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

les capacités du Point d'accès de Distant-périphérie (REAP) introduites avec le réseau sans fil unifié Cisco permettent le déploiement distant du Point d'accès léger de Cisco (recouvrements) du contrôleur Sans fil du RÉSEAU LOCAL (WLAN) (WLC). Ceci leur fait l'idéal pour la succursale et les petits sites du détaillant. 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 :

- La connaissance de WLCs et comment configurer les paramètres de base WLC
- La connaissance du mode de fonctionnement REAP à Cisco 1030 RECOUVREMENTS
- La connaissance de la configuration d'un serveur DHCP externe et/ou d'un serveur de

Système de noms de domaine (DNS)
- La connaissance des concepts de Protocole WPA (Wi-Fi Protected Access)

Composants utilisés

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

- Gamme Cisco 4400 WLC qui exécute la version de microprogramme 4.2
- Cisco 1030 RECOUVREMENTS
- Deux Routeurs de gamme Cisco 2800 qui exécutent la version de logiciel 12.2(13)T13 de Cisco IOS®
- Adaptateur de client de Cisco Aironet 802.11a/b/g qui exécute la version de microprogramme 3.0
- Version 3.0 de Cisco Aironet Desktop Utility

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

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 RECOUVREMENT de résider à travers un lien WAN, et puisse toujours communiquer avec le WLC et fournir la fonctionnalité d'un RECOUVREMENT régulier. Le mode REAP est pris en charge seulement sur les 1030 recouvrements en ce moment.

Afin de fournir cette fonctionnalité, les 1030 REAP sépare l'avion de contrôle de Protocol de point d'accès léger (LWAPP) du plan de données Sans fil. Des Cisco WLC sont encore utilisés pour le contrôle centralisé et la Gestion de la même manière que les Points d'accès basés sur LWAPP réguliers (aps) sont utilisés, alors que toutes les données d'utilisateur pont localement à AP. Access aux ressources en réseau local est mis à jour tout au long des cas de panne du WAN.

Modes de fonctionnement du support deux REAP aps :

- Mode REAP normal
- Mode autonome

Le RECOUVREMENT est placé dans le mode REAP normal quand le lien WAN entre le REAP AP et le WLC est en hausse. Quand les recouvrements fonctionnent dans le mode REAP normal, ils peuvent prendre en charge jusqu'à 16 WLAN.

Quand le lien WAN entre le WLC et le RECOUVREMENT descend, le RECOUVREMENT REAP-activé commute au mode autonome. Tandis qu'en mode autonome, les recouvrements REAP peuvent prendre en charge seulement un WLAN indépendamment sans WLC, si le WLAN est configuré avec le Confidentialité équivalente aux transmissions par fil (WEP) ou n'importe quelle

méthode d'authentification locale. Dans ce cas, le WLAN que le REAP AP prend en charge est le premier WLAN qui est configuré sur AP, WLAN 1. C'est parce que la plupart des autres méthodes d'authentification doivent passer les informations à et du contrôleur et, quand le lien WAN est en baisse, de cette exécution ne sont pas possibles. En mode autonome, les recouvrements prennent en charge un ensemble de fonctionnalités minimal. Cette table prouve à l'ensemble de fonctionnalités que des supports d'un RECOUVREMENT REAP quand il est en mode autonome en comparaison des caractéristiques qu'un RECOUVREMENT REAP prend en charge dans le mode normal (quand le lien WAN est en hausse et transmission au WLC est) :

Caractéristiques qu'un RECOUVREMENT REAP prend en charge dans le 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

La table prouve que des VLAN multiples ne sont pas pris en charge sur des recouvrements REAP en les deux modes. Le multiple VLAN ne sont pas pris en charge parce que les recouvrements REAP peuvent seulement résider sur un sous-réseau unique parce qu'ils ne peuvent pas exécuter l'étiquetage du 802.1Q VLAN d'IEEE. Par conséquent, le trafic sur chacun des identifiants d'ensemble de services (SSID) se termine sur le même sous-réseau que le réseau câblé. En conséquence, le trafic de données n'est pas séparé du côté de câble quoique le trafic Sans fil puisse être segmenté au-dessus de l'air entre le SSID.

Référez-vous au guide de déploiement REAP à la succursale pour plus d'informations sur le déploiement REAP, et comment gérer le REAP et ses limites.

Configurez

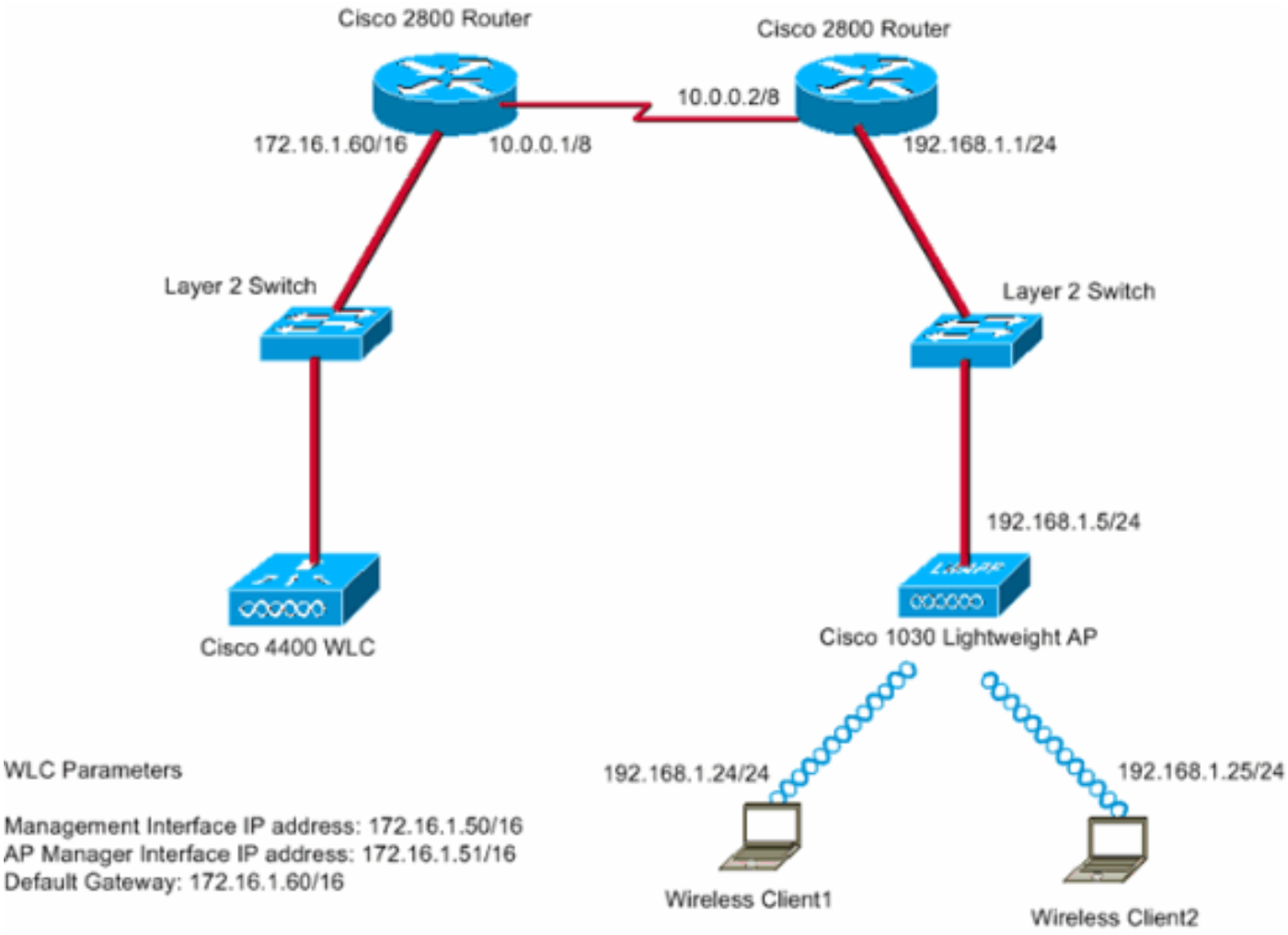
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Afin de configurer les périphériques pour implémenter la configuration réseau, terminez-vous ces étapes :

1. Configurez le WLC pour le fonctionnement de base et configurez les WLAN.
2. Amorcez AP pour l'installation au site distant.
3. Configurez les 2800 Routeurs pour établir le lien WAN.
4. Déployez le RECOUVREMENT REAP au site distant.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Le bureau central se connecte à la succursale à l'utilisation d'une ligne louée. La ligne spécialisée se termine sur des Routeurs de gamme 2800 à chaque extrémité. Cet exemple emploie le Protocole OSPF (Open Shortest Path First) Protocol pour conduire des données sur le lien WAN avec l'encapsulation PPP. Les 4400 WLC sont dans le bureau central et les 1030 RECOUVREMENTS doivent être déployés au bureau distant. Les 1030 RECOUVREMENTS doivent prendre en charge deux WLAN. Voici les paramètres pour les WLAN :

- **WLAN 1**SSID — **SSID1**Authentication openCryptage — **Protocole TKIP (Temporal Key Integrity Protocol) (clé pré-partagée WPA [WPA-PSK])**
- **WLAN 2**SSID — **SSID2**Authentification — **Protocole EAP (Extensible Authentication Protocol)**Cryptage — **TKIPNote**: Pour WLAN 2, la configuration dans ce document utilise le WPA (authentification de 802.1x et TKIP pour le cryptage).

Vous devez configurer les périphériques pour cette installation.

Configurez le WLC pour le fonctionnement de base et configurez les WLAN

Vous pouvez utiliser l'assistant de démarrage de configuration 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 démarrage de configuration sur le CLI.

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

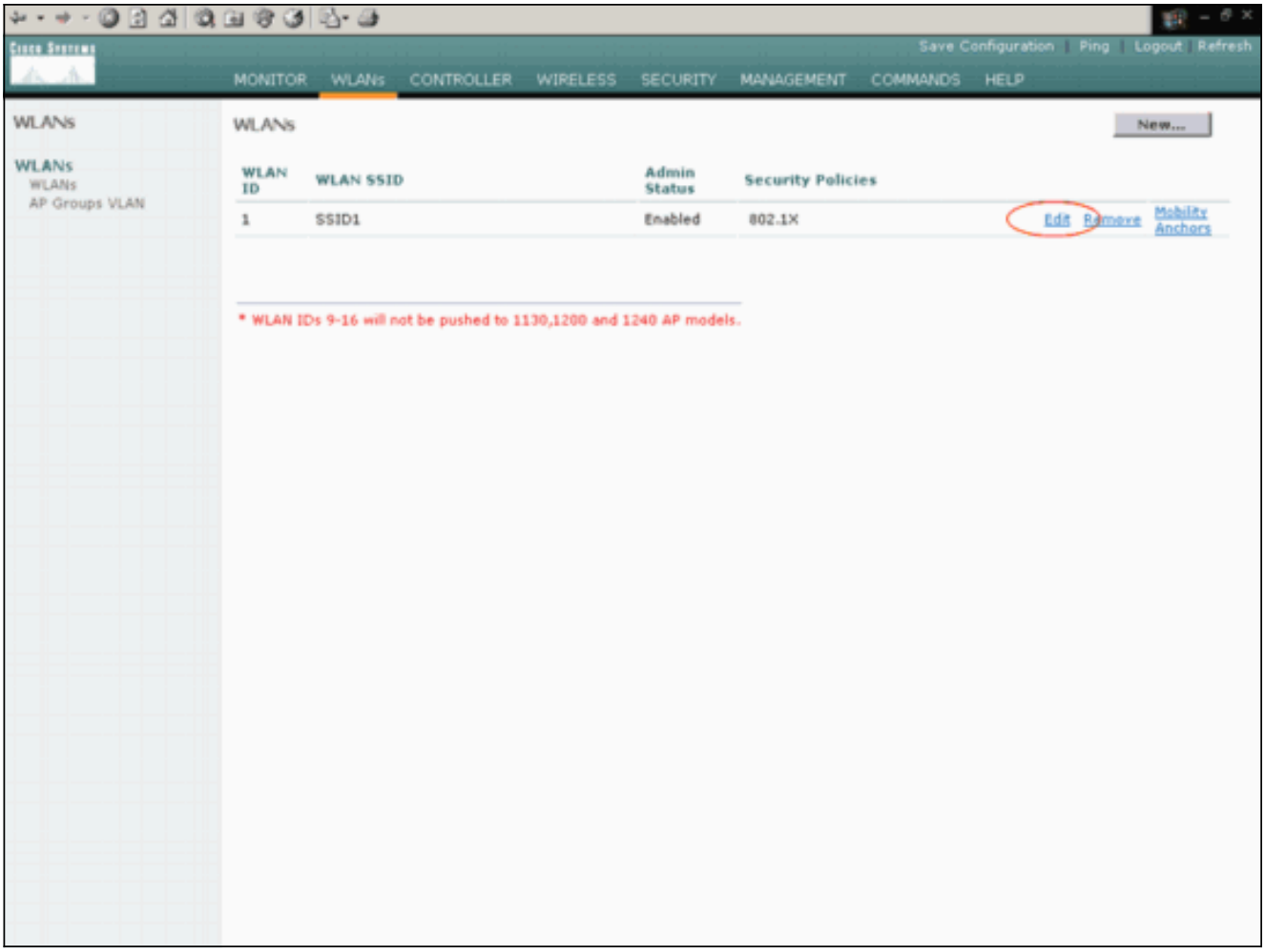
```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: WLC_MainOffice
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 172.16.1.50
Management Interface 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 de système
- Interface de gestion des adresses IP
- adresse IP d'interface d'AP-gestionnaire
- Numéro de port d'interface de gestion
- Identifiant de l'interface de gestion VLAN
- Nom de groupe de mobilité
- SSID
- Beaucoup d'autres paramètres

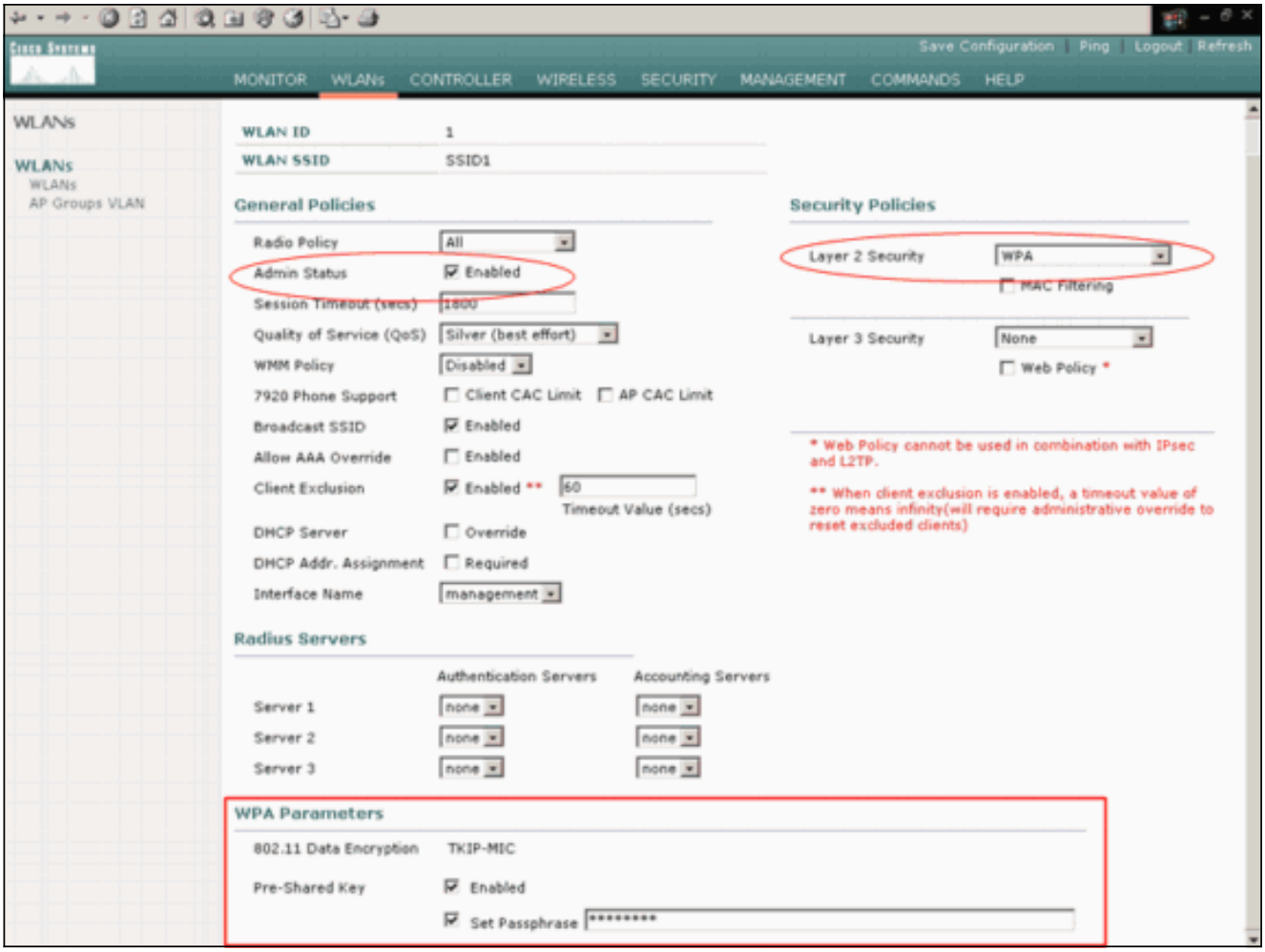
Ces paramètres sont utilisés pour installer le WLC pour le fonctionnement de base. Pendant que la sortie WLC dans cette section affiche, le WLC utilise 172.16.1.50 comme adresse IP d'interface de gestion et 172.16.1.51 comme adresse IP d'interface d'AP-gestionnaire. Afin de configurer les deux WLAN pour votre réseau, terminez-vous ces étapes sur le WLC :

1. Du GUI WLC, clic **WLAN** dans le menu en haut de la fenêtre.La fenêtre de WLAN s'affiche. Cette fenêtre répertorie les WLAN qui sont configurés sur le WLC. Puisque vous avez configuré un WLAN avec l'utilisation de l'assistant de démarrage de configuration, vous devez configurer les autres paramètres pour ce WLAN.
2. Cliquez sur Edit pour le WLAN SSID1.Voici un exemple
   :



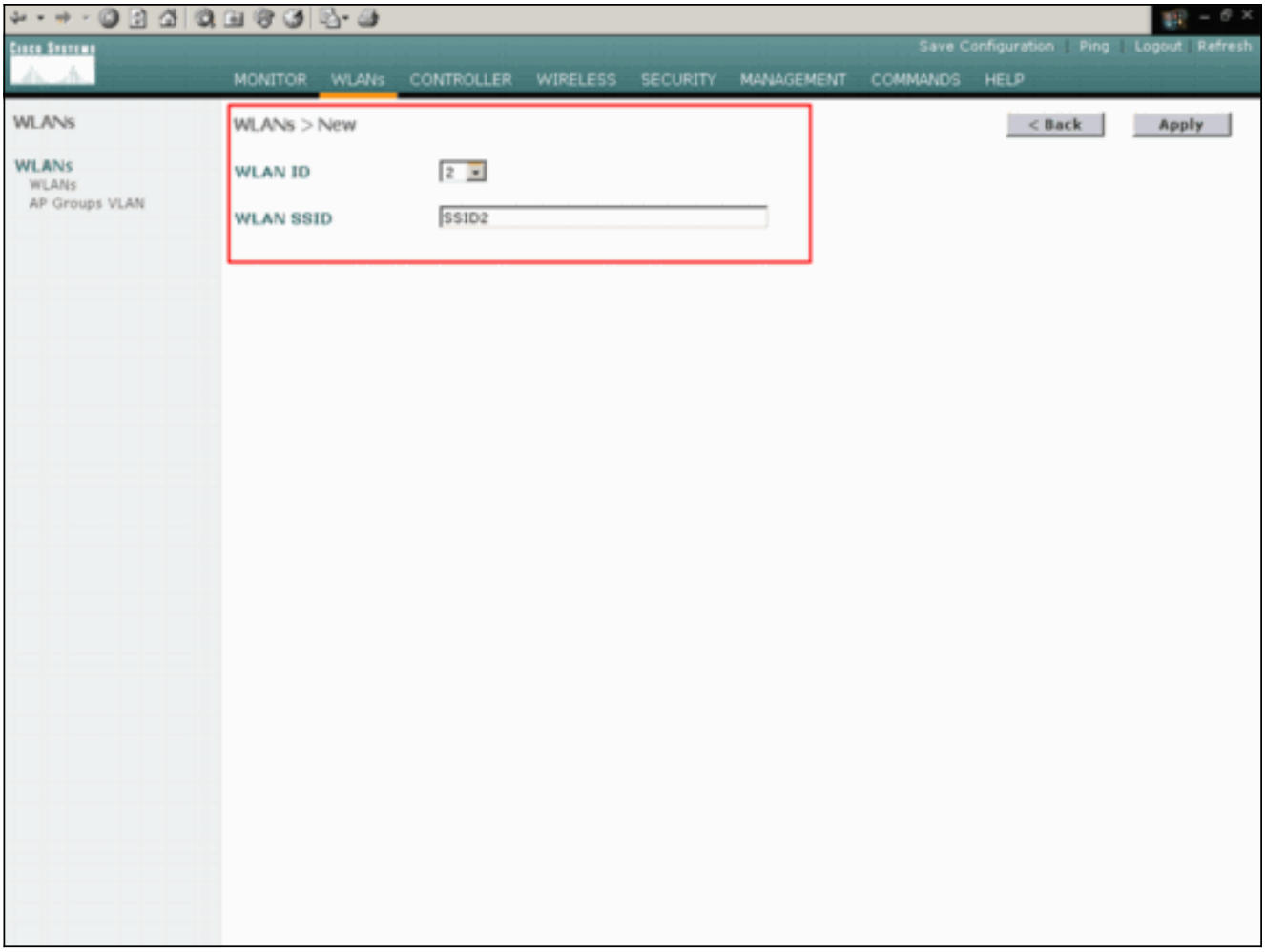
La fenêtre de WLANs > Edit apparaît. Dans cette fenêtre, vous pouvez configurer les paramètres qui sont spécifiques au WLAN, qui inclut des stratégies générales, des stratégies de sécurité, serveur de RAYON, et d'autres.

3. Faites ces sélections dans la fenêtre de WLANs > Edit :Dans la région de stratégies générales, cochez la case **activée** près d'Admin Status afin d'activer ce WLAN.Choisissez le **WPA du** menu déroulant de degré de sécurité de la couche 2 afin d'utiliser le WPA pour WLAN 1.Définissez les paramètres WPA au bas de la fenêtre.Afin d'utiliser le WPA-PSK sur WLAN 1, cochez la case **activée** près de la clé pré-partagée dans la région de paramètres WPA et entrez dans le mot de passe pour le WPA-PSK. Le WPA-PSK utilisera le TKIP pour le cryptage.**Note**: Le mot de passe de WPA-PSK doit apparier le mot de passe qui est configuré sur l'adaptateur de client pour que le WPA-PSK fonctionne.Cliquez sur **Apply**.Voici un exemple
:



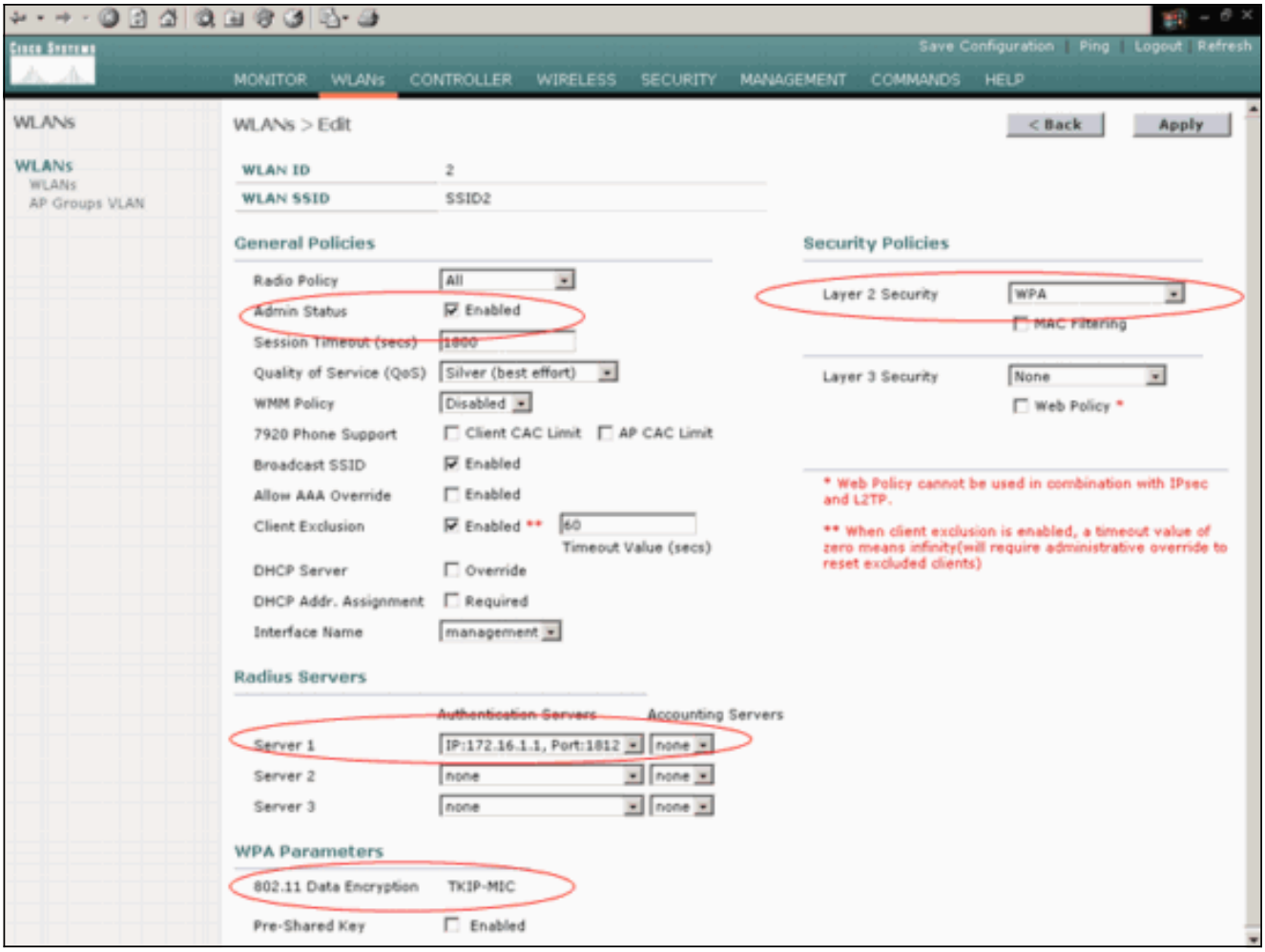
Vous avez configuré le cryptage de WPA-PSK de 1par WLAN.

4. Afin de définir WLAN 2, cliquez sur New dans la fenêtre WLAN.Le WLAN > nouvelle fenêtre apparaît.
5. Dans le WLAN > nouvelle fenêtre, définissent l'ID de WLAN et le WLAN SSID, et cliquent sur Apply.Voici un exemple
   :



La fenêtre de WLAN > Edit pour le deuxième WLAN apparaît.

6. Faites ces sélections dans la fenêtre de WLANs > Edit :Dans la région de stratégies générales, cochez la case **activée** près d'Admin Status afin d'activer ce WLAN.Choisissez le **WPA du** menu déroulant de degré de sécurité de la couche 2 afin de configurer le WPA pour ce WLAN.Dans la région de serveurs de rayon, choisissez le serveur compétent de RAYON pour l'utiliser pour l'authentification des clients.Cliquez sur **Apply**.Voici un exemple :



Note: Ce document n'explique pas comment configurer les serveurs et l'authentification EAP de RAYON. Pour les informations sur la façon dont configurer l'authentification EAP avec WLCs, référez-vous à l'authentification EAP avec l'exemple de configuration des contrôleurs WLAN (WLC).

Amorcez AP pour l'installation au site distant

L'amorçage est un processus par lequel les recouvrements obtiennent une liste de contrôleurs auxquels ils peuvent se connecter. Les recouvrements sont au courant de tous les contrôleurs au groupe de mobilité dès qu'ils se connecteront à un contrôleur simple. De cette façon, les recouvrements apprennent toutes les informations qu'ils doivent afin de joindre n'importe quel contrôleur dans le groupe.

Afin d'amorcer AP REAP-capable, connectez AP au réseau câblé au bureau central. Cette connexion permet à AP pour découvrir un contrôleur simple. Après que le RECOUVREMENT joigne le contrôleur au bureau central, AP télécharge la version du système d'exploitation AP (SYSTÈME D'EXPLOITATION) qui correspond à l'infrastructure WLAN et à la configuration. Les adresses IP de tous les contrôleurs au groupe de mobilité sont transférées vers AP. Quand AP a toutes les informations dont il a besoin, AP peut être connecté au site distant. AP peut alors découvrir et joindre le contrôleur moins-utilisé de la liste, si la connectivité IP est disponible.

Note: Assurez-vous que vous placez les aps au mode « REAP » avant que vous les arrêtiez afin de les expédier aux sites distants. Vous pouvez placer le mode au niveau AP par le contrôleur CLI ou GUI, ou avec l'utilisation des modèles du système de contrôle sans fil (WCS). Des aps sont placés pour exécuter le militaire de carrière, fonctionnalité « locale » par défaut.

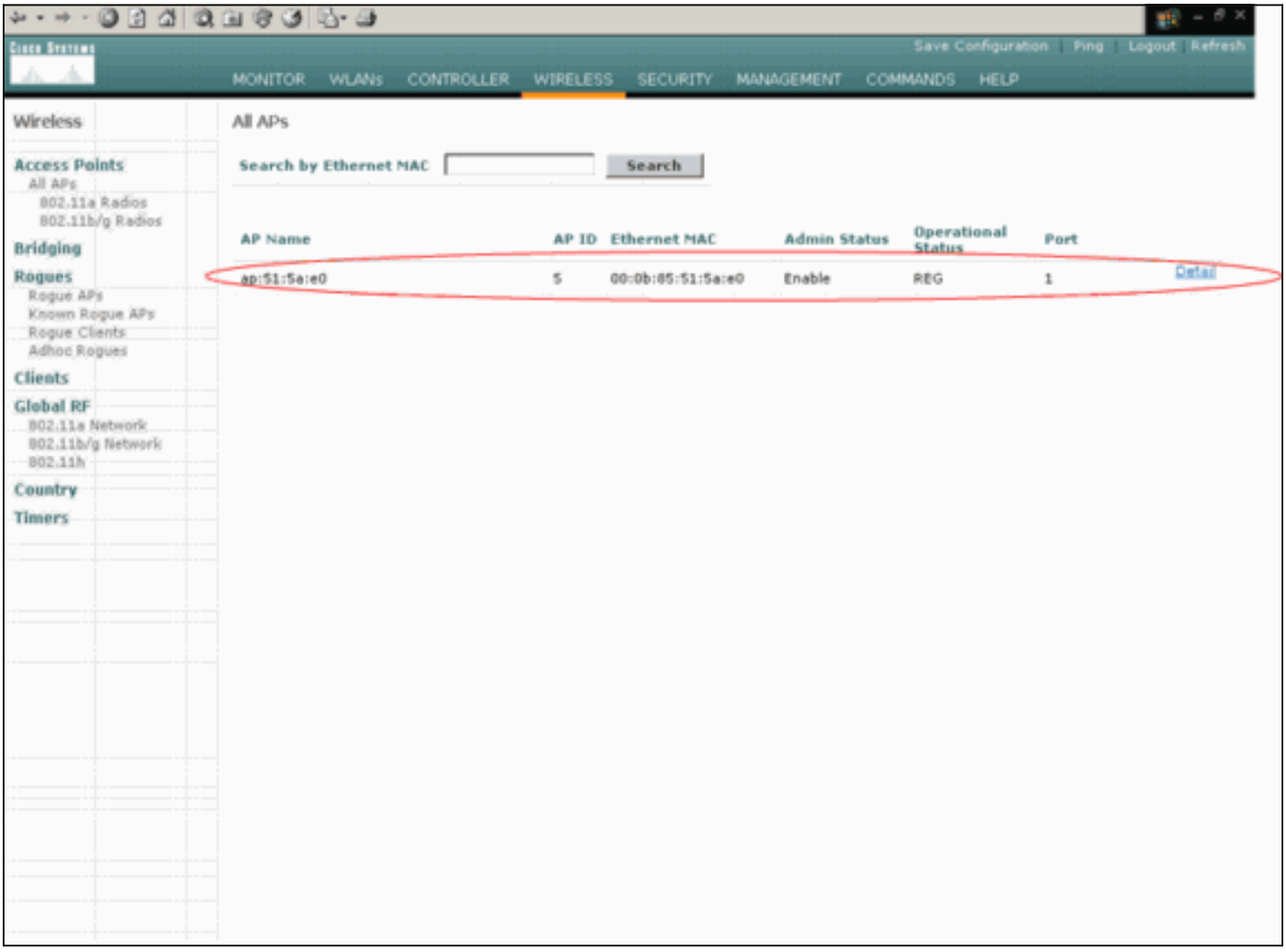
Les recouvrements peuvent employer des n'importe quelles de ces méthodes afin de découvrir le

contrôleur :

- **Détection de la couche 2**
- **Détection de la couche 3**Avec l'utilisation d'une diffusion de sous-réseau localeAvec l'utilisation de l'option 43 DHCPAvec l'utilisation d'un serveur DNSAvec l'utilisation de l'Over-the-Air Provisioning (OTAP)Avec l'utilisation d'un serveur DHCP interne**Note**: Afin d'utiliser un serveur DHCP interne, le RECOUVREMENT doit se connecter directement au WLC.

Ce document suppose que le RECOUVREMENT s'enregistre au WLC avec l'utilisation du mécanisme de détection de l'option 43 DHCP. Pour plus d'informations sur l'utilisation de l'option 43 DHCP d'enregistrer le RECOUVREMENT au contrôleur, aussi bien que les autres mécanismes de détection, référez-vous à l'enregistrement léger AP (RECOUVREMENT) à un contrôleur LAN Sans fil (WLC).

Après que le RECOUVREMENT découvre le contrôleur, vous pouvez voir qu'AP est enregistré au contrôleur dans la fenêtre Sans fil du WLC. Voici un exemple :

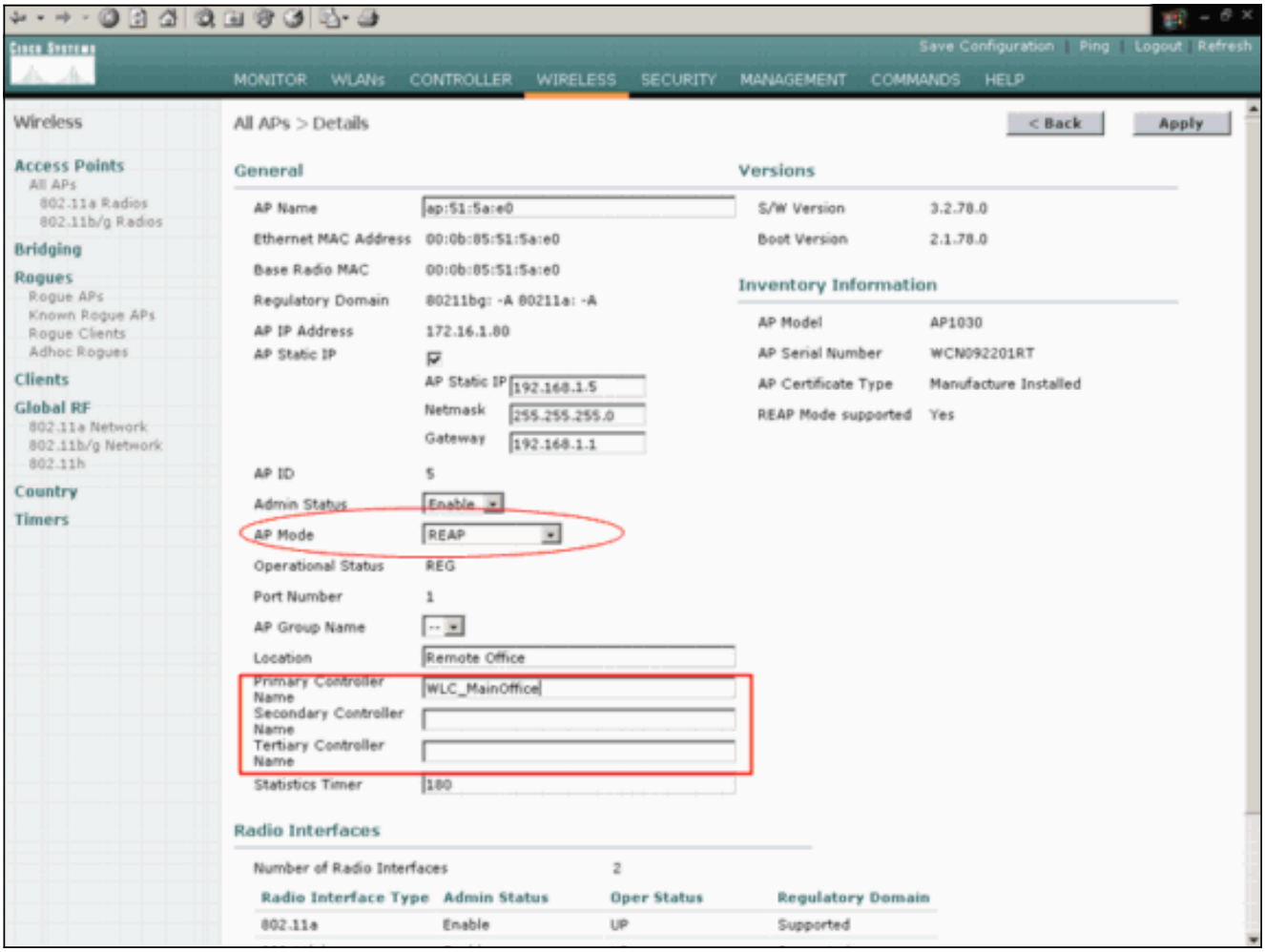


Terminez-vous ces étapes afin de configurer le RECOUVREMENT pour le mode REAP normal :

1. Depuis la GUI du WLC, cliquez sur **Wireless**.La toute la fenêtre aps apparaît. Cette fenêtre répertorie les aps qui sont enregistrés au WLC.
2. Sélectionnez AP que vous devez configurer pour le mode REAP et cliquer sur le **détail**.La fenêtre d'All APs > Detail pour la particularité AP apparaît. Dans cette fenêtre, vous pouvez configurer les divers paramètres d'AP, qui incluent :Nom APAdresse IP (que vous pouvez changer à la charge statique)État d'adminParamètres de sécuritéMode APListe de WLCs à

laquelle AP peut se connecterD'autres paramètres

3. Choisissez le **REAP du** menu déroulant de mode AP.Ce mode est seulement disponible sur des aps REAP-capables.
4. Définissez les noms de contrôleur que les aps les utiliseront pour s'enregistrer et pour cliquer sur Apply.Vous pouvez définir jusqu'à trois noms de contrôleur (primaire, secondaire, et tertiaire). Les aps recherchent le contrôleur dans la même commande que vous fournissez dans cette fenêtre. Puisque cet exemple utilise seulement un contrôleur, l'exemple définit le contrôleur comme contrôleur primaire.Voici un exemple
:



Vous avez installé AP pour le mode REAP, et vous pouvez le déployer au site distant.

Note: Dans cette fenêtre d'exemple, vous pouvez voir que l'adresse IP d'AP est changée à la charge statique et une adresse IP statique 192.168.1.5 est assignée. Cette affectation se produit parce que c'est le sous-réseau à utiliser au bureau distant. Ainsi vous utilisez l'adresse IP du serveur DHCP, 172.16.1.80, seulement pendant l'étape d'amorçage. Après qu'AP soit enregistré au contrôleur, vous changez l'adresse à une adresse IP statique.

Configurez les 2800 Routeurs pour établir le lien WAN

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

MainOffice

```
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-Template1 no ip
address ! interface Serial0 no ip address ! interface
Serial1 !--- 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
```

BranchOffice

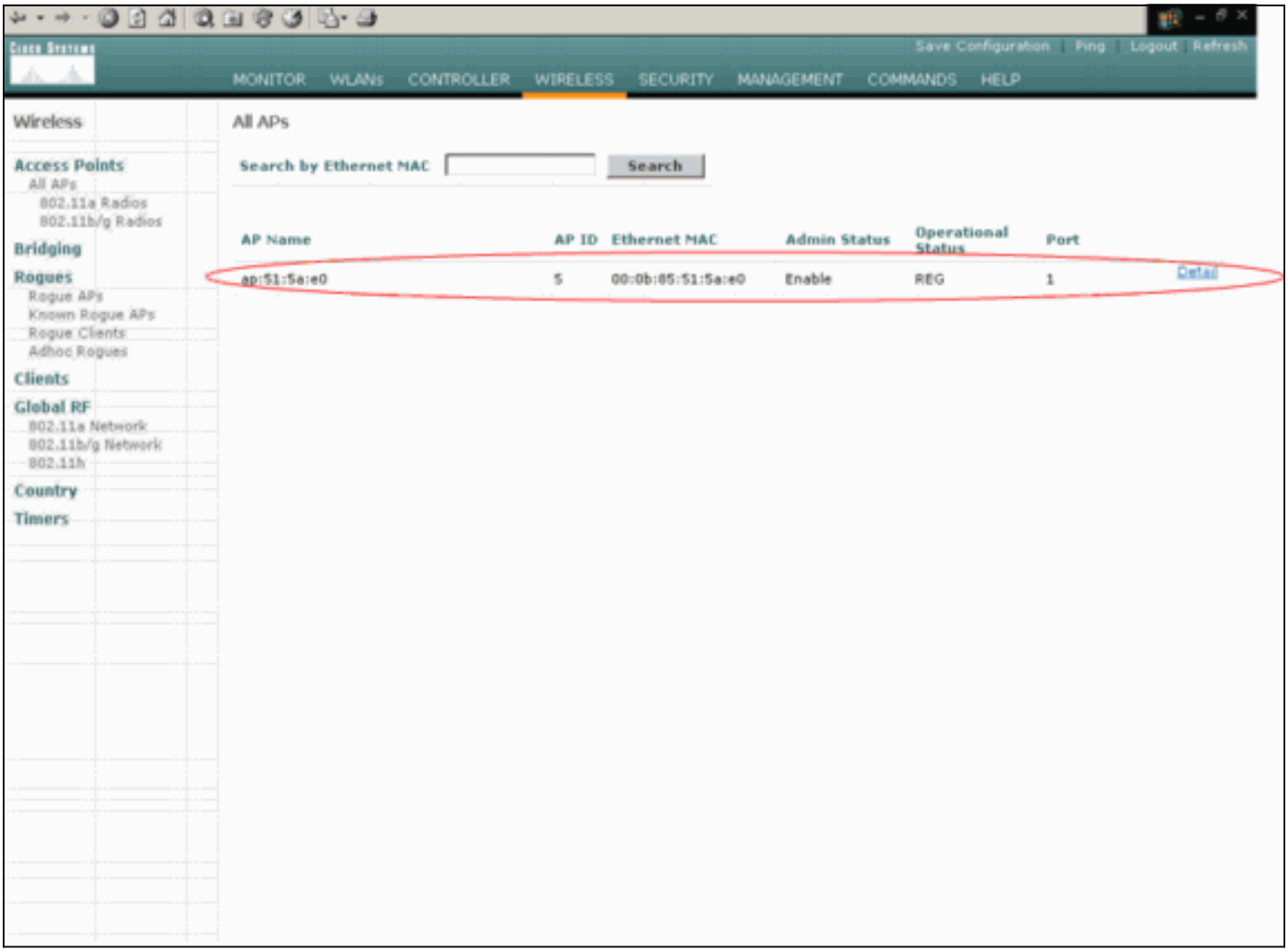
```
BranchOffice#show run
Building configuration...

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 Serial1 !--- 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
```

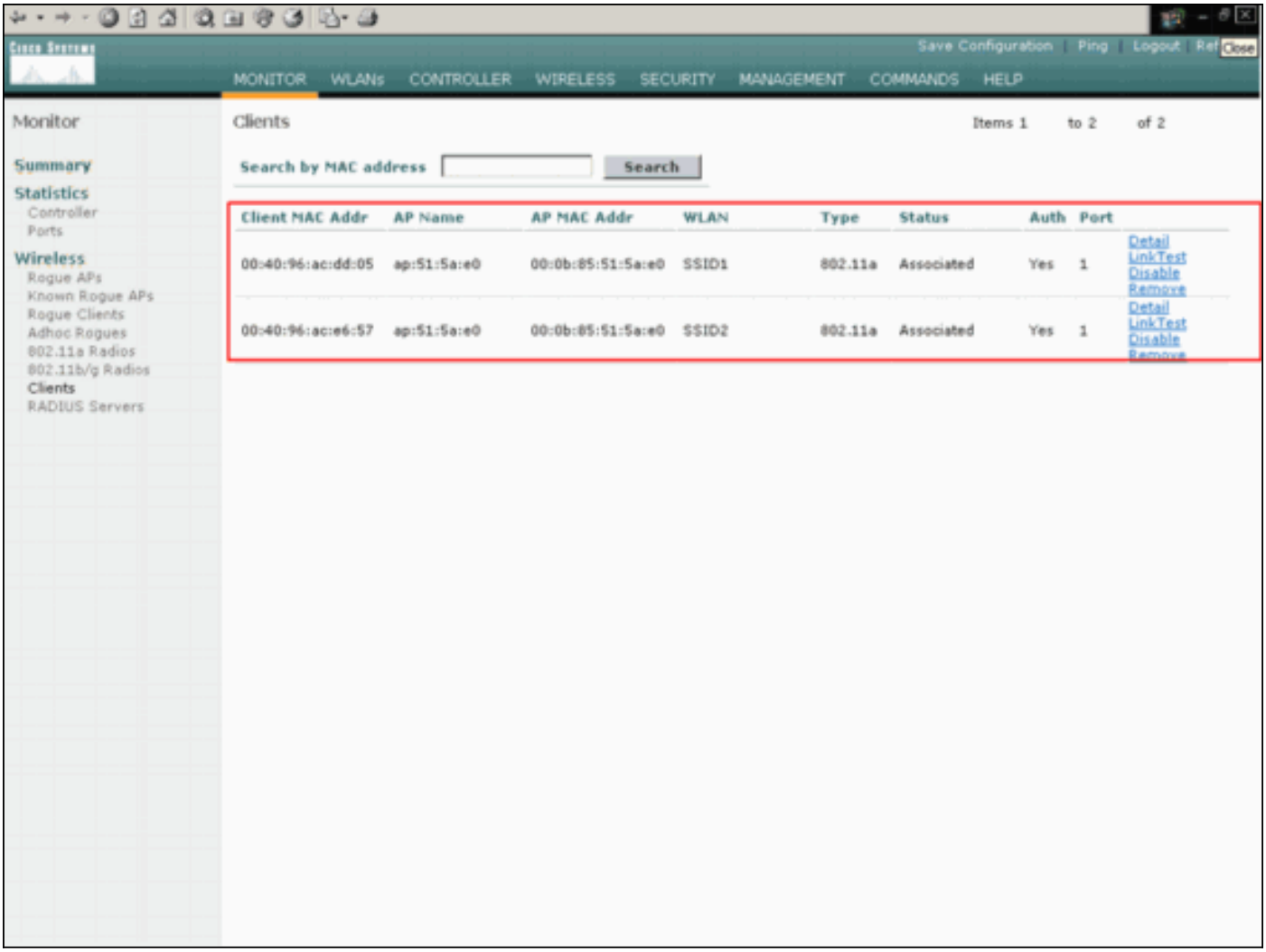
Déployez le REAP AP au site distant

Maintenant que vous avez configuré des WLAN sur le WLCs, les avez amorcé le RECOUVREMENT, et avez établi le lien WAN entre le bureau central et le bureau distant, vous êtes prêt à déployer AP au site distant.

Après que vous mettiez AP sous tension au site distant, AP recherche le contrôleur dans la commande que vous avez configurée dans l'étape d'amorçage. Après qu'AP trouve le contrôleur, AP s'inscrit au contrôleur. Voici un exemple. Du WLC, vous pouvez voir qu'AP a joint le contrôleur sur le port 1 :



Clients qui ont le SSID **SSID1**, et pour quel WPA-PSK est activé, associé à AP sur les clients WLAN 1. qui ont le SSID **SSID2**, et qui font activer l'authentification de 802.1x, associé à AP sur WLAN 2. Voici un exemple qui affiche deux clients. Un client est connecté à WLAN 1, et l'autre client est connecté à WLAN 2 :



Vérifiez

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

Note: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Réduisez le lien WAN. Quand le lien WAN est en baisse, AP perd la Connectivité avec le WLC. Le WLC radie de l'immatriculation alors AP de sa liste. Voici un exemple :

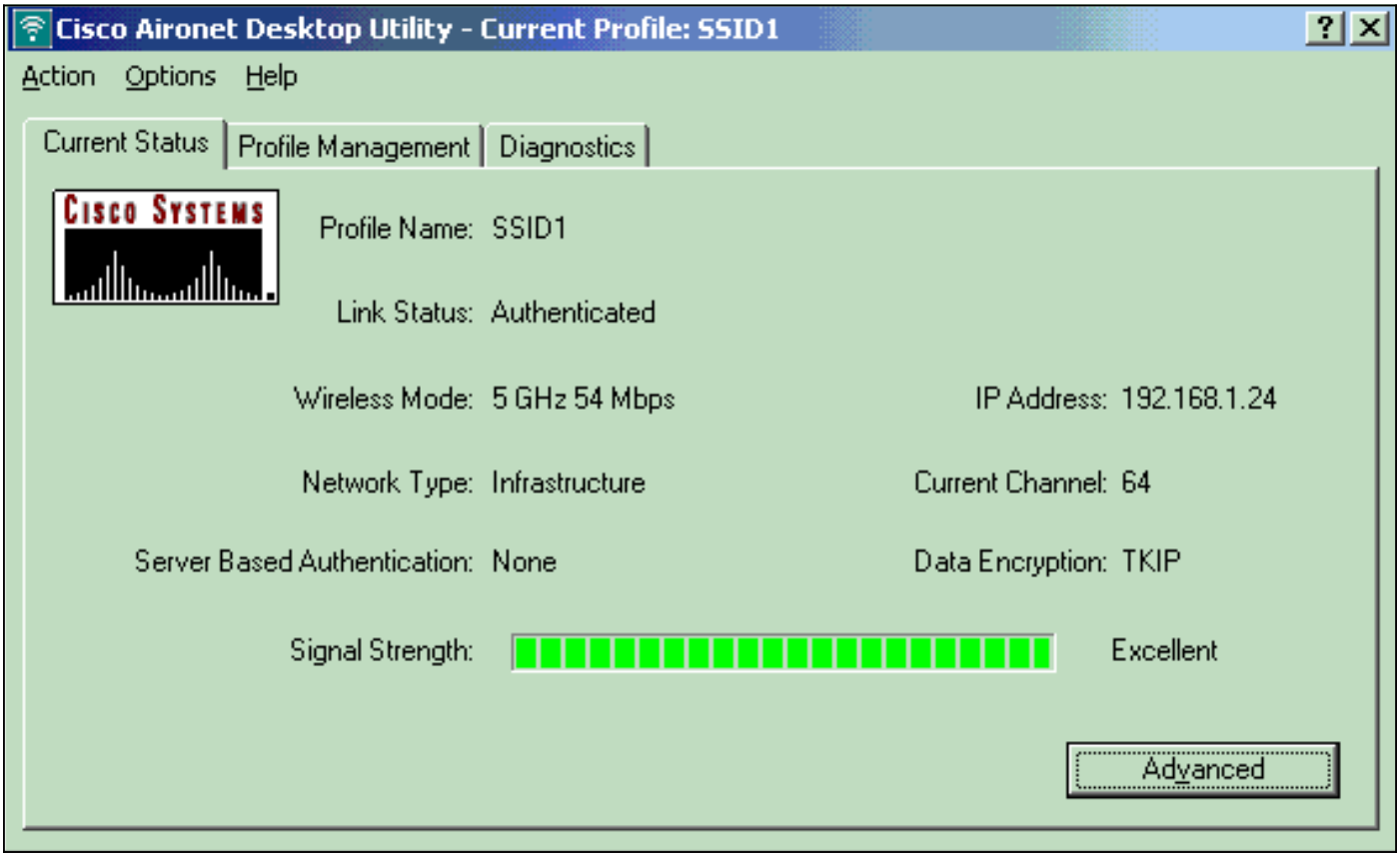
```
(Cisco Controller) >debug lwapp events enable
Wed May 17 15:04:22 2006: Did not receive heartbeat reply from AP 00:0B:85:51:5A:E0
Wed May 17 15:04:22 2006: Max retransmissions reached on AP 00:0B:85:51:5A:E0
(CONFIGURE_COMMAND, 1)
Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: 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
```

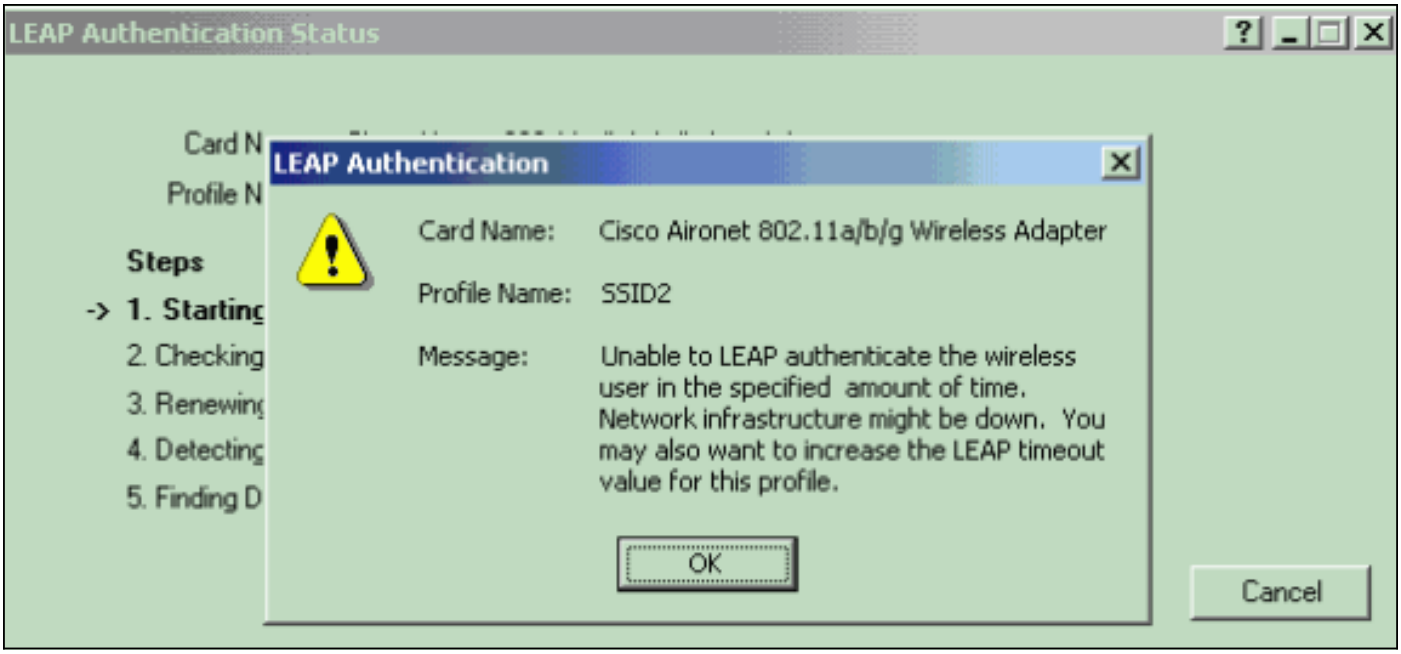
De la sortie de **commande debug lwapp events enable**, vous pouvez voir que le WLC radie de l'immatriculation AP parce que le WLC n'a pas reçu de réponse de pulsation d'AP. Une réponse de pulsation est semblable aux messages de keepalive. Le contrôleur essaye cinq pulsations consécutives, le 1 seconde distant. Si le WLC ne reçoit pas de réponse, le WLC radie de l'immatriculation AP.

Quand AP est en mode autonome, les clignotants LED d'alimentation AP. Les clients qui s'associent au premier WLAN (WLAN 1) sont encore associés à AP parce que les clients dans le premier WLAN sont configurés pour le cryptage de WPA-PSK seulement. Le RECOUVREMENT manipule le cryptage lui-même en mode autonome. Voici un exemple qui affiche l'état (quand le lien WAN est en baisse) d'un client qui est connecté à WLAN 1 à SSID1 et à WPA-PSK :

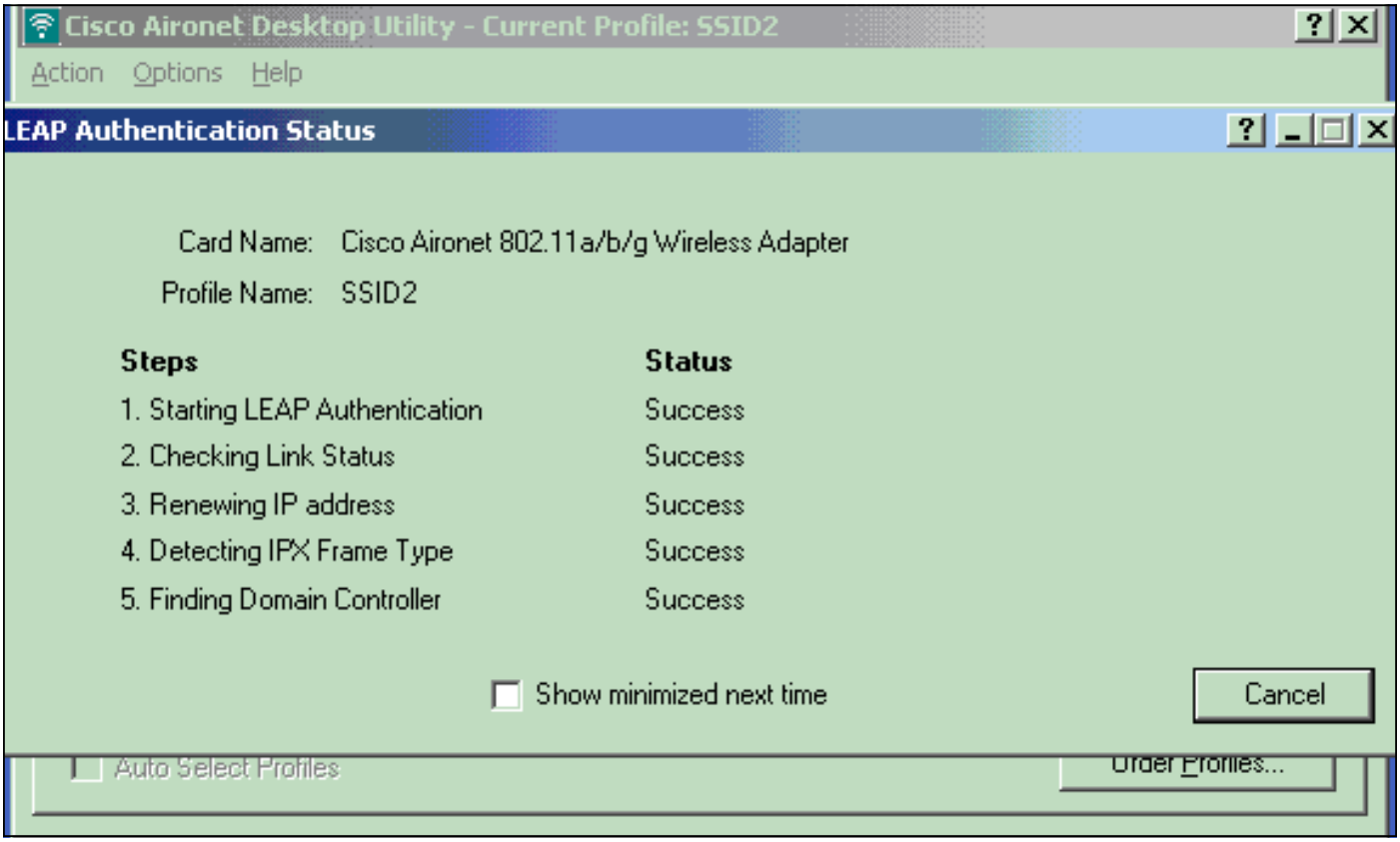
Note: Le TKIP est le cryptage qui est utilisé avec le WPA-PSK.



Les clients qui sont connectés à WLAN 2 sont déconnectés parce que WLAN 2 utilise l'authentification EAP. Cette déconnexion se produit parce que les clients qui utilisent le besoin d'authentification EAP de communiquer au WLC. Voici une fenêtre d'exemple qui prouve que l'authentification EAP échoue quand le lien WAN est en baisse :



Après que le lien WAN soit en hausse, AP commute de nouveau au mode REAP normal et s'inscrit au contrôleur. Le client qui utilise l'authentification EAP également monte. Voici un exemple :



Cette sortie témoin de la **commande debug lwapp events enable** sur le contrôleur donne ces résultats :

```
(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
```

Dépannez

Utilisez cette section pour dépanner votre configuration.

Dépannage des commandes

Vous pouvez utiliser ces commandes de **débogage** de dépanner la configuration.

Note: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **enable d'événements de debug lwapp** — Affiche la séquence d'opérations qui se produisent entre le RECOUVREMENT et le WLC.
- **enable d'erreurs de debug lwapp** — Affiche les erreurs qui se produisent dans la transmission LWAPP.
- **enable de paquet de debug lwapp** — Affiche le débogage d'un tracé de paquets LWAPP.
- **adr de debug mac** — Active l'élimination des imperfections de 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