Points d'accès Cisco Aironet - FAQ

Contenu

Introduction

Ce document apporte des réponses aux questions les plus souvent posées (FAQ) au sujet des points d'accès (AP) Cisco Aironet.

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

FAQ sur la conception

Q. Quel est le nom d'utilisateur et le mot de passe par défaut pour le Cisco IOS® aps articulés autour d'un logiciel ?

A. Le Cisco IOS aps articulés autour d'un logiciel a une configuration par défaut qui inclut une combinaison de nom d'utilisateur et de mot de passe, qui sont **Cisco** (distinguant majuscules et minuscules). Après que vous remettiez à l'état initial aux par défaut d'usine, soyez prêt à donner à Cisco comme chacun des deux le nom d'utilisateur et mot de passe quand le GUI ou l'interface de ligne de commande (CLI) vous incite.

Q. Quel câble dois-je utiliser pour une connexion par console ?

A. Utilisez un câble droit avec connecteurs mâles neuf broches sur femelles neuf broches afin de connecter le port COM1 ou COM2 de votre ordinateur au port RS-232 de l'AP. Utilisez un programme d'émulation de terminal sur votre ordinateur, tel que :

- Microsoft Windows HyperTerminal
- Symantec ProComm
- Minicom

Utilisez ces paramètres de port :

Vitesse :	9 600 bits par seconde (bps)
Bits de données :	8
Bits d'arrêt :	1
Parité :	Aucun

Contrôle de flux :	Xon/Xoff

Remarque: Si le contrôle de flux Xon/Xoff ne fonctionne pas, essayez d'utiliser le contrôle de flux None.

Q. J'ai un AP 1231 pour Aironet. Cisco fait-il un câble d'extension de 50 pieds de sorte que je puisse avoir l'AP dans une zone et l'antenne dans une autre ?

A. Oui, le numéro de pièce du câble de 50 pieds est AIR-CAB050LL-R. Vous pouvez employer ce câble pour connecter votre AP à l'antenne.

Q. Comment contrôler le type radio sur un AP autonome ?

A. Vous pouvez utiliser une commande **show controllers** dans le mode EXEC privilégié sur l'AP pour obtenir les informations sur le type radio.

Q. Comment configurer une adresse IP sur l'AP ?

A. Par défaut, l'AP demande une adresse IP via DHCP.

Les Cisco IOS versions 12.3(2)JA et ultérieures changent le comportement par défaut des aps demandant un IP address d'un serveur DHCP :

- Quand vous connectez une gamme 1200 ou 1230 AP à une configuration par défaut à votre réseau local, AP demande un IP address de votre serveur DHCP. S'il ne reçoit pas une adresse, il continue à envoyer des demandes indéfiniment.
- Quand vous connectez une gamme 1100 AP à une configuration par défaut à votre réseau local, la gamme 1100 AP fait plusieurs tentatives d'obtenir un IP address du serveur DHCP. S'il ne reçoit pas une adresse, il s'assigne l'adresse IP 10.0.0.1 pendant cinq minutes. Pendant ces cinq fenêtre minute, vous pouvez parcourir à l'adresse IP par défaut et configurer une adresse statique. Si après cinq minute AP n'est pas modifié, il jette l'adresse de 10.0.0.1 et retourne à demander une adresse du serveur DHCP. S'il ne reçoit pas une adresse, il envoie des demandes indéfiniment. Si vous manquez aux cinq la fenêtre minute pour parcourir à AP chez 10.0.0.1, vous pouvez arrêt et redémarrage AP répéter le processus.

Vous pouvez également paramétrer manuellement l'adresse IP de l'AP. Sur un PC avec Microsoft Windows qui est connecté au segment Ethernet, dans l'invite DOS, émettez cette commande :

```
arp -s a.b.c.d 00-12-34-56-78-90
```

Remarque: Le terme *a.b.c.d représente l'*adresse IP qui doit être placée sur AP, et 00-12-34-56-78-90is l'adresse MAC. Cette adresse apparaît sur le panneau en bas de l'AP.

Émettez cette commande afin de vérifier l'adresse :

```
ping a.b.c.d
```

Remarque: Cette procédure ne fonctionne pas si l'AP a déjà une adresse IP assignée avec une autre méthode.

Q. Comment activer l'accès HTTPS sur l'AP ?

A. Afin d'activer HTTPS, vous devez ajouter cette commande à votre AP :

```
AP(config)#ip http secure-server
```

Quand vous ajoutez la commande **ip http secure-server**, vous voyez les clés RSA requises pour la communication sécurisée régénérée sur les AP.

Q. Comment un client choisit-il un point d'accès (AP) pour être associé ?

A. Le choix du Point d'accès (AP) est fait sur la radio d'ordinateur du client. En fonction du fabricant, du pilote, du type de carte et ainsi de suite, il peut employer différentes métriques pour faire le choix. Le mécanisme d'affiliation AP le plus commun utilisé dans la plupart des clients est basé sur la puissance du signal reçu par client en provenance des AP. La norme de 802.11 exige seulement que la carte du client sans fil enregistre la puissance du signal avec une métrique simple appelée RSSI (Received Signal Strength Indicator). Le client associe ensuite l'AP avec le signal le plus fort. Il est bien connu que ces algorithmes peuvent mener à des performances médiocres. La principale raison est due à son manque de connaissance de la charge sur différents AP.

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. Comment étendez-vous la couverture d'AP ?

A. Il y a plusieurs façons d'étendre la zone de couverture pour un AP. Voici les méthodes les plus importantes :

- Utilisation d'AP dans le mode répéteur.
- Utilisation d'un AP secondaire en mode AP avec canaux sans chevauchement.
- Changement de paramètre de niveau de puissance d'émetteur de l'AP existant afin d'étendre la couverture.
- Positionnement optimal des AP.

Référez-vous aux Méthodes d'extension de la zone de couverture radio WLAN pour une description complète de la façon d'appliquer ces méthodes.

Q. Quelles sont les implications si votre AP est en mode répéteur ?

A. Le port Ethernet est désactivé dans le mode répéteur. Le débit efficace est coupé de moitié une fois pour chaque saut à partir de l'AP parent.

Afin de configurer des répétiteurs, vous devez activer des extensions Aironet sur le point d'accès parent (racine) et les points d'accès de répétiteur. Les extensions Aironet, qui sont activées par défaut, améliorent la capacité du point d'accès à comprendre les capacités des périphériques clients Cisco Aironet associés au point d'accès. Si vous désactivez des extensions Aironet, vous pouvez parfois améliorer l'interopérabilité entre le point d'accès et les périphériques clients non Cisco. Les périphériques clients non Cisco peuvent trouver la communication difficile avec les

points d'accès de répétiteur et le point d'accès racine auxquels les répétiteurs sont associés.

Le SSID d'infrastructure doit être assigné au VLAN natif. Si plus d'un VLAN est créé sur un point d'accès ou un pont sans fil, un SSID d'infrastructure ne peut pas être assigné à un VLAN non natif. Ce message apparaît quand le SSID d'infrastructure est configuré sur un VLAN non natif :

```
SSID [xxx] must be configured as native-vlan before enabling
 infrastructure-ssid
```

Comme des points d'accès créent une interface virtuelle pour chaque interface radio, les points d'accès de répétiteur s'associent deux fois au point d'accès racine : une fois pour l'interface réelle et une fois pour l'interface virtuelle.

Remarque: vous ne pouvez pas configurer plusieurs VLAN sur des points d'accès de répétiteur. Les points d'accès de répétiteur ne prennent en charge que le VLAN natif.

Q. Quelles sont les fonctionnalités prises en charge par l'option Aironet Extension ?

A. L'extension Aironet est une fonctionnalité propriétaire mise en application par Cisco. Les extensions Aironet contiennent des éléments d'information qui prennent en charge ces fonctionnalités.

- **Équilibrage de charge :** le point d'accès emploie des extensions Aironet pour diriger des périphériques clients vers un point d'accès qui fournit la meilleure connexion au réseau selon des facteurs tels que le nombre d'utilisateurs, les taux d'erreur de bits, la charge et la puissance du signal.L'équilibrage de charge est propriétaire entre des périphériques qui comprennent les extensions Aironet. L'équilibrage de charge est mis en application par des extensions dans des balises AP et/ou des réponses de sondage qui fournissent des informations sur les éléments suivants :Puissance du signal de la station de baseCharge de la station de base (% d'émetteur occupé)Nombre de sauts vers le réseau fédérateurNombre d'associations de clientsLe client évalue ces derniers et s'associe au « meilleur ». Les clients non Cisco ne comprennent pas ces extensions.
- **MIC :** Cisco Proprietary Message Integrity Check (MIC) — MIC est une fonction de sécurité WEP supplémentaire qui empêche des attaques sur des paquets cryptés appelées attaques bit-flip. La MIC est mise en application sur le point d'accès et sur tous les périphériques clients associés.
- **Cisco Proprietary Temporal Key Integrity Protocol (CKIP)**, également connu comme brouillage de clé WEP, est une fonction de sécurité WEP supplémentaire qui défend contre une attaque sur WEP, dans laquelle l'intrus utilise un segment non crypté appelé le vecteur d'initialisation (IV) dans des paquets codés pour calculer la clé WEP.
- En plus de ces derniers, les extensions Aironet diffusent plus d'informations, incluant celles-ci :Charge que l'AP gère actuellementNombre de sauts depuis le réseau câbléType de périphérique, ce qui aide à identifier le produit sous le système Cisco pour la gestionNom du périphériqueNombre de clients associésType radio, une fonctionnalité utilisée pour déterminer certaines caractéristiques radio, telles que le débit de données, le type radio (1310, 1200, 352 ou 342), le type de sécurité (WEP/802.1x), etc.

Les périphériques qui sont compatibles CCX peuvent également tirer profit de certaines des fonctionnalités d'Aironet Extension. Voici une liste des fonctionnalités disponibles avec les différentes versions de Cisco Compatible Extensions :

Cisco Compatible Extensions - Versions et fonctionnalités

Q. Puis-je connecter deux ordinateurs ensemble sans AP via des cartes d'interface sans fil ?

A. Oui. Depuis l'utilitaire Aironet Client Utility (ACU), vous pouvez configurer les clients pour qu'ils fonctionnent en mode ad hoc. Cette connexion est seulement une connexion homologue-à-homologue. Un PC devient le parent et contrôle la connexion. Les autres PC en mode ad hoc sont des stations enfants.

Q. Ai-je besoin d'un matériel spécial pour prendre en charge le cryptage ?

A. Le modèle matériel spécifique détermine le niveau de cryptage pour l'unité :

- Les modèles 341 et 351 prennent seulement en charge le cryptage sur 40 bits.
- Les modèles 342 et 352 prennent en charge le cryptage sur 40 et sur 128 bits.
- Tous les modèles des gammes 1100, 1200 et 1300 prennent en charge le cryptage sur 40 et 128 bits.

Q. Est-il possible de voir tous les AP et leurs clients associés qui appartiennent à ce réseau/cette infrastructure en particulier juste depuis un seul AP ?

A. C'est possible depuis un AP VxWorks. Un seul AP VxWorks peut afficher tous les clients et leurs AP dans un réseau. Ceci peut être réalisé si vous cliquez sur **Association > Entire Network > Apply**. Dans un AP basé sur IOS, il n'affiche pas tous les clients associés dans le réseau sans l'aide d'un périphérique de gestion, tel que WLSE, avec un AP comme WDS ou un contrôleur si l'image dans l'AP est une image LWAPP.

Q. J'utilise CCKM dans mon réseau, mais le processus d'authentification entier se produit toujours à chaque fois que le périphérique client est en itinérance. En bref, l'itinérance rapide et sûre ne fonctionne pas comme prévu. Pourquoi ?

A. C'est probablement en raison du bogue CSCsg10128. Ce bogue est corrigé dans la version 3.1.03.

Q. Les points d'accès Cisco prennent-ils en charge la fonctionnalité UniDirectional Link Detection (UDLD) afin de fermer la connexion Ethernet aux commutateurs s'il y a une panne de câble de couche 1/couche 2 ?

A. Non, les points d'accès Cisco ne prennent pas en charge la fonctionnalité UDLD.

Q. Comment alimentez-vous un AP Aironet ?

A. Les options d'alimentation pour votre AP dépendent du modèle d'AP que vous avez. Référez-vous à Options d'alimentation de produit pour Cisco Aironet et contrôleur WLAN pour plus d'informations.

Q. J'ai un AP1010, AP1030 et un AIR-LAP-1232AG. Peuvent-ils utiliser un WS-PWR-PANEL pour PoE (Power over Ethernet) ?

A. Le WS-PWR-PANEL prend seulement en charge des points d'accès avec radio simple. Référez-vous au tableau de compatibilité disponible dans la section *Cisco PoE et Cisco Intelligent Power Management* de la note Application Cisco Aironet PoE (Power over Ethernet) pour plus d'information.

Q. Comment sauvegarder la configuration de l'AP ?

A. Des modifications à la configuration sont enregistrées immédiatement. Vous pouvez faire une image de la configuration actuelle dans un format texte depuis le **menu Setup**. Puis, choisissez **Cisco Services > Manage System Configuration** et téléchargez la configuration système.

Q. Comment est-ce que je détermine la fréquence ou le canal spécifique que mon AP ou mon pont utilise ?

A. Employez la commande **show controllers dot11Radio0** afin de montrer la fréquence et le canal sur laquelle/lequel l'AP ou le pont est. Cet exemple de sortie montre où trouver les informations :

```
ap#show controllers dot11Radio0 ! interface Dot11Radio0 Radio AIR-AP1242GA, Base Address
0014.1b58.08f Version 5.80.12 Serial number: GAM09200992 Number of supported simultaneous BSSID
on Dot1 Carrier Set: Americas (US ) DFS Required: No Current Frequency: 2412 MHzChannel 1
```

Q. Comment puis-je faire fonctionner mon AP avec d'autres périphériques IEEE 802.11b ?

A. Afin de permettre à AP de communiquer avec un autre appareil 802.11b, arrêtez les Aironet Extension. Cochez la case **Non-Aironet 802.11** dans la fenêtre Express Setup. Sinon, vous pouvez cliquer sur la case d'option **Use Aironet Extension** dans la fenêtre Advanced AP Radio.

Q. Quels périphériques peuvent s'associer à un AP ?

- AP à client
- AP à AP (en mode répéteur)
- AP (en mode répéteur) à station de base (en mode AP)
- AP au pont du groupe de travail

Q. À quelle fréquence un AP communique-t-il ?

A. Aux États-Unis, des AP conformes IEEE 802.11b transmettent et reçoivent dans l'un des 11 canaux à la fréquence de 2,4 GHz. Les AP conformes IEEE 802.11a transmettent et reçoivent dans l'un des huit canaux à la fréquence de 5 GHz. Les AP conformes IEEE 802.11g transmettent et reçoivent dans l'un des 11 canaux à la fréquence de 2,4 GHz. Ce sont des plages de fréquences publiques et sont non enregistrées par la FCC.

Q. Comment sécuriser les données à travers une liaison radio AP ?

A. Il y a plusieurs méthodes pour sécuriser vos données à travers une liaison radio AP. Afin d'en savoir plus sur les différentes méthodes de sécurité, référez-vous à la FAQ sur la sécurité de Cisco Aironet sans fil.

Q. Combien de clients peuvent s'associer à AP ?

A. L'AP a la capacité physique de gérer 2 048 adresses MAC mais, parce que l'AP est un média partagé et agit comme concentrateur sans fil, la performance de chaque utilisateur diminue à mesure que le nombre d'utilisateurs augmente sur un AP individuel. Dans l'idéal, un maximum de 24 clients peut s'associer à l'AP, parce que le débit de l'AP est réduit par chaque client qui s'associe à l'AP.

Q. Y a-t-il une limitation sur le nombre de filtres d'adresses MAC qui peuvent être configurés sur l'AP ?

A. Vous pouvez employer la CLI afin de configurer jusqu'à 2 048 adresses MAC pour le filtrage mais, avec l'utilisation de l'interface du navigateur Web, vous ne pouvez configurer qu'un maximum de 43 adresses MAC pour le filtrage.

Q. Quelle est la portée habituelle pour un AP ?

A. La réponse à cette question dépend de beaucoup de facteurs, qui incluent les suivants :

- Débit de données (bande passante) que vous désirez
- Type d'antenne
- Longueur du câble d'antenne
- Le périphérique qui reçoit la transmission

Dans une installation optimale, la portée peut aller jusqu'à 300 pieds.

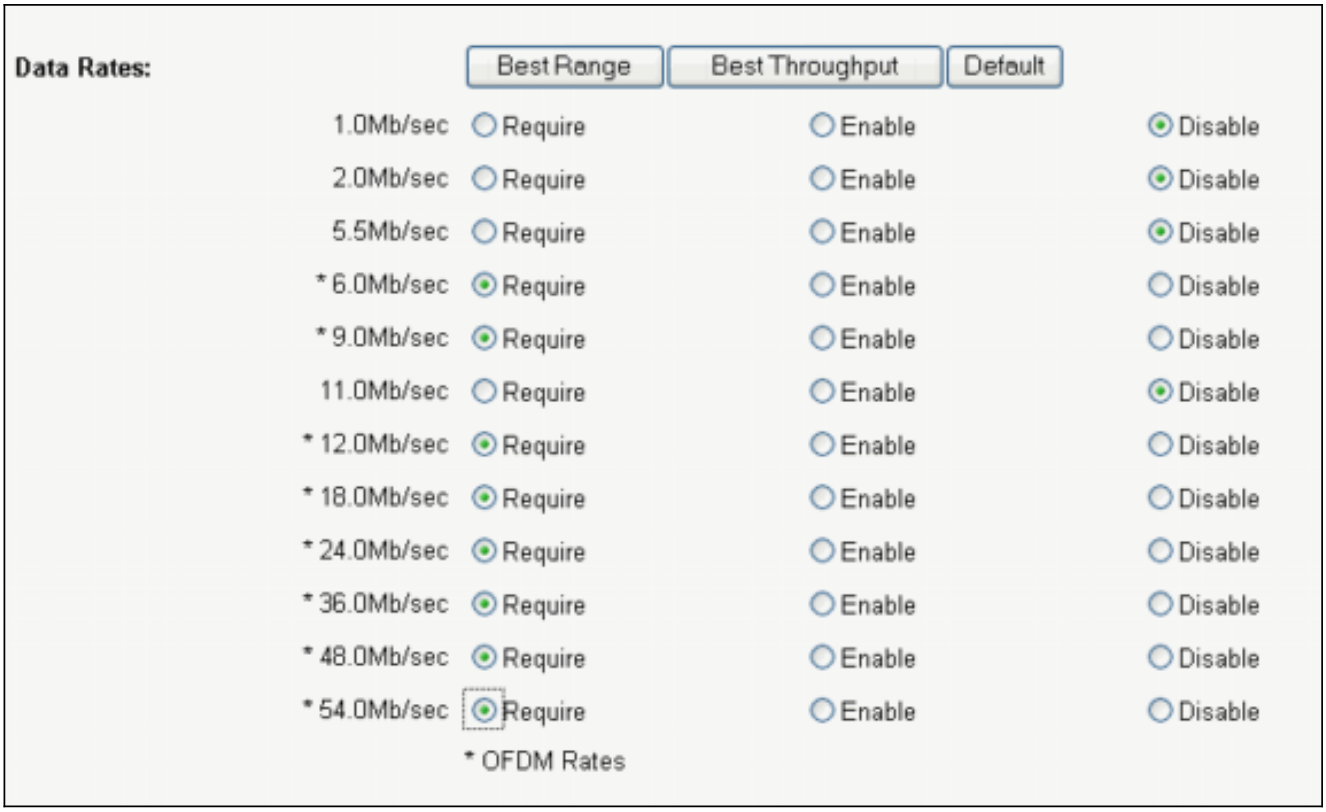
Q. Quel sont les paramètres de niveau de puissance de transmission disponibles un AP 1200 ?

A. Les paramètres de puissance de transmission sont différents et dépendent de la radio qui est utilisée. Référez-vous à la Fiche technique de point d'accès de la gamme Cisco Aironet 1200 pour la liste complète des niveaux de paramétrage de puissance. Les paramètres de puissance variant en fonction du canal, effectuez une analyse du site. L'analyse du site est importante pour obtenir des informations précises sur le paramètre à utiliser. Référez-vous à la FAQ sur l'analyse de site sans fil pour obtenir des détails sur les analyses de site.

Q. Comment puis-je paramétrer l'AP de sorte que seuls les clients IEEE 802.11g puissent se connecter ? Je ne veux pas que les clients IEEE 802.11b se connectent et ralentissent le réseau sans fil. Il y a un second réseau parallèle 802.11b pour les clients non sécurisés.

A. Afin d'AP aux clients 802.11g uniquement récepteurs, terminez-vous ces étapes dans le GUI :

1. Allez dans la section Network Interfaces et cliquez sur **Radio 0-802.11G**.
2. Cliquez sur l'onglet **Settings** en haut de la fenêtre Radio 0-802.11G.
3. Choisissez **Disable** pour ces débits de données : 1.02.05.511.0
4. Choisissez **Require** pour tous les autres débits de données. Voici les autres débits de données : 6.09.012.018.024.036.048.054.0
5. Cliquez sur **Apply** en bas de la fenêtre. Cette fenêtre fournit un exemple :



Q. Est-il vrai que, si j'autorise seulement des clients IEEE 802.11g sur un réseau sans fil, ils ne peuvent pas interférer avec un réseau IEEE 802.11b parallèle, parce qu'ils utilisent différents schémas de modulation ?

A. Non, ceci n'est pas vrai. Ces clients 802.11g peuvent interférer s'ils utilisent la même fréquence. Veillez à utiliser différents canaux. Les trois canaux sans chevauchement sont le 1, le 6 et le 11.

Q. Quelle est le débit du port Ethernet AP ?

A. Le port Ethernet AP prend en charge 10 Mbps ou 100 Mbps via un connecteur RJ-45, en semi-duplex ou en duplex intégral. Paramétrez le débit et le duplex au niveau matériel avec les mêmes paramètres que votre commutateur ou concentrateur.

Q. Y a-t-il un mécanisme pour le basculement ou la redondance pour mon AP ?

A. Oui, vous pouvez configurer un secours immédiat afin de fournir la redondance en cas de panne de l'AP primaire. Référez-vous aux notes de mise à jour pour le pour en savoir plus de Points d'accès de Cisco Aironet.

Q. Qu'est-ce qu'une clé WEP ?

A. Le WEP signifie Wired Equivalent Privacy. Vous pouvez employer WEP pour encrypter et décrypter les signaux de données transmis entre des périphériques sans fil LAN (WLAN). WEP est fonctionnalité facultative de IEEE 802.11 qui empêche la divulgation et la modification de paquets en transit et fournit également un contrôle d'accès pour l'usage du réseau. WEP rend une liaison WLAN aussi sécurisée qu'une liaison câblée. Comme la norme le spécifie, WEP utilise l'algorithme RC4 avec une clé 40 bits ou 10 bits. RC4 est un algorithme symétrique, parce que RC4 utilise la même clé pour le cryptage et le décryptage des données. Quand WEP est activé,

chaque station radio a une clé. La clé est utilisée pour brouiller les données avant la transmission des données par les ondes hertziennes. Si une station reçoit un paquet qui n'est pas brouillé avec la clé appropriée, la station rejette le paquet et ne livre jamais un tel paquet à l'hôte. Référez-vous au Wired Equivalent Privacy (WEP) sur des points d'accès Aironet et exemple de configuration de ponts pour obtenir des informations sur la façon de configurer WEP.

Q. Lors de l'utilisation de Light Extensible Authentication Protocol (LEAP), quel numéro de port spécifier pour communiquer avec son Cisco Secure Access Control Server (ACS) ?

A. Par défaut, l'ACS écoute une requête d'authentification sur le port 1645 et la gestion des comptes sur le port 1646, mais vous pouvez configurer le port 1812 pour l'authentification et le 1813 pour la gestion des comptes. Confirmez que ces ports sont correctement paramétrés à la page Authentication Server Setup de l'AP.

Q. Dans les AP basés sur le logiciel Cisco IOS, est-il possible d'exécuter une clé Wired Equivalent Privacy (WEP) statique et l'Extensible Authentication Protocol (EAP) ensemble sur le même AP pour l'authentification ? Ceci a fonctionné avec des AP basés sur VxWorks.

A. Non, vous ne pouvez pas exécuter des clés WEP statiques pour le cryptage et l'EAP pour l'authentification dans le même Service Set Identifier (SSID). VxWorks a permis cette configuration en raison d'une vulnérabilité logicielle, mais cette capacité n'est pas une fonctionnalité. Ce que vous pouvez faire, c'est créer deux SSID et deux VLAN (un par SSID). Puis, configurez l'ouverture de l'authentification avec WEP pour un SSID et l'authentification EAP pour l'autre SSID.

Q. Est-il vraiment nécessaire de faire faire une analyse du site ?

A. Oui. En raison de la nature sensible des transmissions de radiofréquence (RF), vous devez connaître les autres types de trafic RF qui peuvent être dans votre environnement, même sans que vous ayez connaissance de la présence du trafic. Une analyse du site permet une meilleure compréhension de cette menace invisible au bénéfice de bonnes performances de vos périphériques sans fil. L'analyse du site aide également votre installateur professionnel à assurer la couverture RF désirée. Référez-vous à la FAQ sur l'analyse de site sans fil.

Q. Si j'essaye de modifier l'AP et qu'un nom d'utilisateur et un mot de passe me sont demandés, que faut-il entrer ?

A. Une demande de nom d'utilisateur et de mot de passe signifie que le User Manager a été activé. Référez-vous à votre administrateur AP afin de connaître le nom d'utilisateur et le mot de passe à utiliser. Si vous êtes l'administrateur AP et ne savez pas ce que sont ces comptes d'utilisateur, vous devez exécuter une récupération de mot de passe. Référez-vous à la Procédure de récupération de mot de passe pour l'équipement Cisco Aironet.

Q. Est-il possible d'utiliser deux antennes externes afin de couvrir deux cellules radio (par exemple, antenne 1 pour cellule 1 et antenne 2 pour cellule 2) ?

A. Vous ne pouvez pas utiliser deux Antennes sur un AP afin de couvrir deux cellules radio. Les tentatives d'utiliser les antennes pour couvrir deux cellules radio peuvent avoir comme

conséquence des problèmes de connectivité. Le but des deux antennes est d'améliorer la couverture d'une cellule dans une tentative de surmonter les problèmes qui surgissent avec la distorsion due à la propagation par trajets multiples et les signaux nuls. Référez-vous à Propagation par trajets multiples et diversité pour plus d'informations sur la diversité et les distorsions dues à la propagation par trajets multiples.

Q. À quoi sert l'utilisation de la commande mobility network-id sur un AP ?

A. Vous employez la commande **mobility network-id** afin de configurer la mobilité de couche 3 dans un réseau sans fil. Vous utilisez la commande **mobility network-id ssid** afin d'associer un service set identifier (SSID) à une ID réseau de mobilité de couche 3. Avec la mobilité de couche 3, les clients peuvent être en itinérance sur différents AP qui résident dans différents sous-réseaux. Les clients en itinérance restent connectés à votre réseau et ne changent pas d'adresse IP.

Vous devez utiliser un module de services LAN (WLAN) sans fil (WLSM) comme périphérique de wireless domain services (WDS) afin de configurer correctement la mobilité de couche 3. La mobilité de couche 3 n'est pas prise en charge quand vous utilisez un AP comme votre périphérique WDS. Pour plus d'informations sur la mobilité de couche 3, référez-vous à la section *Compréhension de la mobilité de couche 3* de Configuration de WDS, itinérance rapide et sûr, et gestion de radio.

La commande est censée être utilisée quand l'AP participe à une infrastructure WDS avec un module WLSM (qui agit en tant que périphérique WDS) dans laquelle il y a une mobilité de couche 3. Si vous utilisez cette commande de manière incorrecte, cela entraîne des problèmes de connectivité dans le réseau WLAN, tels que les suivants :

- Les clients n'obtiennent pas d'adresses IP du DHCP.
- Dans certains cas, les clients ne peuvent pas s'associer à l'AP.
- Les clients sans fil ne peuvent pas s'associer à l'AP.
- L'authentification par l'Extensible Authentication Protocol (EAP) ne se produit pas. Quand la commande **mobility network-id** est configurée, l'AP essaye d'établir un tunnel d'encapsulation de routage générique (GRE) pour la transmission des paquets EAP. Si aucun tunnel n'est établi, les paquets ne peuvent aller nulle part.
- L'AP qui est configuré comme périphérique WDS ne fonctionne pas comme prévu et la configuration WDS ne fonctionne pas.

Q. Combien d'identifiants d'ensemble de services (SSID) pouvez-vous avoir par VLAN ?

A. Vous ne pouvez avoir qu'un SSID par VLAN. L'utilisation de SSID multiples sur un seul VLAN n'est pas prise en charge avec les AP Aironet.

Q. Quelle est la valeur BSSID quand des ESSID multiples sont assignés aux AP ?

A. Si l'AP fonctionne en mode léger, alors chaque ESSID sur un AP sera géré via un BSSID différent (où chaque BSSID est basé sur le MAC radio de base et diffère seulement dans le quartet d'ordre bas.)

Si l'AP exécute un IOS, alors tous les ESSID sur l'AP seront gérés via le même BSSID (à moins

que MBSSID soit configuré, dans ce cas ils seront gérés via différents BSSID).

Q. Est-il possible de configurer ma radio A pour un pont et la radio G pour la fonctionnalité AP ? Si oui, comment puis-je le faire ?

A. Oui, il est possible de configurer chaque radio dans votre AP pour des fonctionnalités différentes. Dans votre scénario, cela peut se faire si vous configurez différents Service Set Identifiers (SSID) pour les radios G et A. Puis, configurez le rôle dans un paramètre de réseau radio pour la radio G avec l'AP et pour la radio A avec le pont racine.

Q. Quand deux clients s'associent à deux AP différents qui sont connectés sur le même sous-réseau, la communication se fait-elle par le réseau câblé ou sans fil ?

A. Pour ce scénario, si les deux AP sont paramétrés en mode racine, la communication entre les deux AP se fait par le réseau câblé. Si l'un des AP est paramétré en mode répéteur et l'autre en mode racine, la communication entre les AP se fait sans fil.

Q. Est-il possible d'activer le routage ou la Traduction d'adresses de réseau (NAT) sur des AP Cisco ?

A. Non, le routage et les fonctionnalités NAT ne sont pas pris en charge sur les AP.

Q. Y a-t-il un moyen de programmer une heure à laquelle l'AP basé sur le logiciel Cisco IOS est disponible ? Je veux fournir un accès basé sur l'heure aux clients qui se connectent à l'AP.

A. Vous pouvez configurer des listes de contrôle d'accès (ACL) basées sur l'heure à l'aide de plages temporelles. aide basée sur temps d'ACLs vous pour s'assurer que les utilisateurs peuvent accéder au réseau Sans fil au cours d'un délai prévu particulier, par exemple, 9:00 heure du matin à 5:00 P.M. (0900 1700). L'utilisation d'ACL basées sur l'heure ne ferme pas l'AP ou la radio. Les ACL basées sur l'heure arrête le passage du trafic sur l'AP de façon à ce que les utilisateurs ne puissent pas accéder au réseau. Pour les informations sur la façon dont configurer cette caractéristique, référez-vous à l'*ACLs basé sur temps utilisant la section de plages de temps de* Listes d'accès de ConfiguringIP.

Q. Les AP peuvent-ils avoir plusieurs pools DHCP à travers différents sous-réseaux ?

A. Quand vous configurez l'AP comme un serveur DHCP, des adresses IP sont assignées aux périphériques qui sont sur le sous-réseau que le serveur DHCP. Les périphériques communiquent avec d'autres périphériques sur le sous-réseau, mais ne communiquent pas au delà du sous-réseau. Si vous devez envoyer des données au-delà du sous-réseau, vous devez affecter un routeur par défaut. L'adresse IP du routeur par défaut doit être sur le même sous-réseau que l'AP que vous avez configuré comme le serveur DHCP.

Q. Qu'est-ce que la mesure dBm ? Comment déterminer les valeurs dBm équivalentes pour la puissance du signal (en mW) mentionnée sur mon point d'accès (AP) Aironet ?

A. L'unité dB mesure la puissance d'un signal en fonction de son taux par rapport à une autre valeur normalisée. Cette abréviation dB est souvent combinée avec d'autres abréviations afin de représenter les valeurs qui sont comparées. Ainsi, dBm est la valeur qui résulte de la comparaison entre la dB et une valeur de référence normalisée de 1 mW.

La formule pour calculer cette valeur dBm en mW à partir de la puissance du signal donnée est :

```
Power (in dB) = 10 * log10 (Signal/Reference)
```

Cette liste définit les termes contenus dans la formule. log10 est un logarithme de base 10.

- Signal désigne la puissance du signal (par exemple, 50 mW).
- Reference désigne la puissance de référence (par exemple, 1 mW).

Exemple :

Si vous voulez calculer la puissance en dB d'une puissance de signal de 50 mW, appliquez cette formule :

```
Power (in dB) = 10 * log10 (50/1) = 10 *log10 (50) = 10 * 1.7 = 17 dBm
```

Cette formule a comme conséquence une règle générale qui stipule :

- Pour chaque augmentation de 3 dB (dBm ici), cela entraîne une augmentation par deux de la puissance de transmission actuelle (mW). Pour chaque diminution de 3 dB, cela réduit la puissance de transmission à la moitié de sa valeur courante.
- Pour chaque augmentation de 10 dB (dBm), cela entraîne une augmentation par dix de la puissance de transmission actuelle (mW). Pour chaque diminution de 10 dB, cela réduit la puissance de transmission à un dixième de sa valeur courante.
- Pour chaque augmentation de 30 dB (dBm), cela entraîne une augmentation par 1 000 de la puissance de transmission actuelle. Pour chaque diminution de 30 dB, cela réduit la puissance de transmission à un millième de sa valeur courante.

Ce tableau fournit des correspondances approximatives entre valeurs en dBm et valeurs en mW :

d Bm	m W
0	1
1	1.25
2	1.56
3	2
4	2.5
5	3.12
6	4
7	5
8	6.25
9	8
10	10
11	12.5
12	16
13	20
14	25
15	32
16	40
17	50
18	64
19	80
20	100
21	128
22	160
23	200
24	256
25	320
26	400
27	512
28	640
29	800
30	1000 or 1 W

Référez-vous aux Valeurs de puissance RF pour plus d'informations.

Q. Comment puis-je modifier les paramètres de date et d'heure sur les AP 1231 Cisco ?

A. Allez à l'interface web (GUI), choisissez les **services > le SNTP**, les **paramètres horaires** choisis et puis changez le temps.

Q. Si CCKM n'est PAS configuré sur le client, mais qu'il est configuré sur des AP, le

client sera-t-il capable de s'associer à l'AP ? Les clients peuvent-ils faire de l'itinérance normale ?

A. Le comportement dépend du configuration de l'AP. Si CCKM n'est PAS configuré/pris en charge sur le client, le client ne s'associe pas à un AP qui est paramétré sur CCKM « mandatory ». Si l'infrastructure (AP) est paramétrée sur CCKM « optional », le client s'associe et établit sa liaison non CCKM.

Selon les clients déployés, il est généralement recommandé de paramétré CCKM sur « optional » sur l'infrastructure qui permet l'association de tous les périphériques, mais prend en charge l'itinérance rapide SEULEMENT pour des périphériques compatibles/associés par CCKM.

Q. Quelle est la différence en capacité mémoire entre les AP 1240 et 1230 ?

A. Voici les capacités mémoire des AP 1240 et 1230 :

- L'AP 1240 est une plate-forme AP de 32 Mo.
- L'AP 1230 est une plate-forme AP de 16 Mo.

Q. J'ai deux AP 1240 qui prennent en charge la flexibilité du rôle de la liaison. Je voudrais établir un pont entre eux avec 802.11a, avec des clients joints sur les bandes 802.11b/g. Y a-t-il des restrictions pour faire cela ?

A. La flexibilité de rôle de lien de Point d'accès fournit le support de fonctionnalité de mode de passerelle pour les Points d'accès qui ont la capacité à deux bandes (1200, 1230, et les séries 1240AG). Dans la configuration cible, la radio 802.11a fonctionne en mode pont, alors que la radio 802.11g est en mode point d'accès.

La condition est que quand vous configurez un AP avec flexibilité du rôle de la liaison, l'une des radios de l'AP doit être configurée comme AP racine, et le second AP qui établit le pont en retour doit être en mode répétiteur ou WGB vers l'AP racine.

Q. Combien de combinés téléphoniques de Téléphonie IP sans fil sont recommandés par AP ?

A. Le dimensionnement de réseau de Téléphonie sur IP est essentiel pour s'assurer que la bande passante et les ressources adéquates sont disponibles pour porter le trafic vocal critique. En plus des directives habituelles sur la conception en téléphonie IP pour le dimensionnement des composants, tels que des ports de passerelle PSTN, des transcodeurs, la bande passante WAN, etc., prenez en considération ces problèmes liés à la norme 802.11b lorsque vous dimensionnez votre réseau de téléphonie IP :

- Nombre de périphériques 802.11b par AP : Cisco vous recommande de n'en avoir pas plus de 15 à 25.
- Nombre de téléphones 802.11b par AP

Avant que toute discussion au sujet de projets de réseau n'ait lieu, cela aide à comprendre les fondements de la capacité globale du réseau. Ces directives sur la capacité du réseau s'appliquent au dimensionnement du réseau de téléphonie IP sans fil :

- Pas plus de sept appels G.711 simultanés par AP

- Pas plus de huit appels G.729 simultanés par AP

Remarque: Ces recommandations de conception supposent que la Voice Activity Detection (VAD) a été désactivée sur les téléphones IP sans fil Cisco 7920.

L'utilisation de VAD sur les téléphones Cisco 7920 peut économiser de la bande passante, mais Cisco recommande que vous désactiviez VAD sur tous les serveurs Cisco CallManager pour fournir une meilleure qualité vocale globale. En plus de la détermination de la quantité de bande passante nécessaire pour un appel VoIP 802.11b, vous devez également prendre en compte le conflit radio global pour un canal RF particulier. La règle générale est que vous ne devriez pas déployer plus de 20 à 25 périphériques 802.11b par AP. Plus vous ajoutez de périphériques à un AP, plus vous réduisez la quantité de bande passante et augmentez potentiellement les retards de transmission. Le nombre maximal de téléphones par AP dépend des configurations d'appel des utilisateurs individuels (basé sur des taux d'Erlang). Cisco recommande un maximum de sept appels simultanés utilisez utilisant le G.711 ou huit appels simultanés utilisant le G.729. Au-delà de ce nombre d'appels, quand des données de base excessives sont présentes, la qualité vocale de tous les appels devient inacceptable. Les débits de mise en paquet pour ces recommandations sont basés sur des taux d'échantillonnage de 20 ms avec VAD désactivée. Ce débit produit 50 paquets par seconde (pps) dans chaque direction. Un plus grand échantillon (40 ms par ex.) peut avoir comme conséquence un plus grand numéro d'appels simultanés, mais il augmente également le retard de bout en bout des appels VoIP.

Le nombre de téléphones 802.11b que vous pouvez déployer par sous-réseau de couche 2 ou VLAN dépend de ces facteurs :

- N'utilisez pas plus de sept appels actifs de G.711 ou huit de G.729 par AP.
- Le taux d'appel est utilisé pour déterminer le nombre d'appels actifs et inactifs. Ce taux est souvent déterminé avec des calculatrices d'Erlang. Se basant sur ces facteurs et des taux d'Erlang de haut niveau normaux (entre 3:1 et 5:1), Cisco recommande que vous déployez un maximum de 450 à 600 téléphones Cisco 7920 par sous-réseau de couche 2 ou VLAN.

Référez-vous à la section *Dimensionnement de réseau* de Infrastructure réseau sans fil, ainsi qu'à Votre WLAN est-il compatible voix ? pour plus d'informations détaillées.

Q. Comment puis-je faire pour qu'un AP 1200 arrête de traiter des demandes d'authentification après un nombre de tentatives déterminé ?

A. Vous pouvez utiliser l'option de nombre maximum de nouvelles tentatives sur le serveur AAA pour limiter le nombre de fois qu'ont les clients pour essayer d'accéder à un réseau. La valeur du nombre maximum de nouvelles tentatives peut être configurée manuellement sur le serveur AAA, ou vous pouvez utiliser le nombre de nouvelles tentatives par défaut qui dépend du serveur AAA qui est utilisé.

Q. Où puis-je trouver des informations sur les différences qui existent dans les diverses plates-formes d'AP et de LAP ?

A. Référez-vous aux forums aux questions Sans fil de matériel de Cisco. Ce document contient des informations utiles qui comparent les différents modèles d'AP et de LAP.

Q. Est-ce que le protocole point à point sur Ethernet (PPPoE) est pris en charge dans les points d'accès Cisco Aironet ?

A. Non, PPPoE n'est pas pris en charge dans les points d'accès Cisco Aironet.

Q. Le protocole d'agrégation de VLAN (VTP) est-il pris en charge dans les points d'accès Cisco Aironet ?

A. Non, VTP n'est pas pris en charge dans les points d'accès Cisco Aironet.

Q. Cisco Aironet AP prend en charge-il le point standard Protocol (IAPP) 802.11f Inter-Access ?

A. Non, l'AP Cisco Aironet ne prend pas en charge la norme 802.11f basée sur IAPP. Les points d'accès Cisco offrent leur propre protocole entre points d'accès, robuste, riche en fonctionnalités et éprouvé.

Q. À quoi servent les commandes bridge-group 1 block-unknown-source et bridge-group 1 source-learning dans un AP ?

A. Utilisez la commande d'interface de configuration **bridge-group block-unknown-source** pour bloquer le trafic venant d'adresses MAC inconnues sur une interface spécifique. Utilisez la forme **no** de la commande pour désactiver le blocage de source inconnue sur une interface spécifique.

Pour que STP fonctionne correctement, la commande **block-unknown-source** doit être désactivée pour les interfaces qui participent dans STP.

```
bridge-group group block-unknown-source
```

Quand vous activez STP sur une interface, la commande **block-unknown-source** est désactivée par défaut.

La commande **bridge-group 1 source-learning** fait apprendre à l'AP l'adresse source du client. Utilisez la forme **no** de la commande pour désactiver l'apprentissage par l'AP de l'adresse source du client.

Q. Y a-t-il un moyen de donner la priorité au trafic qui passe par l'AP, de sorte que le trafic venant d'un SSID particulier configuré sur l'AP utilise plus de bande passante que les autres SSID sur le même AP ?

A. Ceci peut être réalisé avec la mise en place de la Qualité de service (QoS) sur des AP.

- Créez des stratégies QoS et appliquez-les aux VLAN configurés sur votre point d'accès. Ces documents expliquent QoS et comment configurer des stratégies QoS sur un AP.Qualité de service sans filConfigurer QoS sur des points d'accès Aironet
- Puis, mappez les SSID configurés sur l'AP pour les VLAN individuels mentionnés. De cette façon, si vous donnez la priorité au trafic basé sur le VLAN, vous pouvez, à son tour, donner la priorité au trafic basé sur le SSID.

Q. Y a-t-il un moyen de limiter le nombre maximal de périphériques clients pouvant se connecter à un seul point d'accès autonome ?

A. Le comportement par défaut d'un périphérique client Cisco est qu'il se connecte à l'AP qui a la

meilleure puissance de signal disponible. Mais vous pouvez limiter les clients pouvant se connecter à n'importe quel AP particulier par l'authentification MAC. Vous devez fournir l'adresse MAC du client à l'AP de sorte que l'AP ne puisse autoriser que ces clients et limiter la connexion à cet AP particulier à tous les autres clients qui ne font pas partie de la liste d'adresses MAC autorisée.

Q. Où puis-je télécharger le dernier logiciel ?

A. L'équipement Cisco Aironet fonctionne mieux quand vous chargez tous les composants avec la version du logiciel la plus en cours. Référez-vous au Centre logiciel sans fil Cisco (clients enregistrés seulement) afin de télécharger les derniers logiciels et pilotes.

Q. Est-il nécessaire de couper tous les ordinateurs portables et autres périphériques sans fil pendant une mise à niveau d'AP ?

A. Non, il n'y a pas besoin de couper les périphériques. La mise à niveau d'AP est processus sûr et tout peut rester allumé. Assurez-vous que vous êtes connecté(e) à un serveur TFTP.

Q. Où puis-je trouver des instructions sur la façon dont mettre à niveau Cisco IOS® sur des AP Cisco Aironet ?

A. Référez-vous à fonctionner avec des images logicielles pour des instructions sur la façon dont améliorer le Cisco IOS sur AP.

Remarque: Utilisez l'option **force-reload** avec la commande **archive download-sw**.

Remarque: Quand vous mettez à niveau le logiciel d'AP ou du système de pontage en entrant la commande **archive download-sw** sur le CLI, vous devez utiliser l'option **force-reload**. Si l'AP ou le pont ne recharge pas la mémoire flash après la mise à niveau, les pages dans l'interface du navigateur Web risquent de ne pas refléter la mise à niveau. Cet exemple montre comment mettre à niveau une plate-forme logicielle en utilisant la commande **archive download-sw** :

```
AP#archive download-sw /force-reload / overwrite tftp://10.0.0.1/image-name
```

Q. J'ai un AP 1100. Je veux mettre à niveau la radio AP, passant de IEEE 802.11b à IEEE 802.11g. Si je mets à niveau la radio dans l'AP, puis-je utiliser les cartes PC existantes ? Ou bien ai-je besoin de mettre à niveau les cartes PC aussi ? Les cartes sont actuellement des cartes 802.11b.

A. Une mise à niveau de la radio, de 802.11b à 802.11g, n'a comme conséquence aucune amélioration des performances si vous utilisez seulement les clients 802.11b. Un avantage de la mise à niveau radio à 802.11g est que vous pouvez connecter des clients 802.11b et 802.11g avec l'AP. Avec la mise à niveau, les clients 802.11b se connectent à 11 Mbps et les clients 802.11g se connectent à 54 Mbps.

Q. Comment rétablir les paramètres d'usine par défaut de l'AP ?

A. Référez-vous à la Procédure de récupération de mot de passe pour l'équipement Cisco Aironet.

FAQ sur le dépannage

Q. J'ai fait quelques modifications dans la configuration de l'AP. Quand j'essaie de sauvegarder les modifications, j'obtiens ce message sur l'AP : **""Error writing new config file "flash: //config.txt.new" nv_done: unable to open "flash: //config.txt.new" nv_done: unable to open "flash: //private-multiple-fs.new"[OK]". Que signifie ce message ?**

A. Ce message d'erreur indique qu'il n'y a aucun espace libre dans la mémoire Flash pour enregistrer la nouvelle configuration. Essayez de supprimer tous les vieux fichiers de crash qui existent. Ou, s'il y a plus d'une version du logiciel Cisco IOS, supprimez celle que vous n'utilisez pas. Ceci peut libérer de l'espace dans la mémoire Flash. Émettez la commande **dir flash** afin de déterminer s'il y a de vieux fichiers crashinfo que vous pouvez supprimer ou de vieilles images qui sont non utilisées. Émettez la commande **write memory** afin de libérer de l'espace, de sorte que vous puissiez écrire la configuration dans la mémoire.

Q. J'utilise Aironet Client Utility (ACU) 6.3 et des points d'accès (AP) Cisco 1200 qui exécutent le logiciel Cisco IOS Version 12.3(8)JA. Quand le client sans fil est associé à l'AP, le nom de l'AP n'est pas affiché sur l'ACU. Pourquoi ?

A. **Le nom AP** est l'adresse Internet pour AP. Si des extensions Aironet sont activées sur l'AP, alors le nom de l'AP est affiché sur l'ACU.

Si vous ne souhaitez pas voir le nom de l'AP, vous pouvez désactiver des extensions Cisco Aironet à la norme IEEE 802.11b (**pas d'extensions dot11 aironet** sous l'interface radio). Les extension Cisco Aironet sont activées par défaut dans l'AP.

Si elles sont précédemment désactivées, vous pouvez activer les extension Cisco Aironet avec cette commande :

```
AP(config-if)#dot11 extension aironet
```

Dans une balise, l'AP inclut un élément d'information propriétaire de Cisco qui contient le nom de l'AP. Si vous arrêtez les extensions Aironet sur l'AP, l'AP ne balise pas son nom. Référez-vous à Désactiver et activer des extensions Aironet pour plus d'informations sur les extensions Aironet.

Q. Mon point d'accès (AP) autorise et se connecte seulement à un client à la fois. Qu'elle peut en être la raison ?

A. Une raison possible pourrait être que le paramètre de **max-associations** est sur **1** dans la configuration du Service Set Identifier (SSID). Employez la commande de mode configuration SSID **max-associations** afin de configurer le nombre maximal d'associations pris en charge par l'interface radio (pour le SSID spécifié). Utilisez la forme **no** de la commande afin de réinitialiser le paramètre à la valeur par défaut. Ce maximum par défaut est 255.

Q. Comment puis-je récupérer des mots de passe oubliés ?

A. Référez-vous à la Procédure de récupération de mot de passe pour l'équipement Cisco Aironet.

Q. Les numéros de série n'apparaissent pas sur BR350 ou AP350s l'un des que nous avons par des commandes. Ceux-ci sont des VxWorks et n'ont pas été convertis en IOS. Comment puis-je récupérer ces informations dans les périphériques ?

A. Les AP et ponts de la gamme 350 qui exécutent VxWorks n'affichent pas le numéro de série dans le logiciel. La seule façon d'identifier le numéro de série sur ces unités est d'inspecter physiquement l'étiquette sur le matériel lui-même.

Q. Quelles sont les sources possibles d'interférence pour la liaison radiofréquence (RF) de l'AP ?

A. L'interférence peut provenir un certain nombre de sources, comme :

- Téléphones sans fil 2,4 GHz
- Fours à micro-ondes incorrectement blindés
- Équipement sans fil que d'autres sociétés fabriquent

Moteurs électriques et les pièces métalliques mobiles de machines peuvent également produire une interférence. Référez-vous à ces documents pour plus d'informations :

- Dépannage des problèmes affectant la communication par radiofréquence
- Problèmes d'intermittence de la connectivité avec les ponts sans fil

Q. Je voie le message d'erreur : %C4K_EBM-4-HOSTFLAPPING:Host [mac-addr] in vlan [num] is flapping between port [num] and port [num] connected to the Access Points. Comment résoudre cela ?

A. Ce message d'erreur se produit quand un commutateur apprend la même adresse MAC via plusieurs ports. Ceci peut être dû à l'une de ces raisons

1. Quand un client est en itinérance d'un AP à un autre AP, le nouvel AP informe le client de l'adresse MAC vers le commutateur. Si les deux AP sont connectés au même commutateur, l'adresse MAC du client est associée aux deux ports de commutateur connectés aux AP. Ceci crée une double entrée pour le client et produit ce message d'erreur jusqu'au moment où le commutateur synchronise sa table CAM. Ce message d'erreur est tout à fait normal dans un environnement sans fil, mais, si trop d'itinérance se produit, cela peut surcharger le CPU du commutateur. Contrôlez le pilote et le microprogramme du client. En outre, assurez-vous que la couverture est bonne de sorte que client ne soit pas souvent en itinérance.
2. Quand il y a une boucle, le commutateur peut apprendre la même adresse MAC via plusieurs ports connectés à d'autres commutateurs. Assurez-vous que le TP est activé sur le commutateur.

Q. Pourquoi la carte du client ne s'associe-t-elle pas à l'AP le plus proche ?

A. S'il y a plusieurs AP dans votre topologie sans fil, votre client maintient une association avec l'AP avec lequel il s'est initialement associé, jusqu'à ce que le client perde les balises keepalive de cet AP. Si le contact est perdu et si les tentatives de reprendre le contact avec l'AP initial continuent d'échouer, le client cherche alors un autre AP. Le client essaye de s'associer à ce nouvel AP si le client a des droits suffisants et une autorisation sur le nouvel AP.

Q. J'ai un AP Cisco et un Cisco Secure Access Control Server (ACS) 3.2. J'ai l'Extensible Authentication Protocol (EAP) mis en application dans le réseau. Des utilisateurs ne sont pas authentifiés par le serveur RADIUS. Quand j'émets des

commandes debug sur l'AP, j'obtiens cette sortie : **""Jun 2 15:58:13.553: %RADIUS-4-RADIUS_DEAD : RADIUS server 10.10.1.172:1645,1646 is not responding. Jun 2 15:58:13.553: %RADIUS-4-RADIUS_ALIVE : RADIUS server 10.10.1.172:1645,1646 has returned. Jun 2 15:58:23.664: %DOT11-7-AUTH_FAILED : Station 0040.96a0.3758 Authentication failed."** Pourquoi ai-je ces messages d'erreur sur l'AP ?

A. Une des raisons pour lesquelles ces messages d'erreur apparaissent est que le secret partagé n'est pas le même dans l'AP et l'ACS. Cette erreur est courante quand vous configurez EAP. S'il y a une erreur de correspondance de secret partagé entre l'AP et l'ACS 3.2, EAP ne fonctionne pas. Le serveur RADIUS n'accepte pas les paquets transmis par l'AP. Assurez-vous que le secret partagé sur l'AP correspond à celui configuré sur le serveur ACS. Pour obtenir des informations sur la façon de déboguer, référez-vous au Débogage d'authentifications.

Q. Quand j'ai regardé les enregistrements sur l'AP, j'ai trouvé cette erreur : **""Mar 9 11:05:26.225 Information Group rad_acct: Radius server 10.10.1.172:1645,1646 is responding again (previously dead). Mar 9 11:03:09.361 Error Group rad_acct: No active radius servers found."** Quelle est la cause de cette erreur et comment puis-je résoudre le problème ?

A. Il est normal de voir cet enregistrement quand le paramètre **radius-server deadtime** est configuré sur l'AP. C'est un enregistrement informatif et n'est pas un problème grave. Utilisez la commande **radius-server deadtime** afin de paramétrer un intervalle pendant lequel l'AP n'essaye pas d'utiliser les serveurs qui ne répondent pas, évitant ainsi d'attendre qu'une requête n'expire avant d'essayer le prochain serveur configuré. Un serveur marqué comme mort est sauté par des demandes supplémentaires pendant la durée en minutes que vous spécifiez, jusqu'à 1 440 (24 heures).

Q. J'ai un AP 1230 avec le logiciel Cisco IOS Version 12.3(4)JA. Quand je mets à jour la liste de contrôle d'accès (ACL), je reçois ce message : **« % d'avertissement : Saving this config to nvram may corrupt any network management or security files stored at the end of nvram. Continuez ? [non] : "**

A. C'est un message d'avertissement et non une erreur. Si vous sélectionnez [no] alors il ne sauvegarde pas sur les points d'accès (AP). Les configurations ne sont pas sauvegardées sur la RAM non volatile (NVRAM), elles sont sauvegardées sur la mémoire Flash.

Bien que ce soit un avertissement, vous avez un problème de mémoire sur cet AP. Vous avez de nombreuses fichiers .rcore qui prennent beaucoup d'espace sur votre mémoire. Cette sortie montre un exemple :

```
3 -rwx 262144 Mar 3 2002 22:40:04 +00:00 r13_5705_9760_1EA7A81E.rcore

4 -rwx 262144 Mar 1 2002 17:21:44 +00:00 r13_5705_9760_709D16F4.rcore

5 -rwx 262144 Mar 7 2002 20:19:12 +00:00 r13_5705_9760_9D2DE9CD.rcore

6 -rwx 262144 Mar 26 2002 23:42:22 +00:00 r13_5705_9760_AAE78172.rcore

151-rwx 262144 Mar 1 2002 17:22:00 +00:00 r13_5705_9760_7187935C.rcore
```

Afin de nettoyer la mémoire, effacez toutes les fichiers .rcore de la mémoire Flash.

Voici une exemple de la commande que vous avez besoin d'entrer en mode enable :

```
ap#delete flash:r13_5705_9760_1EA7A81E.rcore
```

Remarque: émettez la commande **delete flash:** pour chaque fichier .rcore sur votre mémoire Flash.

Q. J'ai un module de services LAN sans fil (WLSM) avec le logiciel Cisco IOS Version 12.4(4)T1 installé. Les connexions aux clients s'arrêtent. Après avoir regardé les enregistrements, j'ai vu de nombreux message du type « Previous authentication no longer valid »et « Disassociated because sending station is leaving (or has left) BSS ». Quel est le problème ?

A. Point de chacun des deux messages vers une question rf. Assignez différents canaux sur l'AP afin de résoudre ce problème.

Q. Les AP Cisco Aironet dans mon réseau WLAN ne diffusent pas les Service Set Identifier (SSID). Qu'elle peut en être la raison ? Dois-je activer une fonctionnalité particulière sur l'AP ?

A. Tant que vous n'activez pas le mode d'invité sous le gestionnaire SSID, AP n'annonce pas le SSID dans des ses balises. Vous pouvez vérifier avec un client et faire une recherche de SSID afin de s'assurer qu'il n'est pas mentionné.

Afin d'activer le mode guest sur un SSID, saisissez cette commande sur l'AP en mode de configuration globale :

```
Ap<config>#dot11 ssid ssid-string Ap<config-ssid>#guest-mode
```

Q. J'ai mon AP AIR-AP1231G-A-K9. Pourquoi est-ce que je ne vois pas d'option pour activer la radio A sur cet AP et que je ne peux voir que l'option pour les radios G ? N'ai-je pas la possibilité d'y associer des clients 802.11b ?

A. L'AP AIR-AP1231G-A-K9 a une radio G. Le numéro de la pièce AP1231G implique qu'il dispose seulement de la radio G. Les radios G sont rétro-compatibles avec les radios B, parce qu'elles fonctionnent sur la même fréquence. Il n'y a aucune radio A sur cette unité et c'est pourquoi vous ne pouvez pas l'allumer. Vous pourriez devoir ajouter le module de radio A. La radio A fonctionne sur une fréquence différente (à 5 GHz) des radios G et B (à 2,4 GHz).

Q. J'ai un téléphone IP Cisco 7920 qui est connecté à un AP Cisco. Je vois que le 7920 est associé à l'AP, mais aucune adresse IP n'est assignée. J'utilise l'Extensible Authentication Protocol (EAP). Je vois le message « Info Station [SEP001121ceb9a4]001121ceb9a4 Authenticated », suivi de « Info Station [SEP001121ceb9a4]001121ceb9a4 Reassociated » et « Warning EAP retry limit reached for Station [SEP001121ceb9a4]001121ceb9a4 ». Puis je vois « Info Deauthenticating [SEP001121ceb9a4]001121ceb9a4, reason 'Previous Authentication No Longer Valid' ». Quel est le problème ?

A. La raison pour laquelle vous avez ces messages est que le secret partagé dans l'AP est différent du secret partagé du serveur RADIUS. Assurez-vous que les clés de secret partagé pour l'EAP sont identiques sur les deux. Vous devez ressaisir la clé de secret partagé dans l'AP et le serveur RADIUS.

Q. J'ai un problème avec mon AP. Il continue à envoyer trop de messages RTS de manière sporadique, ce qui entraîne la dissociation inattendue de clients associés. Ces clients étaient associés à cet AP à un niveau de signal compris entre -91 et -95 dBm. Quelle est la raison de cette dissociation inattendue ? Est-ce un comportement prévu de l'AP ?

A. Oui, c'est un comportement prévu. Votre client est juste en périphérie de la cellule 1 Mbps. Puisque vous le voyez entre -91 et -95 dBm, le comportement erratique est prévu.

Installez plus d'AP afin de résoudre ce problème. Ou, si votre couverture désirée est dans une zone focalisée plutôt qu'omnidirectionnelle, utilisez des antennes directionnelles.

Le RTS est provoqué par l'intervention des mécanismes de relance. Le client devrait répondre à un RTS avec un CTS, mais si le client les voit dans un renifleur comme un groupe d'environ huit trames RTS sans CTS correspondant, alors le client n'entend pas l'AP ou est le client est si loin que l'AP ne peut pas l'entendre. Les deux périphériques doivent s'entendre, que l'AP entende le client n'est pas suffisant. Ainsi, si l'antenne sur le client n'est pas d'une très bonne conception (probable), si son émetteur ne transmet pas à 100 mW (très probable), ou si son récepteur est loin de la sensibilité -90 à -95 dBm (presque garanti si ce n'est pas un client Cisco), alors vous obtenez le fonctionnement que vous décrivez.

Q. Nous utilisons des AP Cisco LWAPP sans fil. Bien que j'aie vu beaucoup de retransmissions TCP et de doubles ACK au niveau des clients, je ne vois pas ces derniers dans notre environnement câblé. Est-ce normal dans un dispositif sans fil ?

A. Les paquets corrompus et les paquets retransmis sont deux des mesures fondamentales d'un 802.11 WLAN. L'analyse des paquets corrompus et retransmis en 802.11 diffère de l'analyse dans un LAN câblé pour trois raisons :

- D'abord, les WLAN 802.11 ont généralement beaucoup plus de paquets corrompus que les LAN câblés, donc l'importance des trames corrompues dans un WLAN 802.11 est plus grande.
- Ensuite, la norme 802.11 définit une couche liaison de données fiable, ce qui signifie que chaque paquet corrompu doit avoir comme conséquence une retransmission. Généralement, les LAN câblés ne définissent pas une couche liaison de données fiable, ainsi une retransmission se produit seulement si un protocole de couche supérieure fiable est en service.
- Enfin, la fiabilité de couche supérieure est en général de bout en bout, ce qui signifie qu'un paquet corrompu où que ce soit entre la source et la destination entraîne une retransmission. Une retransmission 802.11, puisqu'elle se produit au niveau de la couche 2, est mise en application entre les interfaces sans fil, de sorte qu'une retransmission 802.11 peut seulement être provoquée par la corruption sur le « segment » local. Ceci rend l'identification de l'emplacement de la corruption dans un WLAN 802.11 beaucoup plus facile que dans un LAN câblé traditionnel. Explorons les implications de ces différences.

L'un des défis d'un environnement sans fil est qu'il est difficile de déterminer si l'analyseur voit les mêmes choses que les clients. Les différences entre l'analyseur et le client – radios, antennes ou emplacements physiques différents – peuvent faire que l'analyseur voit des choses différentes par rapport à celles que voit le client. Par exemple, si l'analyseur est loin de l'AP, mais que le client sans fil est proche de l'AP, l'analyseur peut voir une trame corrompue, tandis que la station voit

une trame non corrompue. Puisque nous savons que chaque trame corrompue entraîne une retransmission, nous pouvons utiliser les nombres relatifs de retransmissions et de trames corrompues pour évaluer à quel degré l'analyseur voit ce que la station voit sur le réseau.

Q. Nous voyons ce message Syslog diffusé sur notre réseau. Pourquoi est-ce que ceci se produit et comment l'arrêter ? `AP:001f.ca26.bfb4: %LWAPP-3-CLIENTERRORLOG: Decode Msg: could not match WLAN <id>`

A. Ces messages sont les messages d'avertissement et sont vus quand le dépassement WLAN est activé et l'ID de WLAN particulier n'est pas sélectionné ou est annoncé sur un emplacement/radio.

Q. J'ai des problèmes quand je mets à niveau mon AP en utilisant le serveur TFTP. À chaque fois que j'essaye de mettre à niveau, cela ajoute une extension .tar au fichier image de mise à niveau c1200-k9w7-tar.default, ce qui fait que l'AP ne reconnaît pas le fichier. Je ne trouve pas de moyen de supprimer l'extension .tar supplémentaire. (J'ai téléchargé et essayé avec solarwind et tftpd32.) Que devrais-je faire pour résoudre ce problème ?

A. Le problème pourrait être que le système d'exploitation cache le type de fichier connu. Allez dans **Ordinateur**. Cliquez sur **Tools > Folder Options > View**, défilez jusqu'à ce que vous trouviez le paramètre **Hide extensions for known file types**, et décochez la case. Ceci devrait régler le problème.

Q. Mes points d'accès déclenchent souvent un message d'alerte « high CPU utilization ». En pareil cas, un redémarrage matériel remet les points d'accès en condition de fonctionnement. Comment puis-je surmonter ce problème ?

A. Il y a plusieurs raisons pour que des points d'accès arrivent à une « high CPU utilization ».

- Si le point d'accès Cisco (AP) est connecté au réseau via un commutateur, parfois une « high CPU utilization » est observée sur l'AP. C'est parce que, par défaut, tous les VLAN sont autorisés sur l'AP du commutateur auquel l'AP est connecté. Ceci peut créer un problème, particulièrement appliqué à un énorme réseau. Si tous les VLAN sont autorisés sur l'AP, cela peut avoir comme conséquence une **utilisation élevée du CPU** et la connectivité peut être affectée. Les clients associés au point d'accès rencontrent des problèmes de débit et parfois une utilisation élevée du CPU peut également mettre le réseau sans fil en panne.Afin d'éviter ce problème, élaguez les VLAN au niveau du commutateur de sorte que seul le trafic du VLAN dans lequel l'AP se trouve passe par l'AP.
- Si les points d'accès sont configurés avec des interfaces de bouclage, parfois une « high CPU utilization » est observée sur l'AP. Bien que les interfaces de bouclage puissent être configurées sur l'AP Cisco, elles ne sont pas prises en charge sur l'AP, elles ne doivent donc pas être configurées. Il est conseillé de supprimer les interfaces de bouclage si elles sont configurées sur l'AP.**Remarque:** Les AP et ponts ne prennent pas en charge la commande de bouclage de l'interface.

Comme première étape dans la résolution de ce problème, émettez la commande **show process cpu** dans l'AP. Ceci vous donne une idée des processus qui utilisent le CPU.

En outre, si l'AP exécute une version antérieure à la 12.3(2)JA2, mettez-la à niveau avec la

version 12.3(2)JA2, parce qu'il y a un problème identifié dans les versions antérieures, les demandes de service surchargeant le CPU.

Q. Le routeur wifi 871W arrête des sessions établies en wifi, de sorte que la session VPN de l'utilisateur doit être sans cesse rétablie. Quelle en est la raison ?

A. Il y a plusieurs raisons possibles pouvant entraîner ce problème. Connectez les deux antennes au routeur 871W. Passez au canal 1, 6 ou 11 et vérifiez quel canal obtient la meilleure performance. En outre, vous pourriez avoir d'autres AP dans le voisinage qui peuvent entraîner une interférence. Ce n'est qu'une des raisons possibles.

Informations connexes

- Téléchargements Cisco pour produits sans fil (clients enregistrés seulement)
- Gamme Cisco Aironet 1240 AG - Questions/réponses
- Gamme Cisco Aironet 1230 AG - Questions/réponses
- Guide de configuration logicielle de points d'accès Cisco Aironet pour VxWorks
- Guide de configuration du logiciel Cisco IOS pour points d'accès Cisco Aironet, 12.2(13)JA
- Notes techniques de dépannage gamme Cisco Aironet 350
- Assistance produit sans fil
- Support et documentation techniques - Cisco Systems