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

ID de document : 118833

Mis à jour : Mars 02, 2015


PDF de téléchargement


Copie

Commentaires

Produits connexes

- Contrôleurs de réseau LAN fil de la gamme Cisco 4400
- Contrôleurs sans fil de la gamme Cisco 5500
- Cisco Wireless Services Module 2 (WiSM2)
- Contrôleurs sans-fil de la gamme Cisco 2500
- Contrôleurs de réseau local sans fil de la gamme Cisco 2100
- Contrôleurs de réseau local sans fil intégrés Cisco Catalyst 3750
- Modules de services sans fil (WiSM) des gammes Cisco Catalyst 6500/7600
- Contrôleurs de LAN sans fil de la gamme Cisco 2000
- Module contrôleur de réseau local sans fil Cisco
- Contrôleurs de LAN sans fil de la gamme Cisco 4100
- + exposition davantage

Contenu

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 est-ce que je configure le commutateur pour me connecter avec le WLC ?

A. Configurez le port de commutateur, auquel le WLC est connecté, comme port de joncteur réseau de 802.1Q d'IEEE. Assurez-vous que seuls les VLAN nécessaires sont autorisés sur le commutateur. Habituellement, la Gestion et l'interface d'AP-gestionnaire du WLC sont laissées non-marquée. Ceci signifie qu'ils assument le VLAN indigène du commutateur connecté. Ce n'est pas nécessaire. Vous pouvez attribuer un VLAN séparé à ces interfaces. Le pour en savoir plus, se rapportent au *configurer le commutateur pour la* section *WLC de l'*exemple Sans fil de contrôleur LAN et de configuration de base de point d'accès léger.

Q. Tout le trafic réseau et derrière un client WLAN perce-t-il un tunnel par un contrôleur LAN Sans fil (WLC) une fois que le Point d'accès (AP) obtient inscrit au contrôleur ?

A. Quand AP joint un WLC, un contrôle et un ravitaillement de tunnel du protocole de points d'accès sans fil (CAPWAP) est formé entre les deux périphériques. Tout le trafic, qui inclut tout le trafic de client, est envoyé par le tunnel CAPWAP.

La seule exception à ceci est quand AP est en mode hybride-REAP. Les Points d'accès hybride-REAP peuvent commuter le trafic de données de client localement et exécuter l'authentification client localement quand leur connexion au contrôleur est perdue. Quand ils sont connectés au contrôleur, ils peuvent également envoyer le trafic de nouveau au contrôleur.

Q. Est-ce que je peux installer des points d'accès légers (LAP) dans un bureau distant et installer un contrôleur de réseau local sans fil Cisco (WLC) dans mon siège social ? Le LWAPP/CAPWAP fonctionne-t-il au-dessus d'un WAN ?

A. Oui, vous pouvez avoir des WLC sur le WAN depuis les points d'accès. LWAPP/CAPWAP fonctionne au-dessus d'un WAN quand les recouvrements sont configurés en mode de Remote Edge AP (REAP) ou de 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: Les points d'accès légers ne prennent pas tous 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 les modes REAP et H-REAP fonctionnent-ils ?

A. Dans le **mode REAP**, tous les contrôle et trafic d'administration, qui inclut le trafic d'authentification, est percé un tunnel de nouveau au WLC. Mais tout le trafic de données est commuté localement dans le RÉSEAU LOCAL distant de bureau. 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 avec succès pour authentifier et recevoir le service sur ce WLAN dans le temps d'arrêt, configurez la méthode d'authentification pour ce WLAN en tant que le WEP ou WPA-PSK de sorte que l'authentification soit faite localement au REAP. Pour plus d'informations sur le déploiement REAP, référez-vous au guide de déploiement REAP à la succursale.

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. Quand la connexion au WLC est perdue, tous les WLAN sont terminés excepté les 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 avec succès pour authentifier et recevoir le service sur ces WLAN dans le temps d'arrêt, configurez la méthode d'authentification pour ce WLAN en tant que le WEP, le WPA PSK, ou WPA2 PSK de sorte que l'authentification soit faite localement à H-REAP.

Pour plus d'informations sur H-REAP, référez-vous à la conception H-REAP et au guide de déploiement.

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

A. **Le REAP** ne prend en charge pas l'étiquetage du 802.1Q VLAN d'IEEE. En soi, il ne prend pas en charge plusieurs VLAN. Le trafic depuis tous les service set identifiers (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 pris en charge sur WLC ?

A. Depuis la version du logiciel 5.2.157.0, le WLC peut maintenant contrôler jusqu'à 512 WLAN pour des 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 attribué. 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 seulement jusqu'à 16

WLAN.

Remarque: Pour des informations détaillées sur les instructions pour configurer des WLAN sur WLCs, lisez la section de création WLAN du guide de configuration Sans fil de contrôleur LAN de Cisco, release 7.0.116.0.

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

A. Dans le WLC, des VLAN sont attachés à une interface configurée dans un seul IP de sous-réseau. 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 attribuée 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 équipé 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-il les paquets avec l'interface de gestion VLAN ?

A. L'AP ne marque pas les paquets avec l'interface de gestion VLAN. AP encapsule les paquets des clients dans AP léger Protocol (LWAPP) /CAPWAP, et puis passe les paquets en fonction au WLC. Le WLC élimine alors l'en-tête LWAPP/CAPWAP et en avant les paquets à la passerelle avec la balise appropriée VLAN. 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 ?

A. Le WLC utilise l'adresse IP de l'interface de gestion pour n'importe quel mécanisme d'authentification (couche 2 ou couche 3) qui fait participer un serveur AAA. Pour plus d'informations sur des ports et des interfaces sur le WLC, référez-vous à la section *configurante de ports et d'interfaces du* guide de configuration Sans fil de contrôleur LAN de Cisco, release 7.0.116.0.

Q. J'ai dix points d'accès légers (LAP) de la gamme 1000 de Cisco et deux contrôleurs de réseau local 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 ?

A. Le LWAPP/CAPWAP tient compte de la Redondance dynamique et de l'Équilibrage de charge. Par exemple, si vous spécifiez plus d'une adresse IP pour l'option 43, un RECOUVREMENT envoie des demandes de détection LWAPP/CAPWAP à chacune des adresses IP qu'AP reçoit. Dans la réponse de détection WLC LWAPP/CAPWAP, le WLC inclut 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 de réseau local sans fil de la gamme 2100 (WLC) ?

A. Ces caractéristiques 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 :

- Arrêt VPN (tel 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 ?

A. 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 ne devez pas configurer une interface de AP-manager. 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 ?

A. Ces fonctionnalités de contrôleur ne sont pas prises en charge sur des 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 fabricant (MICs) sur un contrôleur LAN Sans fil et des Certificats d'AP léger ?

A. La période de validité d'une MIC sur un WLC est de 10 ans. La même période de validité de 10 ans s'applique aux Certificats d'AP léger à partir de la création (si c'est une MIC ou un certificat Auto-signé (SSC)).

Q. J'ai deux contrôleurs de réseau local sans fil (WLC) appelés 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-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 ?

A. Oui, le LAP se désenregistre bien du WLC1, redémarre, puis de se réenregistre avec le WLC2, si 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 de Lightweight Access Point Protocol (LWAPP) que le contrôleur de réseau local sans fil (WLC) utilise selon sa configuration ? Un WLC qui fonctionne en mode LWAPP de couche 2 peut-il effectuer une itinérance

de couche 3 ?

A. Tant que le groupement de mobilité aux contrôleurs est configuré correctement, l'itinérance de client devrait fonctionner bien. 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 la couche 2 est pris en charge seulement par les gammes Cisco 410x et 440x de WLCs et des Points d'accès de gamme Cisco 1000. La couche 2 LWAPP n'est pas prise en charge en les autres Plateformes Sans fil de point de contrôleur LAN et d'accès léger.

Q. Quel est le processus d'itinérance qui se produit quand un client décide de se déplacer sur un nouveau point d'accès (AP) ou un contrôleur ?

A. Voilà la suite d'opérations qui se produit quand un client se déplace sur un nouvel AP :

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 informations fournies sur le client ; le client passe alors par le procédé de réauthentification, s'il y a lieu. 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 *configurante de Groupes de mobilité du* guide de configuration Sans fil de contrôleur LAN de Cisco, release 7.0.116.0.

Remarque: Le client sans fil n'envoie pas de requête 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 est-ce que je dois permettre pour la transmission LWAPP/CAPWAP quand il y a un Pare-feu dans le réseau ?

A. 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 de réseau local sans fil prennent-ils en charge SSHv1 et SSHv2 ?

A. Support Sans fil seulement SSHv2 de contrôleurs LAN.

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

A. Le Protocole RARP (Reverse Address Resolution Protocol) est un protocole de couche de liaison utilisé pour obtenir une adresse IP pour une adresse de couche liaison donnée telle qu'une adresse d'Ethernets. 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. Est-ce que je peux employer 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) ?

A. 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** sur l'interface graphique du WLC ; cliquez ensuite sur l'option **Internal DHCP Server** dans la zone gauche de la page. Pour plus d'informations sur la façon configurer la portée de DHCP sur le WLC, référez-vous à la section *configurante DHCP du* guide de configuration Sans fil de contrôleur LAN de Cisco, release 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 du WLC antérieures à la version 4.0 ne prennent pas en charge le service DHCP pour les LAP, à moins que les LAP 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 ?

A. Le DHCP exigé 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 va-t-il le travail du Cisco Centralized Key Management (CCKM) dans un environnement LWAPP/CAPWAP ?

A. Pendant l'association client initiale, l'AP ou le WLC négocie une pair-wise master key (PMK) après l'authentification 802.1x du client sans fil. 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 est-ce que je définis les paramètres de duplex du contrôleur de réseau local sans fil (WLC) et les points d'accès légers (LAP) ?

A. Les Produits Sans fil de Cisco fonctionnent meilleur quand le la vitesse et le duplex sont autonégociés, mais vous avez l'option de placer les paramètres bidirectionnels sur le WLC et les recouvrements. 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 qui permet de définir les paramètres du mode duplex par le CLI. Cette commande est prise en charge avec les versions 4.1 et ultérieures seulement.

Afin de définir les paramètres du mode duplex pour les interfaces physiques des WLC, utilisez la commande **config port physicalmode {all | port} {100h | 100f | 10h | 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 n'y a aucune façon de modifier les paramètres de vitesse sur les ports fibre.

Q. Y a-t-il une façon de suivre le nom du point d'accès léger (LAP) quand il n'est pas enregistré dans le contrôleur ?

A. Si votre AP est complètement en panne et n'est pas enregistré dans le contrôleur, il n'y a aucune façon de suivre le LAP par 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 *<mac address>*
Cela vous donne le numéro de port sur le commutateur auquel cet AP est connecté. Puis, tapez cette commande :

show cdp nei *<type/num>* **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 une manière d'augmenter le nombre d'utilisateurs sur le contrôleur LAN Sans fil (WLC) ?

A. La base de données locale des utilisateurs est limitée à un maximum de 2048 entrées à la page de **Security > General**. Cette base de données est partagée des entrées de la liste par les utilisateurs locaux de Gestion (qui inclut des ambassadeurs de lobby), les utilisateurs du réseau (qui inclut des utilisateurs d'invité), les entrées de filtre d'adresses MAC, de Point d'accès autorisation, et des 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 du CLI :

```
<Cisco Controller>config database size ?
<count>  Enter the maximum number of entries (512-2048)
```
Remarque: Vous devez sauvegarder la configuration et remettre à l'état initial le système (utilisant la commande de **système de remise**) pour que la modification la prenne effet.

Q. Comment est-ce que j'impose une stratégie de mot de passe fort sur WLCs ?

A. WLCs te permettent pour définir une stratégie de mot de passe fort. Ceci peut être fait utilisant le CLI ou le GUI.

Dans le GUI, allez à la **Sécurité >** à l'**AAA >** aux **politiques de mot de passe**. Cette page a une gamme d'options qui peuvent être sélectionnées afin d'imposer un mot de passe fort. Voici un exemple :

Afin de faire ceci du WLC CLI, utilisez le fort-**pwd de switchconfig de config** *{dossier-contrôle | consécutif-contrôle | par défaut-contrôle | nom d'utilisateur-contrôle | tout-contrôle} {enable |* commande de *débronchement}* :

- **dossier-contrôle** - Vérifie l'occurrence de la même chose caractère trois fois à la suite.
- **consécutif-contrôle** - Vérifie si les valeurs par défaut ou ses variantes sont utilisées.
- **par défaut-contrôle** - Vérifie si ou nom d'utilisateur ou son l'inverse est utilisé.
- **tout-contrôles** - Activer/tout le fort contrôles de mot de passe.

Q. Comment la fonctionnalité client passive est-elle utilisée sur les contrôleurs LAN Sans fil ?

A. Les clients passifs sont des périphériques sans fil, tels que des échelles et des imprimantes cela sont configurés avec une adresse IP statique. Ces clients ne transmettent aucun IP les informations telles que l'adresse IP, le masque de sous-réseau, et les informations de passerelle

quand ils associé avec un Point d'accès. En conséquence, quand des clients passifs sont utilisés, le contrôleur ne connaît jamais l'adresse IP à moins qu'ils utilisent le DHCP.

WLCs agissent actuellement en tant que proxy pour des demandes d'ARP. Lors de recevoir un ARP la demande, le contrôleur répond avec une réponse d'ARP au lieu du dépassement demande directement au client. Ce scénario a deux avantages :

- Le périphérique en amont qui envoie la demande d'ARP au client va le faire ne pas savoir où le client se trouve.
- Alimentation pour les périphériques à piles tels que des téléphones portables et des imprimantes est préservé parce qu'ils ne doivent pas répondre à chaque ARP demandes.

Puisque le contrôleur sans-fil n'a aucune informations relative IP au sujet des clients passifs, il ne peut pas ne répondre à aucune demande d'ARP. Le courant le comportement ne permet pas le transfert des demandes d'ARP aux clients passifs. Quels l'application qui essaye d'accéder à un client passif échouera.

La fonctionnalité client de passif active les demandes et les réponses d'ARP d'être permuté entre de câble et clients sans fil. Cette caractéristique, une fois activée, permet au contrôleur pour passer des demandes d'ARP de câble aux clients sans fil jusqu'à le client sans fil désiré obtient à l'état de PASSAGE.

Pour les informations sur la façon dont configurer la fonctionnalité client passive, lisez la section en fonction Utilisation le GUI pour configurer le client passif dedans Cisco Guide de configuration Sans fil de contrôleur LAN, release 7.0.116.0.

Q. Comment pouvez I a installé le client pour authentifier à nouveau avec le serveur de RAYON toutes les trois minutes ou une période indiquée ?

A. Le paramètre de dépassement de délai de session sur le WLC peut être utilisé pour accomplir ceci. Par défaut, le paramètre de dépassement de délai de session est configuré pendant 1800 secondes avant une réauthentification se produit.

Changez cette valeur à 180 secondes afin de faire le client authentifiez à nouveau après trois minutes.

Afin d'accéder au paramètre de dépassement de délai de session, cliquez sur Menu **WLAN** dans le GUI. Il affiche la liste de WLAN configuré dans le WLC. Cliquez sur le WLAN auquel le client appartient. Allez à **l'onglet Avancé** et vous trouvent la *session d'enable Paramètre de dépassement de délai*. Changez la valeur par défaut à 180, et cliquez sur **Appliquez** pour les modifications pour le prendre effet.

Une fois introduit un Access-recevoir, avec une valeur d'Arrêt-action de La demande RADIUS, l'attribut de session-timeout spécifie le nombre maximal de secondes de service fournies avant la ré-authentification. Dans ce cas, L'attribut de session-timeout est utilisé pour charger le ReAuthPeriod constant dans Ordinateur d'état de temporisateur de réauthentification de 802.1X.

Q. J'ai un Tunnellisation d'invité, des Ethernets au-dessus du tunnel IP (EoIP), configuré entre mon contrôleur LAN 4400 Sans fil (WLC), qui agit en tant qu'ancre WLC, et plusieurs WLCs distant. Peuvent ce les diffusions de sous-réseau de l'ancre WLC en avant le tunnel d'EoIP du réseau câblé aux clients sans fil a associé avec contrôleurs distants ?

A. Non, le WLC 4400 n'expédie pas des émissions d'IP de sous-réseau du de câble dégrossissez aux clients sans fil à travers le tunnel d'EoIP. Ce n'est pas pris en charge caractéristique. Cisco ne prend en charge pas le Tunnellisation de la diffusion de sous-réseau ou de la Multidiffusion dedans topologie d'accès invité. Puisque le WLAN invité force le point de présence de client à un emplacement très spécifique dans le réseau, en grande partie en dehors du Pare-feu, le Tunnellisation de la diffusion de sous-réseau peut être un problème de Sécurité.

Q. À un point Sans fil Protocol du contrôleur LAN (WLC) et de l'accès léger (LWAPP) installé, quel Differentiated Services Code Point (DSCP) évalue sont passés pour le trafic vocal ? Comment QoS est-il mis en application sur le WLC ?

A. La solution WLAN du réseau sans fil unifié Cisco (UWN) prennent 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 platine QoS, assignez la faible bande passante WLAN pour utiliser QoS en bronze, et pour assigner à tout l'autre le trafic entre les autres niveaux de QoS. Reportez-vous à: Assigner un profil de QoS à un pour en savoir plus WLAN.

Q. Sont les ponts Ethernet de Linksys pris en charge dans Cisco Wireless Unified Solution ?

A. Non, le WLC prend seulement en charge les produits WGB Cisco. Linksys WGBs ne sont pas pris en charge. Bien que la solution de Cisco Wireless Unified ne prenne en charge pas Linksys WET54G et ponts Ethernet WET11B, vous pouvez utiliser ces périphériques dans a La radio a unifié la configuration de solution si vous utilisez ces instructions :

- Connectez un seul périphérique au WET54G ou au WET11B.
- Permettez à la caractéristique de clonage MAC sur le WET54G ou le WET11B de copier périphérique connecté.
- Installez les plus nouveaux gestionnaires et micrologiciel sur des périphériques connectés au WET54G ou WET11B. Cette instruction est particulièrement importante pour des imprimantes de JetDirect parce que des versions de firmware plus tôt posent des problèmes avec le DHCP.

Remarque: D'autres ponts tiers ne sont pas pris en charge. Les étapes mentionnées peuvent également soyez essayé pour d'autres tiers passerelles.

Q. Comment fais j'enregistrez les fichiers de configuration sur le contrôleur LAN Sans fil (WLC) ?

A. Le WLC contient deux genres de mémoire :

- RAM volatile — Tient le contrôleur en cours et actif configuration
- RAM non-volatile (NVRAM) — Tient la réinitialisation configuration

Quand vous configurez le système d'exploitation dans le WLC, vous modifiez la RAM volatile.

Vous devez sauvegarder la configuration de la RAM volatile au NVRAM afin de s'assurer que les réinitialisations WLC en configuration en cours.

Il est important de savoir quelle mémoire vous modifiez quand vous exécutez ces tâches :

- Utilisez l'assistant de configuration.
- Effacez la configuration de contrôleur.
- Saves configuration.
- Remettez à l'état initial le contrôleur.
- Déconnectez de-vous le CLI.

FAQ sur les fonctionnalités

Q. Comment je place le type de Protocole EAP (Extensible Authentication Protocol) sur Contrôleur LAN Sans fil (WLC) ? Je veux authentifier contre un contrôle d'accès L'appliance du serveur (ACS), et moi obtiennent « un EAP sans support » saisissent logs.

A. Il n'y a aucun paramètre distinct de type d'EAP sur le WLC. Pour l'EAP léger (LEAP), EAP Flexible Authentication via Secure Tunneling (EAP-FAST), ou Microsoft L'EAP protégé (MS-PEAP), configurent juste le 802.1x d'IEEE ou l'accès protégé par Wi-Fi (WPA) (si vous utilisez le 802.1x avec le WPA). Tout type d'EAP qui est pris en charge sur L'arrière saison de RAYON et sur le client est prise en charge par l'intermédiaire de la balise de 802.1x. L'EAP l'établissement sur le client et le serveur de RAYON doit s'assortir.

Terminez-vous ces étapes afin d'activer l'EAP par le GUI sur WLC :

1. Du GUI WLC, clic **WLAN**.
2. Une liste de WLAN configurés dans le WLC apparaît. Cliquez sur un WLAN.
3. Dans le **WLANs > Edit**, cliquez sur **Onglet Sécurité**.
4. Cliquez sur la **couche 2**, et choisissez le degré de sécurité de la couche 2 As 802.1x ou WPA+WPA2. Vous pouvez également configurer les paramètres de 802.1x qui sont disponibles dedans la même fenêtre. Puis, WLC les paquets d'authentification EAP en avant entre client sans fil et le serveur d'authentification.
5. Cliquez sur les serveurs d'**AAA**, et choisissez serveur d'authentification du menu déroulant pour ce WLAN. Nous supposons que le serveur d'authentification est déjà configuré globalement. Pour les informations sur la façon dont activez l'option d'EAP sur WLCs par l'interface de ligne de commande (CLI), référez-vous au *Utilisation le CLI pour configurer le RAYON* section de Cisco Guide de configuration Sans fil de contrôleur LAN, release 7.0.116.0.

Q. Qu'est-ce que le Fast SSID Changing ?

A. Le Fast SSID Changing permet à des clients pour se déplacer entre le SSID. Quand le le client envoie une nouvelle association pour un SSID différent, l'entrée de client dans la table de connexion de 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 qu'on permette à des des clients pour se déplacer à un nouveau SSID. Pour les informations sur la façon dont le Fast SSID Changing d'enable, se rapportent au *Configurer Fast SSID Changing* section de Cisco Guide de

configuration Sans fil de contrôleur LAN, release 7.0.116.0.

Q. Peux je fixer une limite sur le nombre de clients qui peuvent se connecter à une radio RÉSEAU LOCAL ?

A. Vous pouvez fixer une limite au nombre de clients qui peuvent se connecter à a WLAN, qui est utile dans les scénarios où vous avez un nombre limité de clients cela peut se connecter à un contrôleur. Le nombre de clients que vous pouvez configurer par WLAN dépend de la plate-forme que vous utilisez.

Lisez la section Configurer le nombre maximal de clients par WLAN de Cisco Guide de configuration Sans fil de contrôleur LAN, release 7.0.116.0 pour les informations sur les limites de client par WLAN pour les différentes Plateformes de Contrôleurs LAN Sans fil.

Q. Ce qui est PKC et comment il fonctionne avec le contrôleur LAN Sans fil (WLC) ?

A. PKC signifie le Key Caching proactif. Il a été conçu comme extension à la norme ieee 802.11i.

PKC est une fonction activée dans des contrôleurs de gamme Cisco 2006/410x/440x quelles autorisations ont correctement équipé des clients sans fil pour errer sans complètement ré-authentification avec un serveur d'AAA. Afin de comprendre PKC, vous d'abord le besoin de comprendre le Key Caching.

Le Key Caching est une fonctionnalité qui a été ajoutée au WPA2. Ceci permet un mobile station pour cacher les clés principales (Pairwise Master Key [PMK]) qu'elle gagne par a l'authentification réussie avec un Point d'accès (AP), et **le réutilisent dans a future association avec même AP**. Ceci signifie qu'un mobile donné le périphérique doit authentifier une fois avec une particularité AP, et cache la clé pour utilisation future. Le Key Caching est manipulé par l'intermédiaire d'un mécanisme connu sous le nom de PMK Identifier (PMKID), qui est des informations parasites du PMK, d'une chaîne, de la station et du MAC adresses d'AP. Le PMKID identifie seulement le PMK.

Même avec le Key Caching, une station Sans fil doit authentifier avec chacun AP qu'il souhaite obtenir le service de. Ceci introduit la latence significative et temps système, aux lesquels retardez le processus de hand-off et pouvez empêcher la capacité applications en temps réel de support. Afin de résoudre ce problème, PKC était introduit avec le WPA2.

PKC permet à une station pour réutiliser un PMK qu'elle avait précédemment gagné par a procédure d'authentification réussie. Ceci élimine le besoin de station à authentifiez contre de nouveaux aps en errant.

Par conséquent, dans une itinérance d'intra-contrôleur, quand un périphérique mobile se déplace d'un AP à l'autre sur le même contrôleur, les re-calculs de client un PMKID utilisant le 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. S'il fait, il évite la procédure d'authentification et immédiatement les initiés de 802.1x l'échange de la clé WPA2. S'il ne fait pas, il passe par le 802.1X standard procédure d'authentification.

Le PKC est activé par défaut avec le WPA2. Par conséquent, quand vous activez le WPA2 As Le degré de sécurité de la couche 2 sous la configuration WLAN du WLC, PKC est activé sur WLC. En outre, configurez le serveur d'AAA et le client sans fil pour l'EAP approprié authentification.

Le suppliant utilisé au côté client devrait également prendre en charge le WPA2 dedans

commande pour que PKC fonctionne. PKC peut également être mis en application dans un inter-contrôleur environnement errant.

Remarque: PKC ne fonctionne pas avec Aironet Desktop Utility (ADU) en tant que client suppliant.

Q. Explications de ces paramètres de délai d'expiration sur le contrôleur : Délai d'attente, User Idle Timeout, et session de Protocole ARP (Address Resolution Protocol) Délai d'attente ?

A. **Le délai d'attente d'ARP** est utilisé pour supprimer des entrées d'ARP sur WLC pour les périphériques a appris du réseau.

Le **User Idle Timeout :** Quand un utilisateur est de veille sans rien transmission avec le RECOUVREMENT pour la durée réglée comme User Idle Timeout, le client est désauthentifié par le WLC. Le client doit authentifier à nouveau et rassociez au WLC. Il est utilisé dans les situations où un client peut lâcher de son RECOUVREMENT associé sans informer le RECOUVREMENT. Ceci peut se produire si la batterie va complètement sur le client ou les associés de client s'écartent.

Remarque: Afin d'accéder à l'ARP et l'User Idle Timeout sur le GUI WLC, allez à le menu de **contrôleur**. Choisissez le **général du** côté gauche pour trouver l'ARP et les champs d'User Idle Timeout.

La Session Timeout est le moment maximum pour un client session avec le WLC. Après ce temps, WLC De-authentifie le client, et le client passe par le procédé entier d'authentification (ré-authentification) de nouveau. Cela fait partie d'une mesure de sécurité, qui sert à modifier les clés de chiffrement. Si vous utilisez une méthode de Protocole EAP (Extensible Authentication Protocol) avec la gestion des clés, la nouvelle saisie se produit à chaque intervalle régulier afin de dériver un nouveau cryptage clé. Sans gestion des clés, cette valeur du dépassement de durée est le temps qui radio le besoin des clients de faire une pleine réauthentification. Le délai d'attente de session est spécifique à le WLAN. Ce paramètre peut être accédé à du des **WLAN > Menu Edit**.

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

A. Le Radio-identification (RFID) est une technologie qui utilise la radio transmission de fréquence pour une transmission assez à courte portée. Un RFID de base le système se compose de tags RFID, de lecteurs de RFID, et de logiciel de traitement.

Aujourd'hui, Cisco prend en charge les balises RFID d'AeroScout et de Pango. Pour plus les informations sur la façon configurer des balises d'AeroScout, se rapportent WLC Configuration pour des tags RFID d'AeroScout.

Q. Est-ce que je peux exécuter l'authentification EAP localement sur le WLC ? Y en a il documentez qui explique cette caractéristique locale d'EAP ?

A. Oui, l'authentification EAP peut être exécutée localement sur le WLC. EAP local est une méthode d'authentification qui permet à des utilisateurs et à des clients sans fil pour être authentifié localement sur le WLC. Il est conçu pour l'usage dans les bureaux distants cela voulez mettre à jour la Connectivité aux clients sans fil quand le système principal devient perturbé, ou le

serveur d'authentification externe descend. Quand vous activez l'EAP local, les servir WLC de serveur d'authentification. Pour plus les informations sur la façon dont configurez un WLC pour l'authentification locale d'EAP-FAST, se réfèrent au Gens du pays Authentification EAP sur le contrôleur LAN Sans fil avec l'EAP-FAST et le serveur LDAP Exemple de configuration.

Q. Qu'est-ce que la fonctionnalité de priorité WLAN ? Comment est-ce que je configure cette fonctionnalité ? Allez le faire les recouvrements mettent à jour les valeurs de priorité WLAN quand ils basculent à la sauvegarde WLC ?

A. La caractéristique de priorité WLAN nous permet de choisir des WLAN de parmi WLAN configurés sur un WLC qui peut être activement utilisé sur une base individuelle de RECOUVREMENT. Complétez ces étapes afin de configurer une priorité de WLAN :

1. Dans le GUI WLC, cliquez sur la **radio** menu.
2. Cliquez sur les **radios d'**option du côté gauche, et choisissez le **802.11 a/n** ou le **802.11 b/g/n.**
3. Cliquez sur le lien de **configurer du** menu déroulant trouvé du côté droit qui correspond au nom d'AP sur lequel vous voulez configurer le dépassement WLAN.
4. Choisissez Enable du déroulant de priorité WLAN menu. Le menu de priorité WLAN est le dernier élément du côté gauche de fenêtre.
5. La liste de tous les WLAN qui sont configurés sur le WLC apparaît.
6. De cette liste, vérifiez les **WLAN aux les**quels vous voulez apparaissez sur le RECOUVREMENT, et cliquez sur Apply pour que les modifications prennent effet.
7. Sauvegardez votre configuration après que vous fassiez ces derniers modifications.

Les aps retiennent les valeurs de priorité WLAN quand ils obtiennent enregistré à l'autre WLCs, à condition que les profils WLAN et le SSID que vous voulez ignorer soient configuré à travers tout le WLCs.

Remarque: Dans la version de logiciel de logiciel contrôleur 5.2.157.0, la caractéristique de priorité WLAN a été retiré du GUI et du CLI de contrôleur. Si votre contrôleur est configuré pour le dépassement et vous WLAN améliorez à la version de logiciel de logiciel contrôleur 5.2.157.0, le contrôleur supprime la configuration WLAN et annonce tous WLAN. Vous pouvez spécifier que seulement certains WLAN soient transmis si vous configurez groupes de Point d'accès. Chaque Point d'accès annonce seulement les WLAN activés cela appartenez à son groupe de Point d'accès.

Remarque: Des groupes de Point d'accès ne permettent pas à des WLAN d'être transmis en fonction par interface par radio d'AP.

Q. Est l'IPv6 pris en charge sur les contrôleurs LAN Sans fil de Cisco (WLCs) et Point d'accès léger (recouvrements) ?

A. Actuellement, les contrôleurs de gammes 4400 et 4100 prennent en charge seulement l'IPv6 fonction émulation de client. Il n'y a aucune prise en charge native de l'IPv6.

Afin d'activer l'IPv6 sur le WLC, vérifiez l'**IPv6 Activez la** case sur la configuration WLAN SSID sous WLAN > Éditez la page.

En outre, le Ethernet Multicast Mode (EMM) est requis pour la prise en charge du IPv6. Si vous désactivez l'EMM, les périphériques de client qui utilisent l'IPv6 perdent la Connectivité. Afin

d'activer L'EMM, vont au contrôleur > page générale et de la Multidiffusion d'Ethernets Le mode relâchent vers le bas le menu, choisissent **Unicast** ou **Multidiffusion**. Ceci active la Multidiffusion ou en mode d'Unicast ou Mode de Multidiffusion. Quand la Multidiffusion est activée comme unicast de Multidiffusion, les paquets sont répliqué pour chaque AP. Ceci peut être processeur intensif, ainsi utilisez-le avec attention. La Multidiffusion activée comme Multidiffusion de Multidiffusion utilise l'assigné à l'utilisateur adresse de multidiffusion pour faire une Multidiffusion plus traditionnelle aux Points d'accès (Aps).

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

En outre, il y a de l'ID de bogue Cisco CSCsg78176, qui empêche utiliser l'IPv6 fonction émulation quand la caractéristique d'AAA Overrride est utilisée.

Q. Fait le Web de support du contrôleur LAN sans fil de la gamme Cisco 2000 (WLC) Authentification pour des utilisateurs d'invité ?

A. L'authentification Web est prise en charge sur tous les Cisco WLC. Authentification Web est une méthode d'authentification de la couche 3 utilisée pour authentifier des utilisateurs avec simple qualifications d'authentification. Aucun chiffrement n'est impliqué. Terminez-vous ces étapes dedans commande pour activer cette caractéristique :

1. Du GUI, cliquez sur le **WLAN** menu.
2. Cliquez sur un **WLAN**.
3. Allez à l'**onglet Sécurité** et choisissez la **couche 3.**
4. Cochez la case de **stratégie de Web** et choisissez **Authentification**.
5. Cliquez sur **Apply** afin de sauvegarder les modifications.
6. Afin de créer une base de données sur le WLC contre au lequel authentifiez les utilisateurs, allez au **menu Security** sur le GUI, choisissez **L'utilisateur du réseau local**, et se terminent ces actions : Définissez le nom d'utilisateur et mot de passe d'invité pour que l'invité l'utilise dedans commande à ouvrir une session. Ces valeurs distinguent les majuscules et minuscules.Choisissez l'ID du WLAN que vous utilisez.**Remarque:** Pour plus de configuration détaillée, référez-vous au Radio Exemple de configuration d'authentification Web de contrôleur LAN.

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

A. WLC peut être géré par le mode Sans fil une fois qu'il est activé. Pour plus les informations sur la façon dont activer le mode Sans fil se rapportent au *Activation Connexions Sans fil au GUI et au CLI* section de Cisco Guide de configuration Sans fil de contrôleur LAN, release 7.0.116.0.

Q. Qu'est-ce que l'agrégation de liaisons (LAG) ? Comment fais j'activez le LAG sur le RÉSEAU LOCAL Sans fil Contrôleurs (WLCs) ?

A. Le LAG empaquette tous les ports sur le WLC dans un EtherChannel simple interface. Le système gère dynamiquement l'Équilibrage de charge et le port du trafic Redondance avec le LAG.

Généralement, l'interface sur le WLC a de plusieurs paramètres associés avec il, qui inclut l'adresse IP, passerelle par défaut (pour l'IP de sous-réseau), primaire port physique, port physique secondaire, balise VLAN, et serveur DHCP. Quand le LAG est non utilisée, chaque

interface est habituellement tracée à un port physique, mais au multiple des interfaces peuvent également être tracées à un port simple WLC. Quand le LAG est utilisé, le système trace dynamiquement les interfaces au Port canalisé agrégé. Ceci aides dans la Redondance et l'Équilibrage de charge de port. Quand un port échoue, l'interface est dynamiquement tracé au prochain port physique disponible, et les recouvrements sont équilibré à travers des ports.

Quand le LAG est activé sur un WLC, WLC les trames de données en avant sur la même chose port sur lequel ils ont été reçus. Le WLC se fonde sur le commutateur voisin à équilibrez la charge le trafic à travers l'EtherChannel. Le WLC n'en exécute pas Équilibrage de charge d'EtherChannel seule.

Q. Ce qui modèle de l'agrégation Sans fil de support de contrôleurs LAN (WLCs) (LAG) ?

A. LAG de support de contrôleurs de gamme Cisco 5500 dans la version de logiciel 6.0 ou plus tard, LAG de support de contrôleurs de gamme Cisco 4400 dans la version de logiciel 3.2 ou plus tard, et LAG est activé automatiquement sur les contrôleurs au sein de Cisco WiSM et le commutateur de contrôleur sans fil LAN intégré du Catalyst 3750G. Sans LAG, chaque port de système de distribution sur des supports d'un contrôleur de gamme Cisco 4400 jusqu'à 48 Points d'accès. Le LAG étant activé, un contrôleur de Cisco 4402 logique le port prend en charge jusqu'à 50 Points d'accès, le port logique d'un contrôleur de Cisco 4404 supports jusqu'à 100 Points d'accès, et le port logique sur le Catalyst 3750G Commutateur de contrôleur sans fil LAN intégré et sur chaque contrôleur de Cisco WiSM supports jusqu'à 150 Points d'accès.

Les WLC Cisco 2106 et 2006 ne prennent pas en charge le LAG. Modèles antérieurs, tels comme gamme Cisco 4000 WLC, ne prenez en charge pas le LAG.

Q. Ce qui est la caractéristique de mobilité d'auto-ancrage dans la radio unifiée Réseaux ?

A. La mobilité d'auto-ancrage (ou la mobilité de WLAN invité) est utilisée pour améliorer le chargement équilibrage et Sécurité pour les clients errants sur vos réseaux locaux Sans fil (WLAN). Sous les états normaux d'itinérance, des périphériques de client joignent un WLAN et sont ancrés au premier contrôleur qu'ils entrent en contact avec. Si un client erre à un différent sous-réseau, le contrôleur auquel le client erre a installé une session étrangère pour client avec le contrôleur d'ancre. Avec l'utilisation de la mobilité d'auto-ancrage caractéristique, vous pouvez spécifier un contrôleur ou un ensemble de contrôleurs comme ancre points pour des clients sur un WLAN.

Remarque: L'ancre de mobilité ne doit pas être configurée pour la mobilité de couche 3. l'ancre de mobilité est utilisée seulement pour le Tunnellisation d'invité.

Q. Peut Cisco 2006 le contrôleur LAN que Sans fil (WLC) soit configuré comme ancre pour un WLAN ?

A. Un WLC de la gamme Cisco 2000 ne peut pas être désigné comme ancre pour un WLAN. Cependant, un WLAN créé sur une gamme Cisco 2000 WLC peut avoir une gamme Cisco 4100 WLC et gamme Cisco 4400 WLC en tant que son ancre.

Q. Quel type de tunnel de mobilité le contrôleur de réseau local sans fil utilise-t-il ?

A. Versions 4.1 de logiciel contrôleur par 5.1 le support chacun des deux asymétriques et Tunnellisation symétrique de mobilité. Version 5.2 de logiciel contrôleur ou plus tard prenez en charge seulement le Tunnellisation symétrique de mobilité, par lequel est maintenant toujours activé par défaut.

Dans le Tunnellisation asymétrique, le trafic de client au réseau câblé est conduit directement par le contrôleur étranger. Ruptures asymétriques de Tunnellisation quand le routeur en amont fait activer le reverse path filtering (RPF). Dans ce cas, le trafic de client est abandonné au routeur parce que le contrôle RPF assure cela le chemin de nouveau à l'adresse source apparie le chemin dont le paquet est livré.

Quand le Tunnellisation symétrique de mobilité est activé, tout le trafic de client est envoyé au contrôleur d'ancre 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 le chemin de paquet de client relâche des paquets parce que l'adresse IP source n'apparie pas le sous-réseau sur lequel les paquets sont reçus, ceci est utile.
- Si le groupe VLAN d'access-point sur le contrôleur d'ancre est différent que l'interface vlan WLAN sur le contrôleur étranger : dans ce cas, client le trafic peut être envoyé sur un VLAN incorrect pendant la mobilité événements.

Q. Comment faites nous accédons au WLC quand le réseau est vers le bas ?

A. Quand le réseau est en panne, le WLC peut être accessible via le port de service. Ce port est assigné une adresse IP dans entièrement un différent sous-réseau d'autre des ports du WLC et ainsi s'appelle la gestion hors bande. Pour en savoir plus, référez-vous *Configurer Ports et interfaces* section de Cisco Guide de configuration Sans fil de contrôleur LAN, release 7.0.116.0.

Q. Faites Cisco les contrôleurs LAN que Sans fil (WLCs) prennent en charge le Basculement (ou caractéristique de Redondance) ?

A. Oui, si vous avez deux WLCs ou plus dans votre réseau WLAN, vous pouvez configurez-les pour la Redondance. Généralement, un RECOUVREMENT se joint au primaire configuré WLC. Une fois que le WLC primaire échoue, le RECOUVREMENT redémarre et joint un autre WLC dans groupe de mobilité. Le Basculement est une caractéristique où le RECOUVREMENT vote pour le WLC primaire et joint le WLC primaire une fois qu'il est fonctionnel. Reportez-vous à la section : WLAN Basculement de contrôleur pour l'exemple de configuration de Point d'accès léger pour plus d'informations.

Q. Ce qui est l'utilisation du Listes de contrôle d'accès (ACL) de pré-authentification dedans Contrôleurs LAN Sans fil (WLCs) ?

A. Avec l'ACL de pré-authentification, comme nom implique, vous peut permettre le client le trafic à et d'une adresse IP spécifique même avant le client authentifie. En utilisant un web server externe pour l'authentification Web, une partie du WLC les Plateformes ont besoin d'un ACL de pré-authentification pour le web server externe (Cisco Contrôleur de gamme 5500, une gamme Cisco 2100 contrôleur, gamme Cisco 2000 et le module réseau de contrôleur). Pour les autres Plateformes WLC, l'ACL de pré-authentification n'est pas obligatoire. Cependant, il est conseillé de configurez un ACL de pré-authentification pour le web server externe en utilisant

authentification de Web externe.

Q. J'ai un WLAN qui filtre les adresses MAC et un WLAN complètement ouvert dans mon réseau. Le client choisit-il le WLAN ouvert par défaut ? Ou fait le client associez-vous automatiquement avec l'ID de WLAN qui est placé sur le filtre d'adresses MAC ? En outre, pourquoi y a-t-il une option de « interface » sur un filtre d'adresses MAC ?

A. Le client peut s'associer à n'importe quel WLAN auquel le client est configuré pour se connecter. L'option d'interface dans le filtre d'adresses MAC donne la capacité de s'appliquer le filtre à un WLAN ou à une interface. Si le multiple WLAN sont attachés au la même interface, vous pouvez appliquer le filtre d'adresses MAC à l'interface sans besoin pour créer un filtre pour chaque WLAN individuel.

Q. Comment peux je configurer l'authentification TACACS pour des utilisateurs de Gestion sur Contrôleur LAN Sans fil (WLC) ?

A. À partir de la version 4.1 WLC, TACACS est pris en charge sur le WLCs. Référez-vous à Configurer TACACS+ afin de comprendre comment configurer TACACS+ pour authentifier utilisateurs de Gestion du WLC.

Q. Ce qui est l'utilisation de la configuration excessive d'échec d'authentification dans a Contrôleur LAN Sans fil (WLC) ?

A. Ce paramètre fait partie des politiques d'exclusion de client. Le client l'exclusion est une fonctionnalité de sécurité sur le contrôleur. La stratégie est utilisée à mettez les clients sur la liste noire afin d'empêcher l'accès illégal au réseau ou aux attaques au réseau Sans fil.

Cette stratégie excessive de panne d'authentification Web étant activé, quand a le nombre de client de tentatives défectueuses d'authentification Web dépasse 5, le contrôleur considère que le client a dépassé les tentatives maximum du Web l'authentification et met le client sur la liste noire.

Terminez-vous ces étapes afin d'activer ou désactiver ceci établissement :

1. Du GUI WLC, allez à la **Sécurité > à la protection sans fil Stratégies > stratégies d'exclusion de client**.
2. Vérifiez ou décochez l'**authentification Web excessive Pannes**.

Q. J'ai converti mon point d'accès autonome (AP) en mode léger. Dans le mode léger AP Protocol (LWAPP) avec le serveur d'AAA RADIUS pour le client rendant compte, normalement le client est dépisté avec la comptabilité de RAYON basée sur Adresse IP du WLC. Est il possible de placer la comptabilité de RAYON basée sur Adresse MAC d'AP associé à cela WLC et pas l'adresse IP du WLC ?

A. Oui, cela est possible du côté de la configuration du WLC. Terminez-vous ces derniers étapes :

1. Du GUI de contrôleur, sous la **Sécurité > le rayon Comptabilité**, il y a une liste déroulante pour le type d'ID de station d'appel. Choisissez **Adresse MAC AP**.
2. Vérifiez-la via le journal de l'AP LWAPP. Là, vous pouvez voir le champ d'ID d'appeler-

station qui affiche Adresse MAC d'AP auquel le client particulier est associé.

Q. Comment vous changez le délai d'attente de prise de contact de Protocole WPA (Wi-Fi Protected Access) valeur sur un contrôleur LAN Sans fil (WLC) par le CLI ? Je sais que je peux faire ceci en fonction Points d'accès de Cisco IOS® (aps) avec la prise de contact du wpa dot11 *valeur du dépassement de durée* commande, mais comment faites-vous exécutez ceci sur un WLC ?

A. La capacité de configurer le délai d'attente de WPA-prise de contact par le WLCs était intégré dans la version de logiciel 4.2 et ultérieures. Vous n'avez pas besoin de cette option dedans des versions de logiciel plus tôt 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 courant de WLCs comportement.

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

Remarque: Sur IOS aps, cette configuration est configurable avec le **dot11** commande de **prise de contact de wpa**.

Vous pouvez également configurer les autres paramètres d'EAP avec les options dessous la commande de **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. Ce qui est le but de la caractéristique diagnostique de canal dans le WLAN > Éditez > avez avancé la page ?

A. La caractéristique de canal de diagnostic te permet de dépanner des problèmes dedans respect à la communication client avec un WLAN. Le client et les Points d'accès peuvent être mettez un ensemble défini de tests pour identifier la cause de transmission les difficultés aux lesquelles les expériences de client et laissent alors des mesures correctives soyez pris pour rendre le client opérationnel sur le réseau. Vous pouvez utiliser le GUI ou le CLI de contrôleur pour activer le canal diagnostique, et vous peut utiliser contrôleur CLI ou WCS pour exécuter les tests de diagnostic.

Le canal diagnostique peut être uniquement utilisé à des fins de test. Si vous essayez à configurez l'authentification ou le cryptage pour le WLAN avec le canal diagnostique activé, vous voyez cette erreur :

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

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

- Un maximum des groupes de 50 Points d'accès pour la gamme Cisco 2100 Contrôleur et modules réseau de contrôleur
- Un maximum des groupes de 300 Points d'accès pour la gamme Cisco 4400 Contrôleur LAN de radio de contrôleurs, de Cisco WiSM, et de Cisco 3750G Commutateur
- Un maximum des groupes de 500 Points d'accès pour la gamme Cisco 5500 Contrôleurs

Informations connexes

- Radio Foire aux questions du contrôleur LAN (WLC)
- Radio Foire aux questions de messages système d'erreur et du contrôleur LAN (WLC)
- Léger Foire aux questions de Point d'accès
- Cisco Guide de configuration Sans fil de contrôleur LAN, version 7.0.116.0
- Support d'IPv6 sur le contrôleur LAN Sans fil
- Radio Assistance sur les produits
- Assistance technique et Documentation - Cisco Systems

Cisco relatif prennent en charge des discussions de la Communauté

Cisco prennent en charge la Communauté est un forum pour que vous posiez et pour répondez à des questions, des suggestions de partage, et collaborez avec vos pairs.

Référez-vous au Conventions relatives aux conseils techniques Cisco pour les informations sur des conventions utilisées dans ce document.

Mis à jour : Mars 02, 2015
ID de document : 118833