Exemple de configuration des modes d'opération des points d'accès H-REAP

Contenu

Introduction

Ce document présente le concept du point d'accès Hybrid Remote Edge Access Point (H-REAP) et explique ses différents modes de fonctionnement avec un exemple de configuration.

Conditions préalables

Conditions requises

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

- La connaissance des contrôleurs LAN Sans fil (WLCs) et comment configurer les paramètres

de base WLC
- La connaissance du REAP

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 7.0.116.0
- Point d'accès léger (LAP) de Cisco 1131AG
- Routeurs de gamme Cisco 2800 qui exécutent la version 12.4(11)T.
- Adaptateur de client de Cisco Aironet 802.11a/b/g qui exécute la version de microprogramme 4.0
- Version 4.0 de Cisco Aironet Desktop Utility
- Cisco Secure ACS qui exécute la version 4.0

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

H-REAP est une solution Sans fil pour des déploiements de succursale et de bureau de distant. H-REAP permet à des clients de configurer et contrôler les Points d'accès (aps) dans un bureau de branchement ou de distant de l'entreprise par un lien WAN sans déployer un contrôleur dans chaque bureau.

Le H-REAP peut commuter le trafic de données de clients localement et exécuter l'authentification de clients localement lorsque la connexion au contrôleur est perdue. Une fois connecté au contrôleur, le H-REAP peut également effectuer une transmission tunnel du trafic de retour au contrôleur. En mode connecté, l'hybride REAP AP peut également exécuter l'authentification locale.

H-REAP est pris en charge seulement en fonction :

- 1130AG, 1140, 1240, 1250, 1260, AP801, AP 802, 1040, et AP3550 aps
- Cisco 5500, 4400, 2100, 2500, et contrôleurs de gamme 7500 de flexible
- Commutateur de contrôleur intégré par 3750G de Catalyst
- Wireless Services Module de gamme Catalyst 6500 (WiSM)
- Module Sans fil de contrôleur LAN (WLCM) pour les Integrated Services Router (ISR)

Le trafic de client sur des H-REAP mettent en boîte soit commuté localement à AP ou percé un tunnel de nouveau à un contrôleur. Ceci dépend de la configuration par-WLAN. En outre, le trafic localement commuté de client sur le H-REAP peut être 802.1Q étiqueté pour prévoir la séparation de câbler-side. Pendant le cas de panne du WAN, le service sur tous localement commutés, des

WLAN localement authentifiés persiste.

Remarque: Si les aps sont en mode H-REAP et sont localement commutés au site distant, l'affectation dynamique des utilisateurs à une particularité VLAN basée sur la configuration du serveur RADIUS n'est pas prise en charge. Cependant, vous devriez pouvoir affecter des utilisateurs à la particularité VLAN basée sur le VLAN statique à la cartographie d'Identifiant SSID (Service Set Identifier) faite localement à AP. Par conséquent, un utilisateur qui appartient à un SSID particulier peut être assigné à une particularité VLAN à laquelle le SSID est tracé localement à AP.

Remarque: Si la Voix au-dessus du WLAN est importante, alors les aps devraient être exécutés en mode local de sorte qu'ils obtiennent CCKM et support du contrôle d'admission de connexion (CAC), qui ne sont pas pris en charge en mode H-REAP.

H-REAP au-dessus de REAP

Référez-vous au point d'accès Remote-Edge (REAP) avec des aps légers et le pour en savoir plus Sans fil d'exemple de configuration de contrôleurs LAN (WLCs) pour aider à comprendre le REAP.

H-REAP a été introduit en raison de ces défauts de REAP :

- Le REAP n'a pas la séparation de câbler-side. Ce doit manquer du support de 802.1Q. Les données des WLAN débarquent sur le même sous-réseau de câble.
- Pendant une panne BLÊME, un REAP AP cesse le service proposé sur tous les WLAN, à moins que le premier ait spécifié dans le contrôleur.

C'est comment H-REAP surmonte ces deux défauts :

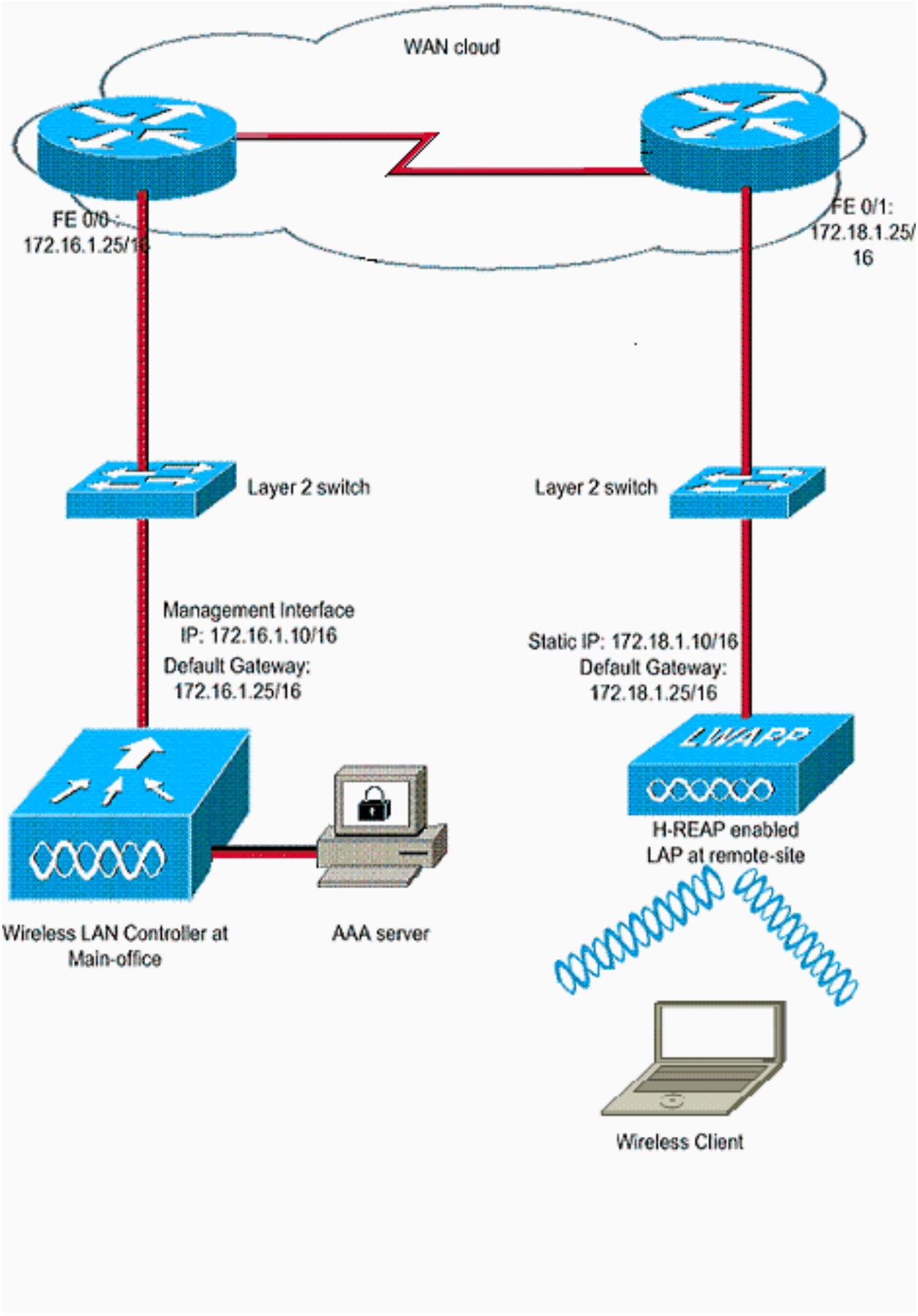
- Fournit le support dot1Q et le VLAN au mappage SSID. Ce VLAN au mappage SSID doit être fait à H-REAP. Tandis que vous exécutez ceci, assurez-vous qu'on permet correctement des VLAN configurés par les ports dans les commutateurs intermédiaires et des Routeurs.
- Fournit le service continu à tous les WLAN configurés pour la commutation locale.

Configurer

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

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configuration

Cet exemple suppose que le contrôleur est déjà configuré avec des configurations de base. Le contrôleur utilise ces configurations :

- Adresse IP d'interface de gestion — 172.16.1.10/16
- Adresse IP d'interface d'AP-gestionnaire — 172.16.1.11/16
- Adresse IP du routeur de passerelle par défaut — 172.16.1.25/16
- Adresse IP virtuelle de passerelle — 1.1.1.1

Remarque: Ce document n'affiche pas des configurations et la configuration BLÊMES des Routeurs et des Commutateurs disponibles entre le H-REAP et le contrôleur. Ceci suppose que vous vous rendez compte de l'encapsulation WAN et des protocoles de routage qui sont utilisés. En outre, ce document suppose que vous comprenez comment les configurer afin de mettre à jour la Connectivité entre le H-REAP et le contrôleur par le lien WAN. Dans cet exemple, l'encapsulation HDLC est utilisée sur le lien WAN.

En amorçant AP avec un contrôleur et configurez H-REAP

Si vous voulez qu'AP découvre un contrôleur d'un réseau distant où les mécanismes de détection CAPWAP ne sont pas disponibles, vous pouvez utiliser l'amorçage. Cette méthode te permet de spécifier le contrôleur auquel AP devrait se connecter.

Afin d'amorcer AP H-REAP-capable, connectez AP au réseau câblé au bureau central. Pendant son amorce, AP H-REAP-capable recherche d'abord une adresse IP pour lui-même. Une fois qu'il saisit une adresse IP par un serveur DHCP, il initialise et recherche un contrôleur pour exécuter la procédure d'enregistrement.

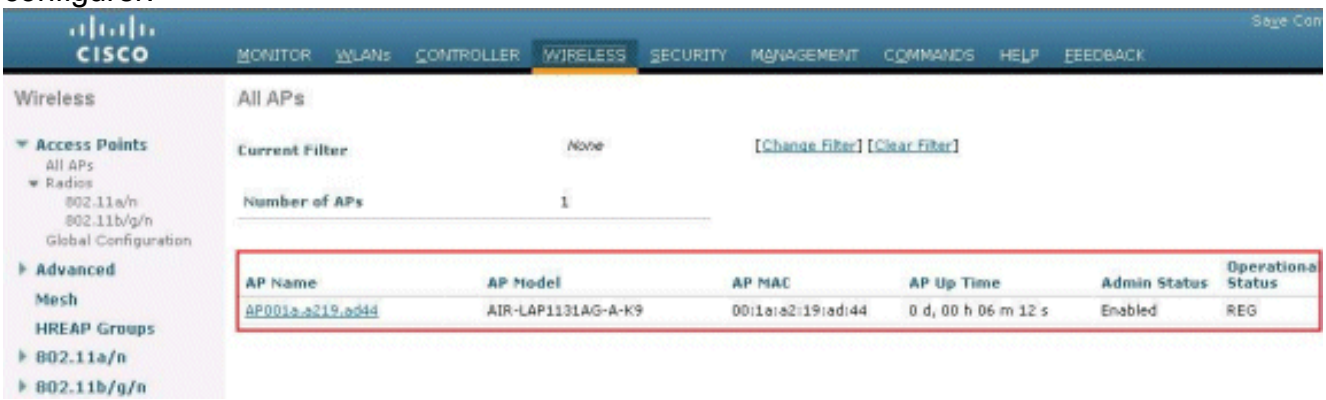
Un H-REAP AP peut apprendre l'adresse IP de contrôleur des manières l'unes des expliquées dans l'enregistrement léger AP (RECOUVREMENT) à un contrôleur LAN Sans fil (WLC).

Remarque: Vous pouvez également configurer le RECOUVREMENT pour découvrir le contrôleur par des commandes CLI à AP. Référez-vous à la détection de contrôleur H-REAP utilisant le pour en savoir plus de commandes CLI.

L'exemple dans ce document emploie la procédure de l'option 43 DHCP pour que le H-REAP apprenne l'adresse IP de contrôleur. Alors il joint le contrôleur, télécharge la dernières image logicielle et configuration du contrôleur, et initialise la liaison radio. Il enregistre la configuration téléchargée dans la mémoire non volatile pour l'usage en mode autonome.

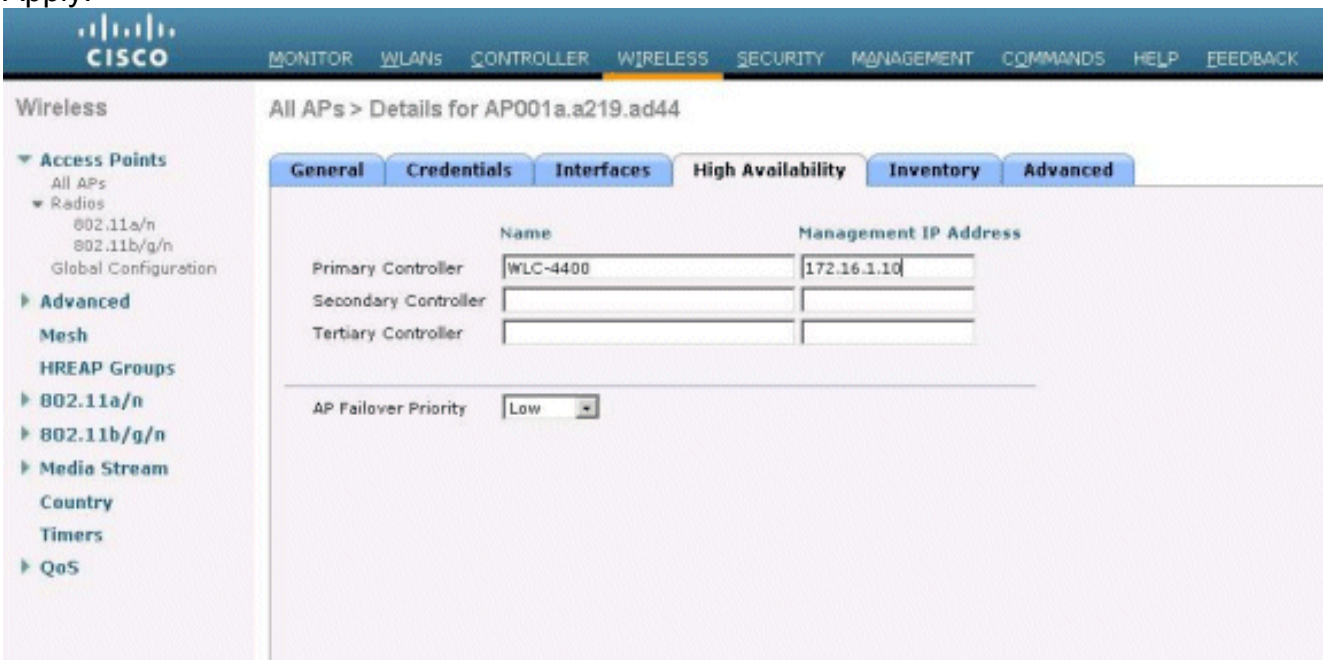
Une fois le RECOUVREMENT est inscrit au contrôleur, se terminent ces étapes :

1. Dans le GUI de contrôleur, choisissez les **points de Wireless>Access**.Ceci affiche le RECOUVREMENT inscrit à ce contrôleur.
2. Cliquez sur en fonction AP que vous voulez configurer.



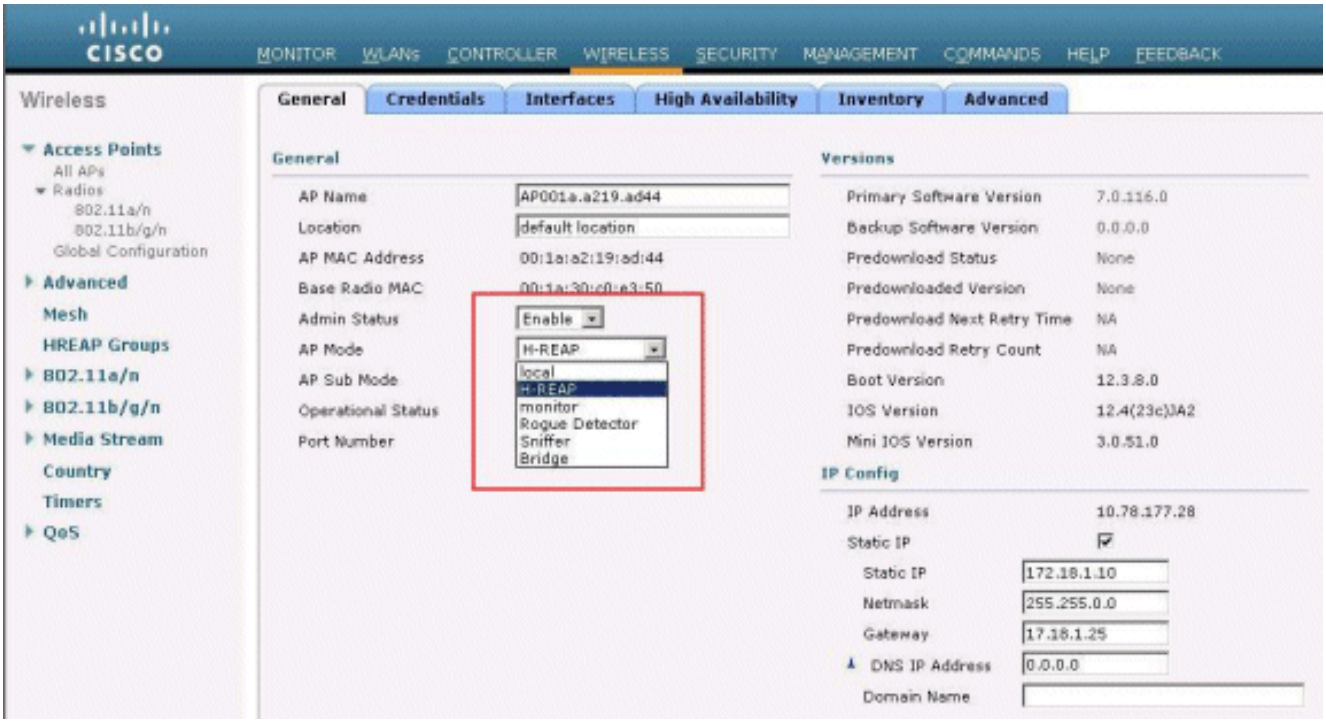
3. Dans la fenêtre d'APs>Details, cliquez sur en fonction l'onglet facilement disponible, et

définissez les noms de contrôleur que les aps les utiliseront pour inscrire, puis cliquent 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.

4. Configurez le RECOUVREMENT pour H-REAP.Afin de configurer le RECOUVREMENT pour fonctionner en mode H-REAP, dans la fenêtre d'APs>Details, sous l'onglet Général, choisissez le **mode AP** comme H-REAP de la correspondance relâchent vers le bas le menu.Ceci configure le RECOUVREMENT pour fonctionner en mode H-REAP.



Remarque: Dans cet exemple, vous pouvez voir que l'adresse IP d'AP est changée au mode statique et l'adresse IP statique 172.18.1.10 a été assignée. Cette affectation se produit parce que c'est le sous-réseau à utiliser au bureau distant. Par conséquent, vous utilisez l'adresse IP du serveur DHCP, mais seulement pendant la première fois par l'étape

d'enregistrement. Après qu'AP soit enregistré au contrôleur, vous changez l'adresse à une adresse IP statique.

Maintenant que votre RECOUVREMENT s'amorce avec le contrôleur et est configuré pour le mode H-REAP, l'étape suivante est de configurer H-REAP sur le côté de contrôleur et de discuter les états de commutation H-REAP.

Théorie H-REAP d'exécutions

Le RECOUVREMENT H-REAP-capable fonctionne dans ces deux modes différents :

- Mode **connecté** :Un H-REAP est dit en mode connecté quand son lien d'avion de contrôle CAPWAP au WLC est en hausse et opérationnel. Ceci signifie que le lien WAN entre le RECOUVREMENT et le WLC n'est pas en baisse.
- Mode **autonome** :Un H-REAP est dit en mode autonome quand son lien WAN au WLC est en baisse. Par exemple, quand ce H-REAP n'a plus la Connectivité au WLC connecté à travers le lien WAN.

Le mécanisme d'authentification utilisé pour authentifier un client peut être défini comme **central** ou **gens du pays**.

- **Authentification centrale** — Se rapporte au type d'authentification qui comporte le processus du WLC du site distant.
- **Authentification locale** — Se rapporte aux types d'authentification qui n'impliquent pas de traiter du WLC pour l'authentification.

Remarque: Tous les authentification de 802.11 et traitement d'association se produit au H-REAP, aucune matière dans laquelle le mode le RECOUVREMENT est. Tandis qu'en mode connecté, proxys H-REAP puis ces associations et authentifications au WLC. En mode autonome, le RECOUVREMENT ne peut pas informer le WLC de tels événements.

Quand un client se connecte à un H-REAP AP, AP en avant tous les messages d'authentification au contrôleur. Après l'authentification réussie, ses paquets de données alors sont commutés localement ou percés un tunnel de nouveau au contrôleur. C'est dans l'accord à la configuration du WLAN auquel elle est connectée.

Avec H-REAP, les WLAN configurés sur un contrôleur peuvent être actionnés dans deux modes différents :

- **Commutation centrale :**On dit qu'Un WLAN sur H-REAP fonctionne en mode central de commutation si le trafic de données de ce WLAN est configuré pour être percé un tunnel au WLC.
- **Commutation locale :**On dit qu'Un WLAN sur H-REAP fonctionne en mode de commutation locale si le trafic de données de ce WLAN se termine localement à l'interface de câble du RECOUVREMENT elle-même, sans obtenir percé un tunnel au WLC.**Remarque:** Seulement WLAN 1 à 8 peuvent être configurés pour la commutation locale H-REAP parce que seulement ces WLAN peuvent être appliqués aux 1130, les gammes 1240 et 1250 aps qui prennent en charge la fonctionnalité H-REAP.

États de commutation H-REAP

Combiné avec les modes d'authentification et de commutation mentionnés dans la section

précédente, un H-REAP peut fonctionner dans l'un de ces états :

- Authentification centrale, commutation centrale
- Authentification vers le bas, commutant vers le bas
- Authentification centrale, commutation locale
- Authentification vers le bas, commutation locale
- Authentification locale, commutation locale

Authentification centrale, commutation centrale

Dans cet état, pour le WLAN donné, AP en avant toutes les demandes d'authentification client au contrôleur et perce un tunnel toutes les données de client au WLC. Cet état est valide seulement quand le H-REAP est en mode connecté. N'importe quel WLAN qui est configuré pour fonctionner en ce mode est perdu pendant le cas de panne du WAN, n'importe ce que la méthode d'authentification est.

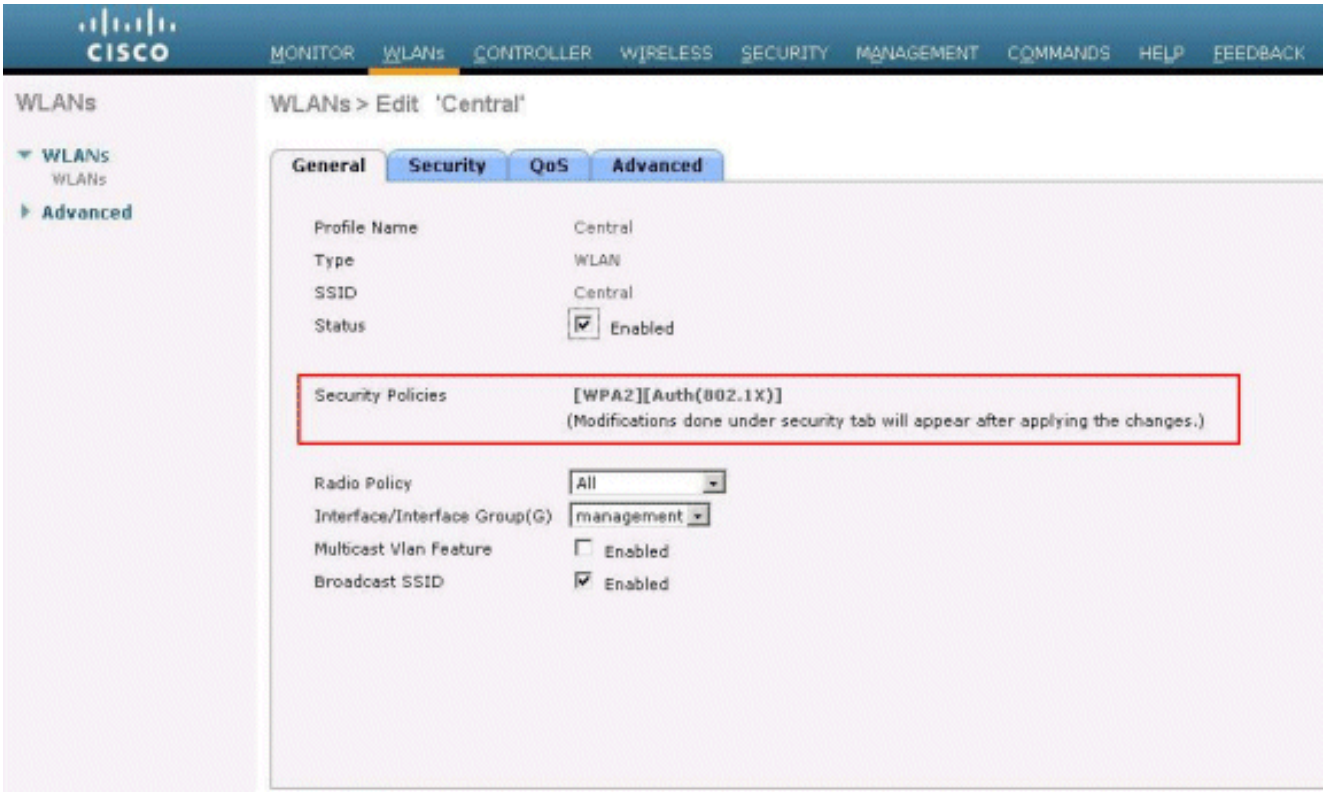
Cet exemple utilise ces paramètres de configuration :

- Nom WLAN/SSID : **Central**
- Degré de sécurité de la couche 2 : **WPA2**
- Commutation locale H-REAP : **désactivé**

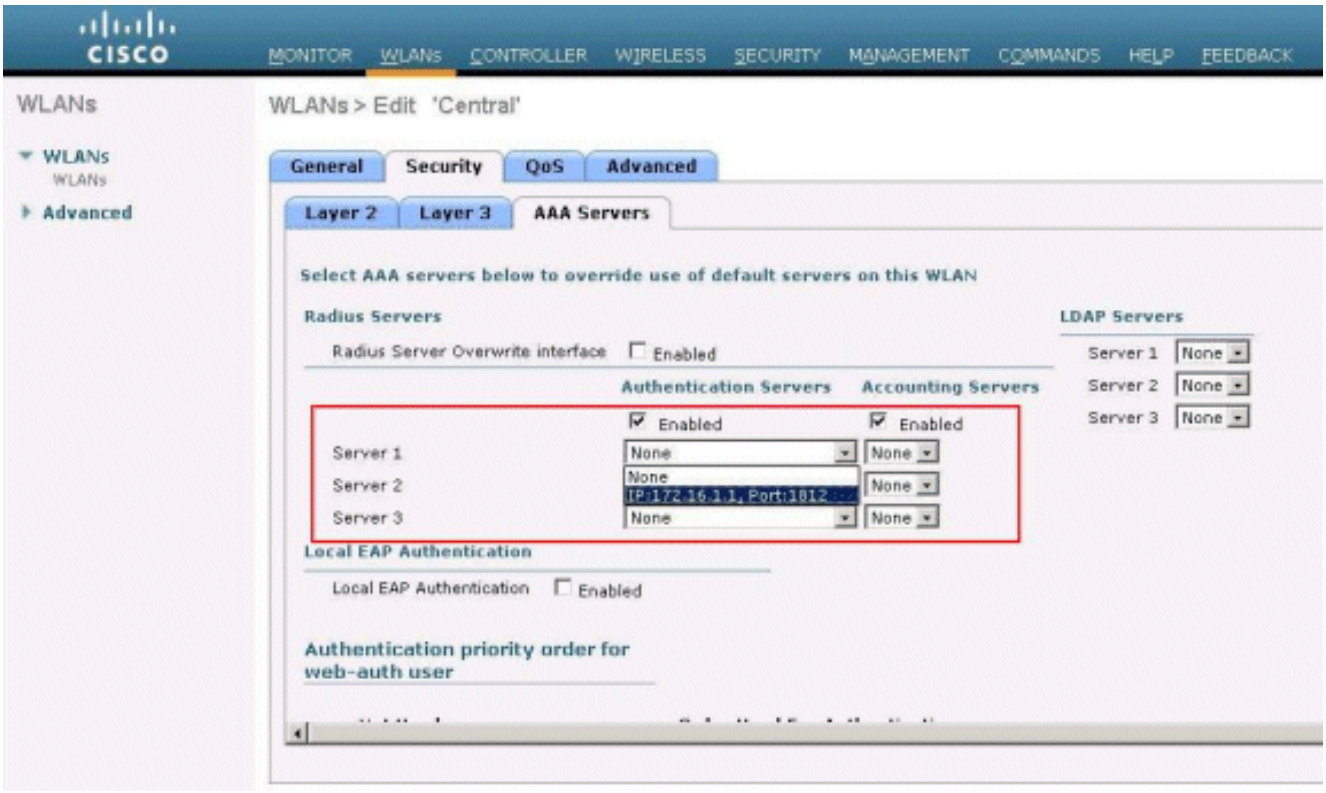
Terminez-vous ces étapes afin de configurer le WLC pour l'authentification centrale, commutation centrale utilisant le GUI :

1. Cliquez sur les **WLAN** afin de créer nouveau **Central** nommé par WLAN, puis cliquez sur Apply.

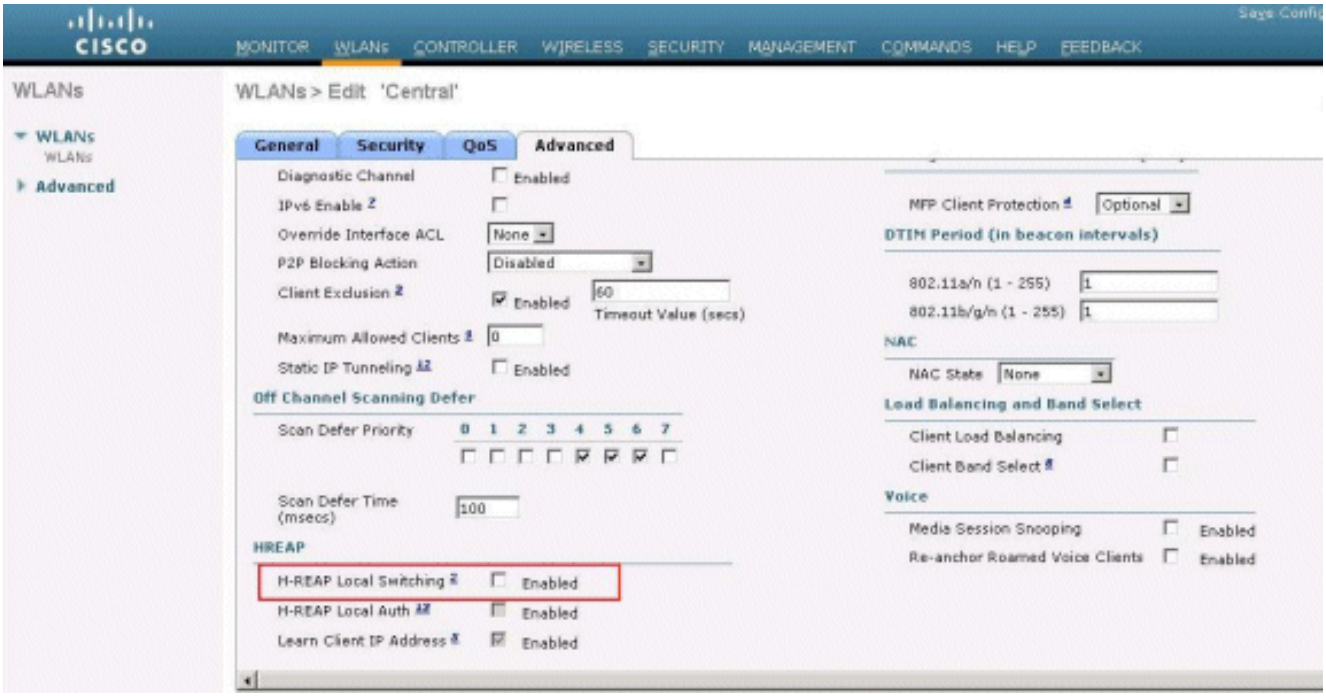
2. Puisque ce WLAN utilise l'authentification centrale, nous utilisons l'authentification WPA2 dans le domaine de degré de sécurité de la couche 2. Le WPA2 est le degré de sécurité par défaut de la couche 2 pour un
WLAN.



3. Choisissez l'onglet AAA Servers, et puis choisissez le serveur compétent configuré pour l'authentification.



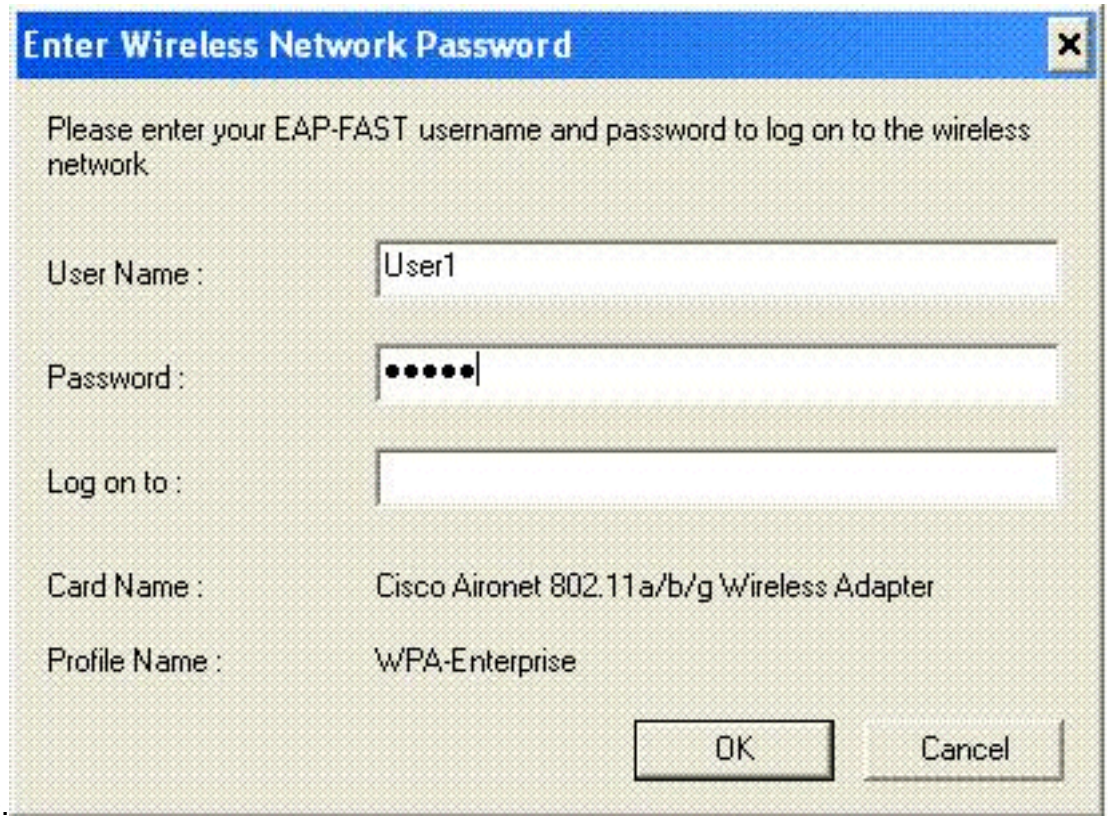
4. Puisque ce WLAN utilise la commutation centrale, vous devez s'assurer que la case de commutation locale H-REAP est désactivée (c.-à-d. la case de commutation locale n'est pas sélectionnée). Cliquez ensuite sur
Apply.



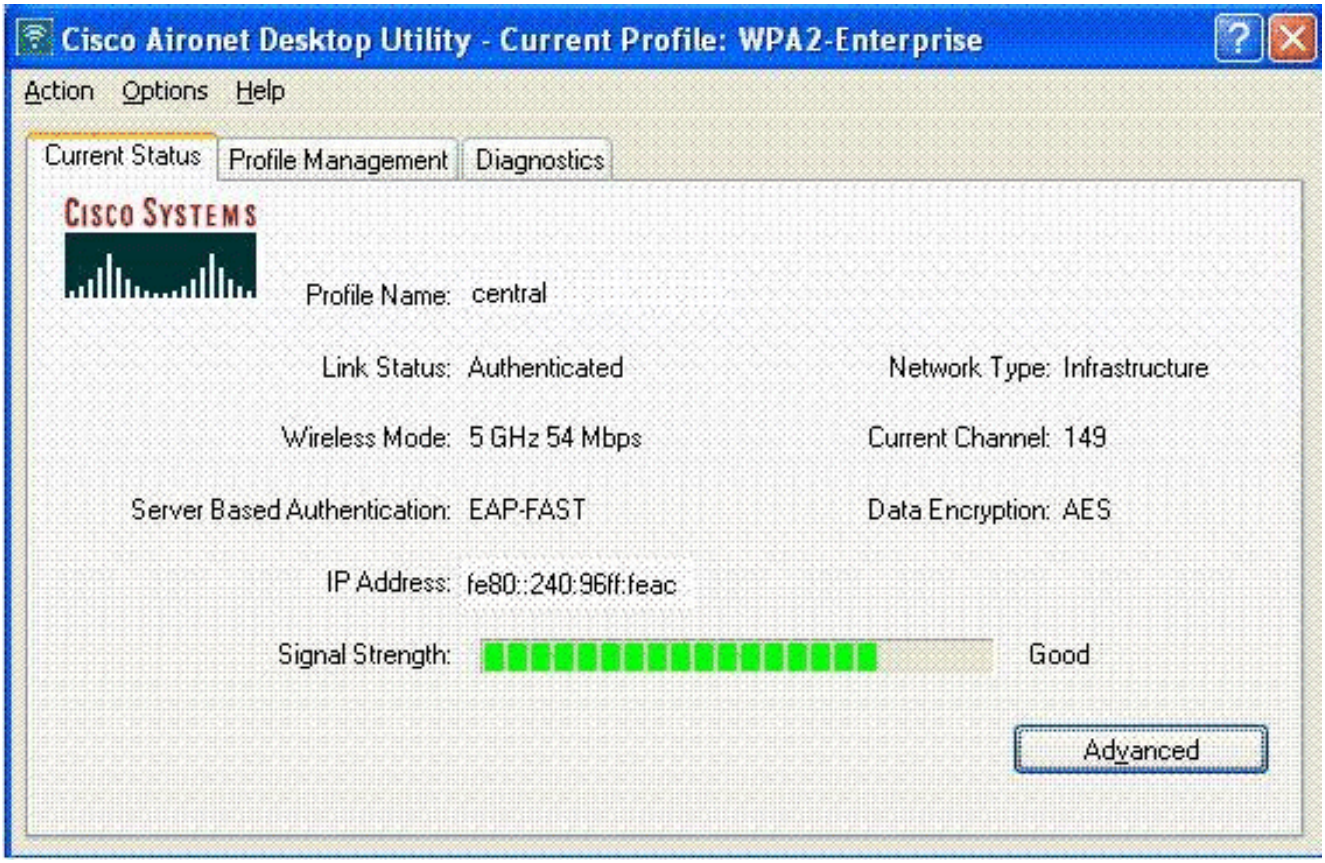
Vérifiez l'authentification centrale, commutation centrale

Procédez comme suit :

1. Configurez le client sans fil avec le mêmes SSID et configurations de sécurité.Dans cet exemple, le SSID est *central* et la méthode de Sécurité est *WPA2*.
2. Écrivez le nom d'utilisateur et mot de passe comme configuré dans le server>User de RADIUS installé afin de lancer le SSID central dans le client.Cet exemple utilise *User1* comme nom d'utilisateur et mot de



passe.Le client est centralement authentifié par le serveur de RADIUS et est associé avec le H-REAP AP. Le H-REAP est maintenant dans l'**authentification centrale, commutation centrale**.



Authentification vers le bas, commutant vers le bas

La même configuration étant expliqué dans l'authentification centrale, la section de commutation centrale, désactivent le lien WAN qui connecte le contrôleur. Maintenant, les attentes de contrôleur une pulsation répondent d'AP. Une réponse de pulsation est semblable aux messages de keepalive. Le contrôleur essaye cinq pulsations consécutives, chaque chacun en second lieu.

Puisqu'il n'est pas reçu avec une réponse de pulsation du H-REAP, le WLC radie de l'immatriculation le RECOUVREMENT.

Émettez la commande d'**enable d'événements de capwap de débogage du** CLI du WLC afin de vérifier le processus de radiation. C'est l'exemple de sortie de cette commande de **débogage** :

```
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Did not receive heartbeat reply from
AP 00:15:c7:ab:55:90
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Down capwap event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Deregister capwap event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Down capwap event for AP 00:15:c7:ab:55:90 slot 1
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Deregister capwap event for AP 00:15:c7:ab:55:90 slot 1
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00:
15:c7:ab:55:90 slot 0!
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15:
c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00:
15:c7:ab:55:90 slot 1!
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15:
c7:ab:55:90 slot 1
```

Le H-REAP entre dans le mode autonome.

Puisque ce WLAN précédemment a été centralement authentifié et centralement commuté, contrôlez et le trafic de données ont été percés un tunnel de nouveau au contrôleur. Par conséquent, sans contrôleur, le client ne peut pas mettre à jour l'association avec le H-REAP et il est déconnecté. Cet état de H-REAP avec l'association et l'authentification de client étant en baisse désigné sous le nom de l'authentification vers le bas, commutant vers le bas.

Authentification centrale, commutation locale

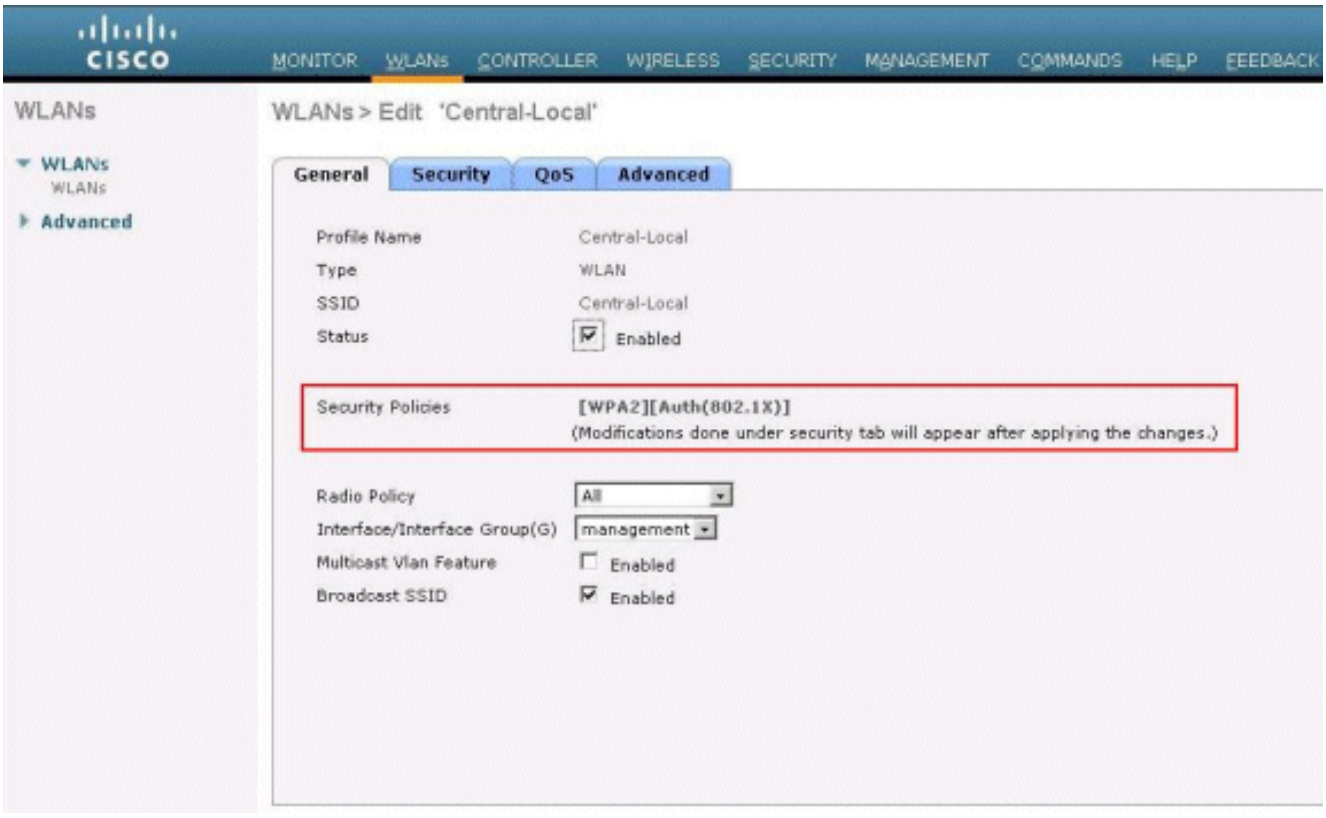
Dans cet état, pour le WLAN donné, le WLC manipule toute l'authentification client, et les paquets de données de Commutateurs de RECOUVREMENT H-REAP localement. Après que le client authentifie avec succès, le contrôleur envoie des commandes de contrôle de capwap au H-REAP et demande au RECOUVREMENT pour commuter que les paquets de données du client donné localement. Ce message est envoyé par client sur l'authentification réussie. Cet état s'applique seulement en mode connecté.

Cet exemple utilise ces paramètres de configuration :

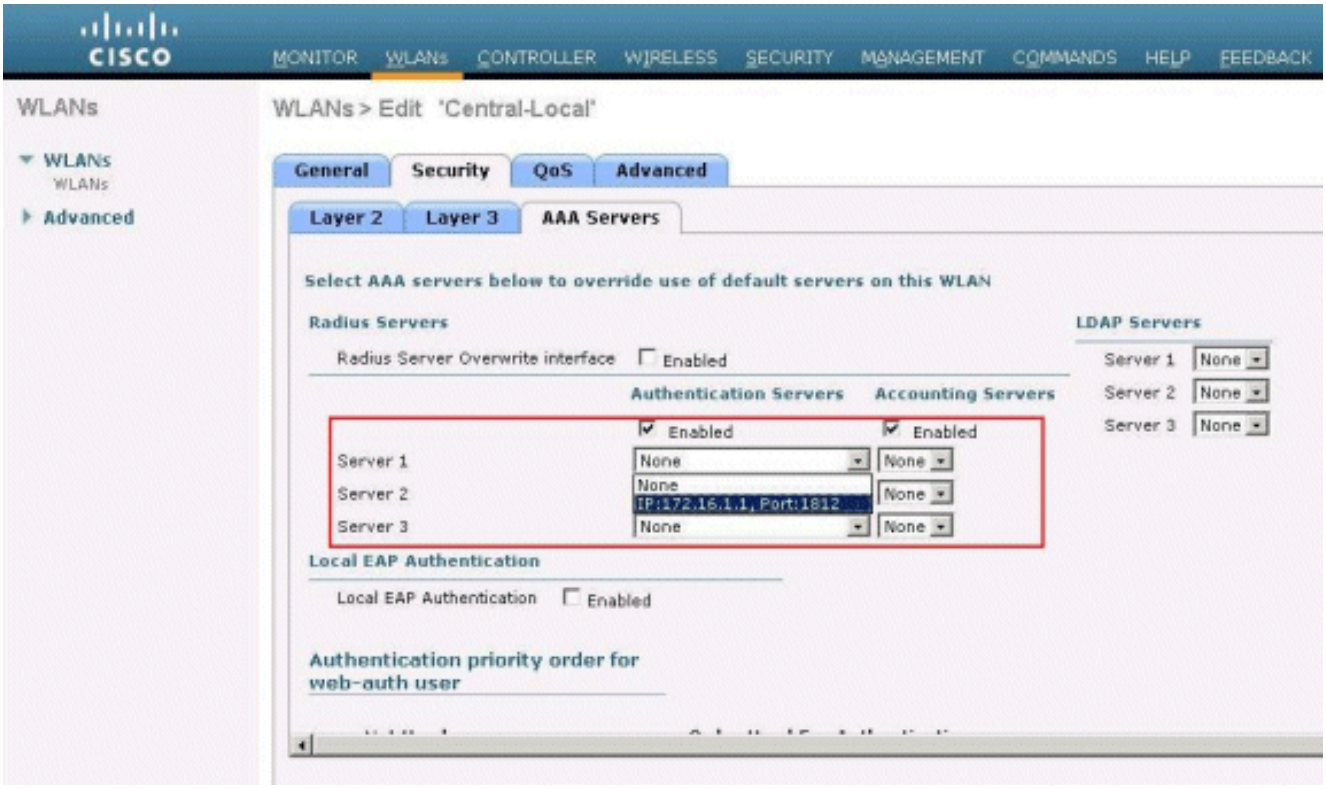
- Nom WLAN/SSID : **Central-gens du pays**
- Degré de sécurité de la couche 2 : **WPA2**.
- Commutation locale H-REAP : **Activée**

Du GUI de contrôleur, terminez-vous ces étapes :

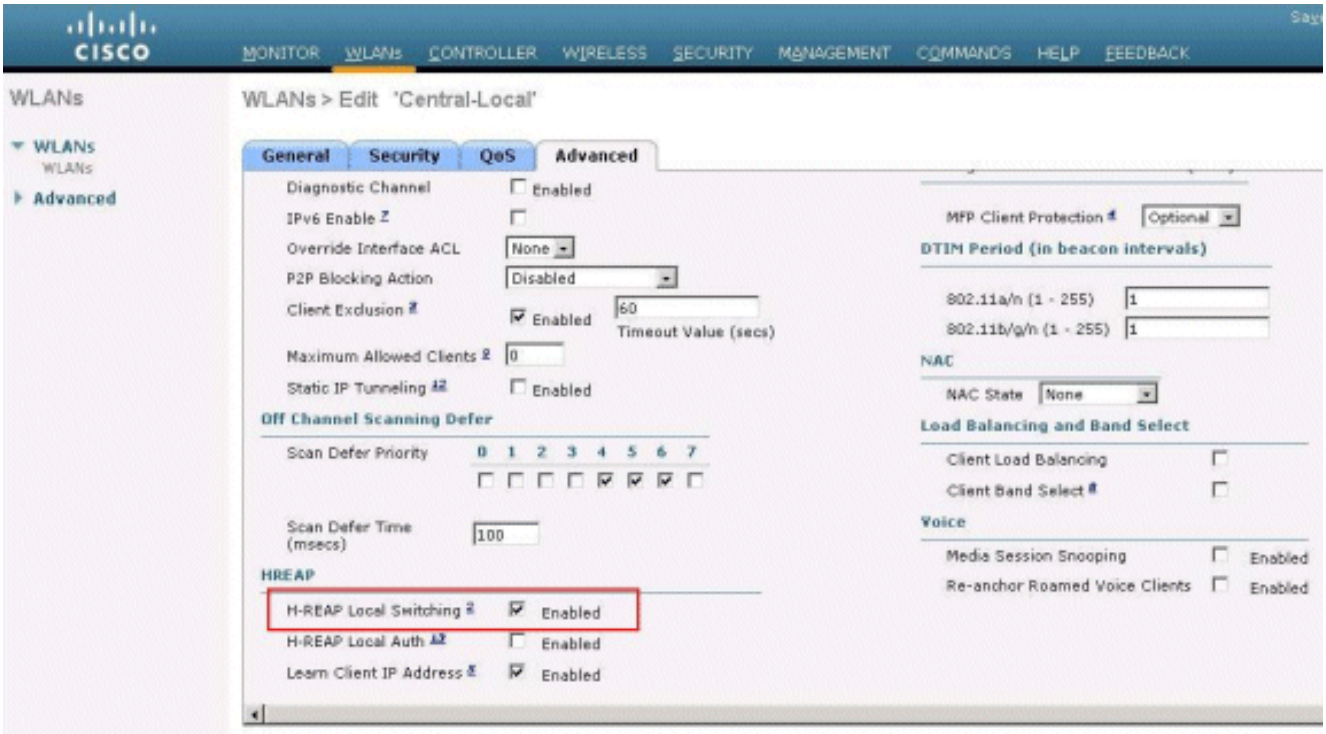
1. Cliquez sur les **WLAN** afin de créer nouveaux Central-Gens du pays nommés par WLAN, puis cliquez sur Apply.
2. Puisque ce WLAN utilise l'authentification centrale, choisissez l'authentification **WPA2** dans le domaine de degré de sécurité de la couche
   2.



3. Sous Radius les serveurs sectionnent, choisissent le serveur compétent configuré pour l'authentification.



4. Cochez la case de **commutation locale H-REAP** afin de commuter le trafic de client qui appartient à ce WLAN localement au H-REAP.

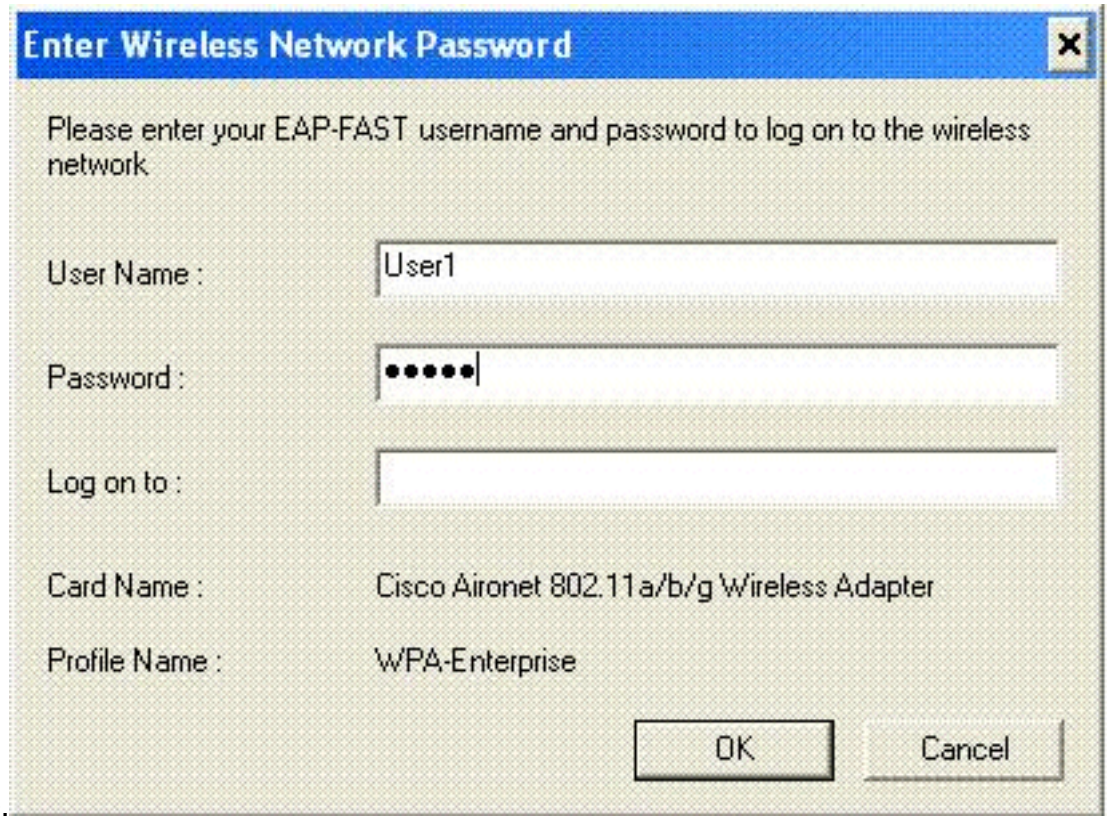


Vérifiez l'authentification centrale, commutation locale

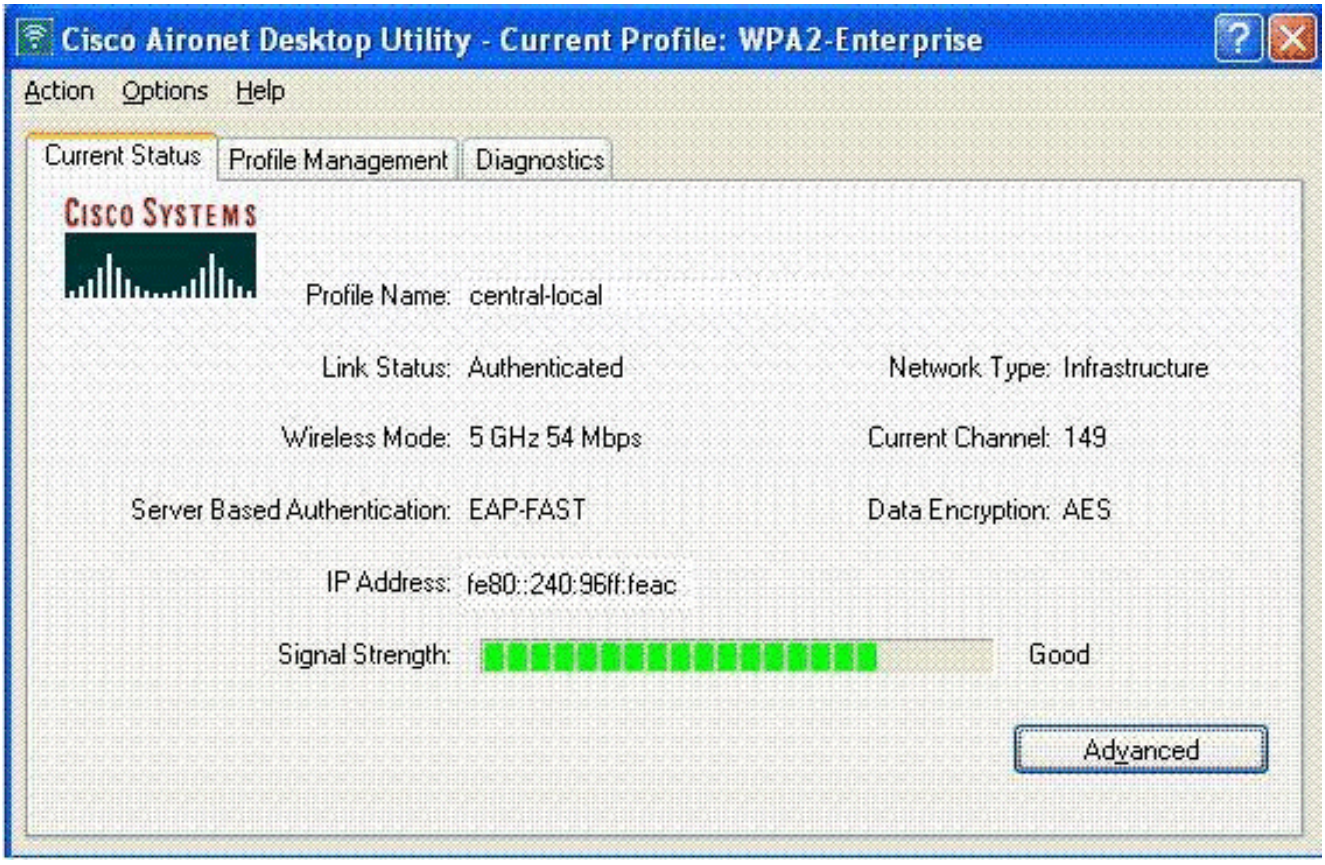
Procédez comme suit :

1. Configurez le client sans fil avec le mêmes SSID et configurations de sécurité.Dans cet exemple, le SSID est des Central-*gens du pays* et la méthode de Sécurité est *WPA2*.

2. Écrivez le nom d'utilisateur et mot de passe comme configuré dans le server>User de RADIUS installé afin de lancer les central-gens du pays SSID dans le client.Cet exemple utilise *User1* comme nom d'utilisateur et mot de passe.



3. Cliquez sur **OK**.Le client est centralement authentifié par le serveur de RADIUS et obtient associé au H-REAP AP. Le H-REAP est maintenant dans l'**authentification centrale, commutation locale**.



Authentification vers le bas, commutation locale

Si un WLAN localement commuté est configuré pour n'importe quel type d'authentification qui est exigé pour être traité sur le WLC (tel qu'authentification EAP [WEP/WPA/WPA2/802.11i], WebAuth, ou NAC dynamique), sur la panne BLÊME, il écrit l'**authentification vers le bas,** état de **commutation locale**. Dans cet état, pour le WLAN donné, le H-REAP rejette tous les nouveaux clients qui essayent d'authentifier. Cependant, il continue à envoyer des balises et des réponses de sonde pour maintenir les clients existants correctement connectés. Cet état est valide seulement en mode autonome.

Afin de vérifier cet état, utilisez la même configuration expliquée dans l'authentification centrale, section de commutation locale.

Si le lien WAN qui connecte le WLC est en baisse, le WLC passe par le processus de radier de l'immatriculation le H-REAP.

Une fois que radié de l'immatriculation, H-REAP entre dans le mode autonome.

Le client associé par ce WLAN met à jour toujours sa Connectivité. Cependant, parce que le contrôleur, l'authentificateur n'est pas disponible, H-REAP ne permet aucune nouvelle connexion de ce WLAN.

Ceci peut être vérifié par le lancement d'un autre client sans fil dans le même WLAN. Vous pouvez constater que l'authentification pour ce client échoue et que le client n'est pas permis pour s'associer.

Remarque: Quand un compte de client WLAN égale zéro, le H-REAP cesse toutes les fonctions associées de 802.11 et ne balise plus pour le SSID donné. Ceci abaisse le WLAN au prochain état H-REAP, **authentification, commutant vers le bas**.

Authentification locale, commutation locale

Dans cet état, le RECOUVREMENT H-REAP manipule des authentifications client et commute des paquets de données de client localement. Cet état est valide seulement en mode autonome et seulement pour les types d'authentification qui peuvent être manipulés localement à AP et ne comportent pas le traitement du contrôleur

Le H-REAP qui était précédemment dans l'**authentification centrale,** état de **commutation locale**, entrées dans cet état, si le type configuré d'authentification peut être manipulé localement à AP. Si l'authentification configurée ne peut pas être manipulée localement, comme l'authentification de 802.1x, alors en mode autonome, le H-REAP descend à l'**authentification,** mode de **commutation locale**.

Ce sont certains des mécanismes d'authentification populaires qui peuvent être manipulés localement à AP en mode autonome :

- Ouvrez-vous
- Partagé
- WPA-PSK
- WPA2-PSK

Remarque: Toutes les procédures d'authentification sont effectuées par le WLC quand AP est en

mode connecté. Tandis que le H-REAP est en mode autonome, ouvert, partagé, et des authentifications WPA/WPA2-PSK sont transférés vers les recouvrements où toute l'authentification client se produit.

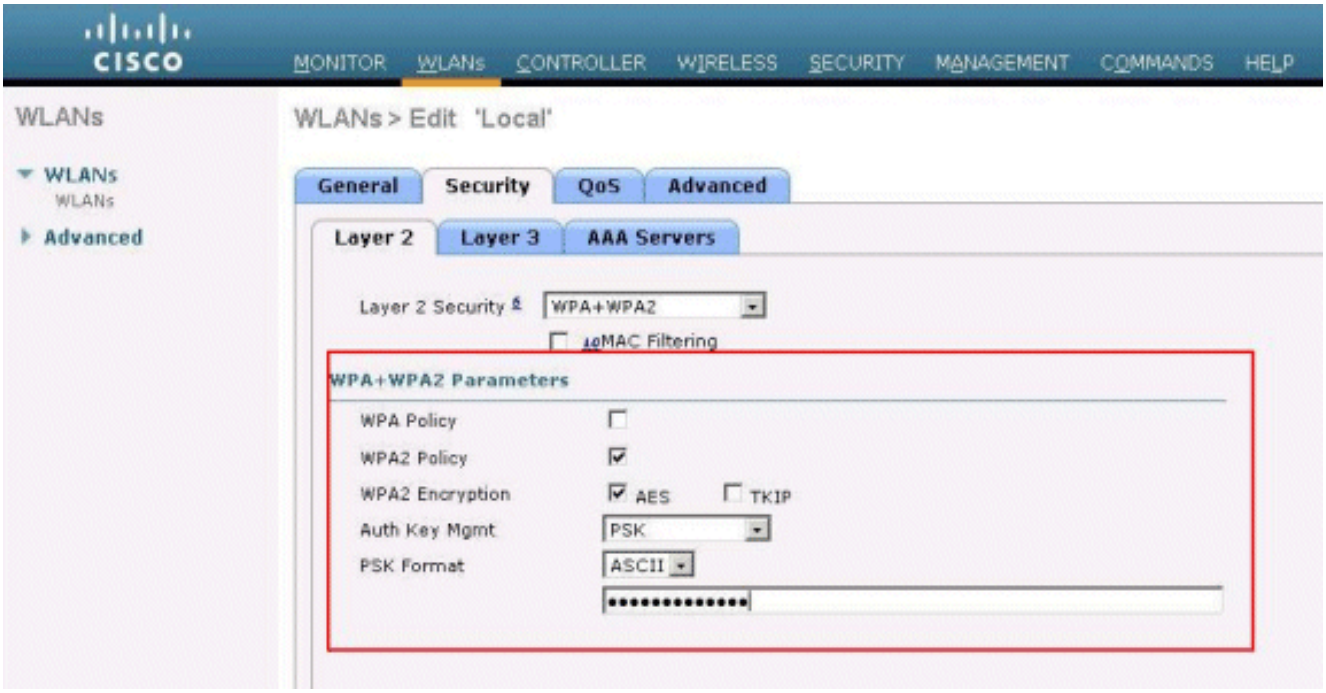
Remarque: L'authentification de Web externe n'est pas prise en charge en utilisant le hybride-REAP avec la commutation locale activée sur le WLAN.

Cet exemple utilise ces paramètres de configuration :

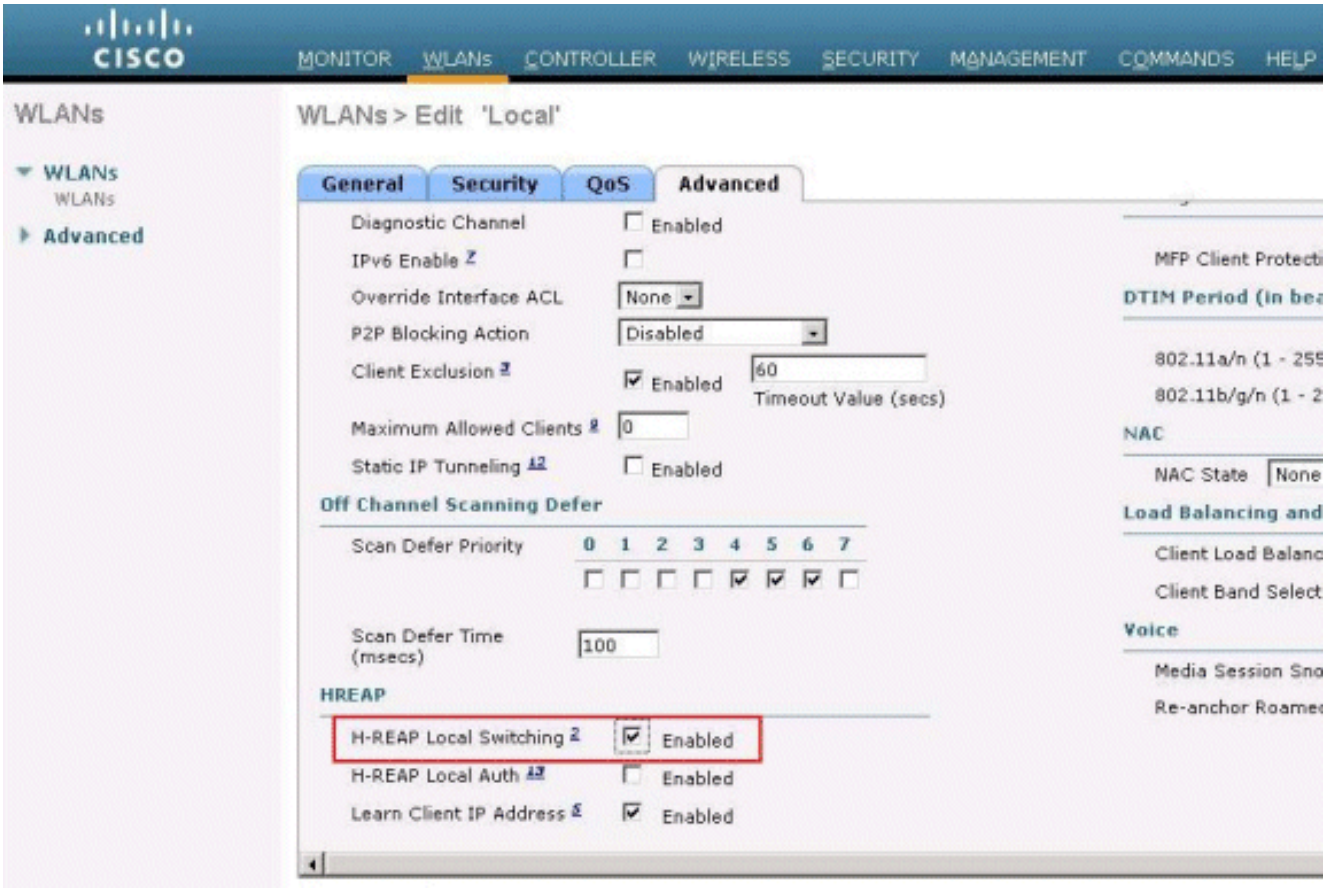
- Nom WLAN/SSID : **Gens du pays**
- Degré de sécurité de la couche 2 : **WPA-PSK**
- Commutation locale H-REAP : **activé**

Du GUI de contrôleur, terminez-vous ces étapes :

1. Cliquez sur les **WLAN** afin de créer nouveaux Local nommés par WLAN, puis cliquez sur Apply.
2. Puisque ce WLAN utilise l'authentification locale, choisissez le **WPA-PSK** ou les mécanismes de sécurité mentionnés l'uns des qui peuvent être manipulés localement dans le domaine de degré de sécurité de la couche 2.Cet exemple utilise le **WPA-PSK**.



3. Une fois que choisi, vous devez configurer la clé/mot de passe pré-partagés à utiliser.Ceci doit être identique au côté client pour que l'authentification soit réussie.
4. Cochez la case de **commutation locale H-REAP** afin de commuter le trafic de client qui appartient à ce WLAN localement au H-REAP.



Vérifiez l'authentification locale, commutation locale

Procédez comme suit :

1. Configurez le client avec le mêmes SSID et configurations de sécurité.Ici, le SSID est *local* et la méthode de Sécurité est *WPA-PSK*.
2. Lancez les gens du pays SSID dans le client.Le client obtient authentifié centralement au contrôleur et s'associe avec le H-REAP. Le trafic de client est configuré pour commuter localement. Maintenant, le H-REAP est dans l'authentification centrale, état de commutation locale.
3. Désactivez le lien WAN qui se connecte au contrôleur.Le contrôleur comme d'habitude passe par le processus de radiation. H-REAP est radié de l'immatriculation du contrôleur.Une fois que radié de l'immatriculation, H-REAP entre dans le mode autonome.Cependant, le client qui appartient toujours à ce WLAN met à jour l'association avec H-REAP.En outre, parce que le type d'authentification ici peut être manipulé localement à AP sans contrôleur, H-REAP permet des associations de n'importe quel nouveau client sans fil par ce WLAN.
4. Afin de vérifier ceci, lancez n'importe quel autre client sans fil sur le même WLAN.Vous pouvez voir que le client est authentifié et associé avec succès.

Dépanner

- Afin de dépanner plus loin des problèmes de connectivité de client au port de console du H-REAP, sélectionnez cette commande :
  `AP_CLI#show capwap reap association`

- Afin de dépanner plus loin des problèmes de connectivité de client au contrôleur et limiter la sortie davantage de d'élimination des imperfections, employez cette commande :
  `AP_CLI#debug mac addr <client's MAC address>`

- Afin de mettre au point les problèmes de connectivité du 802.11 d'un client, utilisez cette commande :
  `AP_CLI#debug dot11 state enable`

- Débuggez la procédure d'authentification et les pannes du 802.1X d'un client avec cette commande :
  `AP_CLI#debug dot1x events enable`

- Des messages principaux controller/RADIUS peuvent être mis au point utilisant cette commande :
  `AP_CLI#debug aaa events enable`

- Alternativement, pour activer un correspondant complet des commandes de **débogage de** client, utilisez cette commande :
  `AP_CLI#debug client <client's MAC address>`

Informations connexes

- Exemple de configuration de base d'un contrôleur LAN sans fil et d'un point d'accès léger
- Exemple de configuration de réseaux VLAN sur des contrôleurs de réseau local sans fil
- Guide de configuration Sans fil de contrôleur LAN de Cisco, version 7.0
- Conception de l'hybride REAP et guide de déploiement
- Dépannage de base d'un point d'accès de périphérie distant hybride (H-REAP)
- Exemple de configuration du basculement du contrôleur de réseau local sans fil pour les points d'accès légers
- Assistance produit sans fil
- Support et documentation techniques - Cisco Systems