

Conception et fonctionnalités du contrôleur de réseau local sans fil - Forum Aux Questions

Table des matières

[Introduction](#)

[FAQ sur la conception](#)

[FAQ sur les fonctionnalités](#)

[Informations connexes](#)

Introduction

Ce document fournit des informations sur les questions les plus fréquentes (FAQ) au sujet des possibilités offertes par un contrôleur de réseau local sans fil (WLC) et ses fonctionnalités disponibles.

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. Comment configurer le commutateur pour qu'il se connecte au WLC ?

R. Configurez le port de commutation, auquel le WLC est connecté, comme port de jonction IEEE 802.1Q. Assurez-vous que seuls les VLAN nécessaires sont autorisés sur le commutateur. Généralement, la gestion et l'interface AP-Manager du WLC ne sont pas balisées. Cela signifie qu'ils supposent le VLAN natif du commutateur connecté. Ce n'est pas nécessaire. Vous pouvez attribuer un VLAN séparé à ces interfaces. Pour plus d'informations, référez-vous à la section [Configuration du commutateur pour le WLC](#) de [Exemple de configuration de base du contrôleur LAN sans fil et du point d'accès léger](#).

Q. Tout le trafic réseau entrant et sortant d'un client WLAN se connecte-t-il en tunnel via un contrôleur de réseau local sans fil (WLC) une fois que le point d'accès (AP) a été enregistré avec le contrôleur ?

R. Lorsque le point d'accès rejoint un WLC, un tunnel CAPWAP (Control and Provisioning of Wireless Access Points protocol) est formé entre les deux périphériques. Tout le trafic, qui inclut tout le trafic client, est envoyé via le tunnel CAPWAP.

La seule exception à cela est quand un AP est en mode hybride-REAP. Les points d'accès REAP hybrides peuvent commuter le trafic de données client localement et effectuer l'authentification client localement lorsque leur connexion au contrôleur est perdue. Lorsqu'ils sont connectés au contrôleur, ils peuvent également renvoyer le trafic au contrôleur.

Q. Puis-je installer des points d'accès légers (LAP) dans un bureau distant et un contrôleur LAN sans fil Cisco (WLC) dans mon siège ? Le protocole LWAPP/CAPWAP fonctionne-t-il sur un réseau étendu ?

R. Oui, vous pouvez avoir les WLC sur le WAN à partir des AP. LWAPP/CAPWAP fonctionne sur un WAN lorsque les LAP sont configurés en mode Remote Edge AP (REAP) ou Hybrid Remote Edge AP (H-REAP). Ces modes permettent le contrôle d'un point d'accès par un contrôleur distant qui est connecté par l'intermédiaire d'une liaison WAN. Le trafic est ponté sur la liaison LAN localement, ce qui évite la nécessité d'envoyer inutilement le trafic local via la liaison WAN. C'est précisément l'un des plus grands avantages qu'offrent les WLC dans votre réseau sans fil.

Remarque : tous les points d'accès légers ne prennent pas en charge ces modes. Par exemple, le mode H-REAP est pris en charge seulement par les points d'accès légers 1131, 1140, 1242, 1250 et AP801. Le mode REAP est pris en charge seulement par les points d'accès 1030, mais les points d'accès 1010 et 1020 ne le prennent pas en charge. Avant que vous prévoyiez d'implémenter ces modes, vérifiez si les points d'accès les prennent en charge. Les AP du logiciel Cisco IOS® (AP autonomes) qui ont été convertis en LWAPP ne prennent pas en charge le mode REAP.

Q. Comment fonctionnent les modes REAP et H-REAP ?

R. En mode **REAP**, tout le trafic de contrôle et de gestion, qui inclut le trafic d'authentification, est renvoyé au WLC par tunnel. Cependant, tout le trafic de données est commuté localement au sein du réseau local du bureau distant. Quand la connexion au WLC est perdue, tous les WLAN sont terminés excepté le premier WLAN (WLAN1). Tous les clients qui sont actuellement associés à ce WLAN sont retenus. Afin de permettre aux nouveaux clients de s'authentifier et de recevoir le service sur ce WLAN pendant les temps d'arrêt, configurez la méthode d'authentification pour ce WLAN en tant que WEP ou WPA-PSK de sorte que l'authentification soit effectuée localement au niveau du REAP. Pour plus d'informations sur le déploiement REAP, consultez le [Guide de déploiement REAP de la filiale](#).

En mode **H-REAP**, un point d'accès retourne en tunnel le trafic de contrôle et de gestion, ce qui inclut le trafic d'authentification, vers le WLC. Le trafic de données d'un WLAN est ponté localement dans le bureau distant si le WLAN est configuré avec la commutation locale H-REAP, ou bien le trafic de données est renvoyé au WLC. Lorsque la connexion au WLC est perdue, tous les WLAN sont terminés à l'exception des huit premiers WLAN configurés avec la commutation locale H-REAP. Tous les clients qui sont actuellement associés à ces WLAN sont retenus. Afin de permettre aux nouveaux clients de s'authentifier et de recevoir le service sur ces WLAN pendant le temps d'arrêt, configurez la méthode d'authentification pour ce WLAN comme WEP, WPA PSK ou WPA2 PSK de sorte que l'authentification soit effectuée localement au niveau de H-REAP.

Pour plus d'informations sur H-REAP, référez-vous au [Guide de conception et de déploiement de H-REAP](#).

Q. Quelle est la différence entre Remote-Edge AP (REAP) et Hybrid-REAP (H-REAP) ?

R. REAP ne prend pas en charge le balisage du VLAN IEEE 802.1Q. En soi, il ne prend pas en charge plusieurs VLAN. Le trafic depuis tous les service set identifiants (SSID) se termine sur le même sous-réseau, mais le H-REAP prend en charge le balisage du VLAN IEEE 802.1Q. Le trafic depuis chaque SSID peut être segmenté à un seul VLAN.

Quand la connectivité au WLC est perdue, c.-à-d., en mode Standalone, REAP sert un seul WLAN, c.-à-d., le premier WLAN. Tout autre WLAN est désactivé. En H-REAP, jusqu'à 8 WLAN sont pris en charge dans le temps d'arrêt.

Une autre principale différence est qu'en mode REAP, le trafic de données peut seulement être ponté localement. Il ne peut pas être commuté de nouveau au site central, mais, en mode H-REAP, vous avez la possibilité de commuter à nouveau le trafic vers le site central. Le trafic depuis les WLAN configurés avec la commutation locale H-REAP est commuté localement. Le trafic de données depuis les autres WLAN est commuté de nouveau au site central.

Consultez l'[Exemple de configuration d'un AP en mode Remote Edge \(REAP\) avec des AP légers et des contrôleurs de réseau local sans fil \(WLC\) pour plus d'informations sur REAP.](#)

Consultez la section [Configuration d'un Hybrid REAP pour plus d'informations sur H-REAP.](#)

Q. Combien de WLAN sont-ils pris en charge sur un WLC ?

R. Depuis la version 5.2.157.0 du logiciel, le WLC peut désormais contrôler jusqu'à 512 WLAN pour les points d'accès légers. Chaque WLAN a un ID WLAN distinct (1 à 512), un nom de profil distinct et un SSID WLAN et des stratégies de sécurisation uniques peuvent lui être attribués. Le contrôleur édite jusqu'à 16 WLAN sur chaque point d'accès connecté, mais vous pouvez créer jusqu'à 512 WLAN sur le contrôleur, puis éditer de manière sélective ces WLAN (en utilisant des groupes de point d'accès) sur différents points d'accès pour mieux gérer votre réseau sans fil.

Remarque : les contrôleurs Cisco 2106, 2112 et 2125 prennent en charge jusqu'à 16 WLAN.

Remarque : pour obtenir des informations détaillées sur les directives de configuration des WLAN sur les WLC, lisez la section [Création de WLAN](#) du [Guide de configuration du contrôleur LAN sans fil Cisco, version 7.0.116.0.](#)

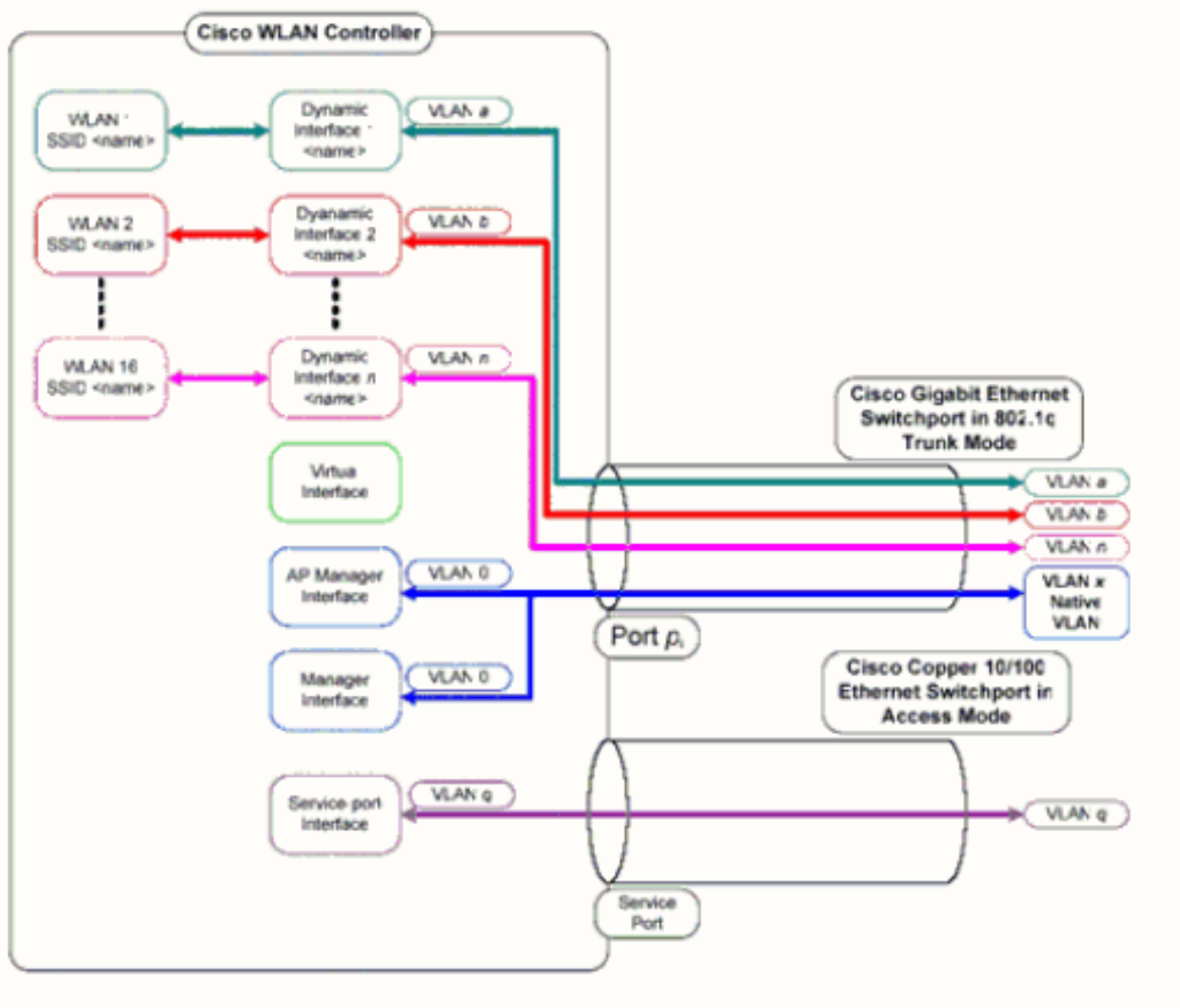
Q. Comment puis-je configurer des VLAN sur mon contrôleur de réseau local sans fil (WLC) ?

R. Dans le WLC, les VLAN sont liés à une interface configurée dans un sous-réseau IP unique. Cette interface est mappée sur un WLAN. Puis, les clients qui s'associent à ce WLAN appartiennent au VLAN de l'interface et une adresse IP leur sont attribuées du sous-réseau auquel l'interface appartient. Afin de configurer des VLAN sur votre WLC, remplissez la procédure dans l'[Exemple de configuration de VLAN sur des contrôleurs de réseau local sans fil.](#)

Q. Nous avons provisionné deux WLAN avec deux interfaces dynamiques différentes. Chaque interface a son propre VLAN, qui est différent de l'interface de gestion VLAN. Cela semble fonctionner, mais nous n'avons pas fourni de ports de jonction utilisés par les WLAN qui autorisent les VLAN. Le point d'accès (AP) marque-t-il les paquets avec l'interface de gestion VLAN ?

R. Le point d'accès n'étiquette pas les paquets avec le VLAN de l'interface de gestion. Le point d'accès encapsule les paquets provenant des clients dans le protocole LWAPP (Lightweight AP Protocol)/CAPWAP, puis transmet les paquets au WLC. Le WLC supprime ensuite l'en-tête LWAPP/CAPWAP et transfère les paquets à la passerelle avec l'étiquette VLAN appropriée. La balise VLAN dépend du WLAN auquel le client appartient. Le WLC dépend de la passerelle qui achemine les paquets à leur destination. Afin de pouvoir passer le trafic pour plusieurs VLAN,

vous devez configurer le commutateur de liaison ascendante comme port de jonction. Ce schéma explique comment les VLAN fonctionnent avec des contrôleurs :



Q. Quelle adresse IP du WLC est utilisée pour l'authentification avec le serveur AAA ?

R. Le WLC utilise l'adresse IP de l'interface de gestion pour tout mécanisme d'authentification (couche 2 ou couche 3) impliquant un serveur AAA. Pour plus d'informations sur les ports et les interfaces sur le WLC, référez-vous à la section [Configuration des ports et des interfaces](#) du [Guide de configuration du contrôleur LAN sans fil Cisco, version 7.0.116.0](#).

Q. J'ai dix points d'accès légers (LAP) de la gamme Cisco 1000 et deux contrôleurs LAN sans fil (WLC) dans le même VLAN. Comment est-ce que j'enregistre six LAP à associer au WLC1 et quatre autres LAP à associer au WLC2 ?

R. Le protocole LWAPP/CAPWAP permet la redondance dynamique et l'équilibrage de charge. Par exemple, si vous spécifiez plusieurs adresses IP pour l'option 43, un LAP envoie des requêtes de détection LWAPP/CAPWAP à chacune des adresses IP que le point d'accès reçoit. Dans la réponse de détection WLC LWAPP/CAPWAP, le WLC incorpore ces informations :

- Les informations sur la charge actuelle du LAP, qui est définie comme le nombre de LAP qui sont connectés au WLC au même moment

- La capacité du LAP
- Le nombre de clients sans fil qui sont connectés au WLC

Le LAP tente ensuite de se connecter au WLC le moins chargé, qui correspond au WLC avec la plus grande capacité disponible de LAP. En outre, après qu'un LAP se connecte à un WLC, le LAP apprend les adresses IP des autres WLC dans le groupe de mobilité depuis le WLC auquel il est connecté.

Une fois qu'un LAP se connecte à un WLC, vous pouvez faire en sorte que le LAP se connecte à un WLC spécifique avant son prochain redémarrage. Afin de faire cela, attribuez un WLC primaire, secondaire et tertiaire à un LAP. Quand le LAP redémarre, il recherche le WLC primaire et se connecte à ce WLC, peu importe sa charge. Si le WLC primaire ne réagit pas, il recherche le secondaire, et, s'il n'y a aucune réponse, le tertiaire. Pour plus d'informations sur la façon de configurer le WLC primaire pour un LAP, consultez la section [Attribution de contrôleurs primaire, secondaire et tertiaire pour un AP léger de l'Exemple de configuration d'un basculement de contrôleur WLAN pour les points d'accès légers.](#)

Q. Quelles sont les fonctionnalités qui ne sont pas prises en charge sur les contrôleurs LAN sans fil (WLC) de la gamme 2100 ?

R. Ces fonctionnalités matérielles ne sont pas prises en charge sur les contrôleurs de la gamme 2100 :

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

Ces fonctionnalités logicielles ne sont pas prises en charge sur les contrôleurs de la gamme 2100 :

- Terminaison VPN (telle qu'IPSec et L2TP)
- 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
- Spanning Tree
- Mise en miroir des ports
- Cranite
- Forteresse
- AppleTalk
- Contrats de bande passante Qos par utilisateur
- Passthrough IPv6
- Agrégation de liaisons (LAG)
- Mode multicast unicast
- Accès invité via câble

Q. Quelles fonctionnalités ne sont pas prises en charge sur les contrôleurs de la gamme 5500 ?

R. Ces fonctionnalités logicielles ne sont pas prises en charge sur les contrôleurs de la gamme 5500 :

- Interface statique de AP-manager **Remarque** : pour les contrôleurs de la gamme 5500, vous

n'êtes pas obligé de configurer une interface de gestionnaire AP. L'interface de gestion agit en tant qu'interface de AP-manager par défaut et les points d'accès peuvent se connecter à cette interface.

- Tunnelisation de mobilité asymétrique
- Protocole Spanning Tree (STP)
- Mise en miroir des ports
- Prise en charge de liste de contrôle d'accès de couche 2 (ACL)
- Terminaison VPN (telle qu'IPSec et L2TP)
- Option de passthrough VPN
- Configuration du pontage 802.3, d'AppleTalk et du Protocole point à point sur Ethernet (PPPoE)

Q. Quelles fonctionnalités ne sont pas prises en charge sur les réseaux maillés ?

R. Ces fonctionnalités de contrôleur ne sont pas prises en charge sur les réseaux maillés :

- Prise en charge multinationale
- CAC basé sur la charge (les réseaux maillés prennent en charge uniquement les CAC basés sur bande passante ou statiques.)
- Haute disponibilité (pulsation rapide et temporisateur de détection de connexion primaire)
- Authentification EAP-FASTv1 et 802.1x
- Priorité de connexion des points d'accès (les points d'accès de maillage ont une priorité fixe.)
- Certificat important localement
- Services de localisation

Q. Quelle est la période de validité des certificats installés par le fabricant (MIC) sur un contrôleur LAN sans fil et des certificats des points d'accès légers ?

R. La période de validité d'un MIC sur un WLC est de 10 ans. La même période de validité de 10 ans s'applique aux certificats du point d'accès léger à partir de la création (qu'il s'agisse d'un MIC ou d'un certificat auto-signé (SSC)).

Q. J'ai deux contrôleurs LAN sans fil (WLC) nommés WLC1 et WLC2 configurés dans le même groupe de mobilité pour le basculement. Mon point d'accès léger (LAP) est actuellement enregistré avec WLC1. Si WLC1 échoue, l'AP enregistré sur le WLC1 redémarre-t-il pendant sa transition vers le WLC de survie (WLC2) ? En outre, pendant ce basculement, le client WLAN perd-il la connectivité WLAN avec le LAP ?

R. Oui, le LAP se désinscrit du WLC1, redémarre, puis se réenregistre auprès du WLC2, si le WLC1 échoue. Puisque le LAP redémarre, les clients WLAN associés perdent la connectivité au LAP qui redémarre. Pour obtenir des informations connexes, consultez la section [Équilibrage de charge des AP et secours des AP dans des réseaux sans fil unifiés](#).

Q. L'itinérance dépend-elle du mode LWAPP (Lightweight Access Point Protocol) que le contrôleur LAN sans fil (WLC) est configuré pour utiliser ? Un WLC qui fonctionne en mode LWAPP de couche 2 peut-il effectuer une itinérance de couche 3 ?

R. Tant que le regroupement de mobilité des contrôleurs est configuré correctement, l'itinérance du client devrait fonctionner normalement. L'itinérance n'est pas affectée par le mode LWAPP (couche 2 ou couche 3). Cependant, nous vous recommandons d'utiliser le LWAPP de couche 3 lorsque c'est possible.

Remarque : le mode de couche 2 est uniquement pris en charge par les WLC des gammes Cisco 410x et 440x et les points d'accès de la gamme Cisco 1000. Le protocole LWAPP de couche 2 n'est pas pris en charge par les autres plates-formes de point d'accès léger et de contrôleur LAN sans fil.

Q. Quel est le processus d'itinérance qui se produit lorsqu'un client décide d'effectuer une itinérance vers un nouveau point d'accès ou contrôleur ?

R. Voici la séquence d'événements qui se produit lorsqu'un client se déplace vers un nouveau point d'accès :

1. Le client envoie une requête de réassociation au WLC via le LAP.
2. Le WLC envoie le message de mobilité aux autres WLC dans le groupe de mobilité afin de découvrir avec quel WLC le client était précédemment associé.
3. Le WLC initial répond en indiquant des informations, telles que l'adresse MAC, l'adresse IP, le QoS, le contexte de sécurité, etc. au sujet du client via le message de mobilité.
4. Le WLC met à jour sa base de données avec les détails du client fournis ; le client passe ensuite par le processus de réauthentification, si nécessaire. Le nouveau LAP auquel le client est actuellement associé est également mis à jour avec d'autres informations dans la base de données du WLC. De cette façon, l'adresse IP du client est retenue sur les itinérances entre les WLC, ce qui aide à fournir une itinérance sans encombres.

Pour plus d'informations sur l'itinérance dans un environnement unifié, référez-vous à la section [Configuration des groupes de mobilité](#) du [Guide de configuration du contrôleur LAN sans fil Cisco, version 7.0.116.0](#).

Remarque : le client sans fil n'envoie pas de demande d'authentification (802.11) pendant la réassociation. Le client sans fil envoie juste la réassociation immédiatement. Puis, il passera à l'authentification 802.1x.

Q. Quels ports dois-je autoriser pour les communications LWAPP/CAPWAP lorsqu'un pare-feu est installé sur le réseau ?

R. Vous devez activer les ports suivants :

- Activez les ports UDP suivants pour le trafic LWAPP :Données - 12222Contrôle - 12223
- Activez ces ports UDP pour le trafic CAPWAP :Données - 5247Contrôle - 5246
- Activez les ports UDP suivants pour le trafic de mobilité :16666 - Mode sécurisé16667 - Mode sans garantie

Des messages de mobilité et de données sont habituellement échangés par paquets EtherIP. **Le protocole IP 97 doit être autorisé sur le pare-feu pour permettre les paquets EtherIP.** Si vous employez l'ESP pour encapsuler des paquets de mobilité, vous devez permettre l'ISAKMP via le pare-feu quand vous ouvrez le port UDP 500. Vous devez également ouvrir le protocole IP 50 pour permettre aux données cryptées de passer par le pare-feu.

Les ports suivants sont facultatifs (selon vos besoins) :

- TCP 161 et 162 pour SNMP (pour le système de contrôle sans fil [WCS])
- UDP 69 pour TFTP
- TCP 80 et/ou 443 pour le HTTP ou HTTPS pour l'accès à la GUI
- TCP 23 et/ou 22 pour le Telnet ou Secure Shell (SSH) pour l'accès de CLI

Q. Les contrôleurs LAN sans fil prennent-ils en charge SSHv1 et SSHv2 ?

R. Les Contrôleurs de réseau local sans fil prennent seulement en charge SSHv2.

Q. Le protocole RARP (Reverse ARP) est-il pris en charge par les contrôleurs LAN sans fil (WLC) ?

R. Le Reverse Address Resolution Protocol (RARP) est un protocole de couche de liaison utilisé pour obtenir une adresse IP pour une adresse donnée de couche-liaison telle qu'une adresse Ethernet. Le RARP est pris en charge avec les WLC dotés d'un microprogramme de la version 4.0.217.0 ou ultérieure. Le RARP n'est pas pris en charge sur les versions antérieures.

Q. Puis-je utiliser le serveur DHCP interne sur le contrôleur de réseau local sans fil (WLC) afin d'attribuer des adresses IP aux points d'accès légers (LAP) ?

R. Les contrôleurs contiennent un serveur DHCP interne. Ce serveur est habituellement utilisé dans les filiales qui n'ont déjà pas un serveur DHCP. Afin d'accéder au service DHCP, cliquez sur le menu **Controller** de l'interface graphique WLC ; puis cliquez sur l'option **Internal DHCP Server** sur le côté gauche de la page. Pour plus d'informations sur la façon de configurer l'étendue DHCP sur le WLC, référez-vous à la section [Configuration DHCP](#) du [Guide de configuration du contrôleur LAN sans fil Cisco, version 7.0.116.0](#).

Le serveur interne fournit des adresses DHCP aux clients sans fil, aux LAP, aux AP en mode appliance sur l'interface de gestion, et les requêtes DHCP qui sont transmises par relais depuis les LAP. Les WLC n'offrent jamais d'adresses aux périphériques en amont dans le réseau câblé. L'option 43 DHCP n'est pas prise en charge sur le serveur interne, ainsi l'AP doit employer une méthode alternative pour localiser l'adresse IP de l'interface de gestion du contrôleur, telle que la diffusion de sous-réseau local, le DNS, l'amorçage, ou la détection Over-the-air.

Remarque : les versions du microprogramme WLC antérieures à la version 4.0 ne prennent pas en charge le service DHCP pour les LAP, à moins que les LAP ne soient directement connectés au WLC. La fonctionnalité interne du serveur DHCP a été utilisée pour seulement fournir des adresses IP aux clients qui se connectent au réseau local sans fil.

Q. Que signifie le champ DHCP Required sous un WLAN ?

R. DHCP Required est une option qui peut être activée pour un WLAN. Elle nécessite que tous les clients qui s'associent à ce WLAN particulier obtiennent des adresses IP par DHCP. Les clients dont l'adresse IP est statique ne sont pas autorisés à s'associer au WLAN. Cette option est accessible sous l'onglet Advanced d'un WLAN. Le WLC permet le trafic sortant/entrant d'un client seulement si son adresse IP est présente dans la table MSCB du WLC. Le WLC enregistre l'adresse IP d'un client pendant sa requête DHCP ou le renouvellement DHCP. Cela nécessite qu'un client renouvelle son adresse IP chaque fois qu'il se réassocie au WLC car chaque fois que le client se dissocie pendant son processus d'itinéraire ou sa session de délai d'expiration, son entrée est effacée de la table MSCB. Le client doit de nouveau s'authentifier et se réassocier au

WLC, qui crée de nouveau l'entrée du client dans la table de routage.

Q. Comment la gestion centralisée des clés (CCKM) de Cisco fonctionne-t-elle dans un environnement LWAPP/CAPWAP ?

R. Lors de l'association initiale du client, le point d'accès ou le WLC négocie une clé principale (PMK) par paire après que le client sans fil ait réussi l'authentification 802.1x. Le WLC ou le WDS de l'AP met en cache le PMK pour chaque client. Quand un client sans fil se réassocie ou se déplace, il ignore l'authentification 802.1x et valide le PMK immédiatement.

La seule implémentation spéciale du WLC dans le CCKM est que les WLC échangent le PMK du client par l'intermédiaire de paquets de mobilité, tels que l'UDP 16666.

Q. Comment définir les paramètres duplex sur le contrôleur de réseau local sans fil (WLC) et les points d'accès légers (LAP) ?

R. Les produits Cisco Wireless fonctionnent mieux quand la vitesse et le mode duplex sont tous deux auto-négociés, mais vous avez le choix de définir les paramètres du mode duplex des WLC et des LAP. Afin de définir les paramètres de vitesse/du mode duplex de l'AP, vous pouvez configurer les paramètres du mode duplex pour les LAP sur le contrôleur et, ensuite, les diffuser aux LAP.

configure ap ethernet duplex <auto/half/full> speed <auto/10/100/1000> <all/Cisco AP Name> est la commande permettant de définir les paramètres duplex via l'interface de ligne de commande. Cette commande est prise en charge uniquement avec les versions 4.1 et ultérieures.

Afin de définir les paramètres du mode duplex pour les interfaces physiques des WLC, utilisez la commande **config port physicalmode {all | port} {100h | 100 f | 10 heures | 10f}**.

Cette commande définit tous (ou spécifiés) les ports Ethernet du panneau avant 10/100BASE-T pour les opérations semi-duplex ou duplex intégral de 10 Mbits/s ou 100 Mbits dédiés. Notez que vous devez désactiver l'auto-négociation avec la commande **config port autoneg disable** avant que vous configuriez manuellement n'importe quel mode physique sur le port. En outre, notez que la commande **config port autoneg** remplace les paramètres précédents sélectionnés avec la commande **config port physicalmode**. Par défaut, tous les ports sont définis en auto-négociation.

Remarque : il est impossible de modifier les paramètres de vitesse sur les ports fibre.

Q. Existe-t-il un moyen de suivre le nom du point d'accès léger (LAP) lorsqu'il n'est pas enregistré auprès du contrôleur ?

R. Si votre AP est complètement arrêté et n'est pas enregistré sur le contrôleur, il n'y a aucun moyen que vous puissiez suivre le LAP à travers le contrôleur. La seule manière qui reste est que vous pouvez accéder au commutateur sur lequel ces AP sont connectés, et vous pouvez trouver le switchport sur lequel ils sont connectés en utilisant cette commande :

```
show mac-address-table address
```

Cela vous donne le numéro de port sur le commutateur auquel cet AP est connecté. Puis, tapez

cette commande :

```
show cdp nei detail
```

Le résultat de cette commande donne également le nom du LAP. Cependant, cette méthode est seulement possible quand votre AP est mis sous tension et connecté au commutateur.

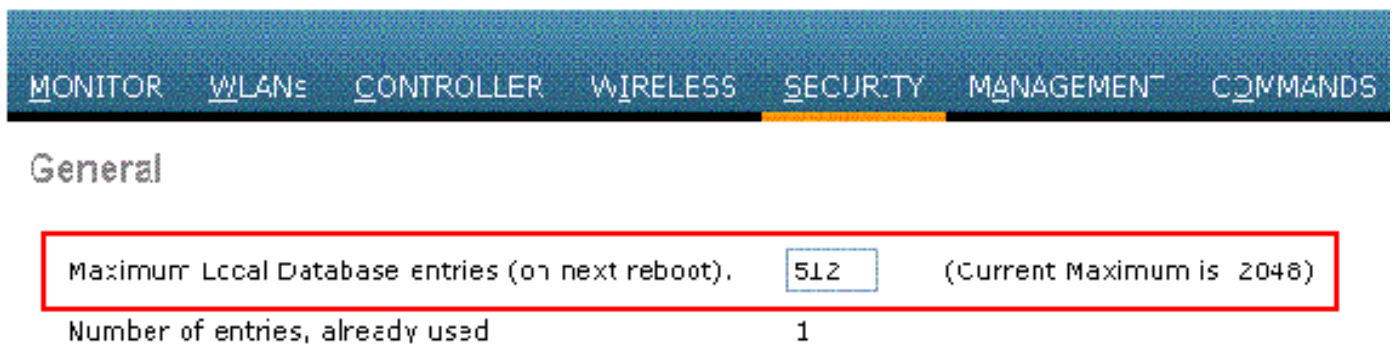
Q. J'ai configuré 512 utilisateurs sur mon contrôleur. Y a-t-il un moyen d'augmenter le nombre d'utilisateurs sur le contrôleur de réseau local sans fil (WLC) ?

R. La base de données locale des utilisateurs est limitée à un maximum de 2 048 entrées sur la page **Sécurité > Général**. Cette base de données est partagée par les utilisateurs de la gestion locale (y compris les ambassadeurs du lobby), les utilisateurs du réseau (y compris les utilisateurs invités), les entrées de filtre MAC, les entrées de la liste d'autorisation des points d'accès et les entrées de la liste d'exclusion. Ensemble, tous ces types d'utilisateurs ne peuvent pas dépasser la taille de la base de données configurée.

Afin d'augmenter la base de données locale, utilisez cette commande à partir de l'interface de ligne de commande :

```
<Cisco Contoller>config database size ?  
<count> Enter the maximum number of entries (512-2048)
```

Remarque : vous devez enregistrer la configuration et réinitialiser le système (à l'aide de la commande **reset system**) pour que la modification prenne effet.



MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS

General

Maximum Local Database entries (on next reboot). (Current Maximum is 2048)

Number of entries, already used 1

Q. Comment appliquer une stratégie de mot de passe fort sur les WLC ?

R. Les WLC vous permettent de définir une stratégie de mot de passe fort. Pour ce faire, utilisez l'interface de ligne de commande ou l'interface utilisateur graphique.

Dans l'interface graphique utilisateur, accédez à **Security > AAA > Password Policies**. Cette page contient une série d'options qui peuvent être sélectionnées afin d'appliquer un mot de passe fort. Voici un exemple :

Afin de faire ceci à partir de l'ILC du WLC, utilisez la commande **config switchconfig strong-pwd {case-check | vérification consécutive | default-check | username-check | all-check} {enable | disable}** commande :

- **case-check** - Vérifie l'occurrence du même caractère trois fois de suite.
- **consécutive-check** - Vérifie si les valeurs par défaut ou leurs variantes sont utilisées.
- **default-check** - Vérifie si le nom d'utilisateur ou l'inverse est utilisé.
- **all-check** - Active/désactive toutes les vérifications de mots de passe forts.

Q. Comment la fonctionnalité de client passif est-elle utilisée sur les contrôleurs LAN sans fil ?

R. Les clients passifs sont des périphériques sans fil, tels que des balances et des imprimantes configurées avec une adresse IP statique. Ces clients ne transmettent aucune information IP telle que l'adresse IP, le masque de sous-réseau et la passerelle lorsqu'ils s'associent à un point d'accès. Par conséquent, lorsque des clients passifs sont utilisés, le contrôleur ne connaît jamais l'adresse IP à moins qu'il n'utilise le DHCP.

Les WLC agissent actuellement comme proxy pour les requêtes ARP. Lors de la réception d'une requête ARP, le contrôleur répond avec une réponse ARP au lieu de transmettre la requête directement au client. Ce scénario présente deux avantages :

- Le périphérique en amont qui envoie la requête ARP au client ne sait pas où se trouve le client.
- L'alimentation des périphériques alimentés par batterie, tels que les téléphones mobiles et les imprimantes, est conservée car ils n'ont pas à répondre à toutes les requêtes ARP.

Comme le contrôleur sans fil ne dispose d'aucune information IP relative aux clients passifs, il ne peut répondre à aucune requête ARP. Le comportement actuel ne permet pas le transfert de requêtes ARP vers des clients passifs. Toute application qui tente d'accéder à un client passif

échoue.

La fonctionnalité de client passif permet aux requêtes et aux réponses ARP d'être échangées entre des clients filaires et sans fil. Cette fonctionnalité, lorsqu'elle est activée, permet au contrôleur de transmettre les requêtes ARP des clients filaires aux clients sans fil jusqu'à ce que le client sans fil souhaité passe à l'état d'exécution.

Pour plus d'informations sur la configuration de la fonctionnalité de client passif, lisez la section [Utilisation de l'interface utilisateur graphique pour configurer le client passif](#) dans le [Guide de configuration du contrôleur LAN sans fil Cisco, version 7.0.116.0](#).

Q. Comment puis-je configurer le client pour qu'il s'authentifie à nouveau auprès du serveur RADIUS toutes les trois minutes ou pendant une période donnée ?

R. Le paramètre session timeout sur le WLC peut être utilisé pour cela. Par défaut, le paramètre de dépassement de délai de session est configuré de sorte qu'il faille attendre 1800 secondes avant qu'une réauthentification se produise.

Modifiez cette valeur à 180 secondes afin d'inciter le client de routage à s'authentifier à nouveau après trois minutes.

Afin d'accéder au paramètre de dépassement de délai de session, cliquez sur le menu **WLAN dans l'interface graphique**. Cela affiche la liste des WLAN configurés dans le WLC. Cliquez sur le WLAN auquel le client appartient. Allez à l'onglet Advanced et localisez le *paramètre Enable Session Timeout*. Modifiez la valeur par défaut sur 180 et cliquez sur **Apply** pour que les modifications entrent en vigueur.

Une fois introduite une acceptation d'accès, accompagnée d'une valeur d'action d'interruption de la requête RADIUS, l'attribut d'expiration de session spécifie le nombre maximal de secondes de service fourni avant la réauthentification. Dans ce cas, l'attribut d'expiration de session est utilisé pour charger le ReAuthPeriod constant dans la machine d'état du Reauthentication Timer de 802.1x.

Q. J'ai un tunnel invité, un tunnel Ethernet sur IP (EoIP), configuré entre mon contrôleur LAN sans fil (WLC) 4400, qui agit comme WLC d'ancrage, et plusieurs WLC distants. Ce WLC ancre peut-il transférer des diffusions de sous-réseau par le tunnel EoIP depuis le réseau câblé vers les clients sans fil associés aux contrôleurs distants ?

R. Non, le WLC 4400 ne transmet pas les diffusions de sous-réseau IP du côté filaire aux clients sans fil via le tunnel EoIP. Ce n'est pas une fonctionnalité prise en charge. Cisco ne prend pas en charge le tunnel de diffusion de sous-réseau ou de multidiffusion en topologie d'accès invité. Puisque le WLAN invité oblige le point de présence client à se placer à un emplacement très spécifique sur le réseau, en grande partie en dehors du pare-feu, le tunnel de la diffusion de sous-réseau peut former un problème de sécurité.

Q. Dans une configuration de contrôleur LAN sans fil (WLC) et de protocole de point d'accès léger (LWAPP), quelles valeurs de point de code de services différenciés (DSCP) sont transmises pour le trafic vocal ? Comment QoS est-il mis en application sur le WLC ?

R. La solution Cisco Unified Wireless Network (UWN) prend en charge quatre niveaux de QoS :

- Platinum/Voix
- Gold/Vidéo
- Silver/Meilleur effort (par défaut)
- Bronze/Arrière-plan

Vous pouvez configurer le trafic vocal WLAN pour utiliser le QoS Platinum, attribuer la faible bande passante en WLAN pour utiliser le QoS Bronze et transférer tout autre trafic entre les autres niveaux de QoS. Référez-vous à [Attribution d'un profil QoS à un WLAN](#) pour plus d'informations.

Q. Les ponts Ethernet Linksys sont-ils pris en charge dans une solution unifiée sans fil Cisco ?

R. Non, le WLC prend uniquement en charge les produits Cisco WGB. Les WGB Linksys ne sont pas pris en charge. Bien que la solution Cisco Wireless Unified ne prenne pas en charge pas les ponts Ethernet Linksys WET54G et WET11B, vous pouvez utiliser ces périphériques dans une configuration Wireless Unified Solution si vous utilisez ces recommandations :

- Connectez un seul périphérique au WET54G ou au WET11B.
- Autorisez la fonctionnalité de clonage MAC sur le WET54G ou le WET11B pour cloner le périphérique connecté.
- Installez les pilotes et les microprogrammes les plus récents sur les périphériques connectés au WET54G ou au WET11B. Cette recommandation est particulièrement importante pour les imprimantes JetDirect parce que des versions anciennes de microprogramme posent des problèmes liés au DHCP.

Remarque : les autres ponts tiers ne sont pas pris en charge. Les étapes mentionnées peuvent également être essayées pour d'autres ponts tiers.

Q. Comment puis-je stocker les fichiers de configuration sur le contrôleur de réseau local sans fil (WLC) ?

R. Le WLC contient deux types de mémoire :

- RAM volatile : conserve la configuration active actuelle du contrôleur
- Mémoire vive non volatile (NVRAM) : contient la configuration de redémarrage

Lorsque vous configurez le système d'exploitation dans le WLC, vous modifiez la mémoire vive volatile. Vous devez enregistrer la configuration de la mémoire vive volatile dans la mémoire vive non volatile afin de vous assurer que le WLC redémarre dans la configuration actuelle.

Il est important de savoir quelle mémoire vous modifiez lorsque vous effectuez ces tâches :

- Utilisez l'assistant de configuration.
- Effacez la configuration du contrôleur.
- Enregistrez les configurations.
- Réinitialisez le contrôleur.
- Déconnectez-vous de la CLI.

FAQ sur les fonctionnalités

Q. Comment définir le type EAP (Extensible Authentication Protocol) sur le contrôleur LAN sans fil (WLC) ? Je veux m'authentifier par rapport à un dispositif Access Control Server (ACS) et j'obtiens le type « unsupported EAP » dans les journaux.

R. Il n'y a pas de paramètre de type EAP distinct sur le WLC. Pour une configuration Light EAP (LEAP), EAP Flexible Authentication via Secure Tunneling (EAP-FAST), ou Microsoft Protected EAP (MS-PEAP), paramétrez juste le standard IEEE 802.1x ou le Wi-Fi Protected Access (WPA) (si vous utilisez la norme 802.1x avec le WPA). N'importe quel type d'EAP qui est pris en charge sur le RADIUS principal et sur le client est pris en charge par l'intermédiaire du balisage 802.1x. Le paramétrage d'EAP sur le client et sur le serveur RADIUS doit correspondre.

Complétez ces étapes afin d'activer l'EAP via l'interface graphique sur le WLC :

1. Depuis l'interface graphique du WLC, cliquez sur **WLAN**.
2. Une liste de WLAN configurés dans le WLC apparaît. Cliquez sur un WLAN.
3. Dans **WLANs > Edit**, cliquez sur l'onglet **Security**.
4. Cliquez sur **Layer 2** et choisissez 802.1x ou WPA+WPA2 pour Layer 2 Security. Vous pouvez également configurer les paramètres de 802.1x qui sont disponibles dans la même fenêtre. Puis, le WLC transfère des paquets d'authentification EAP entre le client sans fil et le serveur d'authentification.
5. Cliquez sur **AAA servers** et choisissez le serveur d'authentification depuis le menu déroulant pour ce WLAN. Nous supposons que le serveur d'authentification est déjà complètement configuré. Pour plus d'informations sur la façon d'activer l'option EAP sur les WLC via l'interface de ligne de commande (CLI), référez-vous à la section [Utilisation de la CLI pour configurer RADIUS](#) du [Guide de configuration du contrôleur LAN sans fil Cisco, version 7.0.116.0](#).

Q. Qu'est-ce que le SSID rapide change ?

R. Le Fast SSID Changing permet à des clients de se déplacer entre les SSID. Quand le client envoie une nouvelle association pour un SSID différent, l'entrée du client dans la table de connexion du contrôleur est effacée avant que le client soit ajouté au nouveau SSID. Quand le Fast SSID Changing est désactivé, le contrôleur impose un retard avant que les clients soit autorisés à se déplacer vers un nouveau SSID. Pour plus d'informations sur la façon d'activer le changement de SSID rapide, référez-vous à la section [Configuration du changement de SSID rapide](#) du [Guide de configuration du contrôleur LAN sans fil Cisco, version 7.0.116.0](#).

Q. Puis-je définir une limite au nombre de clients pouvant se connecter à un réseau local sans fil ?

R. Vous pouvez définir une limite au nombre de clients qui peuvent se connecter à un WLAN, ce qui est utile dans les scénarios où vous avez un nombre limité de clients qui peuvent se connecter à un contrôleur. Le nombre de clients que vous pouvez configurer par WLAN dépend de la plateforme que vous utilisez.

Lisez la section [Configuration du nombre maximal de clients par WLAN](#) du [Guide de configuration](#)

[du contrôleur de réseau local sans fil Cisco, version 7.0.116.0](#) pour obtenir des informations sur les limites de clients par WLAN pour les différentes plates-formes de contrôleurs de réseau local sans fil.

Q. Qu'est-ce que PKC et comment fonctionne-t-il avec le contrôleur de réseau local sans fil (WLC) ?

R. Le PKC signifie Proactive Key Caching. Il a été conçu comme extension du standard IEEE 802.11i.

PKC est une fonction activée dans les contrôleurs Cisco des gammes 2006/410x/440x qui permet aux clients sans fil correctement équipés de se déplacer sans totale ré-authentification avec un serveur AAA. Afin de comprendre le PKC, vous devez d'abord comprendre le Key Caching.

Le Key Caching est une fonctionnalité qui a été ajoutée au WPA2. Il permet à un poste mobile de mettre en cache les clés principales (Pairwise Master Key [PMK]) qu'il gagne via une authentification réussie avec un point d'accès (AP) et **de les réutiliser pour une future association avec le même AP**. Cela signifie qu'un périphérique mobile donné doit s'authentifier une fois avec un AP particulier et mettre en cache la clé pour une utilisation future. Le Key Caching est pris en charge par l'intermédiaire d'un mécanisme connu sous le nom de PMK Identifier (PMKID), qui est un hachage du PMK, d'une chaîne, de la station et des adresses MAC de l'AP. Le PMKID identifie seulement le PMK.

Même avec le Key Caching, une station sans fil doit s'authentifier avec chaque AP dont elle souhaite obtenir le service. Cela introduit de la latence et des surcharges significatives, qui retardent le processus de transfert et peuvent empêcher la prise en charge des applications en temps réel. Afin de résoudre ce problème, le PKC a été introduit avec le WPA2.

Le PKC permet à une station de réutiliser un PMK qu'il avait précédemment gagné via un processus d'authentification réussi. Cela élimine le besoin de la station de s'authentifier par rapport aux nouveaux AP lors de déplacements.

Par conséquent, lors d'un déplacement au sein d'un contrôleur, quand un périphérique mobile se déplace d'un AP à un autre sur le même contrôleur, le client calcule une nouvelle fois un PMKID à l'aide du PMK précédemment utilisé et le présente pendant le processus d'association. Le WLC recherche dans son cache de PMK pour déterminer s'il possède une telle entrée. Si c'est le cas, il contourne le processus d'authentification 802.1x et lance immédiatement l'échange de clés WPA2. Dans le cas contraire, il passe par le processus d'authentification standard 802.1x.

Le PKC est activé par défaut avec le WPA2. Par conséquent, quand vous activez comme Layer 2 security le WPA2 dans la configuration WLAN du WLC, le PKC est activé sur le WLC. En outre, configurez le serveur AAA et le client sans fil pour l'authentification EAP appropriée.

Le demandeur utilisé côté client devrait également prendre en charge le WPA2 pour que le PKC fonctionne. Le PKC peut également être mis en application dans des déplacements entre contrôleurs.

Remarque : PKC ne fonctionne pas avec l'utilitaire Aironet Desktop Utility (ADU) en tant que demandeur client.

Q. Quelles sont les explications pour ces paramètres de délai d'attente sur le contrôleur : Address Resolution Protocol (ARP) Timeout, User Idle Timeout et

Session Timeout ?

R. Le **déla ARP** est utilisé pour supprimer les entrées ARP sur le WLC pour les périphériques appris du réseau.

Déla d'inactivité de l'utilisateur : lorsqu'un utilisateur est inactif sans aucune communication avec le LAP pendant la durée définie comme Déla d'inactivité de l'utilisateur, le client est désauthentié par le WLC. Le client doit s'authentifier à nouveau et se réassocier au WLC. Il est utilisé dans les situations où un client peut s'enlever du LAP auquel il est associé sans le notifier. Cela peut se produire si la batterie est épuisée sur le client, ou si le client associé se déplace.

Remarque : afin d'accéder à ARP et User Idle Timeout sur la GUI du WLC, allez au menu **Controller**. Choisissez **General** dans la zone gauche pour localiser les champs ARP Timeout et User Idle Timeout.

Le **Session Timeout** est la durée maximale d'une session de client avec le WLC. Après cette durée, le WLC annule l'authentification du client, qui passe à nouveau par le processus complet d'authentification (ré-authentification). Cela fait partie d'une mesure de sécurité, qui sert à modifier les clés de chiffrement. Si vous utilisez une méthode d'Extensible Authentication Protocol (EAP) avec la gestion des clés, la nouvelle assignation de clé se produit à intervalle régulier afin de dériver une nouvelle clé de chiffrement. Sans gestion des clés, cette valeur de déla d'expiration correspond au temps dont les clients sans fil ont besoin pour effectuer une ré-authentification complète. Le déla d'expiration de la session est spécifique au WLAN. Ce paramètre est accessible depuis le menu **WLANs > Edit**.

Q. Qu'est-ce qu'un système RFID ? Quelles balises RFID sont actuellement prises en charge par Cisco ?

R. Le Radio Frequency Identification (RFID) est une technologie qui utilise la communication en radiofréquences pour une transmission de courte portée. Un système de base RFID se compose de balises RFID, de lecteurs RFID et d'un logiciel de traitement.

Aujourd'hui, Cisco prend en charge les balises RFID d'AeroScout et de Pango. Pour plus d'informations sur la façon de configurer des balises d'AeroScout, consultez la section [Configuration d'un WLC pour des balises RFID d'AeroScout](#).

Q. Puis-je effectuer l'authentification EAP localement sur le WLC ? Y a-t-il un document qui explique cette fonctionnalité EAP en local ?

R. Oui, l'authentification EAP peut être effectuée localement sur le WLC. L'EAP local est une méthode d'authentification qui permet aux utilisateurs et aux clients sans fil de s'authentifier localement sur le WLC. Il est conçu pour une utilisation dans les bureaux distants qui veulent mettre à jour la connectivité aux clients sans fil quand le système principal est perturbé, ou que le serveur d'authentification externe est en panne. Quand vous activez l'EAP local, le WLC sert de serveur d'authentification. Pour plus d'informations sur la façon de configurer un WLC pour l'authentification locale d'EAP-FAST, consultez l'[Exemple de configuration d'une authentification d'EAP locale sur le contrôleur de réseau local sans fil avec l'EAP-FAST et le serveur LDAP](#).

Q. Qu'est-ce que la fonction de remplacement WLAN ? Comment est-ce que je configure cette fonctionnalité ? Les LAP mettront-ils à jour les valeurs de priorité WLAN quand ils basculent vers le WLC de sauvegarde ?

R. La fonctionnalité de remplacement WLAN nous permet de choisir des WLAN parmi les WLAN configurés sur un WLC qui peuvent être activement utilisés sur une base LAP individuelle. Complétez ces étapes afin de configurer une priorité de WLAN :

1. Dans l'interface graphique du WLC, cliquez sur le menu **Wireless**.
2. Cliquez sur l'option **Radios dans la zone gauche et choisissez 802.11 a/n ou 802.11 b/g/n**.
3. Cliquez sur le lien **Configure depuis le menu déroulant accessible dans la zone droite et qui correspond au nom de l'AP sur lequel vous voulez configurer le WLAN de priorité**.
4. Choisissez **Enable depuis le menu déroulant WLAN Override**. Le menu WLAN Override est le dernier élément situé dans la zone côté gauche de la fenêtre.
5. La liste de tous les WLAN qui sont configurés sur les WLC apparaît.
6. Depuis cette liste, activez les **WLAN que vous voulez voir apparaître sur le LAP et cliquez sur Apply** pour que les modifications entrent en vigueur.
7. Sauvegardez votre configuration après avoir apporté ces modifications.

Les AP retiennent les valeurs de priorité WLAN quand elles sont enregistrées sur les autres WLC, à condition que les profils et les SSID des WLAN que vous voulez remplacer soient configurés à travers tous les WLC.

Remarque : dans la version 5.2.157.0 du logiciel du contrôleur, la fonction de remplacement WLAN a été supprimée de l'interface graphique utilisateur et de l'interface de ligne de commande du contrôleur. Si votre contrôleur est configuré pour la priorité de WLAN et si vous voulez effectuer une mise à niveau vers la version logicielle 5.2.157.0 du contrôleur, le contrôleur supprime la configuration WLAN et diffuse tous les WLAN. Vous pouvez spécifier que seuls certains WLAN soit transmis si vous configurez des groupes de point d'accès. Chaque point d'accès annonce seulement le WLAN activé qui appartiennent à son groupe de point d'accès.

Remarque : les groupes de points d'accès ne permettent pas la transmission de WLAN sur chaque interface radio du point d'accès.

Q. IPv6 est-il pris en charge sur les contrôleurs LAN sans fil (WLC) et les points d'accès légers (LAP) Cisco ?

R. Actuellement, les contrôleurs des gammes 4400 et 4100 prennent uniquement en charge le passthrough client IPv6. Il n'y a aucune prise en charge native de l'IPv6.

Afin d'activer l'IPv6 sur le WLC, sélectionnez la case à cocher **IPv6 Enable dans la configuration SSID WLAN sur la page WLAN > Edit**.

En outre, le Ethernet Multicast Mode (EMM) est requis pour la prise en charge du IPv6. Si vous désactivez l'EMM, les périphériques client qui utilisent l'IPv6 perdent la connectivité. Afin d'activer l'EMM, allez sur la page Controller > General et depuis le menu déroulant Ethernet Multicast Mode, choisissez **Unicast ou Multicast**. Cela active la multidiffusion en mode Unicast ou Multicast. Quand le multicast est activé en tant que monodiffusion multicast, les paquets sont répliqués pour chaque AP. Cette configuration peut être gourmande en ressources processeur, utilisez-la avec prudence. La multidiffusion activée comme multidiffusion multicast utilise l'adresse de multidiffusion assignée à l'utilisateur pour effectuer un multicast plus traditionnel vers les points d'accès (AP).

Remarque : IPv6 n'est pas pris en charge sur les contrôleurs 2006.

En outre, il existe le bogue d'ID Cisco CSCsg78176 qui empêche d'utiliser le passthrough IPv6

quand la fonctionnalité AAA Override est utilisée.

Q. Le contrôleur de réseau local sans fil de la gamme Cisco 2000 (WLC) prend-il en charge l'authentification Web pour les utilisateurs invités ?

R. L'authentification Web est prise en charge sur tous les WLC Cisco. L'authentification Web est une méthode d'authentification de couche 3 utilisée pour authentifier les utilisateurs avec des informations d'identification simples. Aucun chiffrement n'est impliqué. Complétez ces étapes afin d'activer cette fonctionnalité :

1. Depuis l'interface graphique, cliquez sur le menu **WLAN**.
2. Cliquez sur un **WLAN**.
3. Allez à l'**onglet Security et choisissez Layer 3**.
4. Sélectionnez la case Web Policy et choisissez **Authentication**.
5. Cliquez sur Apply afin de sauvegarder les modifications.
6. Afin de créer une base de données sur le WLC par rapport à laquelle authentifier les utilisateurs, allez au menu **Security sur l'interface graphique et choisissez Local Net User** et complétez ces actions : Définissez le nom d'utilisateur et le mot de passe de l'invité destinés à ouvrir une session. Ces valeurs distinguent les majuscules et minuscules. Choisissez l'ID du WLAN que vous utilisez. **Remarque** : pour obtenir une configuration plus détaillée, reportez-vous à l'[exemple de configuration de l'authentification Web du contrôleur LAN sans fil](#).

Q. Le WLC peut-il être géré en mode sans fil ?

R. Le WLC peut être géré par le mode sans fil une fois qu'il est activé. Pour plus d'informations sur la façon d'activer le mode sans fil, référez-vous à la section [Activation des connexions sans fil à l'interface graphique et à l'interface de ligne de commande](#) du [Guide de configuration du contrôleur LAN sans fil Cisco, version 7.0.116.0](#).

Q. Qu'est-ce que l'agrégation de liens (LAG) ? Comment est-ce que j'active le LAG sur les contrôleurs de réseau local sans fil (WLC) ?

R. Le LAG regroupe tous les ports sur le WLC dans une interface simple EtherChannel. Ce système gère dynamiquement l'équilibrage de charge du trafic et la redondance de port avec le LAG.

Généralement, l'interface sur le WLC a de nombreux paramètres liés à elle, qui comprennent l'adresse IP, la passerelle par défaut (pour le sous-réseau IP), le port physique primaire, le port physique secondaire, la balise VLAN et le serveur DHCP. Quand le LAG n'est pas utilisé, chaque interface est habituellement mappée à un port physique, mais plusieurs interfaces peuvent également être mappées à un port simple du WLC. Quand le LAG est utilisé, le système mappe dynamiquement les interfaces au canal de port regroupé. Cela favorise la redondance et l'équilibrage de charge du port. Quand un port échoue, l'interface est dynamiquement mappée au prochain port physique disponible et les LAP sont équilibrés à travers les ports.

Quand le LAG est activé sur un WLC, le WLC transfère les trames de données sur le même port sur lequel elles ont été reçues. Le WLC se fonde sur le commutateur voisin pour équilibrer la charge du trafic à travers l'EtherChannel. Le WLC n'effectue aucun équilibrage de charge d'EtherChannel tout seul.

Q. Quels modèles de contrôleurs LAN sans fil (WLC) prennent en charge l'agrégation de liens (LAG) ?

R. Les contrôleurs de la gamme Cisco 5500 prennent en charge le LAG dans la version logicielle 6.0 ou ultérieure, les contrôleurs de la gamme Cisco 4400 prennent en charge le LAG dans la version logicielle 3.2 ou ultérieure, et le LAG est activé automatiquement sur les contrôleurs dans le WiSM Cisco et le commutateur de contrôleur LAN sans fil intégré Catalyst 3750G. Sans LAG, chaque port du système de distribution d'un contrôleur Cisco 4400 prend en charge jusqu'à 48 points d'accès. Lorsque le LAG est activé, le port logique d'un contrôleur Cisco 4402 prend en charge jusqu'à 50 points d'accès, le port logique d'un contrôleur Cisco 4404 prend en charge jusqu'à 100 points d'accès et le port logique du commutateur de contrôleur LAN sans fil intégré Catalyst 3750G et de chaque contrôleur Cisco WiSM prend en charge jusqu'à 150 points d'accès.

Les WLC Cisco 2106 et 2006 ne prennent pas en charge le LAG. Les modèles antérieurs, tels que la gamme de WLC Cisco 4000, ne prennent pas en charge le LAG.

Q. Quelle est la fonction de mobilité d'ancrage automatique dans les réseaux sans fil unifiés ?

R. La mobilité d'auto-ancrage (ou mobilité de WLAN invité) est utilisée pour améliorer l'équilibrage de charge et la sécurité pour les clients itinérants sur votre réseau local sans fil (WLAN). Dans des conditions de déplacement normales, les périphériques client se connectent à un WLAN et sont ancrés au premier contrôleur avec qui ils entrent en contact. Si un client se déplace sur un sous-réseau différent, le contrôleur sur lequel le client se déplace met en place une session étrangère pour le client avec le contrôleur ancre. Avec l'utilisation de la fonctionnalité de mobilité d'auto-ancrage, vous pouvez spécifier un contrôleur ou un ensemble de contrôleurs comme points d'ancre pour les clients situés sur un WLAN.

Remarque : l'ancrage de mobilité ne doit pas être configuré pour la mobilité de couche 3. L'ancre de mobilité est seulement utilisée pour la tunnelisation invitée.

Q. Un contrôleur de réseau local sans fil (WLC) Cisco 2006 peut-il être configuré comme point d'ancrage d'un réseau local sans fil ?

R. Un WLC de la gamme Cisco 2000 ne peut pas être désigné comme point d'ancrage pour un WLAN. Cependant, un WLAN créé sur un WLC Cisco de la gamme 2000 peut utiliser un WLC Cisco de la gamme 4100 et un WLC Cisco de la gamme 4400 en tant qu'ancre.

Q. Quel type de tunnellation de mobilité le contrôleur LAN sans fil utilise-t-il ?

R. Les versions logicielles 4.1 à 5.1 de contrôleur prennent en charge le tunnel de mobilité asymétrique et symétrique. Le logiciel du contrôleur version 5.2 ou ultérieure ne prend en charge que le tunneling de mobilité symétrique, qui est désormais toujours activé par défaut.

Dans le tunnel asymétrique, le trafic client au réseau câblé est acheminé directement via le contrôleur étranger. Le tunnel asymétrique se casse quand un routeur en amont a activé le reverse path filtering (RPF). Dans ce cas, le trafic client est abandonné au niveau du routeur parce que le contrôle RPF s'assure que le chemin vers l'adresse source correspond au chemin par lequel le paquet arrive.

Quand le tunnel de mobilité symétrique est activé, tout le trafic client est envoyé au contrôleur

ancrer et peut alors avec succès passer le contrôle RPF. Le tunnel symétrique de mobilité est également utile dans ces situations :

- Si une installation de pare-feu dans l'itinéraire de paquet du client abandonne des paquets parce que l'adresse IP source ne correspond pas au sous-réseau sur lequel les paquets sont reçus, cela s'avère utile.
- Si le VLAN de groupe de points d'accès sur le contrôleur d'ancrage est différent du VLAN d'interface WLAN sur le contrôleur étranger : dans ce cas, le trafic client peut être envoyé sur un VLAN incorrect lors d'événements de mobilité.

Q. Comment pouvons-nous accéder au WLC lorsque le réseau est en panne ?

R. Lorsque le réseau est en panne, le WLC est accessible par le port de service. Une adresse IP dans un sous-réseau totalement différent des autres ports du WLC a été attribuée au port, d'où le nom d'administration hors bande. Pour plus d'informations, référez-vous à la section [Configuration des ports et des interfaces](#) du [Guide de configuration du contrôleur LAN sans fil Cisco, version 7.0.116.0](#).

Q. Les contrôleurs LAN sans fil (WLC) Cisco prennent-ils en charge la fonctionnalité de basculement (ou de redondance) ?

R. Oui, si vous avez deux WLC ou plus dans votre réseau WLAN, vous pouvez les configurer pour la redondance. Généralement, un LAP se connecte au WLC primaire configuré. Une fois que le WLC primaire échoue, le LAP redémarre et se connecte à un autre WLC dans le groupe de mobilité. Le basculement est une fonctionnalité avec laquelle le LAP interroge le WLC primaire et s'y connecte une fois qu'il est fonctionnel. Consultez l'[Exemple de configuration de basculement d'un contrôleur WLAN pour des points d'accès légers](#) pour plus d'informations.

Q. À quoi servent les listes de contrôle d'accès (ACL) de pré-authentification dans les contrôleurs de réseau local sans fil (WLC) ?

R. Avec la liste de contrôle d'accès de pré-authentification, comme son nom l'indique, vous pouvez autoriser le trafic client vers et depuis une adresse IP spécifique avant même que le client ne s'authentifie. Lorsque vous utilisez un serveur Web externe pour l'authentification Web, certaines plates-formes WLC ont besoin d'une liste de contrôle d'accès de pré-authentification pour le serveur Web externe (le contrôleur de la gamme Cisco 5500, un contrôleur de la gamme Cisco 2100, la gamme Cisco 2000 et le module de réseau du contrôleur). Pour les autres plates-formes WLC, la liste de contrôle d'accès de pré-authentification n'est pas obligatoire. Cependant, il est recommandé de configurer une liste de contrôle d'accès de pré-authentification pour le serveur Web externe lors de l'utilisation de l'authentification Web externe.

Q. J'ai un WLAN filtré par MAC et un WLAN complètement ouvert dans mon réseau. Le client choisit-il le WLAN ouvert par défaut ? Ou bien le client s'associe-t-il automatiquement à l'ID du WLAN qui est défini sur le filtre d'adresse MAC ? En outre, pourquoi y a-t-il une option d'« interface » sur un filtre d'adresses MAC ?

R. Le client peut s'associer à n'importe quel WLAN auquel il est configuré pour se connecter. L'option d'interface dans le filtre d'adresses MAC donne la possibilité d'appliquer le filtre à un WLAN ou à une interface. Si plusieurs WLAN sont attachés à la même interface, vous pouvez

appliquer le filtre d'adresses MAC sur l'interface sans avoir besoin de créer un filtre pour chaque WLAN individuel.

Q. Comment puis-je configurer l'authentification TACACS pour les utilisateurs de gestion sur le contrôleur de réseau local sans fil (WLC) ?

R. À partir de la version 4.1 du WLC, TACACS est pris en charge sur les WLC. Consultez la section [Configuration de TACACS+ afin de comprendre comment configurer TACACS+ pour authentifier les utilisateurs de gestion du WLC.](#)

Q. Quelle est l'utilisation du paramètre d'échec d'authentification excessif dans un contrôleur de réseau local sans fil (WLC) ?

R. Ce paramètre est l'une des stratégies d'exclusion de client. L'exclusion de client est une fonction de sécurité sur le contrôleur. Cette politique est utilisée pour mettre des clients sur liste noire afin d'empêcher l'accès illégal au réseau ou des attaques au réseau sans fil.

Avec l'activation de cette politique d'échec d'authentification Web excessive, quand un nombre de tentatives infructueuses d'authentification Web d'un client dépasse le nombre de 5, le contrôleur considère que le client a dépassé le nombre maximum de tentatives d'authentification Web et met le client sur liste noire.

Complétez ces étapes afin d'activer ou de désactiver ce paramètre :

1. Depuis l'interface graphique du WLC, allez sur la page **Security > Wireless Protection Policies > Client Exclusion Policies**.
2. Sélectionnez ou désélectionnez **Excessive Web Authentication Failures**.

Q. J'ai converti mon point d'accès autonome (AP) en mode léger. En mode Lightweight AP Protocol (LWAPP) avec le serveur AAA RADIUS pour la gestion des comptes client, le client est habituellement suivi avec la gestion des comptes RADIUS basée sur l'adresse IP du WLC. Est-il possible de définir la gestion des comptes RADIUS sur l'adresse MAC de l'AP associé au WLC et non sur l'adresse IP du WLC ?

R. Oui, cela peut être fait avec la configuration côté WLC. Procédez comme suit :

1. Depuis l'interface graphique du contrôleur, dans la section **security > radius accounting**, il y a une zone de liste déroulante correspondant au Call Station ID Type. Choisissez **AP MAC Address**.
2. Vérifiez-la via le journal de l'AP LWAPP. Ici, vous pouvez voir le champ appelé station ID qui affiche l'adresse MAC de l'AP auquel ce client particulier est associé.

Q. Comment modifiez-vous la valeur du délai d'attente de connexion Wi-Fi Protected Access (WPA) sur un contrôleur de réseau local sans fil (WLC) via l'interface de ligne de commande ? Je sais que je peux le faire sur des points d'accès Cisco IOS® (AP) avec la commande `dot11 wpa handshake timeout valeur`, mais comment le faites-vous sur un WLC ?

R. La possibilité de configurer le délai d'attente WPA-Handshake via les WLC a été intégrée dans la version logicielle 4.2 et ultérieure. Vous n'avez pas besoin de cette option dans les versions logicielles antérieures du WLC.

Ces commandes peuvent être utilisées pour modifier le délai d'expiration de la connexion WPA :

```
config advanced eap eapol-key-timeout <value>
config advanced eap eapol-key-retries <value>
```

Les valeurs par défaut continuent à refléter le comportement actuel des WLC.

- the default value for eapol-key-timeout is 1 second.
- the default value for eapol-key-retries is 2 retries

Remarque : sur les points d'accès IOS, ce paramètre peut être configuré avec la commande **dot11 wpa handshake**.

Vous pouvez également configurer les autres paramètres d'EAP avec les options disponibles sous la commande **config advanced eap**.

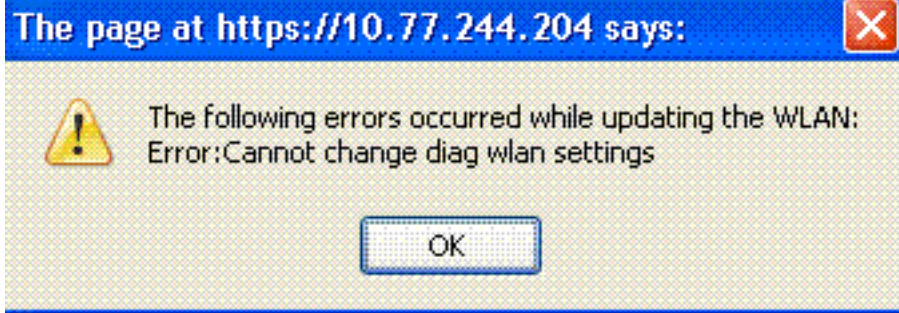
(Cisco Controller) >config advanced eap ?

```
eapol-key-timeout
  Configures EAPOL-Key Timeout in seconds.
eapol-key-retries
  Configures EAPOL-Key Max Retries.
identity-request-timeout
  Configures EAP-Identity-Request Timeout in seconds.
identity-request-retries
  Configures EAP-Identity-Request Max Retries.
key-index
  Configure the key index used for
  dynamic WEP(802.1x) unicast key (PTK).
max-login-ignore-identity-response
  Configure to ignore the same username count
  reaching max in the EAP identity response
request-timeout
  Configures EAP-Request Timeout in seconds.
request-retries
  Configures EAP-Request Max Retries.
```

Q. Quelle est la fonction de la fonction de canal de diagnostic dans la page WLAN > Edit > Advanced ?

R. La fonction de canal de diagnostic vous permet de résoudre les problèmes liés à la communication client avec un WLAN. Le client et les points d'accès peuvent être placés par un ensemble défini de tests pour identifier la cause des difficultés de transmission que le client subit et permettent alors de prendre des mesures correctives pour rendre le client opérationnel sur le réseau. Vous pouvez utiliser l'interface graphique ou le CLI du contrôleur pour activer le canal diagnostique et vous pouvez employer le CLI du contrôleur ou le WCS pour exécuter les tests de diagnostic.

Le canal diagnostique peut être uniquement utilisé à des fins de test. Si vous essayez de configurer l'authentification ou le chiffrement pour le WLAN tout en activant le canal diagnostique, cette erreur apparaît :



Q. Quel est le nombre maximal de groupes AP qui peuvent être configurés sur un WLC ?

R. Cette liste montre le nombre maximal de groupes AP que vous pouvez configurer sur un WLC :

- Un maximum de 50 groupes de points d'accès pour les modules de contrôleur et de réseau de la gamme Cisco 2100
- Un maximum de 300 groupes de points d'accès pour les contrôleurs de la gamme Cisco 4400, Cisco WiSM et le commutateur de contrôleur LAN sans fil Cisco 3750G
- 500 groupes de points d'accès maximum pour les contrôleurs de la gamme Cisco 5500

Informations connexes

- [Contrôleur de réseau local sans fil \(WLC\) - Forum Aux Questions](#)
- [Messages d'erreur et système du contrôleur de réseau local sans fil - Forum Aux Questions](#)
- [Point d'accès léger - Forum Aux Questions](#)
- [Guide de configuration du contrôleur LAN sans fil Cisco, version 7.0.116.0](#)
- [Prise en charge IPv6 sur le contrôleur LAN sans fil](#)
- [Assistance produit sans fil](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.