Contrôleur de réseau local sans fil (WLC) - Forum Aux Questions

Contenu

Introduction

Ce document fournit des informations sur le les questions les plus souvent posées (FAQ) au sujet du contrôleur de réseau local Cisco (Wireless LAN Controller ou WLC).

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

FAQ générales

Q. Qu'est-ce qu'un contrôleur LAN sans fil ?

A. Les réseaux Sans fil sont devenus une nécessité aujourd'hui. Beaucoup d'environnements d'entreprise exigent le déploiement de réseaux sans fil à grande échelle. Cisco est à l'origine du concept de la solution de réseau sans fil unifié Cisco (Cisco Unified Wireless Network, ou CUWN), qui facilite la gestion de tels déploiements à grande échelle. WLC est un périphérique qui joue un rôle central dans le CUWN. Les rôles traditionnels des points d'accès, tels que l'association ou l'authentification des clients sans fil, sont assumés par le WLC. Les points d'accès, appelés « points d'accès légers Cisco Aironet® » (Lightweight Acess Points, ou LAP) dans l'environnement unifié, s'enregistrent eux-mêmes auprès d'un WLC et canalisent tous les paquets de gestion et de données vers les WLC, qui les commutent entre les clients sans fil et la partie câblée du réseau. Toutes les configurations sont faites sur le WLC. Les LAP téléchargent toute la configuration des WLC et agissent en tant qu'interface sans fil auprès des clients. Pour plus d'informations sur la façon dont un LAP s'enregistre auprès d'un WLC, référez-vous au document Enregistrement d'un point d'accès léger Cisco Aironet® (LAP) auprès d'un contrôleur de LAN sans fil (WLC).

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. Y a-t-il des directives pour l'utilisation de CAPWAP ?

A. Suivez ces directives quand vous utilisez CAPWAP :

- Si votre pare-feu est actuellement configuré pour autoriser le trafic seulement à partir des points d'accès qui utilisent LWAPP, vous devez changer les règles du pare-feu pour autoriser le trafic depuis les points d'accès qui utilisent CAPWAP.
- Assurez-vous que les ports UDP CAPWAP 5246 et 5247 (semblables aux ports UDP LWAPP 12222 et 12223) sont activés et ne sont pas bloqués par un équipement intermédiaire qui pourrait empêcher un point d'accès de joindre le contrôleur.
- Si les listes de contrôle d'accès (ACL) sont dans le chemin de contrôle entre le contrôleur et ses points d'accès, vous devez ouvrir de nouveaux ports de protocole pour empêcher les points d'accès de devenir orphelins.

Les points d'accès emploient un port source UDP aléatoire pour atteindre ces ports de destination sur le contrôleur. Dans la version de logiciel 5.2 du contrôleur, LWAPP a été supprimé et remplacé par CAPWAP, mais si vous avez un nouveau point d'accès prêts à l'emploi, il pourrait essayer d'utiliser LWAPP pour entrer en contact avec le contrôleur avant qu'il télécharge l'image CAPWAP du contrôleur. Une fois que le point d'accès télécharge l'image CAPWAP du contrôleur, il emploie seulement CAPWAP pour communiquer avec le contrôleur.

Note: Après 60 secondes d'essai pour joindre un contrôleur avec CAPWAP, le point d'accès recommence à utiliser LWAPP. S'il ne peut pas trouver un contrôleur utilisant LWAPP dans les 60 secondes, il essaye de nouveau de joindre un contrôleur utilisant CAPWAP. Le point d'accès répète ce cycle de la commutation de CAPWAP à LWAPP et vice-versa toutes les 60 secondes jusqu'à ce qu'il joigne un contrôleur.

Un point d'accès avec l'image de reprise LWAPP (un point d'accès converti du mode autonome ou un point d'accès prêt à l'emploi) utilise seulement LWAPP pour essayer de joindre un contrôleur avant de télécharger l'image CAPWAP du contrôleur.

Q. Comment est-ce que je configure mon WLC pour le fonctionnement de base ?

A. Afin de configurer le WLC pour le fonctionnement de base, référez-vous à l'exemple Sans fil de contrôleur LAN et de configuration de base de point d'accès léger.

Q. Quelles sont les diverses options disponibles pour accéder au WLC ?

A. Voici la liste des options disponibles pour accéder au WLC :

- Accès à l'interface graphique GUI avec HTTP ou HTTPS
- Accès à la CLI avec Telnet, SSH ou accès à la console
- Accès par le port de service

Pour plus d'informations sur la façon d'activer ces modes, référez-vous à la section Utilisation du navigateur Web et des interfaces CLI du Guide de configuration du contrôleur LAN sans fil Cisco, version 5.1. Habituellement, l'adresse IP de l'interface de gestion est utilisée pour l'accès à la GUI et à la CLI. Les clients sans fil peuvent accéder au WLC seulement quand l'option **Enable Controller Management to be accessible from Wireless Clients** est cochée. Afin d'activer cette option, cliquez sur le menu **Management** du WLC et cliquez sur **Mgmt via Wireless** côté gauche. L'accès à WLC peut également se faire avec une de ses adresses IP d'interface dynamique. Employez la commande **config network mgmt-via-dynamic-interface** pour activer cette fonctionnalité. Les ordinateurs câblés ne peuvent avoir que l'accès CLI avec l'interface dynamique du WLC. Les clients sans fil ont l'accès CLI et GUI avec l'interface dynamique.

Q. Comment utiliser le port de console USB sur le contrôleur de réseau local sans fil de la gamme Cisco 5500 ?

A. Le port de console USB sur les contrôleurs de la gamme 5500 se connecte directement au connecteur USB d'un PC à l'aide d'un câble USB type A 5 broches à mini USB type B.

Note: Le connecteur mini type B à 4 broches est facilement confondu avec le connecteur mini type B à 5 broches. Ils ne sont pas compatibles. Seul le connecteur mini type B à 5 broches peut être utilisé.

Pour un fonctionnement avec Microsoft Windows, le pilote de console USB Cisco Windows doit être installé sur n'importe quel PC connecté au port de console. Avec ce pilote, vous pouvez brancher et débrancher le câble USB au port de console sans affecter le fonctionnement de HyperTerminal de Windows. Seulement un port de console peut être actif à la fois. Quand un câble est branché dans le port de console USB, le port RJ-45 devient inactif. Réciproquement, quand le câble USB est enlevé du port USB, le port RJ-45 devient actif

Pour des informations détaillées, référez-vous à Utilisation du port de console des contrôleurs de la gamme Cisco 5500.

Q. Comment accéder à l´Assistant de configuration GUI sur un contrôleur 4400 ?

A. Afin de configurer les paramètres de base sur un contrôleur 4400 utilisant l'assistant de

configuration GUI, vous devez se connecter au port de service du contrôleur. Ensuite, configurez votre PC pour qu'il utilise le même sous-réseau que le port de service du contrôleur ; l'adresse IP sur le port de service lors de la configuration du WLC pour la première fois est 192.168.1.1. Démarrez Internet Explorer 6.0 SP1 (ou ultérieur) ou Firefox 2.0.0.11 (ou ultérieur) sur votre PC, et accédez à http://192.168.1.1. L'Assistant de configuration GUI apparaît.

Pour des informations détaillées sur ce sujet, référez-vous à Guide de configuration du contrôleur LAN sans fil Cisco, version 6.0.

Q. Comment accéder au WLC depuis un site distant ?

A. Vous pouvez utiliser Telnet et SSH pour accéder à WLC depuis un site distant. Telnet est un protocole utilisé pour l'accès à distance ; SSH est également un protocole utilisé pour l'accès à distance, mais il inclut une sécurité supplémentaire. Pour plus d'informations, référez-vous à la section Configuration des sessions SSH et Telnet du Guide de configuration du contrôleur LAN sans fil Cisco, version 6.0.

Q. Est-ce que je peux configurer une connexion de LAG qui la répartit à travers des plusieurs commutateurs ?

A. Oui. TRAÎNEZ avec le VSS, ou un commutateur empilé (3750/2960) a installé, fonctionnera tant que les fragments d'un paquet IP sont envoyés au même port. L'idée est que si vous allez aux plusieurs commutateurs, les ports doivent appartenir au même L2 « entité » quant aux décisions d'Équilibrage de charge.

Q. Comment un WLC commute-t-il les paquets ?

A. Tous les paquets client (802.11) sont encapsulés dans un paquet LWAPP par le LAP et envoyés au WLC. WLC décapsule le paquet LWAPP et agit selon l'adresse IP de destination dans le paquet 802.11. Si la destination est l'un des clients sans fil associés au WLC, elle encapsule le paquet de nouveau avec le LWAPP et l'envoie au LAP du client, où il est décapsulé et envoyé au client sans fil. Si la destination est du côté câblé du réseau, elle supprime l'en-tête 802.11, ajoute l'en-tête Ethernet et envoie le paquet au commutateur connecté d'où il est envoyé au client câblé. Quand un paquet provient du côté câblé, WLC supprime l'en-tête Ethernet, ajoute l'en-tête 802.11, l'encapsule avec LWAPP et l'envoie au LAP où il est décapsulé, et le paquet 802.11 est livré au client sans fil. Pour plus d'informations sur ceci, référez-vous à la section Principes fondamentaux de LWAPP du document Déploiement des contrôleurs de réseau local sans fil de la gamme Cisco 440X.

Q. Quand devrait utiliser le mode contrôleur principal sur un WLC ?

A. Quand il y a un contrôleur principal activé, tous les points d'accès nouvellement ajoutés sans contrôleurs primaires, secondaires ou tertiaires affectent un associé au contrôleur principal sur le même sous-réseau. Ceci permet à l'opérateur de vérifier la configuration des points d'accès et d'assigner les contrôleurs primaires, secondaires et tertiaires au point d'accès à l'aide de la page **Tous les AP > Détails**.

Le contrôleur principal est normalement utilisé seulement lors de l'ajout de nouveaux points d'accès à la solution de réseau local sans fil de Cisco. Quand plus aucun point d'accès n'est ajouté au réseau, la solution WLAN de Cisco recommande que vous désactiviez le contrôleur principal.

Q. Les 4400 WLC conduisent-ils des paquets entre les VLAN ?

A. WLC 4400 est un dispositif qui est relié à votre réseau, mais qui ne fonctionne pas comme un routeur. Il doit y avoir un périphérique de la couche 3 qui achemine les paquets entre les VLAN. Le WLC mappe le SSID des clients au sous-réseau VLAN et les retourne sur l'interface de gestion pour que les routeurs ascendants acheminent les paquets.

Q. Comment configurer WLAN sur un WLC ?

A. Le WLAN est semblable à celui du SSID aux Points d'accès. Un client doit de s'associer à son réseau sans fil. Afin de configurer un WLAN sur un WLC, référez-vous à l'exemple de configuration du document Exemple de configuration d'un WLAN invité et WLAN interne à l'aide des WLC.

Q. Comment fonctionne DHCP avec le WLC ?

A. Le WLC est conçu pour agir en tant qu'agent de relais DHCP au serveur DHCP externe et il agit comme un serveur DHCP au client. Voici la séquence d'événements qui se produit :

1. Généralement, WLAN est lié à une interface qui est configurée avec un serveur DHCP.
2. Quand le WLC reçoit une requête DHCP du client sur un WLAN, il relaye la requête au serveur DHCP avec son adresse IP de gestion.
3. Le WLC montre son adresse IP virtuelle, qui doit être une adresse non routable, habituellement configurée en tant que 1.1.1.1, comme serveur DHCP au client.
4. Le WLC transmet la réponse DHCP du serveur DHCP au client sans fil avec son adresse IP virtuelle. **Note**: Vous pouvez également configurer le WLC pour qu'il agisse en tant que serveur DHCP. Pour plus d'informations sur la façon configurer un WLC en tant que serveur DHCP, référez-vous à la section Configuration des portées DHCP du Guide de configuration du contrôleur LAN sans fil Cisco, Version 5.1.

Q. Comment changer la puissance et les canaux pour un LAP ?

A. Une fois qu'un LAP s'enregistre auprès d'un WLC, toute la configuration pour un LAP se fait sur le WLC. Il existe une fonctionnalité intégrée dans WLC, appelée « RRM », par laquelle le WLC exécute en interne un algorithme et ajuste automatiquement les paramètres du canal et de la puissance selon le déploiement des LAP. Par défaut, RRM est activé sur le WLC. Vous n'avez pas besoin de changer les paramètres du canal et de la puissance pour un LAP, mais vous pouvez ignorer la fonctionnalité RRM et assigner statiquement ces paramètres pour un LAP. Pour plus d'informations sur la façon de configurer manuellement les paramètres des canaux et de la puissance, référez-vous à la section Affectation statique des paramètres du canal et de la puissance de transmission aux radios de point d'accès du Guide de configuration du contrôleur LAN sans fil Cisco, version 5.1.

Q. J'ai plusieurs WLC dans mon réseau. Y a-t-il périphérique ou un logiciel disponible pour gérer plusieurs WLC dans mon réseau ?

A. Oui, Wireless Control System (WCS) est un logiciel de serveur qui peut gérer plusieurs WLC sur le réseau. Il contrôle le WLC, leurs points d'accès associés et clients. Pour plus d'informations sur le WCS, référez-vous au Guide de configuration du contrôleur LAN sans fil Cisco, version 5.0.

Q. Comment puis-je modifier le fichier de configuration de WLC ?

A. Quand vous sauvegardez la configuration de WLC, le contrôleur l'enregistre au format XML dans la mémoire flash. Afin de vous permettre de lire facilement et de modifier le fichier de configuration, le logiciel de contrôleur (version 5.2 ou ultérieure) le convertit dans un format CLI.

Quand vous téléchargez le fichier de configuration sur un serveur TFTP ou FTP, le contrôleur lance la conversion de XML en CLI. Vous pouvez alors lire ou modifier le fichier de configuration dans le format CLI sur le serveur. Quand vous avez fini, vous téléchargez de nouveau le fichier sur le contrôleur, où il est converti dans un format XML et sauvegardé.

Pour des instructions pas à pas sur la façon de modifier le fichier de configuration, référez-vous à la section Édition de fichiers de configuration du Guide de configuration de WLC 6.0.

Q. Puis-je diffuser des configurations d'un WLC directement à d'autres WLC ?

A. Non. Vous ne pouvez pas diffuser des configurations d'un WLC directement à d'autres WLC. Pour transférer le fichier à d'autres WLC, vous devez télécharger le fichier de configuration d'un WLC sur le serveur TFTP, puis télécharger le fichier du serveur TFTP sur le WLC désiré.

Afin de télécharger un fichier de WLC sur le serveur TFTP, référez-vous à la section Gestion du logiciel et des configurations des contrôleurs du Guide de configuration du contrôleur LAN sans fil Cisco, version 5.0.

Note: Avant de transférer le fichier de WLC au serveur TFTP, assurez-vous que les deux WLC exécutent la même version logicielle.

Q. Comment trouver la version du code qui est exécuté sur le WLC ?

A. Depuis l'interface utilisateur graphique (GUI) du contrôle de réseau local sans fil, cliquez sur **Monitor > Summary**. Dans la page Résumé, le champ **Version logicielle** montre la version du microprogramme qui fonctionne sur le contrôleur LAN sans fil.

Pour trouver la version du microprogramme qui fonctionne sur le WLC par l'interface de ligne de commande (CLI) de WLC, utilisez la commande **show run-config**.

```
(Cisco Controller) >show run-config

Press Enter to continue...

System Inventory
Burned-in MAC Address.......................... 00:0B:85:33:52:80

Press Enter to continue Or <Ctl Z> to abort

System Information
Manufacturer's Name............................ Cisco Systems Inc.
Product Name................................... Cisco Controller
Product Version................................ 4.0.217.0
RTOS Version................................... 4.0.217.0
Bootloader Version............................. 4.0.217.0
Build Type..................................... DATA + WPS
Compact Flash Size............................. 256 MB
```

Afin d'afficher l'image de démarrage active, utilisez la commande **show boot**

```
(Cisco Controller) >show boot
Primary Boot Image.............................. 4.0.217.0 (active)
Backup Boot Image.............................. 4.0.155.5
```

Q. Qu'arrive-t-il au réseau sans fil quand j'exécute une mise à niveau logicielle ? Est-ce que *tous* les points d'accès (AP) enregistrés auprès d'un WLC deviennent inactifs jusqu'à ce qu'ils soient mis à niveau, ou sont-ils mis à niveau un par un de sorte que le réseau sans fil puisse rester actif (excepté pour les AP spécifiques qui subissent la mise à niveau) ?

A. Une fois que le WLC est mis à niveau, il doit être redémarré pour que les modifications entrent en vigueur. Pendant ce temps, la connectivité au WLC est perdue. Les LAP enregistrés auprès d'un WLC perdent leur association au WLC de sorte que le service aux clients sans fil est interrompu. Quand vous mettez à niveau le logiciel du contrôleur, le logiciel sur les points d'accès associés du contrôleur est également automatiquement mis à niveau.

Quand un point d'accès charge le logiciel, chacune de ses LED clignote l'une après l'autre. Jusqu'à 10 points d'accès peuvent être simultanément mis à niveau à partir du contrôleur. N'éteignez pas le contrôleur ou tout point d'accès pendant ce processus ; vous risquez de corrompre l'image du logiciel. La mise à niveau d'un contrôleur avec un grand nombre de points d'accès peut prendre jusqu'à 30 minutes, selon la taille de votre réseau. Cependant, avec un nombre plus élevé de mises à niveau de point d'accès simultanées prises en charge dans la version de logiciel 4.0.206.0 et ultérieure, le temps de mise à niveau devrait être sensiblement réduit. Les points d'accès doivent demeurer sous tension, et le contrôleur ne doit pas être réinitialisé pendant ce temps.

Q. Quelles sont les directives à suivre avant d'exécuter une mise à niveau du contrôleur de réseau local sans fil ?

A. Cisco recommande que la mise à jour soit exécutée au-dessus d'un RÉSEAU LOCAL ou de toute autre haute vitesse, lien de faible latence. Une connexion réseau très lente pourrait entraîner l'interruption de TFTP, et la mise à niveau ne sera pas réussie.

Cisco recommande que le contrôleur soit mis à niveau seulement depuis un daemon TFTP sur le même segment que le contrôleur LAN sans fil quand vous utilisez TFTP comme mode de transfert.

Quand vous essayez de mettre à niveau le contrôleur à l'aide d'un client sans fil associé en tant que serveur TFTP ou FTP, la mise à niveau échoue. Le contrôleur LAN sans fil ne permet pas un transfert (T) FTP d'un daemon qui est situé sur un client associé à un AP joint au WLC. (Voir CSCsi73129 pour plus d'informations.)

En plus de ces derniers, suivez les directives documentées dans la section Directives pour mettre à niveau le logiciel du contrôleur du guide de configuration.

Q. Quelles fonctions du contrôleur exigent un redémarrage ?

A. Après avoir rempli ces fonctions sur le contrôleur, vous devez redémarrer le contrôleur pour que les modifications entrent en vigueur :

- Activez ou désactivez l'agrégation de liaison (LAG).
- Activez une fonctionnalité qui dépend des certificats (telle que https et l'authentification Web).
- Ajoutez de nouveaux utilisateurs SNMP v3 ou modifiez ces utilisateurs existants.
- Installez une licence, changez le jeu de fonctionnalités de la licence ou changez la priorité d'une licence d'évaluation comptant les AP sur un contrôleur.

Q. Un point d'accès (AP) basé sur le logiciel Cisco IOS qui a été converti au mode léger peut-il s'enregistrer auprès de WLC de la gamme Cisco 4100 ?

A. Non, les AP basés sur le logiciel Cisco IOS qui sont convertis en léger mode ne peuvent pas s'enregistrer auprès des WLC Cisco 40xx, 41xx ou 3500. Ces AP légers (LAP) peuvent uniquement s'enregistrer auprès des WLC de la gamme Cisco 4400 et 2000. Pour des informations sur les restrictions des AP qui sont convertis en mode léger, référez-vous à la section *Restrictions* de Mise à niveau des points d'accès autonomes Cisco Aironet vers le mode léger.

Q. Quel est le nombre maximal d'AP pris en charge sur les contrôleurs LAN sans fil 4402 et 4404 (WLC) ?

A. La limitation du nombre de points d'accès pris en charge est basée sur le matériel que vous avez. Les WLC 4402 avec deux ports Ethernet Gigabit viennent dans des configurations qui prennent en charge 12, 25 et 50 points d'accès légers (LAP). Les WLC 4404 avec quatre ports Ethernet Gigabit prennent en charge 100 LAP.

Note: Les points d'accès maillés sont également disponibles dans des déploiements intérieurs et extérieurs. Pour plus d'informations sur le nombre de points d'accès (y compris maillés) pris en charge sur chaque modèle de contrôleur, référez-vous au tableau 8-3 *Points d'accès maillés pris en charge par le modèle de contrôleur* dans la section Contrôle des point d'accès maillés du Guide de configuration du contrôleur LAN sans fil 6.0.

Q. J'ai exécuté un downgrade d'image de 7.0.98.0 à 6.0.200.22 sur mes 5508 WLC. Cependant, après que le downgrade, le nombre maximal d'aps pris en charge sur le WLC ait changé de 500 à 250 aps. Pourquoi ?

A. C'est un comportement prévu. Avec la version 6.0 WLC, les 5508 supports de contrôleur seulement jusqu'à 250 Points d'accès léger. Avec la version 7.0.98.0, un contrôleur Sans fil de seule gamme Cisco 5500 peut prendre en charge jusqu'à 500 Cisco Aironet aps.

Q. Comment se produit l'itinérance dans un environnement WLC ?

A. L'itinérance est un processus où le client peut retenir des sessions ininterrompues d'application sur son mouvement. Quand un client sans fil s'associe et s'authentifie auprès d'un WLC, il place une entrée pour ce client dans sa base de données client. Cette entrée inclut les adresses MAC et IP du client, le contexte et les associations de sécurité, les contextes de la qualité de service (QoS), le WLAN et le LAP associé. Quand un client est en itinérance vers un autre LAP associé au même WLC, il met à jour la base de données client avec les nouvelles informations du LAP pour que les données puissent être expédiées convenablement au client. Quand un client esst en itinérance vers un LAP associé avec un différent WLC, soit dans les mêmes sous-réseaux soit dans des sous-réseaux différents, il envoie les informations dans la base de données client au nouveau WLC. Ceci aide le client à retenir son adresse IP à travers les itinérances et maintient les sessions TCP ininterrompues. Pour plus d'informations sur l'itinérance dans l'environnement WLC,

référez-vous à la section Configuration des groupes de mobilité du *Guide de configuration du contrôleur LAN sans fil Cisco, version 5.1*.

Q. Comment est-ce que les utilisateurs invités sont gérés par WLC ?

A. Les utilisateurs d'invité sont des utilisateurs de réseau tiers, qui a besoin de l'accès limité aux ressources de réseau et à la connexion à internet. WLC fournit un accès invité sans fil et câblé à l'aide de l'infrastructure réseau sans fil existante. Habituellement, un SSID distinct est donné pour des utilisateurs invités sans fil. Les utilisateurs invités sur les réseaux câblés et sans fil sont assignés à des VLAN distincts, ce qui fournit l'isolement du trafic invité du reste du trafic de données. Ceci fournit un meilleur contrôle du trafic invité et une plus grande sécurité du réseau. Les utilisateurs invités sont habituellement authentifiés par l'authentification Web. Pour plus d'informations sur l'accès invité, référez-vous au FAQ sur l'accès invité.

Afin d'obtenir les journaux des utilisateurs invités, activez les comptes Radius pour les utilisateurs et utilisez cette commande : **debug aaa all enable**

Q. Comment configurer une base de données locale sur le contrôleur LAN sans fil (WLC) ? Quels sont les caractères spéciaux qui peuvent être utilisés pour le nom d'utilisateur et les mots de passe du réseau local ?

A. La base de données des utilisateurs locaux enregistre les qualifications (nom d'utilisateur et mot de passe) de tous les utilisateurs du réseau local. Ces qualifications sont alors utilisées pour authentifier les utilisateurs. Vous pouvez configurer les utilisateurs du réseau local par la GUI ou la CLI. Vous pouvez entrer jusqu'à 24 caractères alphanumériques. Tous les caractères spéciaux peuvent être utilisés quand vous configurez le nom d'utilisateur et les mots de passe par la CLI, mais le caractère d'apostrophe ne peut pas être utilisé quand vous configurez le nom d'utilisateur et le mot de passe par la GUI.

Depuis la CLI, utilisez ces commandes pour créer un utilisateur du réseau local :

- **config netuser add <username> <password> wlan <wlan_id> userType permanent description <description>** - Ajoute un utilisateur permanent à la base de données des utilisateurs locaux sur le WLC.
- **config netuser add <username> <password> {wlan | guestlan} {wlan_id | guest_lan_id} userType guest lifetime seconds description <description>** - Ajoute un utilisateur invité sur un WLAN ou un utilisateur câblé LAN à la base de données des utilisateurs locaux sur le WLC.

Dans l'interface GUI, vous pouvez configurer les utilisateurs du réseau local depuis la page **Sécurité > AAA > Utilisateurs du réseau local**.

Q. Est-il possible de supprimer automatiquement l'utilisateur du réseau local sur le WLC ?

A. Des utilisateurs du réseau locaux ne sont pas automatiquement supprimés. Vous devez les supprimer manuellement. Afin de supprimer l'utilisateur, allez à la page **Sécurité > AAA > Utilisateurs du réseau local**. Pour supprimer un utilisateur, placez la souris sur l'icône et cliquez sur **Remove**. Si un utilisateur du réseau local est configuré en tant qu'utilisateur invité, vous devez spécifier la durée de vie après laquelle l'utilisateur est automatiquement supprimé. La plage configurable se situe entre 60 et 2.592.000 secondes.

Q. Qu'est-ce qu'un groupe de mobilité ?

A. Le groupe de mobilité est un groupe de WLCs a configuré avec le même nom de groupe de mobilité. Le client peut être en itinérance de façon transparente entre les WLC dans le même groupe de mobilité. Dans un groupe de mobilité, les WLC autorisent la redondance parmi eux. Pour plus d'informations sur les groupes de mobilité, référez-vous à FAQ sur les groupes de mobilité des contrôleurs de réseau local sans fil (WLC).

Q. Combien WLCs peut-il j'avoir au même groupe de mobilité ?

A. Vous pouvez placer jusqu'à 24 WLC (gamme Cisco 2000, 4100 et 4400) réguliers dans un seul groupe de mobilité. Vous pouvez configurer jusqu'à 12 lames de cartes de services sans fil (WiSM) dans un groupe de mobilité. Par conséquent, jusqu'à 3.600 points d'accès (AP) au maximum sont pris en charge dans un groupe de mobilité.

Note: Avec WLC version 5.1, il peut y avoir jusqu'à 72 WLC dans un domaine de mobilité.

Q. La gamme Cisco 4400 WLC prend en charge-elle le protocole de l'Internetwork Packet Exchange (IPX) ? Est-ce qu'un produit Airespace prend en charge le protocole IPX ?

A. Non, le protocole IPX n'est pris en charge sur aucune plate-forme du WLC de Cisco.

Q. Quelles sont les conditions préalables pour accéder à l'interface utilisateur graphique (GUI) du contrôleur LAN sans fil (WLC) ?

A. L'interface GUI des contrôleurs LAN sans fil est entièrement compatible avec Microsoft Internet Explorer version 6.0 SP1 (ou ultérieure) et Mozilla Firefox 2.0.0.11 (ou ultérieur).

Note: Opera et Netscape ne sont pas pris en charge.

Note: Internet Explorer 6.0 SP1 (ou ultérieur) et Mozilla Firefox 2.0.0.11 (ou ultérieure) sont les seuls programmes de navigation pris en charge pour accéder à l'interface GUI du contrôleur et pour utiliser l'authentification Web.

Q. Comment récupérer les MIB des contrôleurs de réseau local sans fil (WLC) Cisco sur le Web ?

A. Vous pouvez télécharger les MIB WLC Cisco depuis la page Téléchargements pour produits sans fil (clients enregistrés seulement).

Complétez ces étapes pour télécharger les MIB WLC :

1. Depuis la page des téléchargements des produits sans fil, cliquez sur **Contrôleur LAN sans fil** et choisissez la plate-forme WLC pour laquelle vous avez besoin des MIB.
2. La page de téléchargement du logiciel pour le WLC apparaît. Cette page contient tous les fichiers pour le WLC, y compris les MIB.
3. Choisissez une version logicielle et téléchargez les MIB standard et les MIB Cisco. Ces deux fichier devraient être téléchargés et contenir les MIB. Les noms de fichier sont semblables à

cet exemple :

Standard-MIBS-Cisco-WLC4400-2000-XXXXXX.zip

Cisco-WLC-MIBS-XXXX.zip

Q. Dans la tunnellisation invitée, combien de tunnels Ethernet sur IP (EoIP) peuvent être formés entre un WLC de point d'attache et différents WLC internes ?

A. Un WLC de point d'attache prend en charge jusqu'à 71 tunnels EoIP avec un tunnel par WLC interne. Ces WLC peuvent être de différents groupes de mobilité.

Q. Quelles sont les différences fonctionnelles entre les WLC de la gamme 2100 et ceux de la gamme 4400 ?

A. Les principales différences entre les WLC des gammes 2100 et 4400 résident dans les caractéristiques qu'elles prennent en charge.

Cette fonctionnalité de matériel n'est pas prise en charge par les WLC de la gamme 2100.

- Port de service (interface Ethernet distincte d'administration hors bande 10/100 Mbps)

Ces fonctionnalités logicielles ne sont pas prises en charge par les WLC de la gamme 2100 :

- Terminaison VPN (telle qu'IPSec et L2TP)
- Option de passthrough VPN
- Terminaison des tunnels de contrôleur invité (l'origine des tunnels de contrôleur invité est prise en charge)
- Liste des serveurs Web d'authentification Web externe
- LWAPP de couche 2
- protocole STP
- Mise en miroir des ports
- AppleTalk
- Contrats de bande passante Qos par utilisateur
- Passthrough IPv6
- Agrégation de liaisons (LAG)
- Mode Multicast-unicast

Un WLC de la gamme 4400 prend en charge toutes les fonctionnalités matérielles et logicielles mentionnées ci-dessus.

Q. Quels points d'accès légers (LAP) les WLC de la gamme 4100 prennent-ils en charge ?

A. Seulement l'Airespace 1200, 1250, les gammes Cisco 1000 et les LAP Cisco 1500 fonctionnent avec les WLC de la gamme 4100.

Q. Puis-je utiliser ce serveur ASA/PIX comme serveur DHCP au lieu du serveur Windows DHCP pour attribuer des adresses IP à mes clients sans fil ?

A. Oui, vous pouvez utiliser ASA/PIX comme un serveur DHCP pour les clients sans fil. Assurez-vous que l'interface du WLAN auquel appartient le client est sur le même sous-réseau que l'interface ASA/PIX sur laquelle le serveur est activé. Cependant, vous ne pouvez pas attribuer la passerelle par défaut aux clients. PIX/ASA s'auto-déclare comme passerelle par défaut aux clients. Pour plus d'informations sur la façon de configurer l'ASA comme un serveur DHCP, consultez la rubrique Exemple de configuration d'un serveur PIX/ASA comme serveur DHCP et exemple de configuration d'un client.

Q. Est-il possible de revenir dans l'assistant de configuration du WLC et d'apporter des modifications au moment de la configuration initiale ?

A. Oui, c'est possible à l'aide de la touche **-** (trait d'union). Utilisez cette touche pour entrer de nouveau la valeur du paramètre précédent.

Par exemple, vous utilisez l'assistant de configuration WLC pour configurer le WLC pour la première fois.

Au lieu d'entrer le nom d'utilisateur **admin**, vous avez entré **adminn**. Pour corriger cela, entrez **-** (touche trait d'union) à l'invite suivante, puis cliquez sur **Entrer**. Le système revient au paramètre précédent.

Standard-MIBS-Cisco-WLC4400-2000-XXXXXX.zip

Cisco-WLC-MIBS-XXXX.zip

Q. Conformément à RFC 1907 pour le protocole de gestion de réseau simple (SNMP), le champ « SNMP location » doit prendre en charge de 1 à 255 caractères. Cependant, je n'arrive pas à entrer plus de 31 caractères dans le champ « SNMP location ». Pourquoi ?

A. Cela est dû au bogue Cisco ayant l'ID CSCsh58468 (clients enregistrés seulement). Un utilisateur peut entrer seulement 31 caractères. Il n'y a pas de contournement pour ce problème actuellement.

Q. Avec la fonction Management via Wireless activée sur des WLC dans un groupe de mobilité, je peux seulement accéder à un WLC depuis un groupe de mobilité, pas à tous. Pourquoi ?

A. C'est un comportement prévu. Une fois activée, la fonctionnalité Management via Wireless permet à un client sans fil d'atteindre ou de gérer uniquement le WLC sur lequel son point d'accès associé est enregistré. Le client ne peut pas gérer d'autres WLC, même si ces WLC sont dans les mêmes groupes de mobilité. Cela est mis en oeuvre pour des raisons de sécurité et, récemment, cette restriction a été portée à un seul WLC afin de limiter l'exposition.

La fonctionnalité Management over Wireless de la solution WLAN de Cisco permet aux opérateurs de contrôler et de configurer les WLC locaux à l'aide d'un client sans fil. Cette fonctionnalité est prise en charge pour toutes les tâches de gestion, sauf les téléchargements vers et depuis le WLC.

Elle peut être activée via la CLI WLC avec la commande **config network mgmt-via-wireless enable**.

Sur la GUI, cliquez sur **Management** ; faites un clic droit sur **Mgmt Via Wireless**, puis cochez la case **Enable Controller Management to be accessible from Wireless Clients**.

Note: Quand vous activez cette option, vous pouvez exposer les données. Assurez-vous que vous avez activé une authentification et un plan de cryptage appropriés.

Q. Est-il possible d'attribuer un contrôleur intégré dans un commutateur 3750 et un WLC 4400 dans le même groupe de mobilité ?

A. Oui, il est possible de créer un groupe de mobilité entre un commutateur Catalyst 3750 avec un contrôleur intégré et un WLC 4400.

Q. Y a-t-il des exigences de base à respecter quand j'utilise la fonctionnalité de point d'attache de mobilité pour configurer des WLC pour un accès invité ?

A. Il y a deux exigences de base que vous devez respecter lorsque vous utilisez le point d'attache de mobilité pour configurer les WLC pour un accès invité.

- Le point d'attache de mobilité du WLC local doit indiquer le WLC de point d'attache, et le point d'attache de mobilité du WLC de point d'attache doit pointer uniquement sur lui-même.**Note**: Vous pouvez configurer des WLC de point d'attache redondants. Le WLC local les utilise dans l'ordre de configuration des WLC.
- Assurez-vous de configurer la même politique de sécurité pour le SSID (Service Set Identifier) sur le WLC local et sur le WLC de point d'attache. Par exemple, si le SSID est « guest » et si vous activez l'authentification Web sur le WLC local, assurez-vous que le même SSID et la même politique de sécurité sont également configurés sur le WLC de point d'attache.
- Pour que la fonctionnalité de point d'attache de mobilité fonctionne, assurez-vous que le WLC de point d'attache et le WLC local utilisent la même version IOS.

Q. Quelles sont les options qui peuvent être configurées sur un WLC Cisco pour améliorer son interopérabilité avec des périphériques autres que Cisco ?

A. L'interopérabilité d'un WLC peut être améliorée par ces options :

- Les fonctionnalités propriétaires réduisent les possibilités d'interopérabilité avec des équipements fournis par un autre constructeur. Voici les fonctionnalités propriétaires de Cisco :Aironet IE - Aironet IE contient les informations, telles que le nom du point d'accès, la charge, le nombre de clients associés, etc. envoyées par le point d'accès dans les réponses de la balise et de la sonde du WLAN. Les clients CCX emploient ces informations pour choisir le meilleur point d'accès auquel s'associer.MFP : Management Frame Protection est une fonctionnalité introduite pour protéger les trames de gestion, telles que la dé-authentification, la désassociation, les balises et les sondes, par laquelle le point d'accès ajoute un élément MIC IE (Message Integrity Check Information Element) à chaque trame de gestion. Toute anomalie dans l'élément MIC IE produit une alerte.Ces fonctionnalités sont activées par défaut pour tout WLAN créé sur le WLC. Afin de désactiver ces fonctionnalités, cliquez sur le menu des WLAN dans le WLC. La liste des WLAN configurés sur le WLC s'affiche. Cliquez

sur le WLAN auquel le client veut s'associer. Sous l'onglet Advanced des WLAN, dans la page Edit, désactivez les cases à cocher qui correspondent à Aironet IE et MFP.

- Short Preamble - Un préambule court améliore les performances du débit et est activé par défaut. Certains périphériques, tels que les téléphones SpectraLink, peuvent fonctionner seulement avec des préambules longs. En pareil cas, il est également utile de désactiver les préambules courts. Afin de désactiver le préambule court, cliquez sur le menu **Wireless** de la GUI du WLC. Cliquez ensuite sur le menu du réseau **802.11b/g >** à gauche. Désactivez la case **Short Preamble**.
- Enable the broadcast service set identifier (SSID) on the WLAN - Lorsque le SSID de diffusion est activé, les informations WLAN/SSID sont envoyées dans les balises. Cela aide également les clients qui exécutent des balayages passifs (qui ne transmettent pas de demande de la sonde), tout comme les clients configurés sans SSID, à s'associer avec le WLC par ce WLAN.**Note**: Assurez-vous que vous utilisez des mécanismes d'authentification poussés car des clients fortuits peuvent s'associer à votre réseau sans fil.
- Désactivez globalement l'équilibrage de charge agressif sur le WLC.

Q. Un WLC peut-il être contrôlé par des CiscoWorks (utilisés pour gérer des routeurs et des commutateurs) ?

A. Oui. Les modèles WLC de la gamme 4400 (tels que les 4402 et les 4404) peuvent être contrôlés par des CiscoWorks.

Q. Qu'est-ce qu'un AP non autorisé ? Puis-je bloquer automatiquement les AP non autorisés dans mon réseau sans fil ?

A. Des aps qui ne sont pas une partie de votre déploiement Sans fil s'appellent les aps escrocs. Il peut s'agir d'un AP autonome ou d'un AP léger qui se trouve dans la plage des AP autorisés. Les AP non autorisés ne peuvent pas être automatiquement bloqués. Cela doit être fait manuellement. La raison en est que, quand un AP non autorisé est trouvé, l'AP qui cherche désassocie les clients de l'AP non autorisé, ce qui provoque un déni de service aux clients. Cela peut provoquer des problèmes légaux si l'AP du voisin est détecté comme étant non autorisé et ses clients subissent un déni de service. Pour plus d'informations sur la façon dont les AP non autorisés sont détectés par le WLC, référez-vous à la section Détection de périphériques non autorisés dans les réseaux sans fil unifiés.

Q. Quel est le nombre maximal de points d'accès (AP) non autorisés pris en charge par le WLC ?

A. Le WLC de la gamme 4400 prend en charge jusqu'à 625 périphériques non autorisés, incluant ceux reconnus, tandis que les WLC de la gamme 2100 prennent en charge 125 périphériques non autorisés.

Q. Le WLC peut-il envoyer des notifications par e-mail à l'administrateur lorsqu'un événement critique se produit ?

A. Le WLC n'envoie pas d'e-mails, mais il peut envoyer des messages déroutés aux stations NMS (Network Management System), comme HP OpenView (HPOV). HPOV peut exécuter des opérations telles que l'exécution de scripts pour envoyer des e-mails en cas de réception de messages déroutés spécifiques.

HPOV est une gamme de produits Hewlett-Packard qui se compose d'un portefeuille étendu de produits et systèmes de gestion réseau. HPOV est plus généralement décrit comme une suite d'applications qui permettent la gestion de systèmes et réseaux à grande échelle des actifs IT d'une organisation. HPOV inclut des centaines de modules facultatifs HP ainsi que des milliers de modules tiers, qui se connectent dans un cadre bien défini et communiquent entre eux.

Q. Si les WLC dans le même groupe de mobilité sont séparés par des bornes de traduction d'adresses réseau (NAT), peuvent-ils envoyer des messages de mobilité l'un à l'autre ?

A. Dans les versions du logiciel du contrôleur antérieures à 4.2, la mobilité entre les contrôleurs dans le même groupe de mobilité ne fonctionne pas si un des contrôleurs est derrière un périphérique de traduction d'adresses de réseau (NAT). Ce comportement crée un problème pour la fonctionnalité de point d'attache d'invité lorsqu'un contrôleur est supposé être à l'extérieur du pare-feu.

Les charges utiles des messages de mobilité diffusent des informations d'adresse IP sur le contrôleur source. Cette adresse IP est validée avec l'adresse IP de la source de l'en-tête IP. Ce comportement pose un problème quand un périphérique NAT est introduit dans le réseau parce qu'il change l'adresse IP de la source dans l'en-tête IP. Par conséquent, dans la fonctionnalité WLAN de l'invité, n'importe quel paquet de mobilité qui est routé par un périphérique NAT est rejeté en raison de l'erreur de non-correspondance d'adresse IP.

Dans la version 4.2 du logiciel du contrôleur, la recherche du groupe de mobilité est modifiée pour utiliser l'adresse MAC du contrôleur source. Puisque l'adresse IP de la source est changée en raison du mappage dans le périphérique NAT, la base de données du groupe de mobilité est interrogée avant qu'une réponse ne soit envoyée pour obtenir l'adresse IP du contrôleur qui fait la demande. Cela se fait avec l'adresse MAC du contrôleur qui fait la demande.

Référez-vous à la section Utilisation des groupes de mobilité avec les périphériques NAT pour plus d'informations.

Q. Les ports physiques sur le WLC sont actuellement définis pour fonctionner à la vitesse de 1000 Mo/s. Est-il possible de modifier cette vitesse de port à 100 Mo/s ?

A. Non, la vitesse du port sur le WLC ne peut pas être changée. Ils sont définis pour 1000 Mo/s, vitesse en mode duplex intégral seulement.

Q. J'ai défini la gestion des ressources radio (RRM) selon les paramètres par défaut sur mon WLC. Cependant, je n'arrive pas à faire en sorte que ma RRM règle automatiquement le canal et les niveaux de puissance. Pourquoi ?

A. RRM probablement ne fonctionne pas pour l'un de ces raisons

- La RRM fonctionne seulement si un AP entend des signaux RF provenant de 3 AP voisins au moins, avec un voisin tiers qui transmet une force de signal plus grande que -65 dBm. Si l'une de ces conditions n'est pas remplie, la RRM ne fonctionne pas.
- La fonctionnalité de RRM automatique inclut le réglage de canal, le réglage de puissance et la détection d'absence de couverture. Ces fonctionnalités ne marchent pas si elles sont désactivées ou si la méthode d'affectation manuelle est choisie.

Lorsqu'un nouvel AP s'amorce, la puissance est initialement maintenue à la valeur par défaut de 1 (la plus élevée). Quand 3 ou plus AP avec des niveaux de puissance supérieurs à -65 dBm apparaissent (dans le même domaine de mobilité RF et dans le même canal), il tente d'abord avec la RMM (changement de canaux). Si ça ne réussit pas parce que les canaux sont réglés manuellement ou parce qu'il y a plus d'AP que de canaux disponibles, l'AP relâche son niveau de puissance.

Référez-vous à la section Gestion des ressources radio : concepts pour plus d'informations sur la façon dont RRM fonctionne.

Q. Fait-il le contrôleur LAN Sans fil (WLC) prennent en charge-ils localement l'authentification EAP-PEAP ?

A. Dans la version 4.1, PEAP n'est pas pris en charge localement sur le WLC. Vous avez besoin d'un serveur RADIUS externe. Avec le WLC version 4.2 ou ultérieures, l'EAP local prend maintenant en charge l'authentification **PEAPv0/MSCHAPv2** et **PEAPv1/GTC**.

Q. Pouvons-nous placer le point d'accès léger (LAP) sous NAT ? Est-ce que le protocole de point d'accès léger (LWAPP) du point d'accès (AP) au WLC fonctionne par des bornes NAT ?

A. Oui, vous pouvez placer le LAP sous NAT. Du côté AP, vous pouvez avoir n'importe quel type de configuré NAT, mais, du côté WLC, vous pouvez faire configurer seulement 1:1 (NAT statique). PAT ne peut pas être configuré du côté du WLC parce que les LAP ne peuvent pas répondre aux WLC si les ports sont traduits vers des ports autres que 12222 ou 12223, qui sont désignés pour des données et des messages de contrôle.

Q. Est-ce que je peux placer le point d'accès léger (LAP) sous le Traduction d'adresses de réseau (NAT) ? Est-ce que contrôle de norme IETF et le ravitaillement des points d'accès sans fil Protocol (CAPWAP) du Point d'accès (AP) à WLC fonctionne par des bornes NAT ?

A. Oui, vous pouvez placer le LAP sous NAT. Du côté AP, vous pouvez avoir n'importe quel type de NAT configuré.

Mais du côté WLC, vous pouvez avoir seulement 1:1 (NAT statique) configuré et l'IP address NAT externe configuré sur l'interface de gestion dynamique AP (seulement pour des contrôleurs de gamme Cisco 5500). PAT ne peut pas être configuré du côté WLC parce que les recouvrements ne peuvent pas répondre à WLCs si les ports sont traduits aux ports autres que 5246 ou 5247, qui sont signifiés pour des messages de contrôle et de données.

Note: Sélectionnez la case **NAT d'adresse d'enable** et écrivez l'IP address NAT externe si vous voulez pouvoir déployer votre contrôleur de gamme Cisco 5500 derrière un routeur ou tout autre périphérique de passerelle qui utilise le Traduction d'adresses de réseau (NAT) de cartographie linéaire. NAT permet à un périphérique, tel qu'un routeur, pour agir en tant qu'agent entre l'Internet (public) et un réseau local (privé). Dans ce cas, il trace les adresses IP de l'intranet du contrôleur à une adresse externe correspondante. L'interface dynamique du l'AP-gestionnaire du contrôleur doit être configurée avec l'adresse IP NAT externe de sorte que le contrôleur puisse envoyer l'adresse IP correcte dans la réponse de détection.

Note: Avec CAPWAP, WLC derrière NAT n'est pas pris en charge avec la gamme 4400, les contrôleurs LAN Sans fil de gamme 2100 et le WiSM.

Q. Comment puis-je configurer le WLC pour autoriser uniquement les clients 802.11g ?

A. Utilisez la commande **config 802.11b disable** pour désactiver ou activer les transmissions 802.11b/g pour l'ensemble du réseau ou pour une radio Cisco individuelle.

Note: Vous devez employer cette commande pour désactiver le réseau avant d'utiliser d'autres commandes de configuration 802.11b. Cette commande peut être utilisée quand l'interface CLI est active.

Voici la syntaxe.

```
config 802.11b disable {network | Cisco_AP}
```

Voici un exemple de la façon dont vous pouvez désactiver des transmissions AP01 802.11b/g :

```
config 802.11b disable network
```

Pour désactiver des transmissions **AP01** 802.11b/g, utilisez cette commande :

```
config 802.11b disable AP01
```

Alternativement, vous pouvez utiliser cette commande afin de désactiver les débits de données 802.11b :

```
config 802.11b rate {disabled | mandatory | supported} rate
```

Q. Quelle est la procédure pour la mise à niveau du logiciel de l'OS sur un WLC Cisco ?

A. Référez-vous à la Mise à niveau logicielle sur un contrôleur de réseau local sans fil (WLC) qui présente la procédure pour une mise à niveau logicielle sur votre WLC.

Q. Puis-je mettre à niveau le WLC d'une version majeure directement à une autre ?

A. Vous pouvez mettre à niveau le logiciel du WLC, ou passer à une version antérieure, uniquement entre deux versions. Pour mettre à niveau ou passer à une version antérieure entre deux versions, vous devez d'abord installer une version intermédiaire. Par exemple, si votre WLC exécute la version 4.2 ou 5.0, vous pouvez le mettre à niveau directement avec la version de logiciel 5.1.151.0. Si votre WLC exécute une version 3.2, 4.0 ou 4.1, vous devez le mettre à niveau vers une version intermédiaire avant la mise à niveau vers 5.1.151.0. Pour connaître le

chemin de mise à niveau pour une version WLC donnée, reportez-vous aux Notes de publication de la version correspondante.

Q. Qu'est-ce que la technologie de mise en forme de faisceaux ?

A. Beamforming (également appelé ClientLink) est un mécanisme de spatial-filtrage utilisé à un émetteur pour améliorer la puissance du signal reçue ou le rapport (SNR) signal/bruit à un récepteur destiné (client). La technologie de mise en forme de faisceaux utilise plusieurs antennes émettrices pour focaliser les transmissions en direction d'un client 802.11a ou 802.11g, ce qui augmente la liaison descendante SNR et le débit de données au client, réduit les absences de couverture et améliore les performances globales du système. La technologie de mise en forme de faisceaux est prise en charge sur les points d'accès de la gamme Cisco Aironet 1140 et 1250 et fonctionne avec tous les clients 802.11a et 802.11g existants. Elle est désactivée par défaut.

Pour plus d'informations sur la configuration de la technologie de mise en forme de faisceaux, référez-vous à la section Configuration de la technologie de mise en forme de faisceaux du du guide de configuration du WLC.

Q. Est-ce que je peux télécharger une bannière de connexion pour le contrôleur LAN sans fil ?

A. Vous pouvez télécharger un fichier de bannière de connexion en utilisant la GUI ou la CLI du contrôleur. La bannière de connexion est le texte qui s'affiche sur l'écran avant l'authentification de l'utilisateur quand vous accédez à la GUI ou à la CLI du contrôleur en utilisant une connexion Telnet, SSH ou de port de console.

FAQ sur le dépannage

Q. Nous avons terminé notre déploiement initial des points d'accès légers (LAP). Quand nos clients se déplacent d'une extrémité du bâtiment à l'autre, ils restent associés à l'AP duquel ils étaient les plus proches. Les clients ne semblent pas être transférés vers l'AP le plus proche suivant tant que la puissance du signal en provenance de l'AP initial n'est pas complètement épuisée. pourquoi ?

A. La zone de couverture d'AP est entièrement contrôlée par le WLC. Le WLC parle entre ses AP et gère la puissance de leur signal sur la base de la façon dont chaque AP détecte les autres AP. Cependant, le déplacement du client d'un AP à l'autre est entièrement contrôlé par le client. La radio dans le client détermine quand le client veut se déplacer d'un AP à l'autre. Aucun paramètre sur le WLC, l'AP ou le reste de votre réseau ne peut influencer la décision du client de se déplacer vers un autre AP.

Q. J'ai connecté mon WLC à des commutateurs Cat6500 configurés pour le routage, et j'ai configuré HSRP entre ces commutateurs. Cependant, je ne peux pas atteindre d'autres sous-réseaux via le WLC. Comment faire pour résoudre ce problème ?

A. Quand HSRP est en place, une adresse IP et une adresse MAC virtuelles sont habituellement configurées pour le groupe HSRP, qui est utilisé pour le routage. Les hôtes continuent à transférer les paquets IP à ces adresses IP et MAC cohérentes même lorsqu'un des commutateurs s'arrête

et qu'une activation d'un périphérique de secours a lieu. Suivez ces étapes pour résoudre le problème de routage :

1. Assurez-vous que l'adresse IP virtuelle est configurée comme passerelle par défaut sur le WLC.**Note**: Certaines versions antérieures du WLC ne transfèrent pas les paquets à l'adresse MAC HSRP, ce qui a comme conséquence un échec du routage des paquets. Mettez à niveau me WLC pour résoudre ce problème.
2. Assurez-vous que l'interface virtuelle sur le WLC est correctement configurée. Pour plus d'informations sur les interfaces, référez-vous à la section Configuration des ports et des interfaces du Guide de configuration des WLC.

Q. Comment empêcher les boucles sur le WLC ?

A. Vous pouvez activer STP sur le WLC pour empêcher les boucles. **Du contrôleur de** clic GUI WLC, naviguez alors vers le sous-menu **avancé** situé du côté gauche de l'application. Cliquez sur l'option **Spanning Tree**, et choisissez **Enable** pour **Spanning Tree Algorithm** situé sur le côté droit de l'application.

Par défaut, STP n'a pas besoin d'être activé pour empêcher les boucles. Comme chaque interface qui est mappée à un WLAN sur le WLC est mappée au port principal et au port de secours, un seul port est utilisé à un moment donné. Le trafic en provenance du WLAN est transféré seulement via le port principal. Le WLC n'utilise jamais le port secondaire quand le port principal est actif. Le WLC utilise le port secondaire seulement quand le port principal est inactif, de sorte qu'aucune boucle ne se produira par défaut.

Q. Y a-t-il une option permettant de fournir une sécurité supplémentaire au réseau ?

A. Vous pouvez employer l'option 82 afin de fournir une sécurité supplémentaire. L'option 82 bloque les adresses IP aux clients non autorisés qui accèdent au réseau. Pour plus d'informations, référez-vous à la section Configuration de l'option DHCP 82 du Guide de configuration du contrôleur LAN sans fil Cisco, version 6.0.

Q. Y a-t-il un moyen de récupérer mon mot de passe pour le WLC ?

A. Si vous oubliez votre mot de passe dans le WLC version 5.1 et ultérieures, vous pouvez utiliser la CLI de la console de série du contrôleur afin de configurer un nouveau nom d'utilisateur et mot de passe. Suivez les étapes suivantes afin de configurer un nouveau nom d'utilisateur et mot de passe.

1. Après le démarrage du contrôleur, entrez **Restore-Password** à l'invite utilisateur.**Note**: Pour des raisons de sécurité, le texte que vous entrez n'apparaît pas sur la console du contrôleur.
2. ÀI'invite Enter User Name, entrez un nouveau nom d'utilisateur.
3. ÀI'invite Enter Password, entrez un nouveau mot de passe.
4. ÀI'invite Re-enter Password, entrez à nouveau le nouveau mot de passe.Le contrôleur valide et stocke vos entrées dans la base de données.
5. Quand l'invite User réapparaît, entrez votre nouveau nom d'utilisateur.
6. Quand l'invite Password apparaît, entrez votre nouveau mot de passe.Le contrôleur vous connecte avec vos nouveaux nom d'utilisateur et mot de passe.

Note: Pour les WLC qui exécutent des versions du firmware antérieures (avant la version 5.1), il

n'y a aucune façon de récupérer le mot de passe. Si vous utilisez le Système de contrôle sans fil Cisco (WCS) pour gérer le WLC, le Module contrôleur de réseau local sans fil (WLCM) ou Wireless Services Module WiSM), vous devez pouvoir accéder au WLC à partir du WCS et créer un nouvel utilisateur administratif sans vous connecter au WLC lui-même. Ou, si vous n'avez pas enregistré la configuration sur le WLC après avoir supprimé l'utilisateur, un redémarrage (mise hors tension) du WLC devrait le rappeler avec l'utilisateur supprimé toujours dans le système. Si vous n'avez pas le compte d'administrateur par défaut ou un autre compte utilisateur avec lequel vous pouvez vous connecter, votre seule option est d'appliquer par défaut au WLC les paramètres d'usine et de le reconfigurer à partir de zéro.

Q. J'ai changé le mode de point d'accès léger (LAP) de mon point d'accès (AP) 1030 du mode Local au mode Bridge, et le WLC 2006 ne le détecte plus. Comment puis-je restaurer l'AP 1030 dans son mode d'AP local ?

A. Afin de configurer la passerelle en mode local, terminez-vous ces étapes :

1. Allez dans la GUI du WLC et choisissez **Wireless**. **Cela affiche la liste des AP qui sont actuellement enregistrés auprès du WLC. Cliquez sur l'AP pour lequel vous devez changer le mode**.**Note**: Contrôlez si l'AP prend en charge le mode REAP. Ce doit être **YES** pour les AP de pontage interne.
2. Contrôlez l'option AP mode. Si elle indique Bridge, rétablissez-la à **Local**. Cela rétablit l'AP Bridge en AP Normal.

Pour plus d'informations sur la façon de configurer le mode pont, référez-vous à Exemple de configuration de pontage Ethernet dans un réseau maillé sans fil point à point.

Q. J'ai configuré un LAN sans fil invité et le WLC est physiquement séparé de mon LAN interne. J'ai décidé d'utiliser la fonctionnalité DHCP interne de ce WLC, mais mes clients sans fil n'obtiennent pas d'adresses IP du WLC. Comment les utilisateurs invités sans fil obtiennent-ils des adresses IP du WLC quand ils sont connectés sur un réseau séparé physiquement ?

- Contrôlez si la portée DHCP est activée sur le WLC. Pour ce faire, cliquez sur le menu **Controller** et cliquez sur **Internal DHCP server** sur le côté gauche.
- Généralement, le serveur DHCP est spécifié sur l'interface, qui mappe au WLAN. Assurez-vous que l'adresse de l'interface de gestion du WLC est spécifiée comme serveur DHCP sur l'interface qui mappe au WLAN de l'utilisateur invité. Alternativement, vous pouvez activer l'option de remplacement de serveur DHCP sur la page **WLANs > Edit** et spécifiez l'adresse de l'interface de gestion du WLC dans le champ **DHCP server IP Addr**.

Q. J'ai un contrôleur de réseau local sans fil (WLC) de la gamme 4400 et des points d'accès légers (LAP) enregistrés auprès du WLC. J'ai configuré des WLAN pour que les clients se connectent sur le WLC. Le problème est que le WLC ne diffuse pas les Service Set Identifier (SSID) que j'ai configurés pour les WLAN. Pourquoi ?

A. Les paramètres Admin Status et Broadcast SSID sont désactivés par défaut. Suivez les étapes suivantes afin d'activer Admin Status et Broadcast SSID :

1. Accédez à la GUI du WLC et choisissez **Controller > WLANs**. La page WLANs s'affiche.

Cette page répertorie les WLAN qui sont configurés.
2. Sélectionnez le WLAN pour lequel vous voulez activer la diffusion du SSID, puis cliquez sur **Edit**.
3. Dans la page WLAN > Edit, activez **Admin Status** afin d'activer le WLAN. En outre, activez **Broadcast SSID** afin de s'assurer que le SSID est diffusé dans les messages de balise envoyés par l'AP.

Q. Fait-elle la prise en charge des solutions de Cisco Unified Wireless WLCs redondant dans le DMZ pour le Tunnellisation d'invité ?

A. Oui, les WLC dans le DMZ prennent en charge les WLC redondants dans le DMZ pour la tunnellisation invitée. Pour plus d'informations sur la façon de configurer les WLC redondants, référez-vous à la section Configuration de la mobilité des points d'attache automatiques du document Guide de configuration du contrôleur LAN sans fil Cisco, version 5.1.

Q. Les clients Sans fil de RÉSEAU LOCAL associés avec le Point d'accès léger ne peuvent pas obtenir des adresses IP du serveur DHCP. Comment procéder ?

A. Le serveur DHCP pour un client est habituellement marqué sur l'interface, qui mappe au WLAN auquel client veut s'associer. Contrôlez si l'interface est configurée convenablement. Pour plus d'informations sur la façon de dépanner les problèmes liés à DHCP, référez-vous à la section Problèmes liés aux adresses IP du document Dépannage des problèmes liés aux clients dans le réseau sans fil unifié Cisco.

Q. Y a-t-il des documents qui expliquent le dépannage des problèmes de connectivité du client dans un réseau sans fil unifié Cisco ?

A. Pour des informations détaillées sur des questions de client de dépannage, référez-vous à ces documents.

- Réseau sans fil unifié : Dépanner les problèmes des clients
- Présentation de la commande debug client sur des contrôleurs de réseau local sans fil (WLC)

Q. Mon point d'accès léger (LAP) 1131 ne s'enregistre pas auprès de mon contrôleur LAN sans fil (WLC) 4402. Quelle peut en être la raison ?

A. Une raison courante est que le mode Transport du protocole Lightweight Access Point Protocol (LWAPP) est configuré sur le WLC. Un WLC 4402 peut fonctionner dans le mode LWAPP à la fois de couche 2 et de couche 3. En revanche, un LAP 1131 peut seulement fonctionner dans le mode de couche 3. Le mode de couche 2 n'est pas pris en charge sur le LAP 1131. Donc, si le WLC est configuré avec le mode Transport LWAPP de couche 2, votre LAP ne joint pas le WLC. Afin de surmonter ce problème, changez le mode transport LWAPP du WLC de couche 2 en couche 3.

Afin de changer le mode Transport LWAPP à l'aide de la GUI, allez à la page WLC et recherchez la deuxième sélection dans le champ principal, qui est LWAPP Transport Mode. Remplacez-la par Layer 3 et redémarrez le WLC. Maintenant, votre LAP peut s'enregistrer auprès du WLC. Pour plus d'informations sur des questions relatives à l'enregistrement des LAP, référez-vous au document Dépanner un point d'accès léger ne joignant pas un contrôleur LAN sans fil.

Q. Aucun message dérouté n'est produit par le WLC pour les systèmes indésirables Ad-Hoc et les débogages SNMP sur le WLC ne montrent aucun message dérouté depuis le WLC pour Ad-Hoc, même si la GUI du WLC a signalé des systèmes indésirables Ad-Hoc. Le WLC exécute le firmware version 3.2.116.21. Que se passe-t-il ?

A. Cela est dû au bogue Cisco ayant l'ID CSCse14889 (clients enregistrés seulement). Le WLC envoie constamment des messages déroutés pour les points d'accès (AP) non autorisés détectés mais pas pour les systèmes indésirables Ad-Hoc. Ce bogue est corrigé dans le firmware versions 3.2.171.5 et ultérieures du WLC.

Q. Nous avons une infrastructure de WLAN Cisco Airespace d'entreprise. Les clients WLAN ne peuvent pas accéder à un domaine Microsoft Active Directory (AD). Ce problème est constaté dans l'un de nos bâtiments. Les autres bâtiments n'ont pas ce problème. Nous n'utilisons aucune liste de contrôle d'accès (ACL) en interne. En outre, quand un client ayant échoué est câblé, il peut immédiatement accéder au domaine Microsoft AD. Quel a pu être le problème ?

A. Une des raisons peut être que le mode multidiffusion est désactivé sur le WLC. Activez le mode multidiffusion sur le WLC et contrôlez si vous pouvez accéder au domaine Microsoft AD.

Q. La mobilité de la couche 3 fonctionne-t-elle avec une configuration du groupe VLAN du Point d'accès (AP) ?

A. Oui, la mobilité de couche 3 fonctionne avec une configuration de VLAN de groupe d'AP. Actuellement, les sources de trafic en provenance d'un client sans fil en itinérance de couche 3 sont mises sur l'interface dynamique assignée sur le WLAN ou sur l'interface du VLAN du groupe d'AP.

Q. Pourquoi nos points d'accès (AP) qui sont enregistrés auprès d'autres WLC qui sont dans le même groupe de RF sont affichés comme des systèmes indésirables ?

A. Cela peut être dû au bogue Cisco ayant l'ID CSCse87066 (clients enregistrés seulement). Les AP LWAPP du même groupe de RF sont vus comme des AP non autorisés par un autre WLC pour l'une des raisons suivantes :

- L'AP voit plus de 24 voisins. La taille de la liste des voisins est de 24, donc le 25ème AP est signalé comme non autorisé.
- AP1 peut entendre le client qui communique à AP2, mais AP2 ne peut pas être entendu. Par conséquent, il ne peut pas être validé comme voisin.

La solution de contournement consiste à définir manuellement les AP comme des AP internes connus sur le WLC et/ou le WCS. Suivez ces étapes sur le WLC pour définir manuellement les AP comme internes connus :

1. Allez dans la GUI du WLC et choisissez **Wireless**.
2. Cliquez sur **Rogue Aps** dans le menu situé sur le côté gauche.
3. Dans la liste Rogue-AP, choisissez le point d'accès spécifique et cliquez sur Edit.
4. Dans le menu Update Status, choisissez **Known internal**.

5. Cliquez sur **Apply**. Ce bogue est corrigé dans la version 4.0.179.11.

Q. J'ai un point d'accès léger (LAP) 1200 à enregistrer auprès de mon contrôleur de réseau local sans fil (WLC). J'ai configuré mon serveur DHCP avec l'option 43. Comment puis-je vérifier si l'option DHCP 43 fonctionne correctement ?

A. Avec l'option DHCP 43, le serveur DHCP fournit l'adresse IP des WLC avec l'adresse IP fournie via DHCP. Cela peut être vérifié à partir du LAP si l'AP est un AP Lightweight Access Point Protocol (LWAPP) Cisco IOS, tel que le LAP 1242 ou 1131AG. Dans ces cas, émettez la commande **debug dhcp detail** du côté de l'AP afin de voir si l'AP reçoit avec succès les informations de l'option 43 et ce qu'il reçoit.

Q. Mon WLC 2006 montre que différents canaux ont été assignés aux points d'accès (AP) enregistrés. Cependant, quand j'effectue une analyse avec l'utilitaire Aironet Desktop Utility (ADU) ou Netstumbler, tous les AP sont dans le même canal (1). Quelle en est la raison ?

A. Ce problème se pose quand ces AP enregistrés sont très proches les uns des autres. Vous pouvez consulter le bogue Cisco ayant l'ID CSCsg03420 (clients enregistrés seulement).

Q. Quand j'émets la commande ipconfig/all à l'invite de commande de mon PC, l'adresse d'un serveur DHCP différent s'affiche. Il affiche 1.1.1.1 comme adresse IP de serveur DHCP. C'est l'adresse IP de l'interface virtuelle du WLC et pas l'adresse du serveur DHCP. Pourquoi cela s'affiche-t-il comme serveur DHCP ?

A. C'est parce que l'adresse d'interface virtuelle 1.1.1.1 agit en tant que proxy DHCP pour le serveur DHCP initial. Si vous voulez voir l'adresse du serveur DHCP initial dans la sortie de la commande **ipconfig/all**, désactivez la fonctionnalité de proxy DHCP dans le WLC auquel le client est associé. Elle peut être désactivée avec la commande **config dhcp proxy disable**.

Cette commande remplacera l'adresse d'interface virtuelle 1.1.1.1, qui s'affiche elle-même comme serveur DHCP, par l'adresse IP du serveur DHCP réelle que vous avez définie sur l'interface ou dans l'option prioritaire du WLAN.

Q. Nous avons deux serveurs Access Control Server (ACS) qui authentifient les clients sans fil associés aux contrôleurs LAN sans fil (WLC). Un ACS agit en tant que serveur d'authentification principal et l'autre comme serveur de basculement. Si le serveur principal est défaillant, le WLC bascule vers le secondaire pour authentifier les clients sans fil. Une fois que le serveur principal redevient actif, le WLC ne rebascule pas vers le serveur principal. Pourquoi ?

A. C'est un comportement prévu. Les étapes suivantes se produisent quand un client est authentifié via le WLC dans plusieurs déploiements d'ACS :

1. Lors du démarrage, le WLC détermine l'ACS actif.
2. Quand cet ACS actif ne répond pas à la demande RADIUS en provenance du WLC, le WLC effectue une recherche et fait un basculement vers l'ACS secondaire.
3. Même lorsque l'ACS principal redevient actif, le WLC ne rebascule pas vers lui tant que

l'ACS sur lequel le WLC effectue actuellement l'authentification n'est pas défaillant.

En pareil cas, redémarrez le WLC pour que le WLC identifie de nouveau l'ACS principal et rebascule vers lui. Ce basculement ne se produit pas immédiatement après le démarrage. Cela peut prendre du temps.

Q. Je ne peux pas appliquer le Secure Shell (SSH) dans le contrôleur LAN sans fil (WLC) quand j'utilise le logiciel client SecureCRT SSH v2 SH. Mon WLC exécute la version 4.0.179.8.

A. SecureCRT fonctionne seulement avec WLCs qui exécutent la version 4.0.206.0 ou plus tard. Mettez à niveau votre WLC vers cette version. Ensuite, vous pouvez utiliser le client SecureCRT SH pour appliquer SSH dans le WLC.

Q. Comment chiffrer les fichiers de configuration sur le WLC ?

A. Le cryptage des fichiers de configuration est déjà disponible dans WLCs. Si vous choisissez **Commands > Upload File** dans la GUI du WLC, vous voyez la case à cocher **Configuration File Encryption**.

Vous pouvez forcer le fichier à être chiffrer via WCS de cette façon.

- Dans la GUI de WCS, choisissez **Configure controller**. Cela affiche la liste des WLC configurés dans WCS. Cliquez sur un WLC.
- Sur le côté gauche, cliquez sur l'option **commands**. Vous recevez une liste de commandes de contrôleur.
- Sous **Upload/Download Commands**, choisissez **download config** dans le menu déroulant. À ce stade, vous voyez le message suivant : **Note**: **Configuration file encryption key is not set. Downloading configuration file will fail if encryption key is needed. Please click here to setup encryption.**

Fondamentalement, vous pouvez forcer WCS à toujours définir une clé de chiffrement pour les configurations de WLC. Le chiffrement n'est pas activé par défaut, mais il peut être activé à la fois dans les WLC et dans WCS, si nécessaire.

Q. Comment les WLC prennent-ils en charge les points d'accès surdimensionnés ?

A. Te permet la version 5.0 de logiciel contrôleur ou plus tard pour améliorer à une image de Point d'accès surdimensionnée en supprimant automatiquement l'image de reprise pour créer le suffisamment d'espace. Cette fonctionnalité affecte seulement les points d'accès avec 8 Mo de mémoire flash (les points d'accès de la gamme 1100, 1200 et 1310). Tous les points d'accès plus récents ont une taille de mémoire flash supérieure à 8 Mo. Depuis août 2007, il n'y a aucune image de point d'accès surdimensionnée, mais à mesure que de nouvelles fonctionnalités seront ajoutées, la taille des images de point d'accès continuera à augmenter. Pour plus d'informations, référez-vous à la section Prise en charge des images de point d'accès surdimensionnées du Guide de configuration du contrôleur LAN sans fil Cisco, version 6.0.

Informations connexes

- Modules du contrôleur LAN sans fil
- Contrôleurs LAN sans fil Cisco - Questions/réponses

- Compteurs MAC de 802.11 sur WLC
- Guide de configuration Sans fil de contrôleur LAN de Cisco, version 7.0
- Page de prise en charge du mode sans fil
- Support et documentation techniques - Cisco Systems