Point d'accès léger - Forum Aux Questions

Contenu

[Introduction](#)
[FAQ LAP](#)
[Informations connexes](#)

Introduction

Ce document fournit des informations sur les questions fréquemment posées (FAQ) au sujet des Points d'accès légers (LAP) Cisco.

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

FAQ LAP

Q. Qu'est-ce qu'un Point d'accès léger (LAP) Cisco ?

A. Le LAP Cisco fait partie de l'architecture de réseau sans fil unifié Cisco. Un LAP est un AP conçu pour être connecté à un contrôleur (WLC) de réseau local sans fil (WLAN). Le LAP offre une prise en charge bi-bande pour IEEE 802.11a, 802.11b, et 802.11g ainsi qu'une surveillance de l'air simultanée pour la gestion dynamique et en temps réel de radiofréquence (RF). En outre, les LAP Cisco gère des fonctions à durée limitée, telles que le cryptage de couche 2, qui permet aux WLAN Cisco une prise en charge sécurisée d'applications vocales, vidéo et de données.

Les AP sont « légers », ce qui veut dire qu'ils ne peuvent pas agir indépendamment d'un contrôleur LAN sans fil (WLC). Le WLC contrôle les configurations et le microprogramme de l'AP. Les AP ont un déploiement « mains libres », et la configuration individuelle des PA n'est pas nécessaire. Les Ap sont également légers car ils gèrent uniquement la fonctionnalité MAC en temps réel. Les AP laissent le WLC traiter toutes les fonctionnalité MAC qui ne sont pas en temps réel. Cette architecture est appelée « split MAC ».

Q. Puis-je configurer le LAP pour fonctionner indépendamment d'un contrôleur LAN sans fil (WLC) ?

A. Non, les LAP ne peuvent pas fonctionner indépendamment des WLC. Les LAP fonctionnent uniquement en tandem avec un WLC. La raison est que le WLC fournit tous les paramètres de configuration et le microprogramme dont le LAP a besoin pour la procédure d'enregistrement.

Q. Qu'est-ce qu'un Protocole d'AP léger (LWAPP) ?

A. LWAPP est un projet de protocole de l’Internet Engineering Task Force (IETF) qui définit la

messagerie de contrôle pour la configuration et l'authentification des commandes exécutées et des parcours. LWAPP définit également le mécanisme de transmission tunnel pour le trafic de données.

Un LAP détecte un contrôleur à l'aide des mécanismes de détection LWAPP. Le LAP envoie une requête d'enregistrement LWAPP au contrôleur. Le contrôleur envoie au LAP une réponse d'enregistrement LWAPP, qui permet au PA de se connecter au contrôleur. Quand le LAP se connecte au contrôleur, le LAP télécharge le logiciel du contrôleur si les révisions du LAP et du contrôleur ne correspondent pas. Ensuite, le LAP est complètement sous le contrôle du contrôleur. Le LWAPP sécurise la communication de contrôle entre le LAP et le contrôleur au moyen d'une distribution de clé sécurisée. La distribution de clé sécurisée exige que les certificats numériques X.509 soient déjà attribués au LAP et au contrôleur. Des certificats d'origine sont référencés avec le terme « MIC » (certificat installé en usine). Les AP Cisco Aironet expédiés avant le 18 juillet 2005 n'ont pas de MIC. Ainsi ces AP créent un certificat auto-signé (SSC) quand ils sont mis à niveau afin de fonctionner en mode léger. Les contrôleurs sont programmés pour accepter les SSC pour l'authentification d'AP spécifiques.

Q. Qu'est-ce que le CAPWAP ?

A. Dans la version du logiciel de contrôleur 5.2 ou ultérieure, les points d'accès légers Cisco utilisent le standard IETF de protocole de contrôle et de configuration des points d'accès sans fil (CAPWAP) afin de communiquer entre le contrôleur et d'autres points d'accès légers du réseau. Les versions du logiciel de contrôleur antérieures à 5.2 utilisent le protocole de point d'accès léger (LWAPP) pour ces communications.

Le CAPWAP, qui est basé sur le LWAPP, est un protocole standard interopérable qui permet à un contrôleur de gérer un ensemble de points d'accès sans fil. Le CAPWAP est mis en application dans la version 5.2 du logiciel de contrôleur pour ces raisons :

- Pour fournir une solution de mise à niveau des Produits Cisco qui utilisent le LWAPP vers les produits Cisco de nouvelle génération qui utilisent le CAPWAP
- Pour prendre en charge les lecteurs RFID et d'autres périphériques semblables
- Pour permettre aux contrôleurs d'interopérer avec des points d'accès tiers à l'avenir

Les points d'accès compatibles LWAPP sont capables de détecter et de joindre un contrôleur CAPWAP, et la conversion vers un contrôleur CAPWAP est sans faille. Par exemple, le processus de détection de contrôleur et le processus de téléchargement de microprogramme quand vous utilisez CAPWAP sont identiques avec LWAPP. La seule exception concerne les déploiements de la couche 2, qui ne sont pas pris en charge par CAPWAP.

Les contrôleurs CAPWAP et LWAPP peuvent être déployés sur le même réseau. Le logiciel adapté au CAPWAP permet aux points d'accès de joindre un contrôleur CAPWAP ou LWAPP. La seule exception concerne le point d'accès de gamme Cisco Aironet 1140, qui prend uniquement en charge le CAPWAP et joint donc uniquement les contrôleurs CAPWAP. Par exemple, un point d'accès de la gamme 1130 peut joindre un contrôleur utilisant le CAPWAP ou le LWAPP tandis qu'un point d'accès de la gamme 1140 peut uniquement joindre un contrôleur utilisant le CAPWAP.

Pour plus d'informations, référez-vous à la section Protocoles de communication de point d'accès du guide de configuration.

Q. Comment distinguer un AP classique (autonome) d'un LAP ?

A. Le moyen le plus simple pour faire la distinction entre un AP classique et un LAP est de regarder le numéro de pièce de l'AP.

- Les numéros de pièce des LAP (Lightweight AP Protocol [LWAPP]) commencent toujours par AIR-LAPXXXX.
- Les numéros de pièce des AP autonomes (logiciel Cisco IOS®) commencent toujours par AIR-APXXXX.

Les LAP de la gamme Cisco Aironet 1000 sont une exception à ce critère. Les numéros de pièce des LAP de la gamme 1000 sont :

- AIR-AP1010-A-K9 pour un LAP 1010
- AIR-AP1020-A-K9 pour un LAP 1020
- AIR-AP1030-A-K9 pour un LAP 1030

Remarque : Les références peuvent varier, selon le pays et le domaine réglementaire. Les numéros de pièce fournis dans cette liste sont juste des exemples.

Assurez-vous de commander l'AP approprié pour votre LAN sans fil (WLAN).

Q. Quels modèles d'AP sont capables d'utiliser le protocole d'AP léger (LWAPP) ?

A. Les plates-formes AP Cisco Aironet suivantes sont capables d'utiliser le LWAPP :

- Gamme Aironet 1500
- Gamme Cisco Aironet 1250
- Gamme Aironet 1240 AG
- Gamme Aironet 1230 AG
- Gamme Aironet 1200
- Gamme Aironet 1130 AG
- Gamme Aironet 1000
- AP de la gamme Aironet 1140**Remarque :** L'AP de la gamme 1140 est pris en charge uniquement avec le WLC qui exécute la version 5.2 ou ultérieure.

Remarque : Vous pouvez commander ces AP Aironet avec le logiciel Cisco IOS pour fonctionner en tant qu'AP autonomes ou pour fonctionner avec LWAPP. Le numéro de la pièce détermine si un AP est articulé autour du logiciel Cisco IOS ou basé sur le LWAPP. Voici quelques exemples :

- AIR-AP1242AG-A-K9 est un AP qui s'articule autour du logiciel Cisco IOS.
- AIR-LAP1242AG-P-K9 est un AP basé sur le LWAPP.

Remarque : Les AP de la gamme 1000 et les AP de la gamme 1500 sont des exceptions à ce critère. Tous les AP des gammes 1000 et 1500 prennent uniquement en charge le LWAPP.

Q. Comment installer et configurer un point d'accès adapté au LWAPP ?

A. Les point d'accès compatibles avec LWAPP font partie d'une solution de réseau Cisco avec fonctionnalités sans fil intégrées et ne nécessitent aucune configuration manuelle avant d'être montés. L'AP est configuré par un contrôleur LAN sans fil (WLC) Cisco prenant en charge le LWAPP. Référez-vous au Guide de démarrage rapide pour les points d'accès Aironet Cisco adaptés au LWAPP pour obtenir des informations sur l'installation et la configuration initiale d'un point d'accès adapté au LWAPP.

Q. Comment configurer mon LAP et mon contrôleur LAN Sans fil (WLC) ensemble ?

A. Ces points d'accès allégés suivent le protocole LWAPP, et lorsqu'ils se connectent à un contrôleur réseau sans fil, ce dernier leur enverra le micrologiciel et les paramètres de configuration. Référez-vous à l'Exemple de configuration de base d'un contrôleur LAN sans fil et d'un point d'accès léger pour une configuration de base.

Q. Puis-je connecter un AP autonome à un contrôleur LAN sans fil (WLC) et m'attendre à ce que l'AP fonctionne ?

A. Non, seuls les LAP fonctionnent en connexion avec un WLC. Les AP autonomes ne comprennent pas le protocole d'AP léger (LWAPP) ou CAPWAP que le WLC utilise. Afin de connecter un AP autonome à un WLC, vous devez d'abord faire passer l'AP autonome en mode léger.

Q. Je dispose d'un point d'accès autonome articulé autour du logiciel Cisco IOS. Puis-je le faire passer en mode léger ?

A. Oui, mais tous les modèles d'AP autonomes articulés autour du logiciel Cisco IOS ne peuvent être convertis. Voici les modèles que vous pouvez faire passer en mode protocole d'AP léger (LWAPP) :

- Tous les AP Cisco Aironet 1130 AG
- Tous les AP Aironet 1240 AG
- Pour toutes les plates-formes d'AP modulaires de la gamme Aironet 1200 articulés autour du logiciel Cisco IOS (AP 1200/1220 avec mise à niveau du logiciel Cisco IOS, 1210 et 1230), la possibilité de conversion de l'AP dépend de la fonctionnalité sans fil.Si le standard sans fil est l'IEEE 802.11g, MP21G et MP31G sont pris en charge.Si le standard sans fil est l'IEEE 802.11a, RM21A et RM22A sont pris en charge.Vous pouvez mettre à niveau les AP de la gamme 1200 séries avec n'importe quelle combinaison des radios prise en charge :G uniquementA uniquementG et A

Remarque : Un AP autonome doit exécuter le logiciel Cisco IOS Version 12.3(7)JA ou ultérieure avant de pouvoir le convertir en LWAPP.

Remarque : Seuls les contrôleurs LAN sans fil (WLC) Cisco 4400 et 2006 prennent en charge les points d'accès autonomes convertis en mode léger. Les WLC Cisco doivent utiliser la version logicielle 3.1 au minimum. Le système de commande sans fil (WCS) Cisco doit utiliser la version 3.1 au minimum. L'utilitaire de mise à niveau est pris en charge sur les plates-formes Microsoft Windows 2000 et Windows XP.

Référez-vous à la section Mise à niveau des points d'accès autonomes Cisco Aironet vers le mode léger pour obtenir des détails sur la façon de réaliser la conversion.

Q. Quelles restrictions sont imposées à un point d'accès articulé autour du logiciel Cisco IOS après conversion au mode léger ?

A. Gardez ces directives à l'esprit lorsque vous utilisez des points d'accès autonomes qui ont été convertis en mode léger :

- Les AP convertis au protocole d'AP léger (LWAPP) ne prennent pas en charge Wireless domain services (WDS). Les AP convertis au LWAPP communiquent uniquement les contrôleurs LAN sans fil (WLC) Cisco et ne peuvent pas communiquer avec des périphériques WDS. Cependant, le WLC propose un fonctionnalité équivalente au WDS lorsque l'AP est associé au WLC.
- Les points d'accès convertis prennent uniquement en charge les contrôleurs 2006, 4400, et WiSM. Quand vous convertissez un point d'accès autonome au mode léger, il peut uniquement communiquer avec les contrôleurs Cisco des gammes 2006 et 4400 ou les contrôleurs sur WiSM Cisco.
- Avec la version 4.2 du logiciel de contrôleur, tous les points d'accès légers Cisco prennent en charge 16 BSSID par radio et un total de 16 réseaux locaux sans fil par point d'accès. Dans les versions précédentes, ils prenaient en charge 8 BSSID par radio et un total de 8 LAN sans fil par point d'accès seulement. Quand un point d'accès converti s'associe à un contrôleur, seuls les LAN sans fil avec les ID de 1 à 16 sont diffusés au point d'accès.
- Les AP convertis au LWAPP doivent obtenir une adresse IP et détecter le WLC en utilisant DHCP, un système de noms de domaine (DNS), ou une diffusion de sous-réseau IP.
- Les AP convertis au LWAPP ne prennent pas en charge le LWAPP de couche 2.
- Les AP convertis au LWAPP fournissent un port de console inaltérable.
- L'outil de conversion de mise à niveau ajoute la clé de hachage du certificat auto-signé (SSC) à un seul des contrôleurs sur le WiSM Cisco. Après que la conversion a été complétée, ajoutez la clé de hachage du SSC au deuxième contrôleur du WiSM Cisco en copiant la clé du premier contrôleur sur le deuxième. Pour copier la clé de hachage du SSC, ouvrez la page AP Policies de l'interface graphique du contrôleur (**Security > AAA > AP Policies**), et copiez la clé de hachage du SSC de la colonne de clés de hachage SHA1 dans la liste d'autorisation des AP. Puis, dans l'interface graphique du deuxième contrôleur, ouvrez la même page et collez la clé de hachage dans le champ de clé de hachage SHA1 situé dans Add AP to Authorization List. Si vous disposez de plus d'un WiSM Cisco, utilisez le WCS pour diffuser la clé de hachage du SSC à tous les autres contrôleurs.

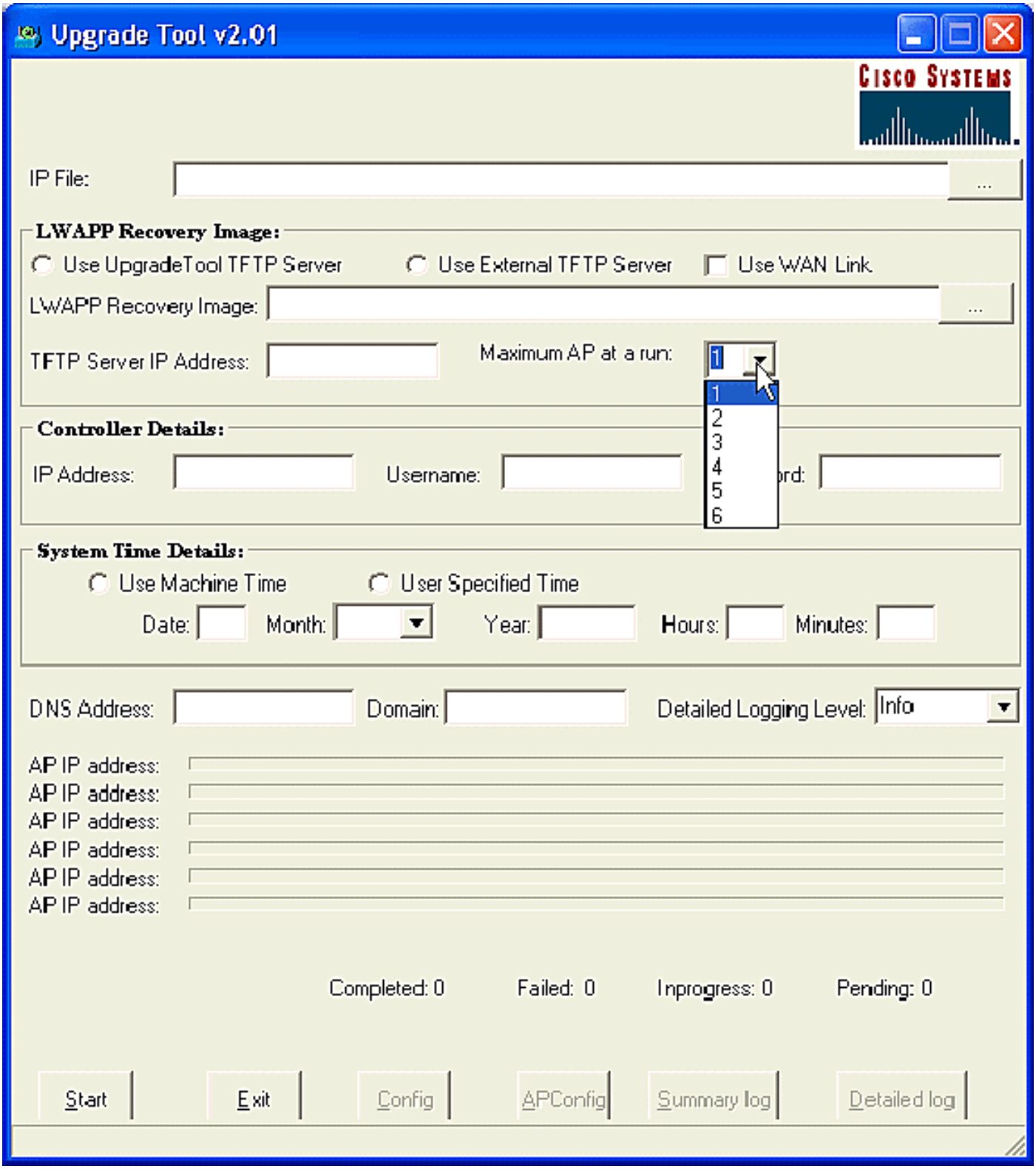
Référez-vous aux Notes de publication relatives aux points d'accès des gammes Cisco Aironet 1130AG, 1200, 1230AG, et 1240AG pour Cisco IOS version 12.3(7)JX pour plus de détails.

Q. J'ai converti mon point d'accès au mode léger, mais je dois le convertir à nouveau au mode autonome. Est-ce possible ?

A. Oui, vous pouvez convertir à nouveau au mode autonome les AP autonomes que vous avez convertis au mode léger. Suivez les étapes de la section Conversion d'un point d'accès léger de nouveau au mode autonome dans Mise à niveau des points d'accès Cisco Aironet autonomes au mode léger.

Q. Combien de points d'accès peuvent être convertis en même temps via l'outil de mise à niveau?

A. Avec la dernière version 2.01 de l'outil, vous pouvez mettre à niveau un maximum de six AP à la fois.



Q. J'ai converti mon AP au protocole d'AP léger (LWAPP), mais l'AP ne s'enregistre pas avec le contrôleur. J'obtiens le message « `LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP.` » D'où vient ce problème ?

A. Cette erreur signifie que les certificats numériques X.509 ne sont pas valides. Il se peut que vous ayez rencontré le bug Cisco ID CSCsd42296 (clients enregistrés uniquement). La solution de contournement pour ce problème est de réinitialiser les AP aux paramètres d'usine.

Une autre possibilité est que certificat auto-signé (SSC) n'est pas enregistré au niveau du WLC. L'ajout manuel du SSC au niveau du contrôleur peut être nécessaire. Référez-vous à la section

Ajout manuel d'un certificat auto-signé au contrôleur pour les AP convertis au LWAPP pour la procédure.

Q. Puis-je configurer un AP articulé autour du logiciel Cisco IOS AP comme pont de groupe de travail et l'associer avec des AP basés sur un protocole AP léger (LWAPP) ?

A. Vous pouvez configurer un point d'accès pour opérer comme pont de groupe de travail de sorte qu'il puisse fournir la connectivité sans fil à un point d'accès léger au nom des clients qui sont connectés via Ethernet au point d'accès de pont de groupe de travail. Quand vous configurez le point d'accès pour opérer comme pont de groupe de travail et pour se connecter à un réseau unifié Cisco, il peut fournir une connectivité sans fil aux clients câblés qui sont connectés par Ethernet au point d'accès de pont de groupe de travail. Par exemple, si vous devez fournir une connectivité sans fil pour un groupe de périphériques câblés, vous pouvez connecter les périphériques à un concentrateur ou à un commutateur, connecter le concentrateur ou le commutateur au port Ethernet du point d'accès, et configurer le point d'accès comme pont de groupe de travail.

The document Exemple de configuration de ponts de groupe de travail dans un réseau sans fil unifié Cisco propose un exemple de configuration.

Q. Un client sans fil peut-il faire de l'itinérance entre des AP LWAPP et des AP autonomes ?

A. Non, le roaming entre les LAP et les AP autonomes n'est PAS pris en charge. La raison est que, lors d'une connexion aux AP LWAPP, le trafic passe par un tunnel LWAPP. Puisqu'il n'y a aucun tunnel de mobilité entre le contrôleur LAN sans fil et les AP autonomes, l'itinérance ne fonctionne pas.

Q. Quelles options d'antenne sont disponibles avec les différents modèles de LAP de la gamme Cisco Aironet 1000 ?

A. Le boîtier du LAP de la gamme 1000 contient :

- Une antenne radio IEEE 802.11a ou 802.11b/g
- Quatre antennes internes à gain élevé (deux 802.11a et deux 802.11b/g)

Vous pouvez activer ou désactiver ces antennes indépendamment afin de créer une zone de couverture sectorielle de 180 degrés ou omnidirectionnelle de 360 degrés. Certains LAP de la gamme 1000 peuvent également utiliser des antennes externes. Les LAP de la gamme 1000 existent en trois modèles :

- LAP 1010
- LAP 1020
- LAP 1030

Les options d'antenne disponibles sont les suivantes :

- LAP 1010 :Quatre antennes internes à gain élevéAucun adaptateur d'antenne externe
- LAP 1020 :Quatre antennes internes à gain élevéUn adaptateur d'antenne externe de 5 GHzDeux adaptateurs d'antenne externe de 2,4 GHz

- LAP 1030 (LAP edge distant) :Quatre antennes internes à gain élevéUn adaptateur d'antenne externe de 5 GHzDeux adaptateurs d'antenne externe de 2,4 GHz

A. External-Antenna Model B. Internal-Antenna Model

Remarque : Les LAP de la gamme 1000 doivent utiliser les antennes internes ou externes fournies en usine afin d'éviter une violation des exigences de la FCC et d'éviter un vide de l'autorité de l'utilisateur pour faire fonctionner l'équipement.

Q. Quelles options de puissance sont disponibles pour les LAP de la gamme Cisco Aironet 1000 ?

A. Le LAP Aironet de la série 1000 peut être alimenté via une alimentation externe 110 à 220 VAC vers 48 VDC ou via des équipements power over Ethernet. L'alimentation externe (AIR-PWR-1000) se branche à une prise électrique sécurisée de 110 à 220 VAC. Le convertisseur produit la sortie 48 VDC nécessaire au LAP de la gamme 1000. La sortie du convertisseur alimente le LAP de la gamme 1000 par le côté via un connecteur 48 VDC.

Remarque : Vous pouvez commander l'alimentation externe AIR-PWR-1000 avec des cordons d'alimentation de prise électrique spécifiques à chaque pays. Contactez Cisco quand vous passez commande afin de recevoir le cordon secteur correct.

Q. Puis-je utiliser Telnet/SSH dans un point d'accès basé sur le LWAPP ?

A. Dans la version 5.0 et ultérieure du contrôleur LAN sans fil, le contrôleur prend en charge l'utilisation des protocoles Telnet ou Secure shell (SSH) pour dépanner les points d'accès légers. Vous pouvez employer ces protocoles afin de faciliter le débogage, particulièrement quand le point d'accès ne peut pas se connecter au contrôleur. Vous pouvez configurer la prise en charge

Telnet et SSH uniquement via le contrôleur CLI.

Afin de d'activer la connectivité Telnet ou SSH sur un point d'accès, utilisez la commande **config ap {telnet | ssh}**. Le point d'accès léger Cisco s'associe à ce contrôleur LAN sans fil Cisco pour toutes les opérations réseau et en cas d'une réinitialisation matérielle.

```
config ap {telnet | ssh} {enable | disable} Cisco_AP
```

Exemples

```
> config ap telnet enable cisco_ap1
> config ap telnet disable cisco_ap1
> config ap ssh enable cisco_ap2
> config ap ssh disable cisco_ap2
```

Q. Comment configurer l'ensemble des authentifiants pour des points d'accès. Quel est le nom d'utilisateur et le mot de passe par défaut dans la version 5.0 ?

A. Les points d'accès Cisco IOS sont livrés avec Cisco comme mot de passe d'activation par défaut. Ce mot de passe permet aux utilisateurs de se connecter en mode non-privilégié et exécuter les commandes d'affichage et de débogage, ce qui constitue une menace de sécurité. Le mot de passe d'activation par défaut doit être changé afin d'empêcher tout accès non autorisé et de permettre aux utilisateurs d'exécuter des commandes de configuration depuis le port de console du point d'accès.

Dans la version du logiciel de contrôleur antérieure à 5.0, vous pouvez configurer le mot de passe d'activation du point d'accès uniquement pour les points d'accès qui sont actuellement connectés au contrôleur. Dans la version 5.0 du logiciel de contrôleur, vous pouvez établir un nom d'utilisateur, un mot de passe et un mot de passe d'activation globaux dont tous les points d'accès héritent lorsqu'ils joignent le contrôleur. Ceci inclut tous les points d'accès qui sont actuellement joints au contrôleur et tous ceux qui se joindront à l'avenir. Si désiré, vous pouvez ignorer les authentifications globales et assigner un seul nom d'utilisateur, mot de passe, et mot de passe d'activation pour un point d'accès spécifique.

Pour plus d'informations sur la configuration des authentifications globales de l'AP, référez-vous à la section Configuration des authentifications globales pour les points d'accès.

Q. J'ai un contrôleur LAN sans fil (WLC) 2006 et un point d'accès (AP) 1242 avec la version de microprogramme 3.2.78.0. J'ai des problèmes avec les points d'accès qui s'y connectent et je reçois les messages d'erreur suivants : « lwapp_clinet_error ; pas de réponse en lecture(3). Lwapp_image_broc ; impossible d'ouvrir le fichier TAR »

A. Les points d'accès AP 1242 sont d'anciens points d'accès utilisant le protocole LWAPP (Lightweight Access Point Protocol). Une fois que vous les convertissez et essayez de les utiliser, ils essaient de rechercher le contrôleur afin de le joindre. Si les AP ne trouvent pas le contrôleur, ce type de message apparaît sur la console. Mais dans ce cas le contrôleur a la version 3.2.78.0 du microprogramme qui n'est pas compatible avec des AP mis à niveau. Vous devez avoir la version 3.2.116.21 du microprogramme afin de travailler avec des AP mis à niveau. Une fois que

le microprogramme du contrôleur est mis à niveau, ces AP joignent le contrôleur et se mettent à fonctionner.

Q. Les clients affichent une adresse MAC de 00:17:0f:37:65:c4 lorsqu'ils sont attachés à un point d'accès, mais le point d'accès affiche une adresse MAC radio de base de 00:17:0f:37:65:c0. Pourquoi le client affiche-t-il un MAC différent du point d'accès ? Y a-t-il un moyen de déterminer l'adresse MAC enregistrée par le périphérique si j'ai deux points d'accès avec des adresses MAC très proches ?

A. Si vous regardez un point d'accès en mode détail, vous pouvez voir qu'il a une adresse MAC sans fil de base et une adresse MAC FastEthernet. En outre, c'est l'adresse MAC sans fil de base qui change avec le WLAN. En réalité, le client voit le BSSID sous la forme d'une adresse MAC.

Q. Je dispose d'un réseau sans fil existant (AP autonomes) avec un point d'accès configuré comme répéteur. Ce réseau doit évoluer en réseau sans fil LWAPP. Les AP LWAPP peuvent-ils être utilisés comme répéteurs ?

A. Les points accès LWAPP doivent se connecter à un contrôleur, et ils ne supportent pas le mode de répétition puisqu'ils doivent tous avoir une certaine connectivité avec le contrôleur au préalable. Les AP autonomes Cisco peuvent être configurés comme répéteurs, mais en raison de la réduction de la bande passante réelle disponible aux clients finaux, les répéteurs ne sont pas la configuration la plus recommandée. N'importe quel modèle d'AP ou de LAP Cisco Aironet peut être utilisé en mode LWAPP ou autonome, mais cette modification nécessite de réimager le logiciel. Ceci est particulièrement complexe du mode autonome au mode LWAPP. Donc, directement, un AIR-LAP1232AG-A-K9 ne prend pas en charge le mode répéteur en configuration native. Il pourrait être chargé avec un logiciel autonome et être configuré pour prendre en charge le mode répéteur, mais cela impliquerait une modification du logiciel et une configuration distincte.

Q. Combien de points d'accès les contrôleurs réseau sans fil (WLC) peuvent-ils prendre en charge?

A. Le nombre d'AP pris en charge par WLC dépend du numéro de modèle :

- **2106 — Un WLC autonome qui prend en charge jusqu'à 6 AP avec 8 interfaces Fast Ethernet.**
- **4402 — Un WLC autonome qui prend en charge 12, 25, ou 50 AP.**
- **4404 — Un WLC autonome qui prend en charge 100 AP.**
- **5500** - Un WLC autonome qui prend en charge 12, 25, 50, 100 ou 250 points d'accès pour les services sans fil stratégiques de toute taille.
- **WLCM — Un module WLC qui est spécifiquement conçu pour la gamme de routeurs à services intégrés (ISR) Cisco.** Il est actuellement disponible en version 6, 8 ou 12 AP.
- **WS-C3750G — Un WLC qui prend en charge 25 ou 50 PA intégrant le commutateur Catalyst 3750.** Les connexions du fond de panier du WLC apparaissent en tant que ports Ethernet 2 Gb qui peuvent être configurés séparément comme joncteurs réseau dot1q pour amener la connexion au commutateur 3750. Les ports Gigabit peuvent être agrégés par liens pour fournir une seule connexion EtherChannel au 3750. Puisque le WLC est intégré directement, il a accès à toutes les fonctionnalités avancées de routage et de commutation disponibles sur les commutateurs 3750 empilables. Ce WLC est idéal pour les bureaux ou les bâtiments de taille moyenne. Le modèle « 50 AP » peut évoluer jusqu'à une capacité de 200 AP lorsque

quatre 3750 sont empilés ensemble comme commutateur virtuel.
- **WiSM — Un module WLC qui est conçu spécifiquement pour la gamme de commutateur Cisco Catalyst 6500.** Il prend en charge jusqu'à 300 AP par module. Selon la plate-forme 6500, plusieurs WISM peuvent être installés pour offrir une extensibilité significative. Le WiSM apparaît en tant que simple interface liaison agrégée sur le 6500 qui peut être configurée comme joncteur réseau dot1 pour amener la connexion dans le fond de panier du 6500. Ce module est idéal pour de grands bâtiments ou campus.

Q. Quel est le nombre maximum d'associations de clients qu'un point d'accès peut accepter?

A. Cela dépend des facteurs suivants :

- Les points d'accès IOS allégés et autonomes peuvent accepter un maximum différent d'associations de clients.
- Il pourrait y avoir une limite par radio et une limite globale par point d'accès.
- Matériel de point d'accès (les points d'accès de 16 Mo ont une limite inférieure à celle des points d'accès de 32 Mo et plus).

Pour plus de détails sur les limites d'association client, reportez-vous à la section « *Client Association Limits » du document «* Cisco Wireless LAN Controller Configuration Guide, Release 7.0 ».

Q. Le point d'accès 1252 prend-il en charge les passerelles?

A. Oui, le mode pont est pris en charge sur les AP de la gamme 1252.

Q. Le protocole LWAPP prend-il en charge les liaisons PPPoE (ordinateur-client vers serveur PPPoE)?

A. Non, l'infrastructure LWAPP ne prend pas en charge le PPPoE. La raison est que le PPPoE Ethertype est abandonné au niveau du contrôleur.

Q. Comment réinitialiser manuellement les LAP de la gamme Cisco Aironet 1000 ?

A. Vous pouvez réinitialiser les AP aux paramètres d'usine via le contrôleur LAN sans fil (WLC). Pour être réinitialisé, le LAP doit être enregistré par le WLC.

Procédez comme suit :

1. Depuis la GUI du WLC, cliquez sur **Wireless**. L'onglet Wireless permet d'accéder à la configuration du réseau sans fil de la solution WLAN Cisco.
2. Sélectionnez **Access Points > Cisco APs**, puis cliquez sur **Detail afin de d'accéder à la fenêtre de l'AP spécifique.**
3. Cliquez sur **Clear Config au bas de cette fenêtre.** Ceci efface la configuration du LAP et le réinitialise aux paramètre par défaut.

Afin de réinitialiser les LAP aux paramètres par défaut à laide de l'interface de ligne de commande (CLI), exécutez la commande **clear ap-config** ***ap-name*** de la CLI du WLC.

Q. Où trouver plus d'informations sur les LAP de la gamme Cisco Aironet 1000 ?

A. Reportez-vous au document « Cisco 1000 Series Lightweight Access Points – Q&A ». Le document apporte des réponses à beaucoup de questions relatives aux LAP de la série 1000.

Q. Quels équipements Cisco prennent en charge le mode Protocole d'AP léger (LWAPP) de couche 2 ?

A. Avec le protocole LWAPP, la couche 2 n'est pris en charge que sur ces appareils Cisco :

- Contrôleur de réseau local sans fil (WLC) de la gamme Cisco 4100
- WLC de la gamme Cisco 4400
- Gamme de LAP Cisco Aironet 1000

Q. J'ai appris que les AP Cisco utilisent une chaîne d'identifiant de classe de fournisseur (VCI) avec l'option DHCP 43 pour la détection de contrôleur. Quelle est la valeur de la chaîne VCI pour les LAP Cisco ?

A. Les points d'accès Cisco Aironet de la série 1000 utilisent un format de chaîne pour l'option DHCP 43, tandis que les autres points d'accès Aironet utilisent le format « type, longueur, valeur » (TLV) pour l'option DHCP 43. Vous devez programmer les serveurs DHCP pour renvoyer l'option sur la base de la chaîne DHCP VCI de l'AP (option DHCP 60). Ce tableau fournit les valeurs des chaînes VCI pour les différents LAP :

Access Point	Vendor Class Identifier (VCI)
Cisco Aironet 1000 series	Airespace.AP1200
Cisco Aironet 1100 series	Cisco AP c1100
Cisco Aironet 1130 series	Cisco AP c1130
Cisco Aironet 1200 series	Cisco AP c1200
Cisco Aironet 1240 series	Cisco AP c1240
Cisco Aironet 1300 series	Cisco AP c1300
Cisco Aironet 1500 series	Cisco AP c1500[1]
	Cisco AP.OAP1500[2]
	Cisco AP.LAP1505[3]
	Cisco AP.LAP1510[4]
	Airespace.AP1200[5]
Cisco 3201 Lightweight Access Point	Cisco AP C3201WMIC

Q. Quelle est l'importance des valeurs de bloc Type-Longueur-Valeur (TLV) en ce qui concerne l'option DHCP 43 ? Comment la valeur TLV est-elle calculée ?

A. L'option DHCP 43 peut être activée sur le serveur DHCP du routeur Cisco IOS en utilisant cette commande :

```
Option 43 hex <string>
```

La chaîne hexadécimale de cette commande est assemblé en enchaînant les valeurs TLV pour la sous-option de l'option 43.

Type + longueur + valeur

- **Le type correspond toujours au code 0xf1 de sous-option.**
- **La longueur est le nombre d'adresses IP de gestion du contrôleur multiplié par 4 en hex.**
- **La valeur est l'adresse IP du contrôleur énumérée séquentiellement en hex.**

Par exemple, supposez qu'il y a deux contrôleurs avec les adresses IP d'interface de gestion 10.126.126.2 et 10.127.127.2 :

- Le type est 0xf1.
- La longueur est 2 * 4 = 8 = 0x08.
- Les adresses IP se traduisent en 0a7e7e02 (10.126.126.2) et 0a7f7f02 (10.127.127.2).
- L'assemblage de la chaîne donne donc f1080a7e7e020a7f7f02. La commande IOS alors ajouté à l'étendue DHCP est la suivante :

  ```
  option 43 hex f1080a7e7e020a7f7f02
  ```

Q. Le contrôleur réseau sans fil prend-il en charge l'équilibrage de charge pour les points d'accès?

A. Oui vous pouvez faire l'équilibrage de charge d'un AP à partir d'un WLC. Référez-vous à la section FAQ de dépannage des contrôleur de LAN sans fil (WLC) pour plus d'informations.

Q. Comment configurer le basculement d'un contrôleur LAN sans fil (WLC) pour les LAP ?

A. Reportez-vous au document « WLAN Controller Failover for Lightweight Access Points Configuration Example » pour plus de détails sur la configuration du basculement du contrôleur.

Q. Comment désactiver le bouton de réinitialisation des AP après une conversion du mode autonome en mode léger ?

A. Vous pouvez désactiver le bouton de réinitialisation des AP que vous avez convertis en mode léger. Le bouton de réinitialisation est étiqueté « MODE » sur l'extérieur de l'AP. Utilisez cette commande afin de désactiver ou activer le bouton de réinitialisation sur un ou tout les AP convertis qui sont associés à un contrôleur :

```
config ap reset-button {enable | disable} {ap-name | all}
```

Le bouton de réinitialisation des AP convertis est activé par défaut.

Q. Est-il possible de connecter un AP compatible avec le protocole d'AP léger (LWAPP) via une liaison WAN issue du contrôleur LAN sans fil (WLC) ? Si c'est le

cas, comment cela fonctionne-t-il ?

A. Oui, certains LAP prennent en charge la fonctionnalité appelée Remote-Edge AP (REP). Avec cette fonctionnalité, il est possible d'avoir un LAP en liaison WAN issue du WLC auquel il est connecté. Le mode REAP permet à un LAP de résider via une liaison WAN tout en étant capable de communiquer avec le WLC et d'agir comme un LAP normal. Référez-vous à la section Exemple de configuration de Remote-Edge AP (REAP) avec des AP légers et des contrôleurs de réseau local sans fil (WLC) pour un exemple détaillé de cette configuration.

Remarque : le mode REAP n'est pris en charge que sur les LAP Cisco Aironet 1030 à ce stade. La fonctionnalité REAP sera proposée sur un gamme plus large de LAP à l'avenir.

Q. Les restrictions WAN sont-elles toujours les mêmes sur les AP en mode surveillance que sur les AP classiques et les AP H-REAP ? Plus précisément, avons-nous besoin d'un RTD de 100 ms entre le contrôleur et un AP en mode surveillance ?

A. Non, un AP en mode surveillance n'a pas la restriction de 100 ms parce qu'il n'y a aucune association client, qui est la raison de la restriction. La limitation de latence de 100 ms a été créée à partir d'exigences d'autorisation de client diverses, et souvent rigoureuses. C'est pourquoi les AP en mode local et H-REAP ont des limitations de latence identiques. Évidemment, les AP en mode surveillance n'ont pas les mêmes limitations de client.

Q. Mon WLC est en version 3.2. Il est configuré pour le protocole de point d'accès léger (LWAPP) de couche 3. Le MTU pour le réseau entre ce WLC et mon point d'accès léger (LAP) est configuré à 900 octets. Mon AP LWAPP ne parvient pas à joindre ce WLC. Quelle peut être la raison de ceci ?

A. Le MTU configuré dans votre scénario est de 900 octets. Mais une requête d'enregistrement LWAPP fait plus de 1 500 octets. Ainsi, ici le LWAPP nécessite un fragment de la requête d'enregistrement LWAPP. La logique pour tous les AP LWAPP est que la taille du premier fragment est de 1500 octets (IP et en-tête UDP) et celle du second fragment est de 54 octets (IP et en-tête UDP). Si le réseau entre les AP LWAPP le WLC a une taille de MTU inférieure à 1500 (VPN, GRE, MPLS, etc.) comme dans votre cas, le WLC ne peut pas traiter la requête d'enregistrement LWAPP. Par conséquent, le LWAPP ne peut pas joindre le contrôleur.

Mettez à niveau votre contrôleur à la version 4.0 afin de régler ce problème. Cette version est capable de traiter des fragments de couche 3. Référez-vous à l'ID bogue Cisco CSCsd94967 (clients enregistrés uniquement) pour plus d'informations sur cette question.

Q. J'ai acquis un WLC provenant de Singapour. Mon intention était connecter un bureau distant à ce WLC (REAP) pour la connectivité sans fil. J'ai des bureaux dans d'autres pays. Cependant, je reçois des messages d'erreur de domaine réglementaire du WLC de Singapour. Y a-t-il un moyen de forcer le WLC à accepter des points d'accès (AP) avec différents domaines réglementaires ? Le message d'erreur reçu est le suivant : « `AP 'AP_NAME' is unable to associate. The Regulatory Domain configured on it '-R' does not match the Controller 'A.B.C.D' country code 'SG - Singapore` »

A. Le WLC ne prend en charge qu'un seul domaine réglementaire. Par conséquent, un WLC qui utilise le domaine réglementaire A peut uniquement être utilisé avec les AP qui utilisent le

domaine réglementaire A (etc.). Dans ce cas, le WLC est configuré sur SG pour Singapour, afin de prendre uniquement en charge les AP du domaine réglementaire de Singapour.

Quand vous achetez des AP et WLC, assurez-vous qu'ils partagent le même domaine réglementaire. C'est la condition nécessaire pour que l'AP s'enregistre auprès du WLC.

Prise en charge de plusieurs codes de pays — Avec un WLC en version 4.1.171.0 ou ultérieure, la prise en charge de plusieurs codes de pays est possible. Avec la version 4.1.171.0 ou ultérieure, vous pouvez configurer jusqu'à 20 codes de pays par contrôleur. La prise en charge de plusieurs codes de pays vous permet de gérer les points d'accès dans plusieurs pays depuis un seul contrôleur. Cette fonctionnalité n'est pas prise en charge pour une utilisation avec les points d'accès maillés Cisco Aironet.

Q. Quels sont les différents modes dans lesquels un point d'accès léger (LAP) peut fonctionner ?

A. Un LAP peut fonctionner dans l'un des modes suivants :

- **Mode local — C'est le mode de fonctionnement par défaut.** Quand un LAP est en mode local, il transmet sur le canal normalement assigné. Cependant, l'AP surveille également tous les autres canaux de la bande pendant une période de 180 secondes pour scanner chacun des autres canaux pendant 60 ms pendant le temps de non-transmission. Au cours de ce délais, l'AP exécute des mesures de bruit de fond et d'interférence et réalise des scans à la recherche d'événements IDS.
- **Mode REAP — Le mode Affilez Remote Edge Access Point (REAP) permet un LAP de résider en liaison WAN link tout en étant capable de communiquer avec le WLC et d'agir comme un LAP normal.** Le mode REAP est uniquement pris en charge par les LAP Cisco Aironet 1030.
- **Mode H-REAP — H-REAP est une solution sans fil pour des déploiements de succursale et de bureau distant.** H-REAP permet aux clients de configurer et contrôler les points d'accès (AP) d'une succursale ou d'un bureau distant du bureau principal via une liaison WAN link sans avoir à 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.
- **Mode surveillance — Le mode surveillance est une fonctionnalité conçue pour laisser les AP adaptés au LWAPP spécifiés s'exclure de la gestion du trafic de données entre les clients et l'infrastructure.** Ils agissent à la place en tant que détecteurs dédiés pour les services de géolocalisation (LBS), la détection de point d'accès non autorisés et la détection des intrusions (IDS). Quand les AP sont en mode surveillance, ils ne peuvent pas servir les clients et passer en continue par tous les canaux configurés en écoutant chaque canal pendant approximativement 60 ms.**Remarque :** à partir de la version 5.0 du contrôleur, les LWAPP peuvent également être configurés en mode LOMM (Location Optimized Monitor Mode), qui optimise la surveillance et le calcul de l'emplacement des balises RFID. Pour plus d'informations sur ce mode, référez-vous à la version 5.0 du logiciel de réseau sans fil unifié.**Remarque :** Avec la version 5.2 du contrôleur, la section **Mode moniteur optimisé pour l'emplacement (LOMM)** a été renommée **Optimisation du suivi**, et la zone de liste déroulante **LOMM activé** a été renommée **Activer l'optimisation du suivi**.**Remarque :** Pour plus d'informations sur la configuration de l'optimisation du suivi, consultez la section Optimisation

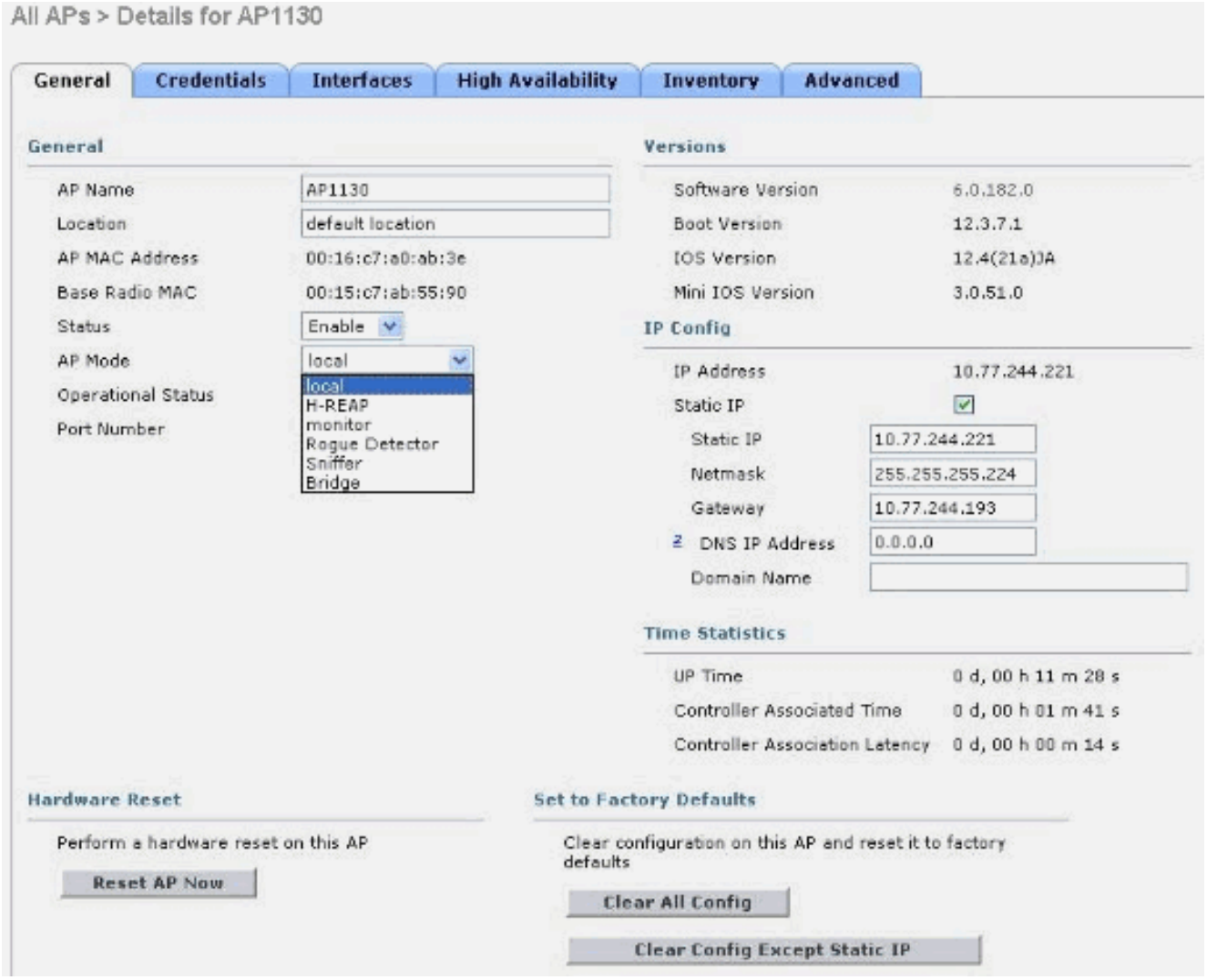
du suivi RFID sur les points d'accès.

- **Mode de détection de serveurs non autorisés — Les LAP fonctionnant en mode de détection de serveurs non autorisés surveillent les AP non autorisés.** Ils ne transmettent ni ne contiennent d'AP non autorisés. L'idée est que le détecteur de serveurs non autorisés doit pouvoir surveiller tous les VLAN du réseau puisque des AP non autorisés peuvent être connectés à n'importe quel VLAN du réseau (nous le connectons donc à un port de liaison). Le commutateur envoie toutes les listes d'adresses de MAC client/AP non autorisé au détecteur de serveurs non autorisés (RD). Le RD les transfère ensuite au WLC afin de comparer avec les MAC des clients que les AP WLC ont détectés sans fil. Si les MAC correspondent, alors le WLC sait que l'AP non autorisé auquel ces clients sont connectés se trouve sur le réseau câblé.
- **Mode renifleur — Un LWAPP en mode renifleur fonctionne comme renifleur ; il détecte et envoie les paquets sur un canal spécifique vers une machine distante qui exécute Airopeek.** Ces paquets contiennent des informations sur l'horodateur, la puissance du signal, la taille de paquet, etc. La caractéristique de renifleur peut être activée seulement si vous exécutez Airopeek, qui est un logiciel analyseur réseau tiers qui prend en charge le décodage des paquets de données.
- **Mode pont - Le mode pont est utilisé quand les points d'accès sont configurés dans un environnement maillé et sont utilisés comme des ponts se reliant mutuellement.**

Q. Comment changer le mode sur un point d'accès léger ?

A. Pour changer le mode d’un point d’accès allégé, suivez ces étapes.

1. Dans la GUI WLC, sélectionnez **Wireless > Access Points > All APs**, puis sélectionnez dans la liste des AP enregistrés l'AP pour lequel le mode doit être changé.
2. La page **All APs > Details for AP s'affiche.** Dans l'**onglet General de cette page, sélectionnez le mode AP dans le menu déroulant, comme**
   illustré :



Q. J'ai nouvellement installé les points d'accès LAP-1131AG qui ont été amorcés à un contrôleur particulier. La version de mon contrôleur est 4.0.155.5. Quand je les lance avec le même contrôleur LAN sans fil (WLC) auquel ils s'amorcent, ils deviennent par la suite vert clair. Selon la documentation, si le voyant d'état est vert clair, cela signifie qu'ils sont connectés au WLC. Mais je n'ai pas trouvé ce point d'accès dans la liste des points d'accès du WLC. Pourquoi cela ? Le protocole de point d'accès léger (LWAPP) s'est-il associé ?

A. Si le point d'accès s'amorce au WLC à une couche 3 WLC mais ne peut pas obtenir d'adresse IP pendant le démarrage, alors la diode d'état du WLC devient vert clair et n'exécute pas la séquence de recherche et de redémarrage avant d'obtenir une adresse IP du DHCP.

Ainsi, dans de tels scénarios, la couleur verte de la diode d'état n'indique pas que le LWAPP est inscrit au contrôleur. Une fois que les points d'accès peuvent obtenir leurs adresses DHCP, ils recherchent le WLC et s'ils ne le trouvent pas, redémarrent et procèdent comme prévu. Un bogue est associé à ceci.

Référez-vous à l'ID du bogue Cisco CSCsf10580 (clients inscrits seulement) pour plus d'informations.

Q. Qu’indiquent les DEL sur le point d’accès allégé?

A. Ceci est un lien vers une courte vidéo qui explique comment interpréter les DEL d'un point d'accès allégé 1130AG :

Interpreting LAP LEDs – LAP1130

Q. Quelle est la différence entre les points d'accès de toit (RAP) et les points d'accès de pôle (PAP) comme modes de points d'accès légers maillés (MAP) ?

A. Ce sont les modes que les MAP extérieurs peuvent utiliser en tant qu'élément du réseau maillé. Cette solution de réseau maillé, qui fait partie de la solution de réseau sans fil unifiée Cisco, permet à deux MAP légers Aironet Cisco ou plus de communiquer entre eux au-dessus via un ou plusieurs sauts sans fils pour rejoindre des LAN multiples ou pour étendre la couverture 802.11b sans fil.

Ces points d'accès sont utilisés en tant qu'élément du réseau maillé et fonctionnent en deux modes :

1. RAP
2. PAP

RAP — Les MAP Cisco qui fonctionnent en mode RAP sont le nœud parent à tout pont ou réseau maillé, et connectent un pont ou un réseau maillé au réseau câblé. Par conséquent, il peut seulement y avoir un RAP pour tout segment de pont ou de réseau maillé. Dans un réseau maillé, les MAP Cisco sont configurés, surveillés et actionnés à partir et par tout contrôleur WLAN (WLC) Cisco déployé. N'importe quel MAP connecté par câble au WLC endosse le rôle du RAP. Ce RAP utilise l'interface sans fil pour communiquer avec les PAP voisins.

PAP — Les MAP Cisco qui fonctionnent en mode PAP ne sont pas connecté à un WLC par un câble. Ils peuvent être des clients d'assistance complètement sans fil qui communiquent avec d'autres PAP ou RAP, ou ils peuvent être utilisés pour se connecter aux périphériques ou à un réseau câblé. Le port Ethernet est désactivé par défaut pour des raisons de sécurité, mais vous devez l'activer pour les PAP.

Référez-vous à la section Configuration mains libres du guide de déploiement de solutions de réseau maillé de Cisco pour plus d'informations sur la façon dont un MAP endosse le rôle du RAP et du PAP.

Q. Comment interprétez-vous le diagramme de rayonnement des antennes de points d'accès légers (LAP) série 1000 ?

A. Les diagrammes d'azimut sont généralement orientés selon l'orientation normale de fonctionnement de l'appareil ou de l'antenne (verticale, sommet vers le haut, au centre pour les omnidirectionnels; horizontal, montage au centre, direction en avant vers "0" sur le diagramme). Le côté A est très probablement en avant et représenté au repère 0 pour l'azimut, et au repère 90 pour l'altitude. Le côté B Est représenté au repère 180 pour l'azimut, et 270 pour l'altitude. Ce diagramme ne change pas dans l'espace libre si l'unité est inversée. Mais les surfaces immédiates peuvent entraîner la réflexion/l'absorbtion et peuvent modifier le diagramme. Les objets métalliques à proximité des radiateurs (dans un rayon d'environ 2 longueurs d'onde) peuvent également déformer le motif de manière significative. Le guide de référence des antennes Aironet de Cisco contient de plus amples informations. Les antennes de la série 1000 sont expliquées dans la dernière section du document.

Q. Pouvons-nous choisir les AP reliés à un contrôleur ? Je vois la page SECURITY/AAA/AP Policies, depuis laquelle vous pouvez autoriser les AP avec le AAA ou le certificat. Je suis en mesure d'ajouter un AP dans Authorization List, mais cette opération restreint-elle seulement mon Authorization List d'AP à rejoindre le contrôleur ?

A. Non, les contrôleurs traitent les AP au fur et à mesure. Vous pouvez probablement jouer avec les champs primaires, secondaires et tertiaires pour augmenter les chances d'obtenir la connexion AP souhaitée.

Q. Avec LWAPP, est-il possible de déterminer les SSID d'un AP a sur une base individuelle ? Quelle est la marche à suivre pour faire en sorte que des AP spécifiques dans une zone utilisent un même SSID, et que tous les autres utilisent un autre ensemble de SSID ?

A. Avec l'option prioritaire WLAN, vous pouvez choisir quels sont les SSID proposés par un AP. Les contrôleurs prennent seulement en charge jusqu'à 16 SSID chacun, ainsi vous pouvez seulement choisir parmi les 16 supportés. Ceci est fait sur AP par AP.

Q. Quand j'active certaines commandes LWAPP sur mon LAP, j'obtiens une erreur qui indique que la commande est désactivée. Pourquoi cela ?

```
AccessPoint#clear lwapp ap controller ip address
ERROR!!! Command is disabled.
```

A. Une fois que votre AP a rejoint un contrôleur avec succès, les commandes LWAPP sont désactivées. Afin d'activer des commandes LWAPP de nouveau, vous devez définir l'identifiant/le mot de passe de l'AP depuis le CLI du contrôleur avec la commande **config ap username <name> password <pwd> <cisco-ap>/all.** Une fois que cela est fait, vous pouvez exécuter la commande **clear lwapp private-config dans le CLI de l'AP pour pouvoir reprendre manuellement les commandes de configuration LWAPP de l'AP.**

Remarque : Si vous exécutez WLC version 5.0 et ultérieure, utilisez cette commande pour définir le nom d'utilisateur et le mot de passe sur l'AP :

```
config ap mgmtuser add username AP_username password AP_password secret secret {all | Cisco_AP}
```

Q. Quand deux AP sont sur le même canal et peuvent se voir, quelles sont les implications (pour le débit d'itinérance, etc.) sur l'utilisation de quatre canaux au lieu de trois ? Comment les AP et les clients réagissent-ils dans une telle situation ?

A. Que les AP soient sur le même canal ou pas, cela n'affecte pas particulièrement l'itinérance client. Ce qui importe, c'est une superposition suffisante de cellules de façon que les clients puissent opérer des transitions fluides à partir de la zone de couverture d'un AP à l'autre. L'intention de passer d'une conception à trois canaux à une conception à quatre canaux est d'augmenter la flexibilité de la conception (en raison du canal « supplémentaires »). Cette approche est limitée parce que, alors que vous ajoutez à la flexibilité de déploiement (puisque

vous disposez d'un autre canal), vous augmentez en fait l'interférence due à l'utilisation d'un même canal. Ce que vous pourriez gagner en flexibilité de conception avec l'approche à quatre canaux, vous le perdez en interférence due à l'utilisation d'un même canal. Conduite à tenir : ne pas utiliser de conception à quatre canaux.

Q. Pouvons-nous contrôler l'itinérance client ? Pouvons-nous laisser une itinérance client se fonder uniquement sur la puissance du signal AP par AP et pour tous les adaptateurs client ?

A. Aujourd'hui, l'itinérance est toujours une fonction du client, et n'est pas mise en application différemment d'un client à un autre. L'itinérance dirigée fait partie de CCX, mais c'est une option qui n'est pas utilisée aujourd'hui.

Q. Existe-t-il des conditions ou des recommandations spécifiques pour un lien WAN qui est mis en application entre un AP REAP/HREAP au niveau du site distant et le WLC au niveau du site principal ?

A. Il s'agit de quelques-uns des facteurs principaux à prendre en compte pour le lien WAN :

- Assurez-vous que la bande passante du lien WAN est d'au moins 128 kbps.
- Assurez-vous que le temps d'attente ou le temps de transmission aller et retour entre les deux sites à travers le lien WAN n'est pas supérieur à 300 ms, parce qu'un tel délai peut causer des problèmes d'authentification au client, particulièrement quand l'authentification centrale est activée.

Q. J'ai fait arrêter un réseau pendant quelques heures, en raison de quoi les LAP ont perdu la communication avec les WLC. Une fois le réseau revenu, les LAP ont pris l'adresse IP du serveur DHCP, même si ces AP étaient configurés avec une adresse IP statique. Dans « `show ap config general <ap-name>` », elle s'affiche en tant que « `Fallback IP Address` ». Que se passe-t-il ?

A. Le LAP essaie de s'associer avec le WLC jusqu'à 20 fois avec les messages de détection LWAPP. S'il n'arrive pas à se connecter, il essaie d'obtenir une nouvelle adresse IP via DHCP. Si le LAP obtient une adresse IP du serveur DHCP, cette adresse IP est l'adresse active, et l'adresse IP statiquement assignée est utilisée comme adresse de secours. L'idée derrière ceci est qu'au cas où les LAP sont déplacés vers un VLAN différent (par exemple, vers un autre bâtiment), ils peuvent récupérer une adresse IP et rejoindre un WLC. Ce comportement est expliqué dans le bogue CSCse66714. Vous devez mettre à niveau le WLC à la version logicielle 4.0.206.0.

Q. Est-il obligatoire de configurer un nom de groupe de ponts pour un réseau maillé ?

A. Un nom de groupe de ponts (BGN) peut être utilisé pour regrouper logiquement les AP dans le réseau maillé. Bien que par défaut, les AP disposent d'un BGN avec une valeur nulle pour permettre l'association, nous vous recommandons de définir un BGN. Vous pouvez effectuer ce changement de configuration via le CLI ou la GUI avec cette commande :

```
config ap bridgegroupname set Bridge Group Name Cisco AP
```

Remarque : les BGN peuvent comporter jusqu'à dix caractères. Si vous entrez plus de 10 caractères dans le champ BGN sur la page de configuration du point d'accès maillé de la GUI du contrôleur, un message d'erreur s'affiche. Une erreur apparaît également quand vous configurez ce paramètre par la commande CLI **config ap bridgegroupname set groupname Cisco_MAP ou WCS (CSCsk64812).**

Quand vous configurez BGN sur un réseau fonctionnant en permanence, assurez-vous que vous configurez depuis le MAP le plus lointain en remontant vers le RAP. C'est très important parce que vous pouvez rendre orphelin un MAP enfant qui ne peut pas s'associer avec un parent, qui peut avoir un BGN mis à jour. Utilisez des BGN différents pour les différentes parties du groupe logique de votre réseau. C'est utile dans les situations où vous disposez de RAP au sein d'une même zone RF et vous voulez conserver les segments de votre réseau maillé séparés.

Si vous voulez ajouter un nouvel AP à un réseau fonctionnant en permanence, vous devez préconfigurer le BGN sur le nouvel AP. Si vous constituez un réseau maillé avec de tout nouveaux AP, le BGN est pré-établi dans les AP à une valeur NULL. Les AP s'associent à un nouveau réseau avec cette valeur par défaut du BGN. Vous pouvez vérifier le BGN d'un AP avec cette commande :

```
show ap config general Cisco AP
```

Q. Que se passe-t-il si le BGN n'est pas configuré correctement ?

A. Si l'AP est incorrectement doté d'un bridgegroupname autre que celui pour lequel on le destine, en fonction de la conception du réseau, cet AP peut ou non rechercher et atteindre le bon secteur ou arbre. S'il ne peut pas atteindre un secteur compatible, il peut devenir orphelin. Afin de récupérer ce type d'AP orphelin, le concept de bridgegroupname par défaut a été introduit. L'idée de base est qu'un AP qui ne peut pas se connecter à un autre AP avec son bridgegroupname configuré, essaie de se connecter avec le bridgegroupname par défaut.

C'est l'algorithme utilisé pour la détection de cet état orphelin et la reprise :

1. Balayez passivement et recherchez tous les nœuds voisins, indépendamment de leur bridgegroupname.
2. L'AP essaie de se connecter à ses voisins qui sont détectés avec leur propre bridgegroupname par le protocole AWPP (Adaptive Wireless Path Protocol).
3. Si l'étape 2 échoue, essayez d'établir une connexion avec le bridgegroupname par défaut avec AWPP.
4. Pour chaque échec de tentative de l'étape 3, mettez le voisin sur la liste d'exclusion et essayez de connecter le meilleur voisin disponible.
5. Si l'AP ne se connecte pas avec tous les voisins dans l'étape 4, redémarrez l'AP.
6. Si connecté avec le bridgegroupname par défaut pendant 30 minutes, rebalayez tous les canaux et essayez d'établir une connexion avec le bridgegroupname correct.

Remarque : Lorsqu'un point d'accès est en mesure de se connecter avec le pont par défaut bridgegroupname, le noeud parent signale le point d'accès en tant qu'entrée enfant/noeud/voisin par défaut sur le contrôleur WLAN, de sorte qu'un administrateur réseau soit conscient du point d'accès échoué. Un tel AP ne peut accepter aucun client ou autres nœuds maillés en tant que ses enfants, ni transmettre de trafic de données.

Q. Un LAP 1030 peut-il se lier avec un autre modèle de pont ? Un LAP 1020 peut-il également supporter un pont ?

A. Le modèle LAP 1020 ne supporte aucun pont. Le LAP 1030 supporte le pont (un saut) vers un autre LAP 1030 mais pas vers un BR1310, BR1400 ou LAP 1500 actuellement.

Q. Est-il possible de configurer un pont sans fil entre deux AP LAP ? Je voudrais qu'une radio de mes LAP sans fil exécute un pont vers les LAP racine câblés (LAP connecté à un WLC). Est-ce possible ?

A. Non. Ceci ne peut pas être fait sur les AP LAP. Les AP maillés peuvent exécuter un pont point à point de base pont dans un réseau sans fil unifié Cisco. Le seul autre pont possible se fait par des AP IOS en mode WGB (pont de groupe de travail). Ces AP IOS agissent comme des clients (avec des périphériques câblés derrière eux) d'un AP LAP. Mais les clients sans fil ne peuvent pas se connecter à ces AP IOS.

Q. Je dispose d'un LAP 1131, et ce point d'accès est enregistré avec succès aux contrôleurs de réseau local sans fil. Quand je connecte ce point d'accès sans injecteur de courant, les radios sont activées (l'état du voyant est vert), mais quand je connecte cet AP avec l'injecteur de courant, les radios sont désactivées (l'état du voyant est orange). Comment puis-je résoudre ce problème ?

A. Ce problème peut être dû à une configuration inexacte des paramètres Power over Ethernet (POE) ; pour résoudre ce problème, effectuez les étapes suivantes :

1. Cliquez sur **Wireless afin d'accéder à ces paramètres.**
2. Cliquez sur le lien **Detail du point d'accès concerné.** Les nouveaux paramètres apparaissent sur la page All APs > Details dans les paramètres POE.
3. Sur la page APs > Details du point d'accès pour les paramètres POE, cliquez sur **Power Injector State**, et sélectionnez **Installed**.
4. Vérifiez la case à cocher pour activer Power Injector State pour le point d'accès. Ce paramètre est requis si le commutateur raccordé ne prend pas en charge l'IPM et qu'un injecteur de courant est utilisé. Ce paramètre n'est pas requis si le commutateur raccordé prend en charge l'IPM.

Q. Dans des AP autonomes, le transfert de paquets sécurisé public (PSPF) est utilisé pour éviter que des périphériques clients associés à cet AP ne partagent par erreur des fichiers avec d'autres périphériques clients sur le réseau sans fil. Y a-t-il une fonctionnalité équivalente dans les AP légers ?

A. La caractéristique ou le mode qui remplit cette fonction de PSPF dans l'architecture légère s'appelle le mode de blocage d'homologue-à-homologue. Le mode de blocage d'homologue-à-homologue est disponible avec les contrôleurs qui gèrent le LAP.

Si ce mode est désactivé sur le contrôleur (qui est la configuration par défaut), il permet aux clients sans fil de communiquer entre eux via le contrôleur. Si mode est activé, il bloque la communication entre les clients par le contrôleur.

Cela fonctionne seulement parmi les AP qui se sont joints au même contrôleur. Une fois activé, ce mode n'empêche pas les clients sans fil qui se terminent sur un contrôleur d'être capables d'accéder aux clients sans fil se terminant sur un contrôleur différent, même dans le même groupe de mobilité.

Q. Un AP LAP peut-il traiter les messages SNMP comme un AP IOS ?

A. Les AP LAP ne peuvent pas traiter les messages SNMP seuls. Afin de traiter les messages SNMP, vous devez configurer la communauté SNMP sur le WLC auquel le LAP est enregistré. Toute l'information AP est gérée par le WLC.

Informations connexes

- Dépannage du contrôleur LAN sans fil (WLC) - FAQ
- Cisco Wireless LAN Controller Modules
- Cisco Wireless LAN Controller (WLC) FAQ
- Guide de configuration du contrôleur LAN sans fil Cisco, version 3.2
- Exemple de configuration de base d'un contrôleur LAN sans fil et d'un point d'accès léger
- Support et documentation techniques - Cisco Systems