Guide de conception et de déploiement d'un point d'accès H-Reap

Contenu

Introduction

Le Point d'accès distant hybride de périphérie (H REAP) est une solution Sans fil pour des déploiements de succursale et de bureau de distant. Il permet à des clients de configurer et contrôler des points d'accès dans une succursale ou bureau distant à partir du siège social de

l'entreprise par un lien de réseau étendu (WAN) sans déployer un contrôleur dans chaque bureau. Les Points d'accès H REAP peuvent commuter le trafic de données de client localement et exécuter l'authentification client localement quand la connexion au contrôleur est perdue. Une fois connecté au contrôleur, H REAP mettent en boîte également le trafic du tunnel de nouveau au contrôleur.

Conditions préalables

Conditions requises

L'hybride REAP est pris en charge seulement sur les 1040, les 1130, les 1140, les 1240, les 1250, les 3500, les 1260, l'AP801, les Points d'accès AP802 et sur Cisco WiSM, Cisco 5500, 4400, 2100, 2500, et des contrôleurs de gamme 7500 de flexible, le commutateur de contrôleur sans fil LAN intégré du Catalyst 3750G, le module réseau de contrôleur pour des Integrated Services Router.

Composants utilisés

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

- Version 7.0 de contrôleurs de Cisco Unified
- Le contrôle et l'approvisionnement des Points d'accès (CAPWAP) 1040 basés sur des protocoles, 1130, 1140, 1240,1250, 1260, AP801, des gammes AP802 et 3500 enroule

Conventions

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

Fond d'exécutions CAPWAP

Le CAPWAP, sur lequel l'architecture de réseau sans fil unifié de Cisco est basée, spécifie deux modes primaires différents d'exécution de point d'accès sans fil :

- **Split MAC** — En mode de split MAC, le système partage les fonctions principales de la spécification de 802.11 entre le Point d'accès et le contrôleur. Dans une telle configuration, le contrôleur est non seulement responsable d'une grande partie du traitement des choses telles que des authentifications de 802.11 et des associations, il agit également en tant que seul point d'entrée et de sortie pour tout le trafic d'utilisateur. Tunnel de Points d'accès de split MAC que tout le trafic de client au contrôleur par l'intermédiaire des données CAPWAP percent un tunnel (le contrôle CAPWAP suit également le même chemin.).
- **MAC local** — Le MAC local, en mettant en application la pleine fonctionnalité de 802.11 au Point d'accès, tient compte du découplage du plan de données du chemin de contrôle en terminant tout le trafic de client au port de câble du Point d'accès. Ceci tient compte non seulement de l'accès Sans fil direct aux ressources locales au Point d'accès, mais il fournit la résilience de lien en permettant au chemin de contrôle CAPWAP (le lien entre AP et le contrôleur) d'être vers le bas tandis que le service sans fil persiste. Cette fonctionnalité est

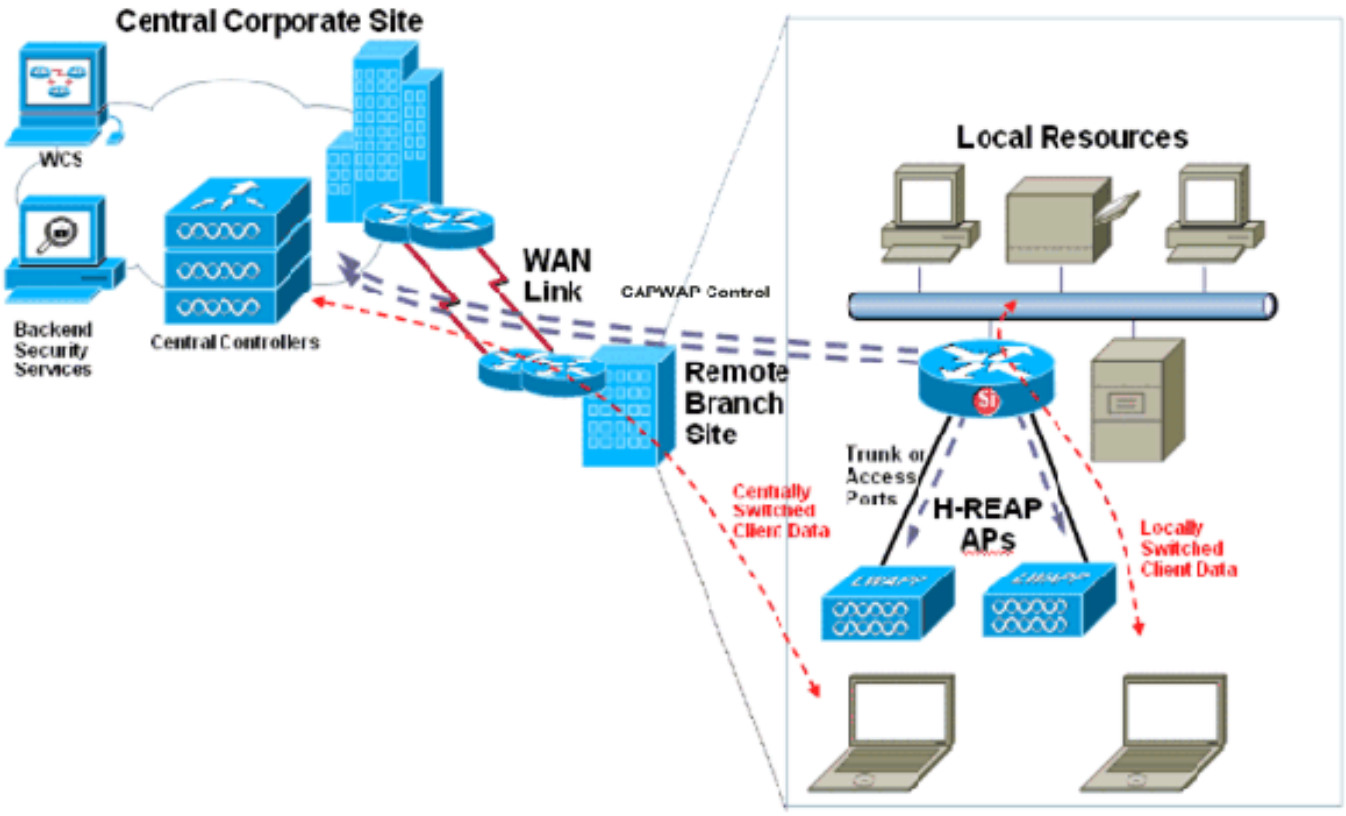
particulièrement utile dans le petits distant et succursales à travers des liens WAN où seulement une poignée de Points d'accès sont nécessaire et le coût d'un contrôleur local n'est pas justifié.

Note: Avant version 5.2 de contrôleur, l'architecture Sans fil unifiée de Cisco a été basée sur le protocole LWAPP.

Le Point d'accès hybride de Distant-périphérie

Le Point d'accès à distance hybride de périphérie, ou H REAP, est une caractéristique prise en charge par 1040, 1130, 1140, 1240, 1250, 3500, 1260, AP801, les Points d'accès AP802 et sur Cisco WiSM, Cisco 5500, 4400, 2100, 2500, et des contrôleurs de gamme 7500 de flexible, le commutateur de contrôleur sans fil LAN intégré du Catalyst 3750G, le module réseau de contrôleur pour des Integrated Services Router. La caractéristique H REAP est prise en charge seulement dans la version 4.0 de contrôleur de réseau sans fil unifié Cisco ou plus tard, la caractéristique sélectionnable de ce logiciel tient compte du fusionnement des exécutions de fractionnement et de gens du pays de MAC CAPWAP pour la flexibilité de déploiement maximum. Le trafic de client sur H REAP mettent en boîte soit commuté localement au Point d'accès ou percé un tunnel de nouveau à un contrôleur, qui dépend de chaque configuration WLAN. De plus, le trafic localement commuté de client sur le H REAP peut être 802.1Q étiqueté afin de prévoir la séparation de côté de câble. Pendant un cas de panne du WAN, le service sur tous localement commutés, des WLAN localement authentifiés persiste.

C'est un diagramme d'une implémentation commune H REAP :



Pendant que ce diagramme indique, H REAP a été conçu et est destiné spécifiquement pour des déploiements de distant et de succursale.

Ce document trace les grandes lignes de la théorie H REAP d'exécutions, configuration de

contrôleur et de Point d'accès, et considérations de conception de réseaux.

Théorie H REAP d'exécutions

Concepts clé H REAP

Il y a quelques modes différents par lesquels la fonctionnalité H REAP fonctionne afin de prévoir la commutation locale et centrale, aussi bien que de capacité de survie de lien WAN. La combinaison de ces deux ensembles de modes, tout en fournissant un choix de fonctionnalité, porte également des limites différentes selon l'appareillement.

Ce sont les deux ensembles de modes :

- **Central contre la commutation locale**WLAN (suites de Sécurité, de QoS, et d'autres paramètres de configuration attachées au SSID) sur H des REAP peuvent ou être placés pour exiger tout le trafic de données soient percés un tunnel de nouveau au contrôleur (appelé la commutation centrale) ou des WLAN peuvent être configurés pour relâcher toutes les données de client localement à l'interface de câble H le REAP (connue sous le nom de commutation locale). Les WLAN localement commutés peuvent sur option porter le 802.1Q étiquetant pour permettre de tels WLAN à segmenter au-dessus du réseau câblé au port Ethernet du Point d'accès.
- **Connecté contre autonome**Un Hybride-REAP est dit en mode connecté quand son avion de contrôle CAPWAP de nouveau au contrôleur est en hausse et opérationnel, signifiant que le lien WAN n'est pas en baisse. Le mode autonome est spécifié comme l'état opérationnel que le H REAP écrit quand il n'a plus la Connectivité de nouveau à son contrôleur.

Note: Toute l'authentification de Sécurité H REAP traitant (comme l'authentification de RAYON et par paires la dérivation principales de clé principale [PMK]) se produit au contrôleur tandis que le Point d'accès est dans l'état connecté. Tous les authentification de 802.11 et traitement d'association se produit au H REAP, aucune matière dans laquelle le mode le Point d'accès est. Quand en mode connecté, proxys H REAP ces associations/authentifications au contrôleur. En mode autonome, le Point d'accès ne peut pas informer le contrôleur de tels événements.

La fonctionnalité H REAP varie selon son mode de fonctionnement (si un H REAP est en mode connecté ou autonome), comment chaque WLAN est configuré pour le commutateur de données (central ou local) et la Sécurité Sans fil.

Quand un client se connecte à un Point d'accès H REAP, le Point d'accès en avant tous les messages d'authentification dans le contrôleur et, sur l'authentification réussie, ses paquets de données alors sont commutés localement ou percés un tunnel de nouveau au contrôleur, selon la configuration du WLAN auquel elle est connectée. En ce qui concerne le mécanisme d'authentification client et l'opération de commutation de données, les WLAN sur H REAP peuvent être dans des n'importe quels des états suivants selon la configuration WLAN et l'état de la Connectivité de Point d'accès/contrôleur :

- **authentification centrale, commutation centrale** — Dans cet état, pour le WLAN indiqué, le Point d'accès en avant toutes les demandes d'authentification client au contrôleur et perce un tunnel toutes les données de client de nouveau au contrôleur, aussi bien. Cet état est valide seulement quand le chemin de contrôle CAPWAP du Point d'accès est. Ceci signifie que le H REAP est en mode connecté. N'importe quel WLAN qui est percé un tunnel de nouveau au

contrôleur est perdu pendant le cas de panne du WAN, aucune matière la méthode d'authentification.

- **authentification centrale, commutation locale** — Dans cet état, pour le WLAN donné, le contrôleur manipule toute l'authentification client, et les paquets de données de Commutateurs de Point d'accès H REAP localement. Après que le client authentifie avec succès, le contrôleur envoie une commande de contrôle CAPWAP au H REAP demandant au Point d'accès 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.
- **authentification locale, commutation locale** — Dans cet état, le Point d'accès 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 au Point d'accès. Quand un Point d'accès hybride-REAP entre le mode autonome, l'authentification WLAN qui sont configurés pour ouvert, partagé, de WPA-PSK, ou WPA2-PSK écrivent l'`authentification locale`, état de `commutation locale` et continuent de nouvelles authentifications client.**Note**: Tous posent le chiffrement de données de 2 radios sont toujours manipulés au Point d'accès. Tous les procédés d'authentification client se produisent sur le contrôleur (ou l'en amont du contrôleur, selon le WLAN et la configuration de contrôleur) tandis qu'AP est dans l'état connecté.
- **authentification vers le bas, commutation locale** — Dans cet état, pour le WLAN donné, le H REAP rejette tous les nouveaux clients qui essayent d'authentifier, mais 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.Si un WLAN localement commuté est configuré pour n'importe quel type d'authentification qui est exigé pour être traité sur (ou au nord de) le contrôleur (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. Précédemment il aurait été dans l'authentification centrale, état de commutation locale. La Connectivité existante de client sans fil est mise à jour et l'accès aux ressources de câble par gens du pays persistent, mais aucune nouvelle association n'est permise. Si la session Web d'un utilisateur chronomètre en utilisant WebAuth ou, si l'intervalle de validité de clé de l'EAP d'un utilisateur expire en utilisant le 802.1X, et exige la nouvelle saisie, les clients existants perdent la Connectivité et sont refusés la Connectivité (cette durée est serveur-particularité de RAYON et ainsi, non standard). En outre, le 802.11 errant des événements (entre H REAP) déclenchent de pleines ré-authentifications de 802.1X et ainsi, représentera le point auquel on ne permet plus à des clients existants la Connectivité.Quand le compte du client d'un tel WLAN égale zéro, le H REAP cesse toutes les fonctions associées de 802.11 et ne balise plus pour le SSID donné, de ce fait déplaçant le WLAN au prochain état H REAP : authentification vers le bas, commutant vers le bas.**Note**: Dans la version 4.2 de logiciel contrôleur ou plus tard, les WLAN qui sont configurés pour le 802.1X, le 802.1X WPA, le 802.1X WPA2, ou le CCKM, peut également fonctionner en mode autonome. Mais ces types d'authentification exigent qu'un serveur RADIUS externe soit configuré. Plus de détails sur ceci est fournis dans les sections pour être livré. Mais, de la version 5.1 de logiciel contrôleur, le H REAP lui-même peut être configuré en tant que serveur de RAYON.
- **authentification vers le bas, commutant vers le bas** — Dans cet état, le WLAN sur un H donné REAP dissocie les clients existants et cesse d'envoyer des balises et des réponses de sonde. Cet état est valide seulement en mode autonome.Quand un Point d'accès H REAP entre le mode autonome, il dissocie tous les clients qui sont sur des WLAN centralement commutés. Pour l'authentification Web WLAN, des clients existants ne sont pas dissociés, mais le Point

d'accès H REAP n'envoie plus des balises quand le nombre de clients associés atteint zéro (0). Il envoie également des messages de dissassociation aux nouveaux clients qui s'associent à l'authentification Web WLAN. des activités Contrôleur-dépendantes telles que le contrôle d'accès au réseau (NAC) et l'authentification Web (accès invité) sont désactivées, et le Point d'accès n'envoie aucun état de système de détection d'intrusions (ID) au contrôleur.**Note**: Si votre contrôleur est configuré pour le NAC, les clients peuvent s'associer seulement quand le Point d'accès est en mode connecté. Quand le NAC est activé, vous devez créer (ou mis en quarantaine) un VLAN malsain de sorte que le trafic de données de tout client qui est assigné à ce VLAN traverse le contrôleur, même si le WLAN est configuré pour la commutation locale. Après qu'un client soit assigné à un VLAN mis en quarantaine, tous ses paquets de données sont centralement commutés.Le Point d'accès hybride-REAP met à jour la Connectivité de client même après qu'il entre le mode autonome. Cependant, une fois que le Point d'accès rétablit une connexion avec le contrôleur, il dissocie tous les clients, applique les nouvelles informations de configuration à partir du contrôleur, et la Connectivité de client de reallows.

Conception H REAP et limites fonctionnelles

Considérations de WAN H REAP

Puisque le H REAP a été conçu spécifiquement pour fonctionner à travers des liens WAN, il a été optimisé pour de telles installations. Bien que H REAP soit flexible quand il s'agit de ces scénarios de conception de réseau distant, il restent quelques instructions qui doivent être honorées architecting un réseau de la fonctionnalité H REAP.

- Un Point d'accès H REAP peut être déployé avec une adresse IP statique ou une adresse DHCP. Dans le cas du DHCP, un serveur DHCP doit être disponible localement et doit pouvoir fournir l'adresse IP pour le Point d'accès au démarrage.
- H REAP prend en charge jusqu'à quatre paquets fragmentés ou un lien WAN de Maximum Transmission Unit du minimum 500-byte (MTU).
- La latence de tour ne doit pas dépasser 300 millisecondes (ms) pour des données et 100 ms pour la Voix et données entre le Point d'accès et le contrôleur, et des paquets de contrôle CAPWAP doivent être donnés la priorité au-dessus de tout autre trafic.
- Le contrôleur peut envoyer des paquets de multidiffusion sous forme d'unicast ou des paquets de multidiffusion au Point d'accès. Dans le mode REAP H, le Point d'accès peut recevoir des paquets de multidiffusion seulement sous la forme d'unicast.
- Afin d'utiliser CCKM jeûnez itinérance avec des Points d'accès H REAP, vous doivent configurer des groupes H REAP.
- Multiple SSID de support de Points d'accès H REAP.
- L'intégration hors bande NAC est prise en charge seulement sur des WLAN configurés pour la commutation centrale H REAP. Il n'est pas pris en charge pour l'usage sur des WLAN configurés pour la commutation locale H REAP.

Note: Pendant une mise à jour, chaque AP doit récupérer une mise à jour du code 4 Mo à travers le lien WAN. Mises à jour et modification Windows de plan en conséquence.

Afin de s'assurer que le soutien de cette limite indiquée de latence est en place, on le recommande fortement qu'entre le Point d'accès et le contrôleur, la priorité soit configurée dans l'infrastructure intermédiaire pour élever CAPWAP (port UDP 5246) à la file d'attente la plus

prioritaire disponible. Sans priorité placée sur le contrôle CAPWAP, les pics dans l'autre trafic réseau peuvent très des Points d'accès de la cause probable H REAP fréquemment décaler de connecté aux modes autonomes pendant que l'encombrement de lien WAN empêche des messages de Point d'accès/contrôleur (et des keeps-alive) d'être livrée. Il est fortement recommandé aux créateurs de réseau, qui prévoient de déployer H REAP AP au-dessus des liens WAN, pour tester toutes leurs applications.

Le lien instable fréquent H REAP entraîne les problèmes de connectivité sérieux. Sans hiérarchisation appropriée de réseau en place, il est prudent de placer des contrôleurs aux sites distants pour assurer l'accès Sans fil cohérent et stable.

Note: Que H REAP soit configuré pour percer un tunnel le trafic de client de nouveau au contrôleur ou pas, le chemin de données CAPWAP est utilisé pour expédier toutes les sondes de client de 802.11 et demandes d'authentification/association, messages voisins RRM, et demandes d'EAP et d'authentification Web de nouveau au contrôleur. En soi, assurez-vous que des données CAPWAP (port UDP 5247) ne sont pas bloquées n'importe où entre le Point d'accès et le contrôleur.

Groupes hybrides REAP

Afin de mieux organiser et gérer vos Points d'accès H REAP, vous pouvez créer des groupes H REAP et assigner les Points d'accès spécifiques à eux. Tous les Points d'accès H REAP dans un groupe partagent le mêmes CCKM, WLAN, et informations de configuration du serveur RADIUS de sauvegarde. Cette caractéristique est utile si vous faites vouloir des Points d'accès du multiple H REAP dans un bureau distant ou sur le plancher d'un bâtiment et de vous les configurer d'un seul trait. Par exemple, vous pouvez configurer un serveur de sauvegarde de RAYON pour un groupe H REAP plutôt que devant configurer le même serveur sur chaque Point d'accès.

Scalability	Flex 7500	WLC 5500/Wism-2/Wism-1
Total Access Points	2,000	500
Total Clients	20,000	7,000
Max HREAP Groups	500	100
Max APs per HREAP Group	50	25
Max AP Groups	500	500

Les versions de logiciel de logiciel contrôleur 5.0.148.0 et contiennent plus tard deux nouvelles caractéristiques de groupe H REAP :

- **Serveur de sauvegarde de RAYON** — Vous pouvez configurer le contrôleur pour laisser un Point d'accès H REAP en mode autonome pour exécuter la pleine authentification de 802.1X à un serveur de sauvegarde de RAYON. Vous pouvez configurer un serveur primaire de RAYON ou un serveur primaire et secondaire de RAYON.

- **Authentification locale** — Vous pouvez configurer le contrôleur pour laisser un Point d'accès H REAP en mode autonome pour exécuter l'authentification RAPIDE de LEAP ou d'EAP jusqu'à 20 utilisateurs statiquement configurés. Avec la version 5.0 de logiciel contrôleur en avant, ceci a été grimpé jusqu'à 100 utilisateurs statiquement configurés. Le contrôleur envoie la liste statique de noms d'utilisateur et mot de passe à chaque Point d'accès H REAP quand il joint le contrôleur. Chaque Point d'accès dans le groupe authentifie seulement ses propres clients associés. Cette caractéristique est idéale pour les clients qui migrent d'un réseau de point d'accès autonome vers un réseau de Point d'accès CAPWAP H REAP et n'ont pas besoin de mettre à jour une grande base de données utilisateur ni d'ajouter un autre périphérique matériel pour remplacer la fonctionnalité de serveur de RAYON disponible au point d'accès autonome.

Les versions de logiciel de logiciel contrôleur 7.0.116.0 et contiennent plus tard ces nouvelles caractéristiques de groupe H REAP :

- **Authentification locale** — Cette caractéristique est maintenant prise en charge même lorsque les Points d'accès H REAP sont en mode connecté.
- **OKC jeûnent itinérance** — Des groupes H REAP sont requis pour que l'itinérance rapide CCKM/OKC travaille avec des Points d'accès H REAP. L'itinérance rapide est réalisée en cachant un dérivé de la clé principale d'une pleine authentification EAP de sorte qu'un échange clé simple et sécurisé puisse se produire quand un client sans fil erre à un Point d'accès différent. Cette caractéristique empêche la nécessité d'exécuter une pleine authentification EAP de RAYON pendant que le client erre d'un Point d'accès à l'autre. Les Points d'accès H REAP doivent obtenir les informations de cache CCKM/OKC pour tous les clients qui pourraient s'associer ainsi ils peuvent les traiter rapidement au lieu de les envoyer de nouveau au contrôleur. Si, par exemple, vous avez un contrôleur avec 300 Points d'accès et 100 clients qui pourraient associer, envoyant le cache CCKM/OKC pour chacun des 100 clients n'est pas pratique. Si vous créez un groupe H REAP comportant un nombre limité des Points d'accès (par exemple, vous créez un groupe pour quatre Points d'accès dans un bureau distant), les clients errent seulement parmi ces quatre Points d'accès, et le cache CCKM/OKC est distribué parmi ces quatre Points d'accès seulement quand les clients s'associent à l'un d'entre eux. Cette caractéristique, avec le rayon et l'authentification locale de sauvegarde (Gens du pays-EAP), n'assure aucun temps d'arrêt opérationnel pour vos filiales.

Note: CCKM jeûnent itinérance parmi H REAP et Points d'accès du non-H REAP ne sont pas pris en charge.

Référez-vous à la section de configuration des groupes Hybride-REAP du guide de configuration Sans fil de contrôleur LAN de Cisco, version 7.0 pour plus d'informations sur la façon configurer des groupes H REAP.

Au joncteur réseau ou pas au joncteur réseau

Des Points d'accès H REAP peuvent être connectés aux liaisons agrégées de 802.1Q ou aux liens non-marqués d'accès. Une fois connectés à une liaison agrégée, les Points d'accès H REAP envoient leur contrôle et trafic de données CAPWAP de nouveau au contrôleur par l'intermédiaire du VLAN indigène. Les WLAN localement commutés peuvent alors avoir leur trafic relâché sur tous les VLAN disponibles (indigène, ou autrement). Quand le positionnement pour traiter un lien d'accès (sans la visibilité de 802.1Q), H REAP expédient tous les messages CAPWAP et données d'utilisateur localement commutées au sous-réseau simple et non-marqué auquel il est connecté.

Les directives générales pour la sélection du mode de switchport pour H REAP sont comme suit :

- Utilisez une liaison agrégée si plus d'un WLAN est configuré pour la commutation locale et si le trafic sur des ces SSID doit être abandonné sur des différents sous-réseaux. Le Point d'accès et le switchport en amont doivent être configurés pour la jonction de 802.1Q. La configuration de H REAP pour la jonction de 802.1Q est la configuration la plus commune et fournit la plupart de flexibilité. Le VLAN indigène doit également être configuré sur le switchport que le H REAP est connecté à en tant que toute la transmission CAPWAP entre AP et le WLC est sur le VLAN indigène.
- Utilisez un lien d'accès quand H REAP n'ont pas plus qu'un WLAN localement commuté simple ou ont le multiple WLAN localement commutés qui n'exigent pas la séparation de câbler-side. Rendez-vous compte qu'une liaison agrégée peut encore être desirable dans ces conditions si la séparation entre la Messagerie CAPWAP et les données d'utilisateur est désirée. Mais, ce n'est ni une configuration requise, ni un risque de sécurité.

Note: Les Points d'accès H REAP se transfèrent pour traiter non-marqué, des interfaces de lien d'accès.

Détection de contrôleur H REAP

H REAP prend en charge chaque mécanisme de détection de contrôleur caractéristique des Points d'accès en architecture de réseau sans fil unifié de Cisco. Une fois que le Point d'accès a une adresse IP (fournie dynamiquement par l'intermédiaire du DHCP, ou par la charge statique adressant) elle tente de découvrir des contrôleurs dans le système par l'intermédiaire de la diffusion IP, l'option 43 DHCP, des DN, et au-dessus du - aérez le ravitaillement (OTAP). En conclusion, H REAP se souviennent les adresses IP du contrôleur auquel elles ont été précédemment connectées. Référez-vous à l'enregistrement léger AP (RECOUVREMENT) à un contrôleur LAN Sans fil (WLC) pour les informations sur les différentes méthodes qu'un RECOUVREMENT peut employer pour s'inscrire à un WLC.

Il y a quelques mises en garde à maintenir dans l'esprit en vue de la détection de contrôleur. Ces considérations s'appliquent à tous les points d'accès Aironet et pas simplement H REAP.

- L'option 43 DHCP est seulement un mécanisme viable de détection pour H REAP si le Point d'accès reçoit son adressage IP par le DHCP.
- L'OTAP fonctionne seulement pour les points d'accès Aironet qui se sont déjà connectés à un contrôleur et à un code téléchargé. Ils se transportent sans microprogramme radio, ainsi l'OTAP ne fonctionne pas directement hors de la case. L'OTAP exige également que d'autres Points d'accès voisins les ont trouvé et se sont connectés à un contrôleur sur lequel l'OTAP est activé. Cette caractéristique est Désuet(e) de la release WLC 6.0 en avant.
- Un Point d'accès sur lequel la fonctionnalité H REAP est prise en charge ne prend en charge pas le mode de la couche 2 LWAPP CAPWAP. Des contrôleurs doivent être placés pour fonctionner avec la couche 3 LWAPP CAPWAP.
- Référez-vous à déployer les contrôleurs LAN Sans fil de gamme de Cisco 440X pour plus d'informations sur la détection de Point d'accès/contrôleur. exécutions

Au delà de ces mécanismes traditionnels de détection de contrôleur, la version de logiciel 4.0 et ultérieures laisse des points d'accès Aironet avec des ports de console pour prendre en charge maintenant l'approvisionnement manuel par la console CLI. Des Points d'accès peuvent être maintenant manuellement configurés pour l'adressage IP statique, l'attribution d'adresse Internet, et les adresses IP des contrôleurs auxquels les Points d'accès devraient se connecter. Ceci

signifie qu'aux sites où d'autres mécanismes de détection ne sont pas disponibles, des Points d'accès puissent être configurés avec toute la configuration nécessaire de Connectivité manuellement par le port de console.

Bien que cette caractéristique soit prise en charge sur chaque point d'accès Aironet avec un port de console, pas simplement ceux ont configuré pour H REAP, cette fonctionnalité est particulièrement utile pour H REAP parce qu'elles sont pour se trouver ont installé dans les sites qui ne sont pas équipés des serveurs DHCP et des mécanismes de détection de contrôleur, tels que dedans une succursale. En soi, ce nouvel accès de console obvie à la nécessité d'expédier H REAP deux fois : une fois à un lieu d'exploitation principal pour le ravitaillement et une deuxième fois au site distant pour l'installation.

Caractéristiques prises en charge par REAP H

Puisque des Points d'accès H REAP sont conçus pour être placés à travers des liens WAN des contrôleurs, y a non seulement il les considérations de conception qui doivent être maintenues dans l'esprit architecting un réseau Sans fil avec H REAP, mais il y a également quelques caractéristiques qui sont complètement ou dans-partie sans support.

Il n'y a aucune restriction de déploiement sur le nombre de Points d'accès H REAP pour chaque emplacement.

Matrice de caractéristique H REAP

Référez-vous à la matrice de caractéristique H REAP pour plus d'informations sur les caractéristiques prises en charge avec H REAP.

Fonctionnalités de sécurité prises en charge

Le support de Sécurité sur le H REAP varie, qui dépend des modes et des états précédemment mentionnés. N'importe quel type de Sécurité qui exige le contrôle du chemin de données tel que le VPN, ne fonctionne pas avec le trafic sur des WLAN localement commutés parce que le contrôleur ne peut pas exercer le contrôle des données qui ne sont pas percées un tunnel de nouveau à lui. Tous autres travaux de type de Sécurité sur WLAN centralement ou localement commutés, si le chemin entre le H REAP et le contrôleur est. Quand ce conduit est vers le bas, seulement un sous-ensemble de ces options de Sécurité permettent à de nouveaux clients pour se connecter aux WLAN localement commutés.

Comme précédemment mentionné, afin de prendre en charge l'authentification EAP de 802.1X, les Points d'accès H REAP en mode autonome doivent avoir leurs propres serveurs de RAYON pour authentifier des clients. Ce serveur de sauvegarde de RAYON peut être celui utilisé par le contrôleur. Vous pouvez configurer un serveur de sauvegarde de RAYON pour différents Points d'accès H REAP par le contrôleur CLI ou pour des groupes H REAP par le GUI ou le CLI. Un serveur de sauvegarde configuré pour un point d'accès individuel ignore la configuration du serveur RADIUS pour un groupe H REAP.

Itinérance sécurisée rapide de support de version 4.2.61.0 et ultérieures WLC avec le Cisco Centralized Key Management (CCKM). Itinérance sécurisée rapide de la couche 2 de supports de mode REAP H avec CCKM. Cette caractéristique empêche le besoin de pleine authentification EAP de RAYON pendant que le client erre d'un Point d'accès à l'autre. Afin d'utiliser CCKM jeûnez itinérance avec des Points d'accès H REAP, vous doivent configurer des groupes H REAP. CCKM

fonctionne en mode autonome pour les clients déjà connectés mais pas pour de nouveaux clients.

Référez-vous à la section de configuration des groupes Hybride-REAP du guide de configuration Sans fil de contrôleur LAN de Cisco, version 7.0 pour plus d'informations sur la façon configurer des groupes H REAP.

Avec H REAP en mode connecté, le contrôleur est libre d'imposer l'exclusion de client/mettre afin d'empêcher sur la liste noire quelques clients d'associer à ses Points d'accès. Cette fonction peut se produire de mode automatisée ou manuelle. Selon global et les configurations par-WLAN, des clients peuvent être exclus pour une foule de raisons, qui s'étend des tentatives répétées d'authentification défaillante au vol IP, et pour n'importe quel temps donné. Des clients peuvent également être présentés dans cette liste d'exclusion manuellement. L'exercice de cette caractéristique est seulement possible tandis que le Point d'accès est en mode connecté. Mais, les clients qui ont été placés sur cette liste d'exclusion restent incapables de se connecter au Point d'accès, même tandis qu'il est en mode autonome.

Note: Les WLAN qui utilisent l'authentification MAC (des gens du pays ou en amont) sont ne permettent plus des authentifications client supplémentaires quand le Point d'accès est en mode autonome, identiques à la manière un WLAN pareillement configuré avec le 802.1X ou WebAuth fonctionnerait en même mode.

Support d'authentification Web

L'authentification de Web interne, hébergée sur le contrôleur LAN Sans fil, est prise en charge pour les WLAN qui centralement ou localement sont commutés. Cependant, l'authentification de Web externe est seulement prise en charge sur un WLAN centralement commuté.

Note: Ni l'une ni l'autre de méthode d'authentification Web n'est prise en charge tandis qu'un H REAP est en mode autonome.

Caractéristiques d'infrastructure prises en charge

RRM

En raison du fait que beaucoup de déploiements distants ont seulement une petite poignée de H REAP, la pleine fonctionnalité de Gestion des ressources radio (RRM) ne pourrait pas être prise en charge à chaque site H REAP. Le plein code RRM est présent dans H REAP, mais les algorithmes de Transmit Power Control (TPC) dans RRM ne sont pas déclenchés jusqu'à quatre Points d'accès ou plus soyez dans la marge de l'un l'autre. Ainsi, quelques installations H REAP pourraient ne jamais mettre leurs radios hors tension. En soi, sans jamais pouvoir mettre leurs radios hors tension en premier lieu, H REAP n'ajustent pas la puissance de transmission de compenser vers le haut en cas d'une détection de trou de couverture.

En mode autonome, RRM fonctionne sur H REAP qui exigent le contrôleur que le traitement ne sont pas pris en charge.

Référez-vous à la gestion des ressources par radio sous le pour en savoir plus de réseaux sans fil unifié et aux petits groupes opérationnels de RRM.

DFS

La sélection dynamique de fréquence (DFS) est prise en charge en modes connectés et

autonomes.

Cheminement d'emplacement

La capacité de prévoir la détermination précise d'emplacement de périphérique varie considérablement de l'emplacement à l'emplacement, basé considérablement sur le nombre, la densité, et le placement de H REAP. La précision d'emplacement s'articule fortement sur la richesse de la collecte d'informations de signal de périphérique, qui la corrèle directement avec le nombre de Points d'accès qui peuvent entendre un périphérique indiqué. Puisque les déploiements H REAP varient dans la portée, cette information d'emplacement peut être considérablement réduite et la précision d'emplacement pourrait souffrir ainsi en conséquence. Tandis que la tentative de déploiements H REAP d'indiquer l'emplacement des périphériques avec la confiance la plus élevée possible, les demandes indiquées de précision de l'emplacement de Cisco ne sont pas prises en charge dans de tels environnements.

Note: H REAP n'a pas été conçu pour fournir des services d'emplacement. Par conséquent, Cisco ne peut pas prendre en charge les demandes indiquées de précision d'emplacement dans des déploiements H REAP.

Mobilité L2 et L3

L'itinérance régulière de la couche 2 est prise en charge pour des WLAN localement commutés. Afin de prévoir une telle itinérance, assurez que les VLAN assignés aux WLAN localement commutés sont cohérents à travers tout le H REAP entre, que l'itinérance est exigé. Ceci signifie que des clients ne sont pas priés au re-DHCP sur des événements d'itinérance. Ceci aide à diminuer les latences associées avec tels erre.

Les événements errants entre H REAP sur les WLAN localement commutés peuvent prendre entre 50 ms et 1500 ms, qui dépendent de la latence BLÊME, des conceptions rf et des caractéristiques environnementales, aussi bien que la Sécurité tape et les réalisations d'itinérance de client-particularité.

L'itinérance de la couche 3 n'est pas prise en charge pour des WLAN localement commutés, mais est prise en charge pour des WLAN centralement commutés.

NAT /PAT

NAT et PAT ne sont pas pris en charge pour des Points d'accès H REAP.

D'autres limites H REAP

- H REAP ne prennent en charge pas WGB.
- Si vous avez configuré un WLAN localement commuté, alors le Listes de contrôle d'accès (ACL) ne fonctionnent pas et ne sont pas pris en charge. Sur un WLAN centralement commuté, ACLs sont pris en charge.
- Tous les changements à une configuration localement commutée WLAN sur la cause de contrôleur une perte provisoire de Connectivité comme nouvelle configuration est appliqués au H REAP. En soi, tous les clients sur ces derniers WLAN localement commuté obtiennent temporairement déconnecté. Le WLAN est activé immédiatement et les clients rassocient de retour.
- Le contrôleur peut envoyer des paquets de multidiffusion sous forme d'unicast ou des paquets de multidiffusion au Point d'accès. En mode hybride-REAP, le Point d'accès peut recevoir des

paquets de multidiffusion seulement sous la forme d'unicast.

Note: Si le H REAP est connecté à la liaison agrégée de 802.1Q et il y a localement des WLAN commutés configurés pour le VLAN, alors la commande de la configuration WLAN devient important due à une limite dans la conception. Si vous changez la commande du WLAN par exemple WLAN 1 est configuré pour le ssid `WLAN-un` et WLAN 2 est configuré pour le ssid `WLAN-b` et leur commande est changée par la configuration WLAN 1 devient ssid `WLAN-b` et WLAN 2 devient ssid `WLAN-un`, alors les les deux les WLAN perdent leur mappage VLAN qui est configuré du WLC.

Note: La même question s'applique d'un H REAP qui joint un contrôleur différent qui a la commande différente des mêmes WLAN. Les contrôleurs primaires et secondaires pour un Point d'accès de l'hybride REAP doivent avoir la même configuration. Autrement, le Point d'accès peut perdre sa configuration, et certaines caractéristiques, telles que le dépassement WLAN, le groupe VLAN AP, numéro de canal statique, et ainsi de suite, ne peuvent pas potentiellement fonctionner correctement. En outre, veillez à reproduire le SSID du Point d'accès H REAP et de son index sur les deux contrôleurs.

Tolérance aux pannes

La tolérance aux pannes H REAP permet à l'accès Sans fil et aux services pour s'embrancher des clients quand :

- Le branchement aps H REAP perdent la Connectivité avec le contrôleur primaire.
- Le branchement aps H REAP commutent au contrôleur secondaire.
- Le branchement aps H REAP rétablissent la connexion au contrôleur primaire.

La tolérance aux pannes H REAP, avec l'EAP local comme tracé les grandes lignes ci-dessus, fournissent ensemble le temps d'arrêt zéro de branchement pendant une panne de réseau. Cette caractéristique est activée par défaut et ne peut pas être désactivée. Il n'exige aucune configuration sur le contrôleur ou l'AP. Cependant, assurer des travaux de tolérance aux pannes sans à-coup et s'applique, ce des critères devrait être mis à jour :

- La commande et les configurations WLAN doivent être identiques à travers les contrôleurs primaires et de sauvegarde.
- Le mappage VLAN doit être identique à travers les contrôleurs primaires et de sauvegarde.
- Le nom de domaine de mobilité doit être identique à travers les contrôleurs primaires et de sauvegarde.
- Il est recommandé pour utiliser la plate-forme de contrôleur en tant que contrôleurs primaires et de sauvegarde.

Résumé

- H REAP ne déconnectera pas des clients quand AP se connecte de nouveau au même contrôleur fourni là n'est aucun changement de configuration sur le contrôleur.
- H REAP ne déconnectera pas des clients quand se connecter au contrôleur de sauvegarde fourni là n'est aucun changement de configuration et le contrôleur de sauvegarde est identique au contrôleur primaire.
- H REAP ne remettra pas à l'état initial ses radios sur se connecter de nouveau au contrôleur primaire fourni là n'est aucun changement de configuration sur le contrôleur.

Limites

- Pris en charge seulement pour H REAP avec le central/authentification locale avec la commutation locale.

- Les clients centralement authentifiés ont besoin de la pleine ré-authentification si le temporisateur de session de client expire avant les passages H REAP AP d'autonome au mode connecté.
- Les contrôleurs primaires et de sauvegarde doivent être dans le même domaine de mobilité.

Configuration H REAP

Préparation de réseau câblé

La première étape à déployer un réseau H REAP est de configurer le commutateur auquel le H REAP se connectera. Cette configuration de commutateur d'exemple inclut une configuration du VLAN natif (le sous-réseau sur laquelle H REAP communiquera avec le contrôleur avec CAPWAP) et deux sous-réseaux sur lesquels les données des clients de deux WLAN localement commutés se termineront. Si l'adressage IP n'est pas fourni aux Points d'accès et aux clients des WLAN localement commutés par l'intermédiaire du commutateur en amont (comme affiché ci-dessous), alors des services DHCP doivent être fournis par l'intermédiaire des autres moyens, ou de satisfaire les besoins d'être fourni statiquement. Bien que le DHCP soit recommandé, certains vraisemblablement choisiront au Point d'accès statique adressant et fourniront des adresses d'utilisateurs de sans fil par l'intermédiaire du DHCP. Des configurations superflues de commutateur ont été retirées de cet exemple pour la simplicité.

```
ip dhcp excluded-address 10.10.10.2 10.10.10.99

ip dhcp pool NATIVE
network 10.10.10.0 255.255.255.0
default-router 10.10.10.1
!
ip dhcp pool VLAN11
network 10.10.11.0 255.255.255.0
default-router 10.10.11.1
!
ip dhcp pool VLAN12
network 10.10.12.0 255.255.255.0
default-router 10.10.12.1
!
interface FastEthernet1/0/1
description H REAP Example Config
switchport trunk encapsulation dot1q
switchport trunk native vlan 10
switchport trunk allowed vlan 10,11,12
switchport mode trunk
!
interface Vlan10
ip address 10.10.10.1 255.255.255.0
!
interface Vlan11
ip address 10.10.11.1 255.255.255.0
!
interface Vlan12
ip address 10.10.12.1 255.255.255.0
end
```

Note: L'adressage IP réel dans cet exemple et toutes les configurations ultérieures est purement à des fins d'illustration. En soi, l'adressage IP DOIT être prévu avec chaque réseau et besoin individuels à l'esprit.

Dans cet exemple de configuration, le H REAP est connecté à la première interface FastEthernet et reçoit l'adressage IP par l'intermédiaire du DHCP du commutateur sur le VLAN indigène (VLAN 10). Des VLAN inutiles sont taillés de la liaison agrégée connectée au H REAP afin de limiter le traitement des paquets étrangers. VLAN 11 et 12 ont été préparés pour fournir l'adressage IP aux clients des deux WLAN qui sont attachés à eux.

Note: Le commutateur auquel H des REAP connectent la Connectivité en amont des besoins à conduire l'infrastructure. Les pratiques recommandées H REAP dictent que l'infrastructure de routage remote-site/WAN donnent la priorité au contrôle CAPWAP (port UDP 5246).

Voici une configuration d'échantillon d'un routeur en amont où le H REAP AP a été connecté afin de donner la priorité au trafic CAPWAP.

```
ip cef
!
frame-relay switching
!
class-map match-all 1
  match access-group 199
!
policy-map mypolicy
  class 1
   bandwidth 256
!
interface Serial0/0
ip address 10.1.0.2 255.255.255.0
encapsulation frame-relay
frame-relay interface-dlci 101
frame-relay intf-type dce
service-policy output mypolicy
!
access  list  199  permit  udp  any  any  eq  5246
```

Détection de contrôleur H-REAP utilisant des commandes CLI

H REAP découvrira le plus généralement les contrôleurs en amont par l'intermédiaire de l'option 43 DHCP ou de la résolution de DN. Sans l'un ou l'autre de ces méthodes disponibles, il peut être desirable de fournir le mode d'emploi détaillé aux administrateurs aux sites distants de sorte que chaque H REAP puisse être configuré avec l'adresse IP des contrôleurs auxquels ils devraient se connecter. Sur option, l'adressage IP H REAP peut être placé manuellement aussi bien (si le DHCP est non disponible ou non désiré).

Détails de cet exemple comment l'adresse IP H un REAP, l'adresse Internet, et l'adresse IP de contrôleur peuvent être placées par le port de console du Point d'accès.

```
AP_CLI#capwap ap hostname ap1130
ap1130#capwap ap ip address 10.10.10.51 255.255.255.0
ap1130#capwap ap ip default-gateway 10.10.10.1
ap1130#capwap ap controller ip address 172.17.2.172
```

Note: Les Points d'accès doivent exécuter la version du logiciel Cisco IOS LWAPP-activée afin de prendre en charge 12.3(11)JX1 d'image de reprise IOS® ou plus tard ces commandes CLI hors de la case. Les Points d'accès avec le préfixe SKU du RECOUVREMENT (par exemple, AIR-LAP-1131AG-A-K9), expédié en fonction ou après juin 13, 2006 exécutent la version du logiciel Cisco IOS 12.3(11)JX1 ou plus tard. Ces commandes sont disponibles à n'importe quel Point d'accès

qui se transporte du fabricant exécutant ce niveau de code, a le code amélioré manuellement à ce niveau, ou est amélioré automatiquement en se connectant à une version 6.0 ou ultérieures courante de contrôleur.

Ces commandes de configuration sont seulement reçues quand le Point d'accès est en mode autonome.

Quand un Point d'accès n'a été jamais connecté à un contrôleur avant, les Points d'accès ont le mot de passe CLI de par défaut de Cisco. Une fois que des Points d'accès sont connectés à un contrôleur, aucune configuration CLI ne peut être faite par la console du Point d'accès jusqu'à ce que le mot de passe soit changé. Cette à commande CLI réservée est sélectionnée au contrôleur avec cette syntaxe :

```
(WLC_CLI)>config ap username <user-id> password <passwd> {all | <AP name>}
```

Pour le Point d'accès ci-dessus, cette commande pourrait être utilisée :

```
(WLC_CLI)>config ap username admin password pass ap1130
```

Note: Bien que cette commande exige la création d'un nom d'utilisateur, ce champ n'est pas actuellement mis en application et est réservé pour une utilisation future.

Note: Toutes les commandes d'**exposition** et de **débogage** fonctionneront bien sans mots de passe par défaut du Point d'accès étant changés.

Configuration de contrôleur H-REAP

Une fois que le H REAP a découvert et a joint le contrôleur, toutes les configurations H REAP sont faites par le Web ou les interfaces de ligne de commande du contrôleur (alternativement, la configuration peut être faite centralement par le système de contrôle sans fil [WCS]). Les configurations H REAP dans cette section sont exécutées par l'interface graphique de contrôleur.

Début en créant et en configurant les WLAN désirés. Pour cet exemple de configuration, les WLAN sont comme suit (des *configurations de tailleur selon les besoins*) :

WLAN SSID	Sécurité	Changement
Entreprise	WPA2 (802.1X)	Gens du pays
RemoteSite	WPA2 - PSK	Gens du pays
Invité	WebAuth	Central

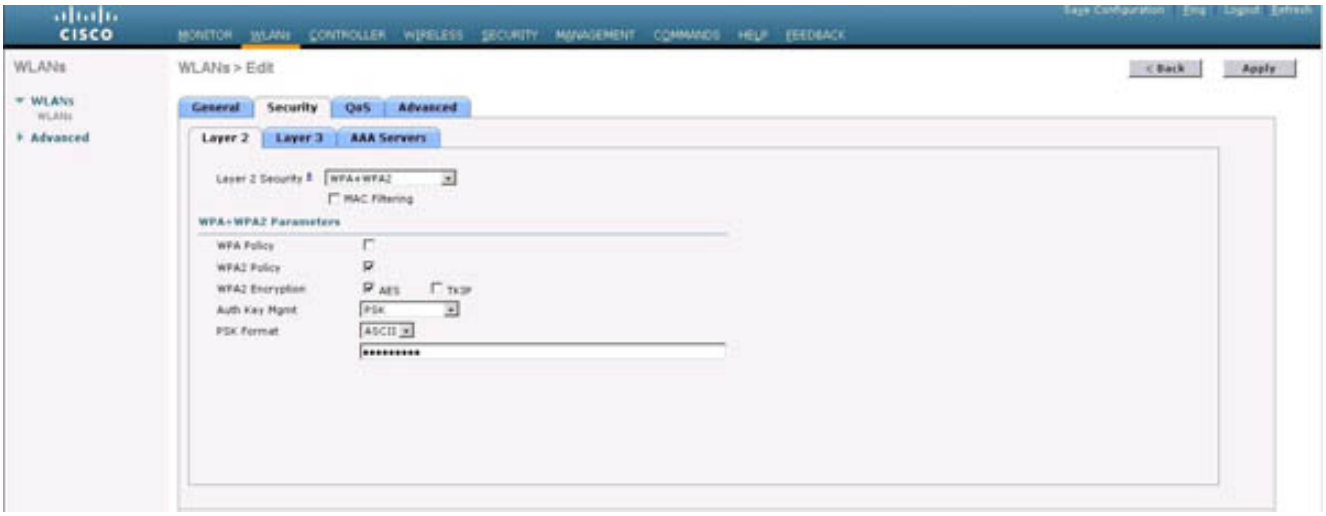
Pour qu'un Point d'accès H REAP fonctionne comme H REAP, le contrôleur auquel il est connecté doit avoir au moins un WLAN localement commuté (sans ceci, fonctionnalité facilement disponible H le REAP ne sera pas réalisé).

Terminez-vous ces étapes afin de configurer un WLAN localement commuté :

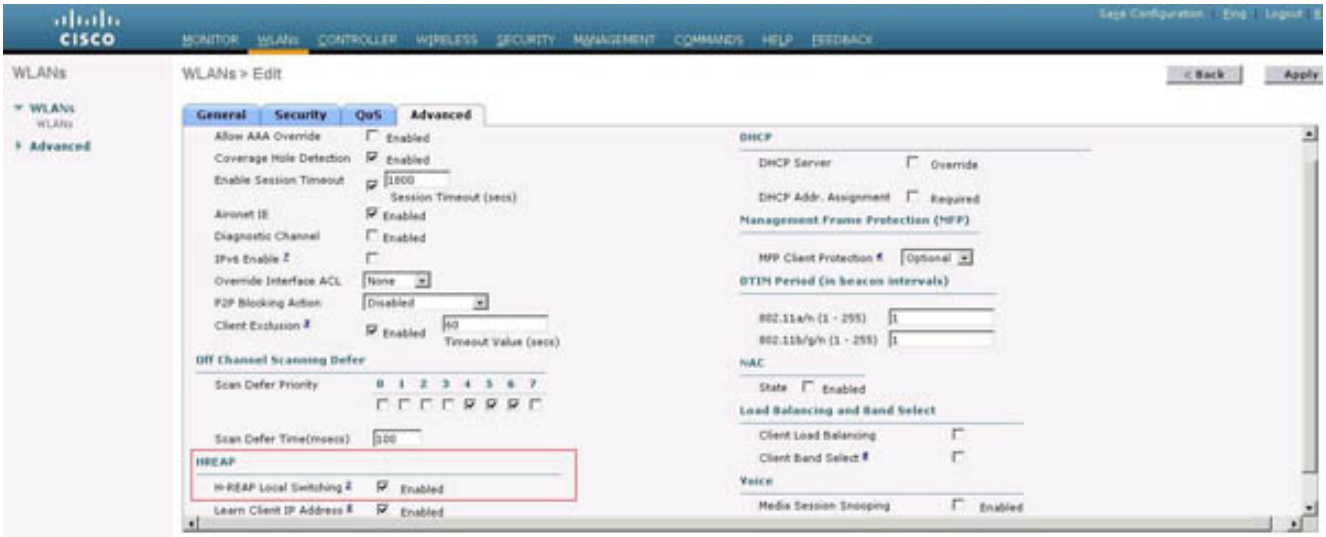
1. Allez à la page principale du contrôleur, choisissez les **WLAN**, et cliquez sur New.
2. Assignez au WLAN un nom, qui est également utilisé comme SSID, et cliquez sur

Apply.

3. Dans la page de WLAN > Edit, cliquez sur l'**onglet Sécurité**. Sous le degré de sécurité de la couche 2, sélectionnez le type de Sécurité.Pour cet exemple, WPA2-PSK est désiré. Choisissez **WPA+WPA2**.



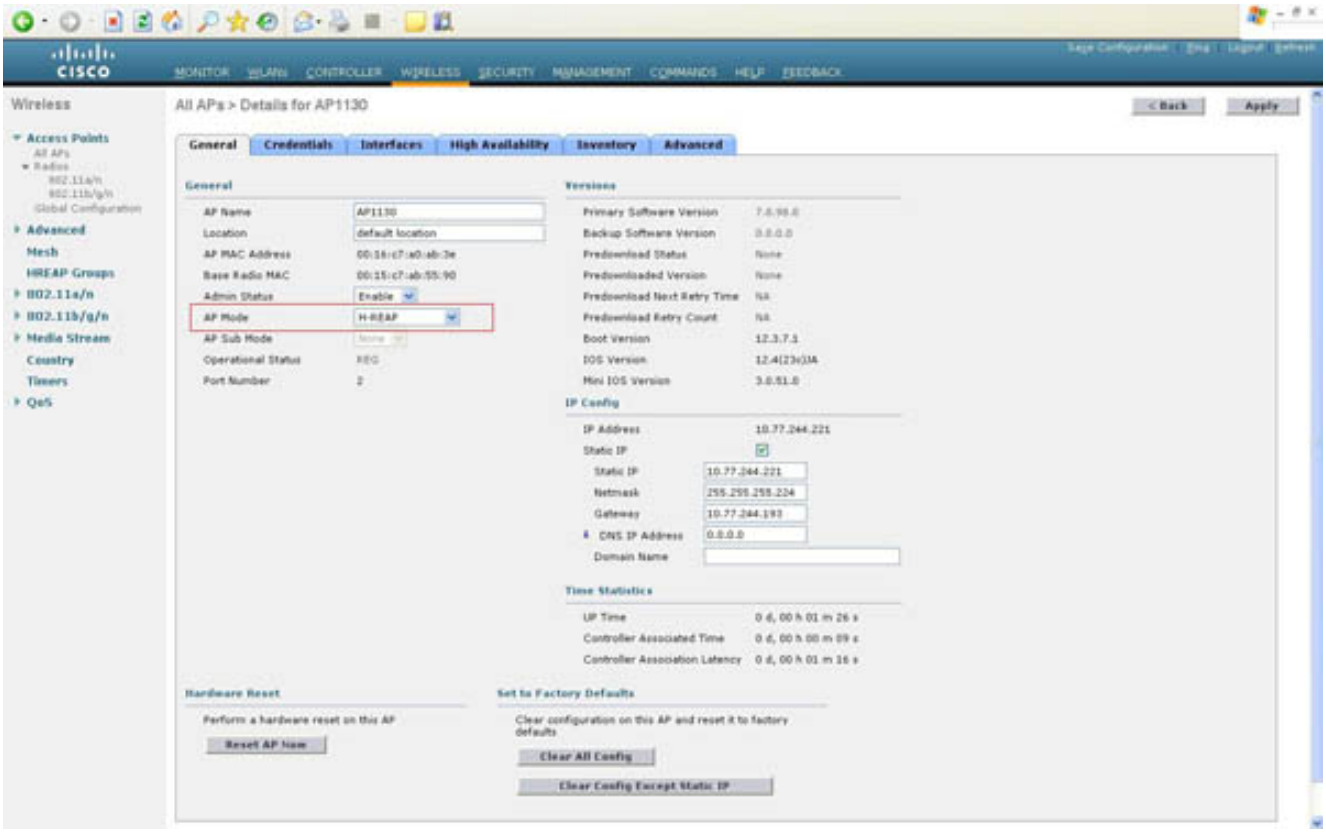
4. Vérifiez la **stratégie WPA2** afin de spécifier les exécutions WPA du WLAN.
5. Contrôle **AES** afin de placer la méthode de cryptage.
6. Sous la clé authentique gestion, choisissez **PSK du** menu déroulant.Selon le format principal désiré, le choix ici s'articule sur la simplicité d'utilisation et le support de client, sélectionne l'**ASCII** ou **ensorcelle**. L'ASCII est en général plus facile parce que des caractères alphanumériques sont reçus. Choisissez l'**ASCII** et introduisez la clé pré-partagée désirée.
7. Cliquez sur l'onglet **Advanced**. Vérifiez la **commutation locale H REAP** et l'assurez que le WLAN est activé pour l'exécution.



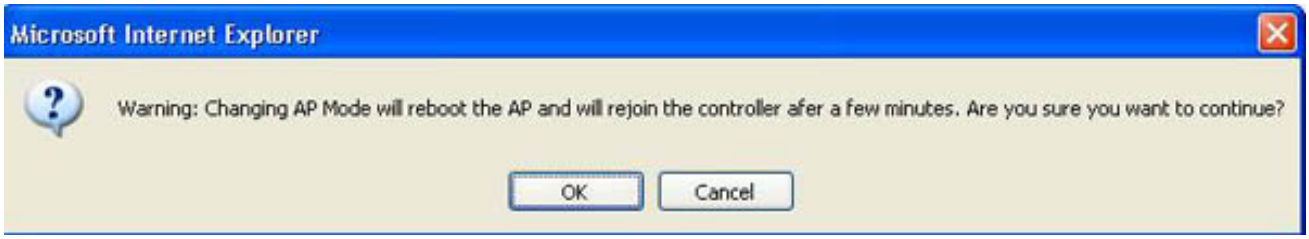
Sans cette étape, le WLAN ne permet pas des données à terminer localement aux Points d'accès H REAP ou n'est pas offert du tout quand le Point d'accès est en mode autonome.**Note**: Les Points d'accès non configurés pour fonctionner dans le mode REAP H

ignorent la position de commutateur local H REAP et tout le trafic de client est percé un tunnel de nouveau au contrôleur.Avec l'installation H REAP WLAN complète, le Point d'accès peut alors être configuré pour fonctionner dans le mode REAP H.

8. Après que le Point d'accès ait découvert et ait joint le contrôleur, allez au GUI de Web de contrôleur sous le titre Sans fil et cliquez sur le **détail** à côté du Point d'accès du choix.
9. Par le titre de mode AP, choisissez **H REAP du** menu déroulant afin de changer le Point d'accès de son exécution par défaut de mode local pour fonctionner dans le mode REAP H.

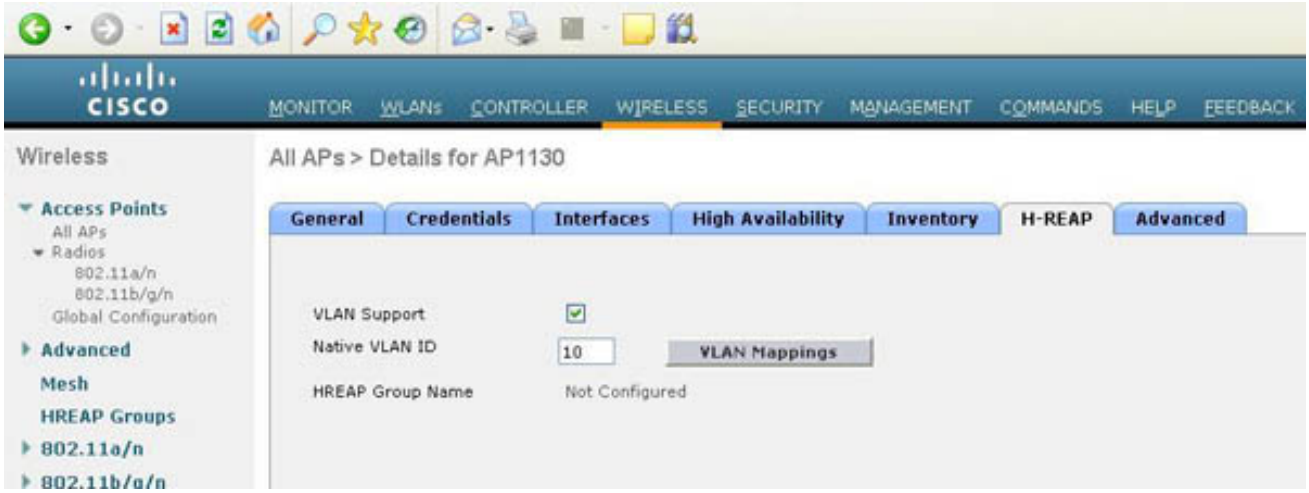


10. Cliquez sur **Apply**. Le Point d'accès doit redémarrer pour que la configuration de mode la prenne
effet.

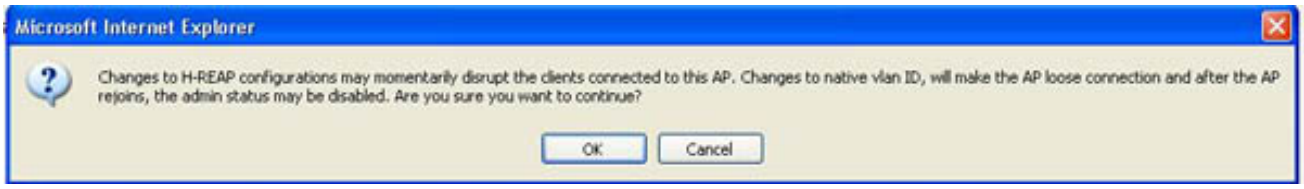


Le Point d'accès redémarre, redécouvre le contrôleur, et joint le contrôleur de nouveau.

11. Revenez au titre **Sans fil du** GUI de contrôleur et sélectionnez le même lien de **détail de** Point d'accès, comme fait avant.Par défaut, le H REAP n'est pas configuré pour traiter une liaison agrégée. Cependant le switchport auquel il est connecté peut être placé à une liaison agrégée, le Point d'accès communique toujours avec le contrôleur au-dessus du VLAN indigène. Si le switchport est une liaison agrégée et on le désire pour faire fonctionner le H REAP en ce mode, le support VLAN doit être activé.
12. Cliquez sur l'onglet **H REAP**. **Support du** contrôle **VLAN**.
13. Basé sur la configuration du switchport auquel le H REAP est connecté, entrez le nombre indigène d'ID DE VLAN du Point d'accès à côté du titre avec le même nom (dans cet exemple, VLAN
10).

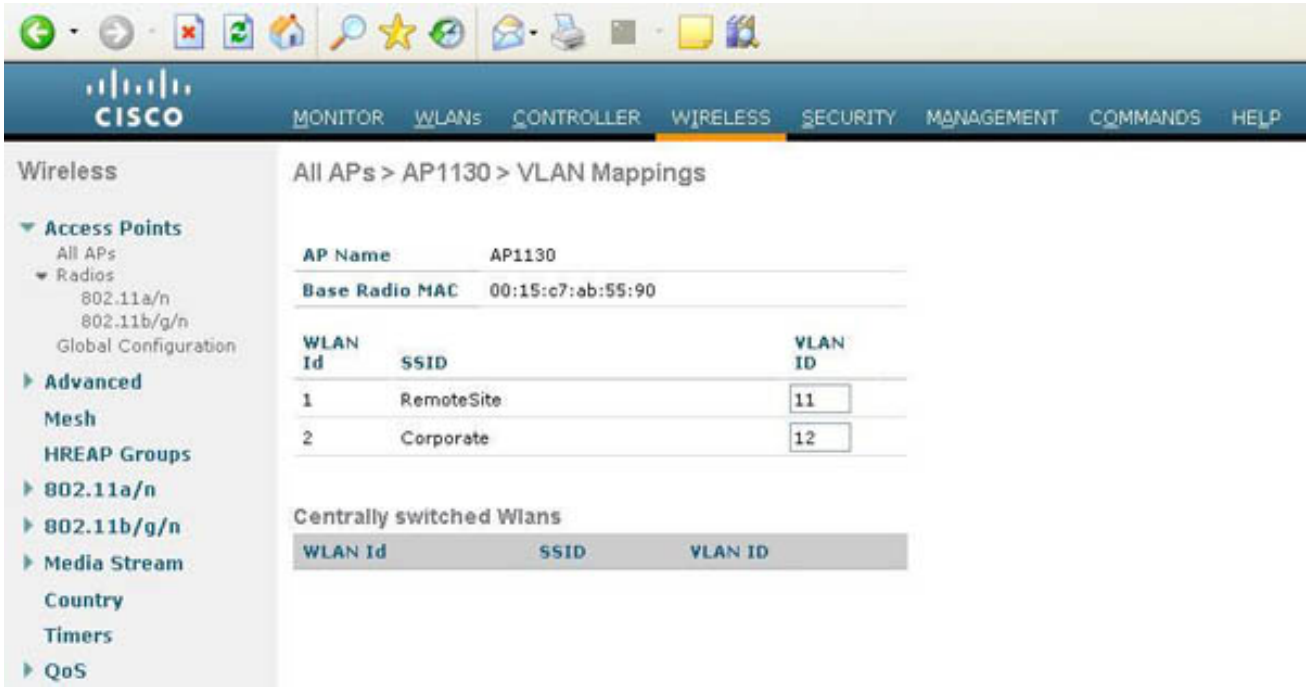


14. Cliquez sur Apply afin de décréter les modifications.Puisque le H REAP remet à l'état initial la configuration de son port Ethernet basé sur les paramètres de configuration donnés, le Point d'accès peut brièvement perdre la Connectivité avec le contrôleur. Une fenêtre contextuelle avertit de cette possibilité. Cliquez sur
OK.



Note: Car l'avertissement instantané indique, il y a une légère occasion que le Point d'accès rejoindra le contrôleur dans l'état handicapé. Resélectionnez que les **détails du** Point d'accès joignent du titre Sans fil du contrôleur. Sélectionnez alors l'**enable** à côté d'Admin Status. Appliquez la configuration et continuez la configuration.

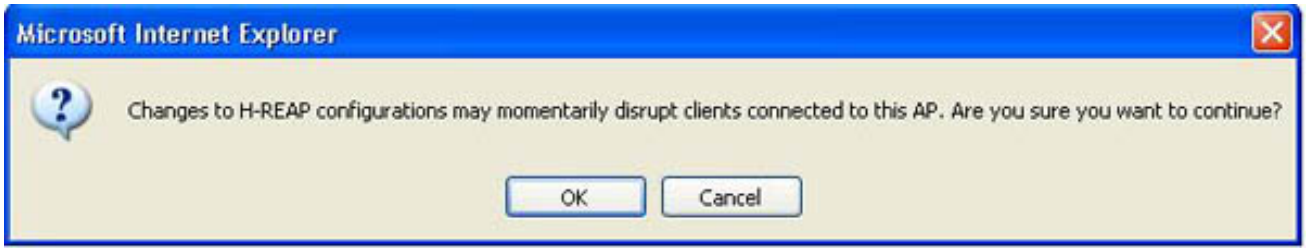
15. Entrez dans la page de détail du Point d'accès désiré, sélectionnez la balise H REAP de nouveau, et cliquez sur le **mappage VLAN** afin de configurer le 802.1Q étiquetant par WLAN localement
commuté.



16. Placez le VLAN par WLAN localement commuté sur lequel le trafic de client doit être terminé.**Note**: Les WLAN non configurés pour prendre en charge la commutation locale H REAP ne permettent pas la balise de 802.1Q à configurer ici. La configuration VLAN pour

ces WLAN est placée dans les paramètres généraux du contrôleur parce que des données de client sont percées un tunnel de nouveau au contrôleur pour l'arrêt.**Note**: Les WLAN localement commutés peuvent tout partager le même ID DE VLAN ou peuvent avoir des affectations discrètes. Il n'y a aucune limite ici, si le VLAN assigné est présent au switchport du H REAP.

17. Cliquez sur **Apply** afin de sauvegarder les modifications.Le service WLAN est perturbé momentanément tandis que le mappage VLAN/WLAN est changé. Cliquez sur OK pour reconnaître
ceci.



Les WLAN nécessaires sont créés et configurés, les Points d'accès réglé pour fonctionner dans le mode REAP H, le support VLAN activé, et les VLAN configurés par WLAN localement commuté. Si les services DHCP sont disponibles sur chaque VLAN, les clients doivent pouvoir se connecter à chaque WLAN, recevoir des adresses sur leurs VLAN respectifs, et passer le trafic. La configuration H REAP est maintenant complète.

Dépannage de H-REAP

Il y a quelques scénarios et situations courants qui surgissent et empêchent la configuration H REAP et la Connectivité douces de client. Cette section fournit à quelques telles situations leurs solutions suggérées.

H-REAP ne joint pas le contrôleur

Ceci peut se produire pour plusieurs raisons. Début en vérifiant ce qui suit :

- **Chaque H REAP doit être correctement IP adressé.**Si le DHCP est utilisé par la console du Point d'accès, vérifiez que le Point d'accès obtient une adresse.
  ```
  AP_CLI#show dhcp lease
  ```

  Si l'adressage de charge statique est utilisé par la console du Point d'accès, le contrôle pour s'assurer l'adressage IP correct est appliqué.
  ```
  AP_CLI#show capwap ip config
  ```

- **Assurez que le Point d'accès a la connectivité IP et peut cingler l'interface de gestion du contrôleur.**Une fois que l'adressage IP est vérifié, le contrôle pour s'assurer le Point d'accès peut communiquer avec le contrôleur en cinglant l'adresse IP de Gestion du contrôleur. Utilisez la **commande ping** par la console du Point d'accès avec cette syntaxe :
  ```
  AP_CLI#ping <WLC management IP address>
  ```

  Si ce n'est pas réussi, assurez que le réseau en amont est correctement configuré et cet accès WAN de nouveau au réseau d'entreprise est disponible. Vérifiez le contrôleur est opérationnel et n'est pas derrière toutes les bornes NAT/PAT. Assurez-vous que les ports UDP 5246 et 5247 sont ouverts sur tous les Pare-feu intermédiaires. Cinglez du contrôleur au

Point d'accès avec la même syntaxe.

- **Vérifiez là est Connectivité CAPWAP entre le Point d'accès et le contrôleur.**Une fois la connectivité IP entre le H REAP et le contrôleur est vérifiée, exécute CAPWAP met au point sur le contrôleur pour confirmer des messages CAPWAP sont communiquées à travers le WAN et pour identifier des problèmes relatifs. Sur le contrôleur, créez d'abord un filtre d'adresses MAC pour limiter la portée de la sortie de débogage. Employez cette commande afin de limiter la sortie de la commande ultérieure à un seul point d'accès.
  AP_CLI#**debug mac addr <AP's wired MAC address>**

  Une fois réglé pour limiter la sortie de débogage, activez l'élimination des imperfections CAPWAP.
  AP_CLI#**debug capwap events enable**

  Si aucun message de débogage CAPWAP n'est vu, assurez que le H REAP a au moins une méthode par laquelle un contrôleur peut être découvert. Si de telles méthodes sont en place (comme option 43 DHCP ou DN), vérifiez-les sont correctement configurés. Si aucune autre méthode heuristique n'est en place, assurez que l'adresse IP du contrôleur est écrite dans le Point d'accès par la console CLI.
  AP_CLI#**capwap ap controller ip address <WLC management IP address>**

- **Vérifiez les exécutions CAPWAP sur le contrôleur et le H REAP.**Si au moins une méthode heuristique simple de contrôleur est disponible au H REAP, vérifiez les messages CAPWAP sont envoyés du Point d'accès au contrôleur. Cette commande est déjà activée par défaut.
  AP_CLI#**debug capwap client errors**

  Les informations supplémentaires au sujet quels contrôleurs le Point d'accès communique avec peuvent être vues par les adresses IP du message d'UDP qu'il envoie. Visualisez la source et les adresses de destination de chaque paquet qui traverse la pile IP du Point d'accès.
  AP_CLI#**debug ip udp**

  S'il apparaît de la console du Point d'accès qu'elle communique avec un contrôleur, il est possible qu'elle ait joint un autre contrôleur dans la batterie. Afin de vérifier si le H REAP est connecté à un contrôleur, utilisez cette commande.
  AP_CLI#**show capwap reap status**

- **Vérifiez que le Point d'accès a joint le contrôleur correct.**Si d'autres adresses IP du contrôleur sont remises au Point d'accès pendant la phase de détection, le H REAP peut avoir joint un autre contrôleur. Vérifiez le contrôleur que l'adresse IP rendue disponible par le mécanisme de détection est correcte. Identifiez le contrôleur auquel le Point d'accès s'est joint.
  AP_CLI#**show capwap reap status**

  Connectez-vous dans ce GUI de Web du contrôleur. Assurez que tous les IP et adresses MAC des contrôleurs sont introduites dans la liste de mobilité du contrôleur et cela ils tous partagent le même nom de groupe de mobilité. Puis, placez le Point d'accès les contrôleurs primaires, secondaires, et tertiaires pour dicter quel contrôleur le Point d'accès joint. Ceci est fait par le lien de détails du Point d'accès. Si le problème se repose avec le H REAP joignant un autre contrôleur, ceci peut être considérablement soulagé à l'aide des capacités de Gestion de Point d'accès WCS au niveau système.

- **Dépannez les questions de certificat si le Point d'accès tente de joindre le contrôleur, mais échouez.**Si des messages CAPWAP sont vus sur le contrôleur, mais le Point d'accès ne se joint pas, ce probable est une question de certificat.

Les commandes de la console du H-REAP ne sont pas opérationnelles et renvoient une erreur

Toutes commandes de configuration (configuration ou effacement de la configuration) exécutées par le retour H REAP CLI l'`ERREUR ! ! ! La commande est` message `désactivé`. Ceci peut se produire pour une de deux raisons :

- Les Points d'accès H REAP qui sont en mode connecté ne permettront pas la configuration ou l'effacement d'aucune configuration par l'intermédiaire de la console. Quand le Point d'accès est dans cet état, des configurations doivent être faites par l'interface de contrôleur. Si l'accès aux commandes de configuration au Point d'accès est exigé, assurez que le Point d'accès est en mode autonome avant de tenter pour sélectionner toutes les commandes de configuration.
- Une fois que le Point d'accès s'est connecté à un contrôleur à un point quelconque (même si le H REAP s'est déplacé de nouveau au mode autonome), la console du Point d'accès ne permettra pas des commandes de configuration jusqu'à ce qu'un nouveau mot de passe soit placé. Chaque le mot de passe H REAP doit être changé. Ceci peut seulement être placé par le CLI du contrôleur auquel le Point d'accès est connecté. Cette syntaxe de commande peut être utilisée au contrôleur pour placer le mot de passe de la console d'un point d'accès individuel ou le mot de passe aux Points d'accès de tout le contrôleur :
  `(WLC_CLI)>`**`config ap username <user-id> password <passwd> {all | <AP name>}`**

  Note: Pour un Point d'accès qui n'a pas eu ses mots de passe de console réglés, rendez-vous compte que cette configuration est seulement envoyée au Point d'accès au point que la commande est sélectionnée au contrôleur. Tous les Points d'accès qui se joignent ultérieurement à ceci exigeront la commande soient entrés de nouveau.Même une fois que le Point d'accès chacun des deux a été indiqué un mot de passe de non-par défaut et le Point d'accès est en mode autonome, le Point d'accès ne permettra néanmoins pas l'accès à ces commandes. Afin d'apporter des modifications à la configuration H le REAP, la suppression de l'adressage IP statique préexistant et des configurations des adresses IP de contrôleur est exigée. Cette configuration s'appelle la configuration privée CAPWAP et devra être retirée avant que toutes les nouvelles commandes CLI de Point d'accès puissent être entrées. Afin de faire ceci, sélectionnez cette commande :
  `AP_CLI#`**`clear capwap private-config`**

  Note: Alternativement, AP peut être retourné aux par défaut d'usine tandis qu'il est joint à un contrôleur. Cliquez sur le bouton de **clear config** dans la page des détails d'AP sous le titre Sans fil dans le GUI WLC. La configuration D'AP est nettoyée et elle est redémarrée.**Note**: Toutes les commandes d'**exposition** et de **débogage** continueront à fonctionner même sans mot de passe de non-par défaut étant placé et avec AP en mode connecté.Seulement en ce moment peuvent toutes les configurations CAPWAP être faites.

Les clients ne peuvent pas se connecter au H-REAP

Procédez comme suit :

1. Vérifiez que le Point d'accès a correctement joint le contrôleur, le contrôleur a au moins un (et activé) WLAN correctement configuré, et s'assure que le H REAP est dans l'état activé.
2. Sur l'extrémité du client, vérifiez que le SSID du WLAN est disponible (au contrôleur, configurer le WLAN pour annoncer son SSID peut aider ce processus de dépannage). Reflétez la configuration de sécurité du WLAN sur le client. Les configurations de sécurité de côté client sont où l'immense majorité de problèmes de Connectivité résident.
3. Assurez que les clients sur des WLAN localement commutés sont correctement IP adressé. Si le DHCP est utilisé, assurez-vous qu'un serveur DHCP en amont est correctement configuré et fournissant des adresses aux clients. Si l'adressage de charge statique est utilisé, assurez que les clients sont correctement configurés pour le sous-réseau correct.
4. Afin de dépanner plus loin des problèmes de connectivité de client au port de console H le REAP, sélectionnez cette commande.
   ```
   AP_CLI#show capwap reap association
   ```
5. 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>
   ```
6. Afin de mettre au point les problèmes de connectivité du 802.11 d'un client, utilisez cette commande.
   ```
   AP_CLI#debug dot11 state enable
   ```
7. Débuggez la procédure d'authentification et les pannes du 802.1X d'un client avec cette commande.
   ```
   AP_CLI#debug dot1x events enable
   ```
8. Des messages principaux controller/RADIUS peuvent être mis au point utilisant cette commande.
   ```
   AP_CLI#debug aaa events enable
   ```
9. Alternativement, pour activer un correspondant complet des commandes de débogage de client, utilisez cette commande.
   ```
   AP_CLI#debug client <client's MAC address>
   ```

H-REAP QAs

Q. Si je configure des recouvrements à un site distant comme H REAP, est-ce que je peux donner à ces recouvrements un contrôleur primaire et secondaire ?

Exemple : Il y a un contrôleur primaire au site A et un contrôleur secondaire au site B.

Si le contrôleur au site A échoue, le RECOUVREMENT fait le Basculement au contrôleur au site B. Si les deux contrôleurs sont indisponibles fait la chute de RECOUVREMENT dans le mode local H REAP ?

A. Oui. D'abord le RECOUVREMENT bascule à son secondaire. Tous les WLAN qui sont localement commutés n'ont aucune modification, et tout qui sont centralement commutées juste font aller le trafic au nouveau contrôleur. Et, si le secondaire échoue, tous les WLAN qui sont marqués pour la commutation locale (et ouvrez-vous/authentification principal pré-partagé/vous

font l'authentificateur AP) restent.

Q. Comment les Points d'accès configurés en **mode local** traitent-ils des WLAN configurés avec la commutation locale H REAP ?

A. Les Points d'accès de mode local traitent ces WLAN en tant que WLAN normaux. L'authentification et le trafic de données sont percés un tunnel de nouveau au WLC. Pendant une panne de lien WAN ce WLAN est complètement vers le bas et aucun client n'est en activité sur ce WLAN jusqu'à ce que la connexion au WLC soit restaurée.

Q. Est-ce que je peux faire l'authentification Web avec la commutation locale ?

Oui, vous pouvez avoir un SSID avec l'authentification Web activée et relâcher le trafic localement après authentification Web. L'authentification Web avec la commutation locale fonctionne bien.

Q. Est-ce que je peux utiliser mon Invité-portail sur le contrôleur pour un SSID, qui est manipulé localement par le H REAP ? Si oui, que se produit si je perds la Connectivité au contrôleur ? Les clients en cours relâchent-ils immédiatement ?

Oui. Puisque ce WLAN est localement commuté, le WLAN est disponible mais aucun nouveau client ne peut authentifier car la page Web n'est pas disponible. Cependant, les clients existants ne sont pas lâchés hors fonction.

Informations connexes

- Guide de configuration du contrôleur LAN sans fil Cisco, version 4.0
- Mise à niveau logicielle du contrôleur LAN sans fil (WLC)
- Dépannage du contrôleur LAN sans fil (WLC) - FAQ
- Support de technologie WLAN
- Exemple de configuration de modes de fonctionnement H REAP
- Dépannage de base distant hybride du Point d'accès de périphérie (H REAP)
- Exemples Sans fil et TechNotes de configuration de contrôleur LAN
- Messages d'erreur et système du contrôleur de réseau local sans fil - Forum Aux Questions
- Messages d'erreur et système du système de contrôle sans fil (WCS)
- Support et documentation techniques - Cisco Systems