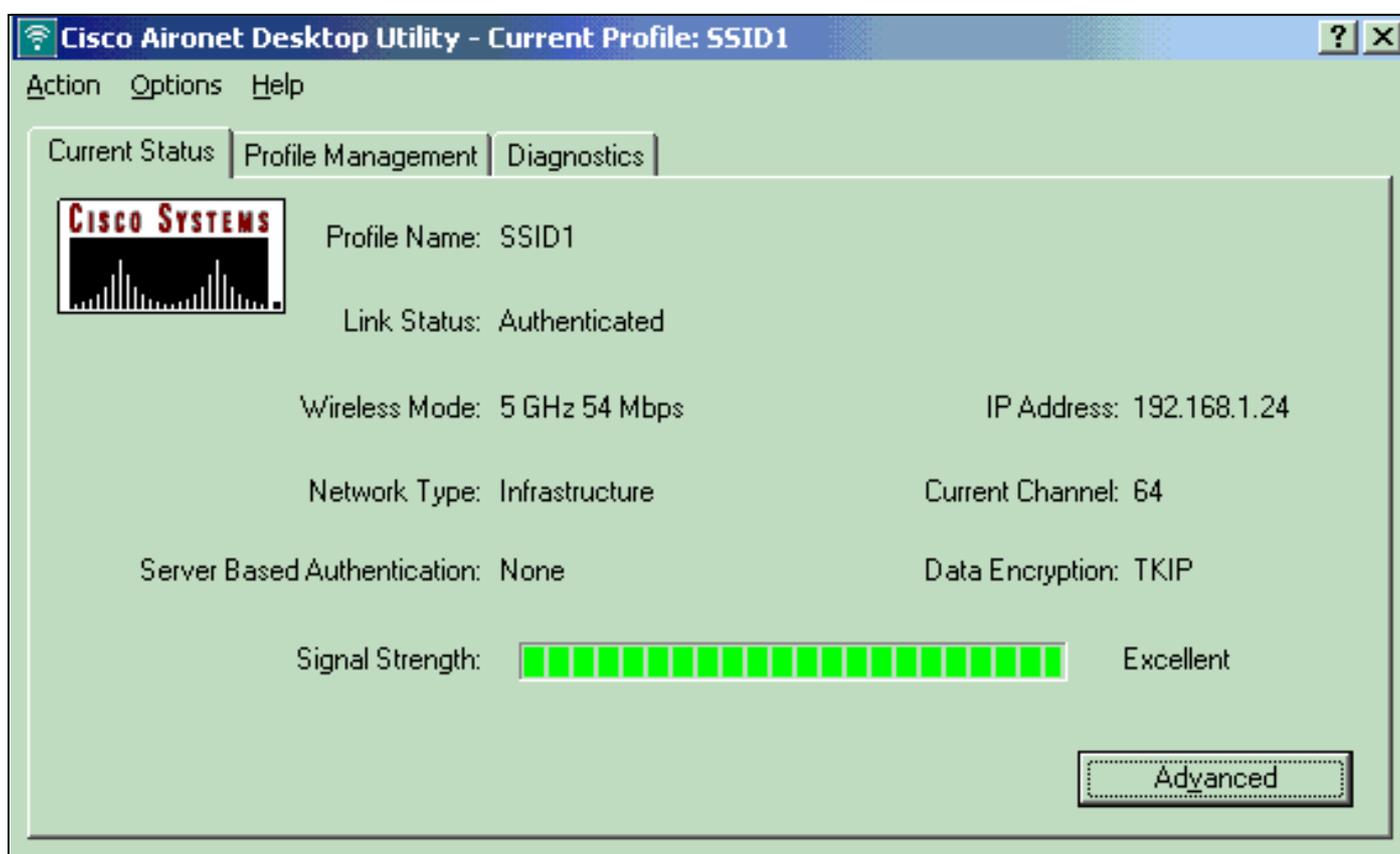
```
(Cisco Controller) >debug lwapp events enable
Wed May 17 15:04:22 2006: Did not receive heartbeat reply from AP 00:0B:85:51:5A:E0
Wed May 17 15:04:22 2006: Max retransmissions reached on AP 00:0B:85:51:5A:E0
(CONFIGURE_COMMAND, 1)
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Down LWAPP event for
AP 00:0b:85:51:5a:e0 slot 0
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event
for AP 00:0b:85:51:5a:e0 slot 0
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Down LWAPP event for
AP 00:0b:85:51:5a:e0 slot 1
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event
for AP 00:0b:85:51:5a:e0 slot 1
Wed May 17 15:04:22 2006: spamDeleteLCB: stats timer not initialized for AP
00:0b:85:51:5a:e0
Wed May 17 15:04:22 2006: Received LWAPP Down event for AP 00:0b:85:51:5a:e0 slot 0!
Wed May 17 15:04:22 2006: Deregister LWAPP event for AP 00:0b:85:51:5a:e0 slot 0
```

Wed May 17 15:04:22 2006: Received LWAPP Down event for AP 00:0b:85:51:5a:e0 slot 1!
Wed May 17 15:04:22 2006: Deregister LWAPP event for AP 00:0b:85:51:5a:e0 slot 1

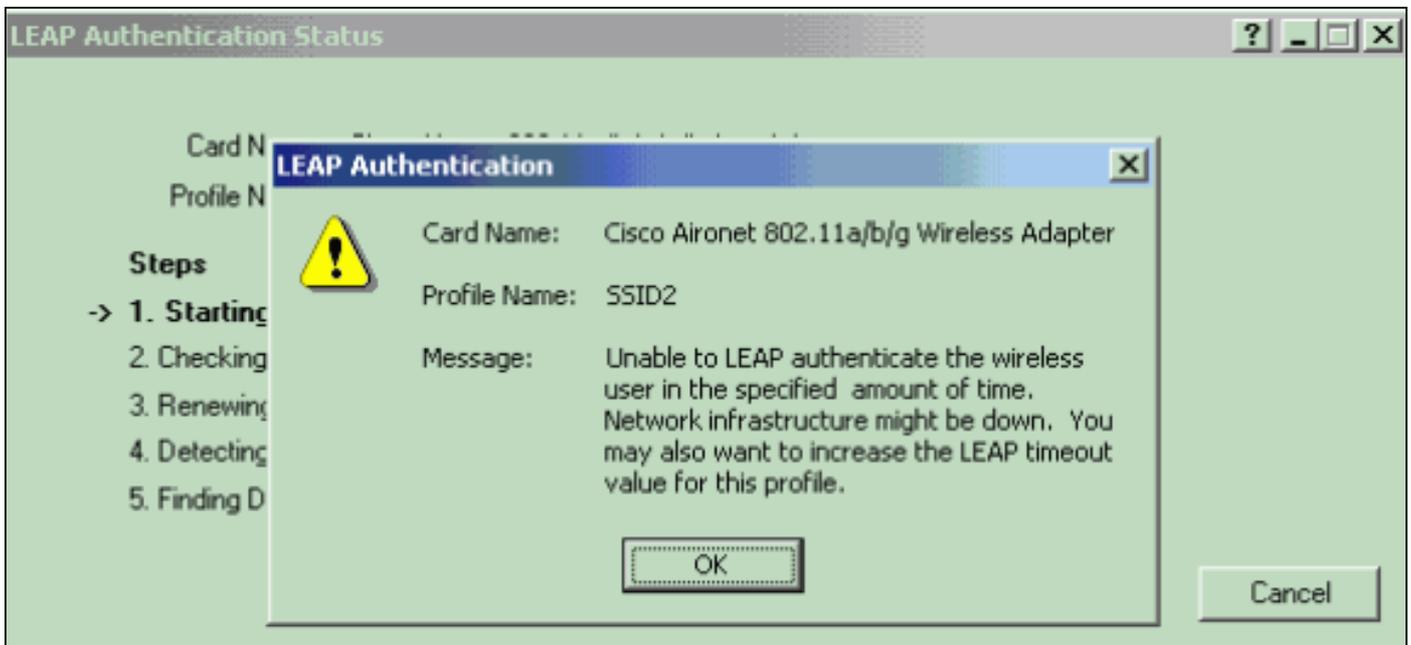
À partir de la sortie de commande **debug lwapp events enable**, vous pouvez voir que le WLC désinscrit l'AP parce que le WLC n'a pas reçu de réponse de pulsation de la part de l'AP. Une réponse de pulsation est similaire aux messages keepalive. Le contrôleur tente cinq pulsations consécutives, à une seconde d'intervalle. Si le WLC ne reçoit pas de réponse, le WLC désinscrit l'AP.

Lorsque le point d'accès est en mode autonome, le voyant d'alimentation du point d'accès clignote. Les clients qui s'associent au premier WLAN (WLAN 1) sont toujours associés au point d'accès car les clients du premier WLAN sont configurés uniquement pour le cryptage WPA-PSK. Le LAP gère le chiffrement lui-même en mode autonome. Voici un exemple qui montre l'état (lorsque la liaison WAN est désactivée) d'un client connecté au WLAN 1 avec SSID1 et WPA-PSK :

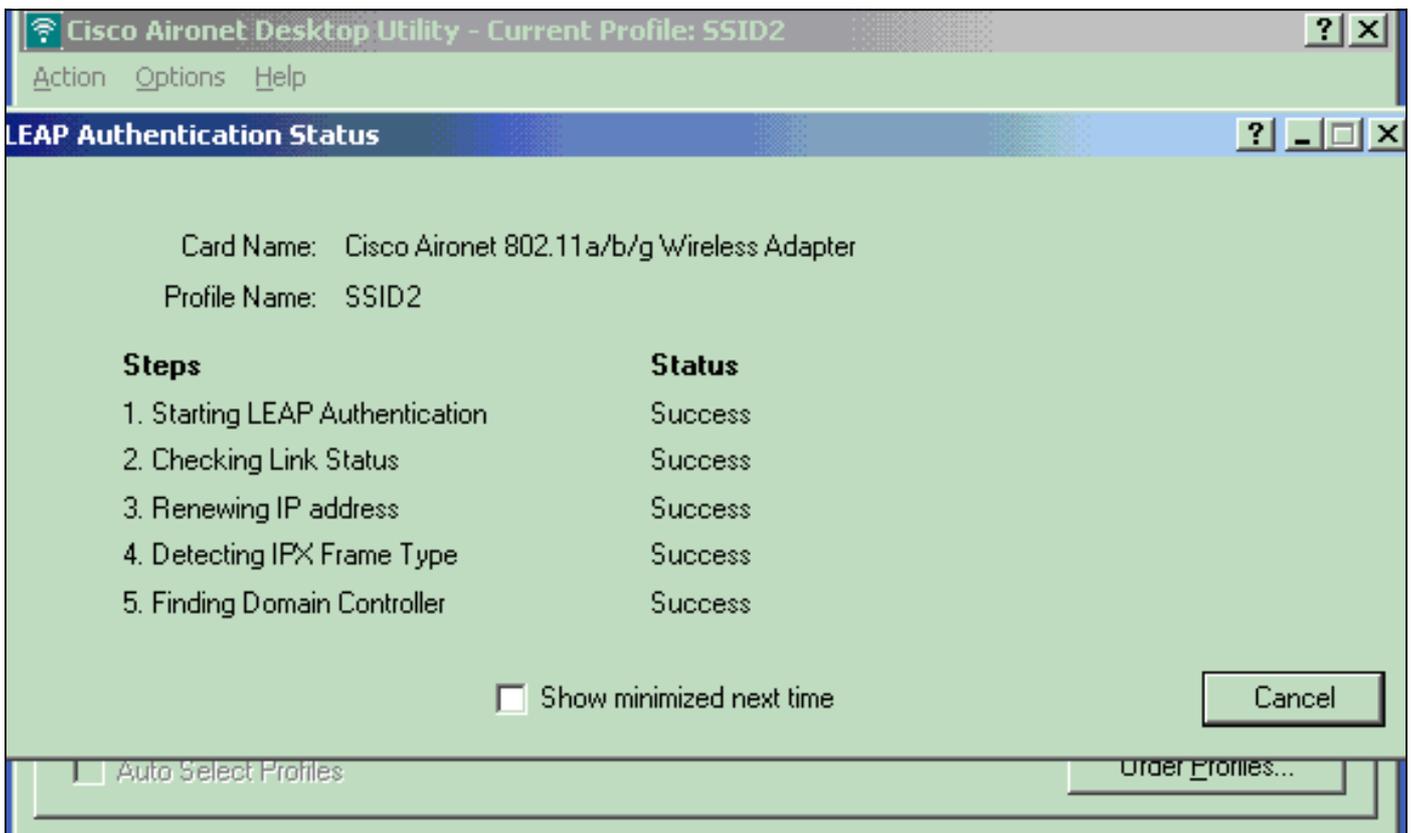
Remarque : TKIP est le chiffrement utilisé avec WPA-PSK.



Les clients connectés au WLAN 2 sont déconnectés car le WLAN 2 utilise l'authentification EAP. Cette déconnexion se produit parce que les clients qui utilisent l'authentification EAP doivent communiquer avec le WLC. Voici un exemple de fenêtre qui montre que l'authentification EAP échoue lorsque la liaison WAN est désactivée :



Une fois la liaison WAN activée, le point d'accès revient au mode REAP normal et s'enregistre auprès du contrôleur. Le client qui utilise l'authentification EAP apparaît également. Voici un exemple :



Cet exemple de sortie de la commande **debug lwapp events enable** sur le contrôleur affiche les résultats suivants :

```
(Cisco Controller) >debug lwapp events enable
Wed May 17 15:06:40 2006: Successful transmission of LWAPP Discovery-Response
to AP 00:0b:85:51:5a:e0 on Port 1
Wed May 17 15:06:52 2006: Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0to
00:0b:85:33:84:a0 on port '1'
Wed May 17 15:06:52 2006: LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0is 1500,
```

```
remote debug mode is 0
Wed May 17 15:06:52 2006: Successfully added NPU Entry for AP 00:0b:85:51:5a:e0(index 51)
Switch IP: 172.16.1.51, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 192.168.1.5, AP
Port: 5550, next hop MAC: 00:d0:58:ad:ae:cb
Wed May 17 15:06:52 2006: Successfully transmission of LWAPP Join-Reply to AP
00:0b:85:51:5a:e0
Wed May 17 15:06:52 2006: Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 0
Wed May 17 15:06:52 2006: Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 1
Wed May 17 15:06:54 2006: Received LWAPP CONFIGURE REQUEST from AP 00:0b:85:51:5a:e0 to
00:0b:85:33:84:a0
Wed May 17 15:06:54 2006: Updating IP info for AP 00:0b:85:51:5a:e0 -- static 1,
192.168.1.5/255.255.255.0, gtw 192.168.1.1
```

Dépannage

Utilisez cette section pour dépanner votre configuration.

Dépannage des commandes

Vous pouvez utiliser ces commandes **debug** pour dépanner la configuration.

Remarque : Consulter les [renseignements importants sur les commandes de débogage](#) avant d'utiliser les commandes de **débogage**.

- **debug lwapp events enable** : affiche la séquence des événements qui se produisent entre le LAP et le WLC.
- **debug lwapp errors enable** : affiche les erreurs qui se produisent dans la communication LWAPP.
- **debug lwapp packet enable** : affiche le débogage d'une trace de paquet LWAPP.
- **debug mac addr** - Active le débogage MAC pour le client que vous spécifiez.

Informations connexes

- [Guide de déploiement des points d'accès REAP au niveau de la filiale](#)
- [Exemple de configuration de l'authentification EAP avec des contrôleurs de réseau local sans fil \(WLC\)](#)
- [Exemple de configuration de base d'un contrôleur LAN sans fil et d'un point d'accès léger](#)
- [Exemple de configuration du basculement du contrôleur de réseau local sans fil pour les points d'accès légers](#)
- [Page de prise en charge du mode sans fil](#)
- [Support et documentation techniques - Cisco Systems](#)