Messages d'erreur et système du contrôleur de réseau local sans fil - Forum Aux Questions

Contenu

Introduction

Ce document fournit des informations sur les questions fréquemment posées (FAQ) à propos des messages d'erreur et des messages système pour les contrôleurs de réseau sans fil (WLAN) Cisco (WLC).

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

FAQ sur les messages d'erreur

Q. Nous avons commencé la conversion de plus de 200 points d'accès (AP) de logiciel Cisco IOS® en un protocole d'AP léger (LWAPP) avec Cisco 4404 WLC. Nous avons finalisé la conversion de 48 AP et nous recevons un message sur le WLC qui énonce : **[[ERROR] spam_lrad.c 4212: AP cannot join because the maximum number of APs on interface 1 is reached.** Pourquoi l'erreur se produit-elle ?

A. Vous devez créer des interfaces du gestionnaire AP supplémentaires afin de prendre en charge plus de 48 AP. Autrement, vous recevrez un message d'erreur tel que :

```
Wed Sep 28 12:26:41 2005 [ERROR] spam_lrad.c 4212: AP cannot join because
the maximum number of APs on interface 1 is reached.
```

Configurez les interfaces multiples du gestionnaire AP et configurez les ports principaux/de secours que d'autres interfaces du gestionnaire AP n'utilisent pas. Vous *devez* créer une deuxième interface du gestionnaire AP afin de mettre en place d'autres AP. Mais assurez-vous que vos configurations de port principal et de port de secours pour chaque gestionnaire ne se superposent pas. En d'autres termes, si le gestionnaire AP 1 utilise le port 1 en tant que port principal et le port 2 comme port de secours, le gestionnaire AP 2 doit utiliser le port 3 en tant que port principal et le port 4 comme port de secours.

Q. J'ai un contrôleur de réseau local sans fil (WLC) 4402 et j'utilise les points d'accès léger (LAP) 1240. J'essaye d'activer le cryptage 128 bits sur le WLC. Quand je sélectionne le cryptage WEP 128 bits sur le WLC, je reçois un message

d'erreur qui indique que le cryptage 128 bits n'est pas pris en charge sur les modèles 1240 : `[[ERROR] spam_lrad.c 12839: Not creating SSID mde on CISCO AP xx: xx : xx : xx : xx : xx because WEP128 bit is not supported.` Pourquoi est-ce que je reçois cette erreur ?

A. Les longueurs de clé montrées sur les WLC sont en fait le nombre de bits qui sont dans le secret partagé et n'incluent pas les 24 bits du vecteur d'initialisation (IV). Beaucoup de produits, dont les produits Aironet, l'appellent une clé WEP 128 bits. En réalité, c'est une clé de 104 bits avec 24 bits de l'IV. 104 bits est la taille de la clé que vous devez autoriser sur le WLC pour le cryptage WEP de 128 bits.

Si vous choisissez 128 bits comme taille de la clé sur le WLC, c'est en fait un cryptage de clé WEP de 152 bits (128 + 24 IV). Seuls les LAP de la gamme Cisco 1000 (AP1010, AP1020, AP1030) permettent l'utilisation des paramètres de la clé WEP de 128 bits WLC.

Q. Pourquoi est-ce que j'obtiens le message d'erreur WEP key size of 128 bits is not supported on 11xx, 12xx and 13xx model APs. `Wlan will not be pushed to these Access Points.` quand j'essaye de configurer le WEP sur un WLC ?

A. Sur un contrôleur de réseau local sans fil, quand vous choisissez le WEP statique comme méthode de sécurité de la couche 2, vous avez ces options ou la taille de clé WEP.

- non défini
- 40 bits
- 104 bits
- 128 bits

Ces valeurs de taille de clé n'incluent pas le vecteur d'initialisation (IV) 24 bits, qui est concaténé avec la clé WEP. Ainsi, pour un WEP de 64 bits, vous devez choisir **40 bits** comme taille de clé WEP. Le contrôleur ajoute le vecteur d'initialisation (IV) de 24 bits afin de faire une clé WEP de 64 bits. De même, pour une clé WEP de 128 bits, choisissez **104 bits**.

Les contrôleurs prennent également en charge les clés WEP de 152 bits (128 bits + IV de 24 bits). Cette configuration n'est pas prise en charge sur les modèles d'AP 11xx, 12xx et 13xx. Ainsi quand vous essayez de configurer le WEP avec 144 bits, le contrôleur donne un message indiquant que cette configuration WEP n'est pas applicable aux modèles d'AP 11xx, 12xx et 13xx.

Q. Les clients ne peuvent pas authentifier à un WLAN qui est configuré pour le WPA2 et le contrôleur affiche l'`apf_80211.c:1923 APF-1-PROC_RSN_WARP_IE_FAILED : Could not process the RSN and WARP IE's. station not using RSN (WPA2) on WLAN requiring RSN.MobileStation:00:0c:f1:0c:51:22, SSID:` <>. Pourquoi est-ce que je reçois cette erreur ?

A. Ceci se produit en grande partie en raison d'une incompatibilité du côté du client. Essayez de réaliser ces étapes afin de résoudre ce problème :

- Vérifiez si le client est certifié Wi-Fi pour le WPA2 et vérifiez la configuration du client pour le WPA2.
- Vérifiez la fiche technique afin de voir si l'utilitaire client prend en charge le WPA2. Installez n'importe quel correctif sorti par le fournisseur pour prendre en charge le WPA2. Si vous utilisez l'utilitaire Windows, assurez-vous que vous avez installé le correctif WPA2 de

Microsoft afin de prendre en charge le WPA2.
- Mettez à jour le pilote et le microprogramme du client.
- Désactivez les extensions Aironet sur le WLAN.

Q. Une fois que je redémarre le WLC, j'obtiens le message d'erreur Mon Jul 17 15:23:28 2006 MFP Anomaly Detected - 3023 Invalid MIC event found as violated by the radio 00:XX:XX:XX:XX and detected by the dot11 interface at slot 0 of AP 00:XX:XX:XX:XX in 300 seconds when observing Probe responses, Beacon Frames. Pourquoi cette erreur se produit-elle et comment est-ce que je me débarrasse d'elle ?

A. Ce message d'erreur apparaît quand des trames avec des valeurs MIC incorrectes sont détectées par les LAP activés par MFP. Consultez la section Exemple de configuration de Management Frame Protection (MFP) pour infrastructures avec WLC et LAP pour plus d'informations sur MFP. Réalisez une de ces quatre étapes :

1. Vérifiez et supprimez tous les AP ou clients non autorisés ou non valides dans votre réseau, qui génèrent des trames non valides.
2. Désactivez l'infrastructure MFP, si MFP n'est pas activé sur d'autres membres du groupe de mobilité car les LAP peuvent entendre les trames de gestion des LAP d'autres WLC dans le groupe qui n'ont pas MFP activé. Consultez la section FAQ sur les groupes de mobilité du contrôleur de réseau local sans fil (WLC) pour plus d'informations sur le groupe de mobilité.
3. Le correctif pour ce message d'erreur est disponible dans les versions WLC 4.2.112.0 et 5.0.148.2. Mettez à jour les WLC avec l'une ou l'autre de ces versions.
4. Comme dernière option, essayez de recharger le LAP qui génère ce message d'erreur.

Q. Le client AIR-PI21AG-E-K9 s'associe avec succès avec un Point d'accès (AP) utilisant l'authentification Protocol-flexible d'authentification extensible par l'intermédiaire du Tunnellisation sécurisé (EAP-FAST). Cependant, quand l'AP associé est éteint, le client ne se déplace pas à un autre AP. Ce message apparaît continuellement dans le journal des messages du contrôleur : **""Fri Jun 2 14:48:49 2006 [SECURITY] 1x_auth_pae.c 1922: Unable to allow user into the system - perhaps the user is already logged onto the system? Fri Jun 2 14:48:49 2006 [SECURITY] apf_ms.c 2557: Unable to delete username for mobile 00:40:96:ad:75:f4". Pourquoi** ?

A. Quand la carte client doit faire de l'itinérance, elle envoie une demande d'authentification, mais elle ne prend pas correctement en charge les clés (n'informe pas AP/contrôleur, ne répond pas aux réauthentifications).

Ceci est documenté dans l'ID de bogue Cisco CSCsd02837 (clients enregistrés seulement). Ce bogue a été réparé avec l'Assistant d'installation 3.5 des adaptateurs client de Cisco Aironet 802.11a/b/g.

Généralement, le message Unable to delete username for mobile apparaît également en raison de :

- Le nom d'utilisateur particulier est utilisé sur plus d'un périphérique client.
- La méthode d'authentification utilisée pour ce WLAN a une identité anonyme externe. Par exemple, dans PEAP-GTC ou dans EAP-FAST, il est possible de définir un nom d'utilisateur

générique en tant qu'identité (visible) externe, et le vrai nom d'utilisateur est masqué à l'intérieur du tunnel TLS entre le client et le serveur radius, ainsi le contrôleur ne peut pas le voir et l'utiliser. En pareil cas, ce message peut apparaître. Ce problème apparaît plus généralement avec des clients tiers et des clients de microprogramme ancien.

Q. Quand j'installe la nouvelle lame de Wireless Services Module (WiSM) dans les commutateurs 6509 et implémente Protected Extensible Authentication Protocol (PEAP) avec le serveur Microsoft IAS, je reçois cette erreur : **Mar 1 00:00:23.526: %LWAPP-5-CHANGED : LWAPP changed state to DISCOVERY *Mar 1 00:00:23.700: %SYS-5-RELOAD : Reload requested by LWAPP CLIENT.Reload Reason: FAILED CRYPTO INIT. **Mar 1 00:00:23.700: %LWAPP-5-CHANGED : LWAPP changed state to DOWN *Mar 1 00:00:23.528: %LWAPP-5-CHANGED : LWAPP changed state to DISCOVERY *Mar 1 00:00:23.557: LWAPP_CLIENT_ERROR_DEBUG: lwapp_crypto_init_ssc_keys_and_certs no certs in the SSC Private File *Mar 1 00:00:23.557: LWAPP_CLIENT_ERROR_DEBUG: **Mar 1 00:00:23.557: lwapp_crypto_init: PKI_StartSession failed *Mar 1 00:00:23.706: %SYS-5-RELOAD : Reload requested by LWAPP CLIENT. . Pourquoi ?

A. RADIUS et le dot1x met au point l'exposition que le WLC envoie à une demande d'accès, mais il n'y a aucune réponse du serveur d'IAS. Suivez ces étapes afin de résoudre ce problème :

1. Contrôlez et vérifiez la configuration du serveur IAS.
2. Vérifiez le fichier journal.
3. Installez un logiciel tel que Ethereal, qui peut vous fournir des détails sur l'authentification.
4. Arrêtez et remettez en marche le service IAS.

Q. Les points d'accès léger (LAP) ne s'inscrivent pas auprès du contrôleur. Quel pourrait être le problème ? Je vois ces messages d'erreur sur le contrôleur : Thu Feb 3 03:20:47 2028: LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP 00:0b:85:68:f4:f0. Thu Feb 3 03:20:47 2028: Unable to free public key for AP 00:0B:85:68:F4:F0.

A. Quand le point d'accès (AP) envoie la demande d'enregistrement du protocole Lightweight Access Point Protocol (LWAPP) au WLC, il inclut son certificat X.509 dans le message LWAPP. Il génère également une ID de session aléatoire qui est incluse dans la demande d'enregistrement LWAPP. Quand le WLC reçoit les demandes d'enregistrement LWAPP, il valide la signature du certificat X.509 en utilisant la clé publique des AP et vérifie que le certificat a été délivré par une autorité de certification de confiance. Il regarde également la date et l'heure de début pour l'intervalle de validité du certificat AP et les compare à ses propres date et heure.

Ce problème peut se poser en raison d'un paramétrage incorrect de l'horloge sur le WLC. Afin de régler l'horloge sur le WLC, lancez les commandes **show time** et **config time**.

Q. Un protocole Lightweight Access Point Protocol (LWAPP) AP ne peut pas se connecter à son contrôleur. Le journal du contrôleur de réseau local sans fil (WLC) affiche un message semblable à ceci : LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP 00:0b:85:68:ab:01. Pourquoi ?

A. Vous pouvez recevoir ce message d'erreur si le tunnel LWAPP entre l'AP et le WLC traverse un chemin réseau avec une MTU inférieure à 1500 octets. Ceci entraîne la fragmentation des paquets LWAPP. C'est un bogue connu dans le contrôleur. Consultez l'ID de bogue Cisco CSCsd39911 (clients enregistrés seulement).

La solution est de mettre à jour le microprogramme du contrôleur à 4.0(155).

Q. J'essaye d'établir un tunnel invité entre mon contrôleur interne et le contrôleur d'ancrage virtuel sur la zone démilitarisée (DMZ). Cependant, quand un utilisateur tente de s'associer à un invité SSID, l'utilisateur n'arrive pas à recevoir l'adresse IP de la DMZ, comme prévu. Par conséquent, le trafic de l'utilisateur n'est pas relié par tunnel au contrôleur sur la DMZ. Le résultat de la commande debug mobile handoff affiche un message semblable à ceci : **Security Policy Mismatch for WLAN <Wlan ID>. Anchor Export Request from Switch IP:** <controller Ip address> Ignored. Quel est le problème ?

A. Le Tunnellisation d'invité fournit la Sécurité supplémentaire pour l'accès d'invité-utilisateur au réseau Sans fil entreprise. Ceci aide à s'assurer que les utilisateurs invités ne peuvent pas accéder au réseau de l'entreprise sans passer d'abord par le pare-feu de l'entreprise. Quand un utilisateur s'associe à un WLAN qui est indiqué comme WLAN invité, le trafic utilisateur est relié par tunnel au contrôleur WLAN qui se trouve sur la DMZ hors du pare-feu de l'entreprise.

Maintenant, compte tenu de ce scénario, il peut y avoir plusieurs raisons pour que ce tunnel invité ne fonctionne pas comme prévu. Comme l'implique la sortie de la commande **debug**, le problème pourrait être dû à la non correspondance entre les différentes politiques de sécurité configurées pour ce WLAN particulier dans l'interne aussi bien que dans les contrôleurs DMZ. Vérifiez si les politiques de sécurité ainsi que d'autres paramètres, tels que les paramètres de temps d'expiration de la session, correspondent.

Une autre raison courante pour ce problème est que le contrôleur DMZ n'est pas ancré à lui-même pour ce WLAN particulier. Pour qu'un tunnel invité fonctionne correctement et que la DMZ gère l'adresse IP de l'utilisateur (utilisateur qui appartient à un WLAN invité), il est essentiel que l'ancrage approprié soit fait pour ce WLAN particulier.

Q. Je vois beaucoup de messages "CPU Receive Multicast Queue is full on Controller" sur le contrôleur de réseau local sans fil 2006 mais pas sur les WLC 4400. Pourquoi ? J'ai désactivé le multicast sur les contrôleurs. Quelle est la différence dans la limite de file d'attente Multicast entre les plates-formes WLC 2006 et 4400 ?

A. Puisque le multicast est désactivé sur les contrôleurs, les messages qui entraînent cette alarme pourraient être des messages de Protocole de résolution d'adresse (ARP). Il n'y a aucune différence dans la profondeur de la file d'attente (512 paquets) entre les WLC 2000 et 4400. La différence est que le 4400 NPU filtre les paquets ARP tandis que tout est fait par logiciel sur le 2006. Ceci explique pourquoi le WLC 2006 voit les messages mais pas le WLC 4400. Un WLC 44xx traite les paquets multicast par l'intermédiaire du matériel (par CPU). Un WLC 2000 traite les paquets multicast par l'intermédiaire du logiciel. Le traitement par CPU est plus efficace que celui par logiciel. Par conséquent, la file d'attente du 4400 est plus rapidement effacée, tandis que le WLC 2006 a un peu de difficulté quand il voit beaucoup de ces messages.

Q. Je vois le message d'erreur "[SECURITY] apf_foreignap.c 763: **STA [00:0A:E4:36:1F:9B] Received a packet on port 1 but no Foreign AP configured for this port."** sur un de mes contrôleurs. Que signifie cette erreur et quelles étapes dois-je suivre pour résoudre ce problème ?

A. Ce message apparaît quand le contrôleur reçoit une requête DHCP pour une adresse MAC pour laquelle il n'a pas de machine d'état. Ceci apparaît souvent d'un pont ou d'un système qui exécute une machine virtuelle comme VMWare. Le contrôleur écoute les requêtes DHCP parce qu'il réalise une surveillance DHCP. Ainsi, il sait quelles adresses sont associées aux clients qui sont rattachés à ses points d'accès (AP). Tout le trafic pour les clients sans fil traverse le contrôleur. Quand la destination d'un paquet est un client sans fil, elle va au contrôleur et puis traverse le tunnel du protocole Lightweight Access Point Protocol (LWAPP) jusqu'à l'AP puis le client. Une chose qui peut être faite pour aider à diminuer l'apparition de ce message est d'autoriser seulement les VLAN qui sont utilisés sur le contrôleur sur la jonction réseau qui va au contrôleur avec la commande **switchport vlan allow** du commutateur.

Q. Pourquoi est-ce que je vois ce message d'erreur sur la console : Msg 'Set Default Gateway' of System Table failed, Id = 0x0050b986 error value = 0xfffffffc?

A. Ceci peut être dû à la charge élevée du CPU. Quand le contrôleur CPU est fortement chargé, comme quand il fait des copies de fichier ou d'autres tâches, il n'a pas le temps pour traiter tous les ACK que le NPU envoie en réponse aux messages de configuration. Quand ceci se produit, le CPU génère des messages d'erreur. Cependant, les messages d'erreur n'affectent pas le service ou la fonctionnalité.

Ceci est documenté dans la section Contrôleur CPU fortement chargé des notes de publication relatives aux Contrôleurs de réseau local sans fil Cisco et Points d'accès léger pour la version 3.2.116.21.

Q. Je reçois ces messages d'erreur de clé Wired Equivalent Privacy (WEP) sur mon système de contrôle sans fil (WCS) : `The WEP Key configured at the station may be wrong. Station MAC Address is 'xx: xx : xx : xx : xx : xx', AP base radio MAC is 'xx: xx : xx : xx : xx : xx'` and Slot ID is '1'. Cependant, je n'utilise pas le WEP comme paramètre de sécurité de mon réseau. J'utilise seulement le Wi-Fi Protected Access (WPA). Pourquoi est-ce que je reçois ces messages d'erreur WEP ?

A. Si toutes vos configurations liées à la sécurité sont parfaites, les messages que vous recevez en ce moment sont dus à des bogues. Il y a quelques bogues identifiés dans le contrôleur. Consultez les bogues Cisco CSCse17260 (clients enregistrés seulement) et CSCse11202 (clients enregistrés seulement), qui indiquent « La clé WEP configurée à la station peut être erronée avec des **clients WPA et TKIP respectivement** ». En fait, **CSCse17260** est un doublon de **CSCse11202**. Le correctif pour **CSCse11202** est déjà disponible avec la version WLC 3.2.171.5.

Remarque: Les dernières versions WLC ont un correctif pour ces bogues.

Q. Nous utilisons un serveur RADIUS externe pour authentifier les clients sans fil par le contrôleur. Le contrôleur envoie ce message d'erreur régulièrement : no radius servers are responding. Pourquoi voyons-nous ces messages d'erreur ?

A. Quand une requête sort du WLC pour aller au serveur RADIUS, chaque paquet a un numéro de séquence auquel le WLC attend une réponse. S'il n'y a aucune réponse, il y a un message qui indique radius-server not responding.

Le temps par défaut pour que le WLC ait une réponse du serveur RADIUS est de 2 secondes. Ceci est défini à partir de l'interface graphique utilisateur WLC dans la section **Security >**

authentication-server. Le maximum est de 30 secondes. Par conséquent, il pourrait être utile de définir cette valeur de temps d'expiration à son maximum afin de résoudre ce problème.

Parfois, les serveurs RADIUS effectuent des **« annulations silencieuses »** du paquet de requête qui provient du WLC. Le serveur RADIUS peut rejeter ces paquets car le certificat ne correspond pas ou pour plusieurs autres raisons. C'est une action valide par le serveur. En outre, en pareil cas, le contrôleur signalera le serveur RADIUS comme ne répondant pas.

Afin de maîtriser les annulations silencieuses, désactivez la fonctionnalité **basculement agressif** dans le WLC.

Si la fonctionnalité **basculement agressif** est activée dans le WLC, le WLC est trop agressif pour signaler le serveur AAA comme ne répondant pas. Cependant, ceci ne devrait pas être fait car le serveur AAA peut ne pas répondre seulement à ce client particulier (en faisant une annulation silencieuse). Cela peut être une réponse à d'autres clients valides (avec des certificats valides). Cependant, il se peut que le WLC signale encore le serveur AAA comme ne répondant pas et comme étant non fonctionnel.

Afin de résoudre ce problème, désactivez la fonctionnalité de **basculement agressif**. Émettez la commande de **débronchement d'agressif-Basculement de rayon de config du** contrôleur CLI afin d'exécuter ceci. Si cela est désactivé, alors le contrôleur bascule seulement au prochain serveur AAA s'il y a 3 clients consécutifs qui ne reçoivent pas de réponse du serveur RADIUS.

Q. Plusieurs clients ne peuvent pas s'associer à un LWAPP et le contrôleur indique le message d'erreur lAPP-3-MSGTAG015: `iappSocketTask :` iappRecvPkt returned error. Que se passe-t-il ?

A. Ceci se produit en grande partie en raison d'un problème avec les adaptateurs Intel qui supportent CCX v4, mais qui exécutent une version du client antérieure à 10.5.1.0. Si vous mettez à jour le logiciel à 10.5.1.0 ou à une version postérieure, ceci répare le problème. Consultez l'ID de bogue Cisco CSCsi91347 (clients enregistrés seulement) pour plus d'informations sur ce message d'erreur.

Q. Je vois ce message d'erreur sur le contrôleur de réseau local sans fil (WLC) : Reached Max EAP-Identity Request retries (21) for STA 00:05:4e:42:ad:c5. Pourquoi ?

A. Ce message d'erreur apparaît quand l'utilisateur essaye de se connecter à un réseau WLAN protégé EAP et a dépassé le nombre de tentatives EAP possible. Quand l'utilisateur ne s'authentifie pas, le contrôleur exclut le client et le client ne peut pas se connecter au réseau jusqu'à ce que le temps d'exclusion expire ou soit manuellement remplacé par l'administrateur.

L'exclusion détecte les tentatives d'authentification faites par un seul dispositif. Quand ce périphérique dépasse un nombre maximal de pannes, on ne permet plus à cette adresse MAC de s'associer.

L'exclusion se produit :

- Après 5 échecs d'authentification consécutifs pour des authentifications partagées (le 6ème essai est exclu)
- Après 5 échecs d'association consécutifs pour l'authentification MAC (le 6ème essai est

exclu)
- Après 3 échecs d'authentification EAP/802.1X consécutifs (le 4ème essai est exclu)
- Tout échec de politique externe du serveur (NAC)
- Toute instance de duplication d'adresse IP
- Après 3 échecs d'authentification web consécutifs (le 4ème essai est exclu)

Le compteur pour déterminer combien de temps un client est exclu peut être configuré et l'exclusion peut être activée ou désactivée au niveau du contrôleur ou du WLAN.

Q. Je vois ce message d'erreur sur le contrôleur de réseau local sans fil (WLC) : `An Alert of Category Switch is generated with severity 1 by Switch WLCSCH01/10.0.16.5 The message of the alert is Controller '10.0.16.5'.` RADIUS server(s) are not responding to authentication requests. Quel est le problème ?

A. Ceci peut être dû à l'ID de bogue Cisco CSCsc05495. En raison de ce bogue, le contrôleur injecte périodiquement une paire AV incorrecte (attribut 24, « état ») dans les messages de demande d'authentification qui violent un RADIUS RFP et posent des problèmes pour quelques serveurs d'authentification. Ce bogue est réparé dans 3.2.179.6.

Q. Je reçois un message d'échec Noise Profile sous Monitor > 802.11b/g Radios. Je veux comprendre pourquoi je vois ce message FAILED ?

A. L'état du Noise Profile ACCEPTÉ/REJETÉ est défini après le résultat de test fait par le WLC et en comparaison avec le seuil fixé actuellement. Par défaut, la valeur du bruit est définie à -70. L'état FAILED indique que la valeur du seuil pour ce paramètre ou point d'accès (AP) particulier a été dépassée. Vous pouvez régler les paramètres dans le profil, mais il est recommandé de modifier les paramètres après avoir clairement compris la conception du réseau et comment cela affectera la performance du réseau.

Les seuils PASSED/FAILED de la Gestion des ressources radio (RRM) sont globalement définis pour tous les AP dans les pages **802.11a Global Parameters > Auto RF** et **802.11b/g Global Parameters > Auto RF**. Les seuils ACCEPTÉ/REJETÉ de la RRM sont individuellement définis pour cet AP à la page **802.11 AP Interfaces > Performance Profile**.

Q. Je ne peux pas définir le port 2 comme port de secours pour l'interface du gestionnaire AP. Le message d'erreur envoyé est Could not set port configuration. Je peux définir le port 2 comme port de secours pour l'interface de gestion. Le port actif actuellement pour les deux interfaces est le port 1. Pourquoi ?

A. Un gestionnaire AP n'a pas de port de secours. Il était pris en charge dans les versions antérieures. Depuis la version 4.0, le port de secours pour l'interface du gestionnaire AP n'est pas pris en charge. En règle générale, un gestionnaire AP unique devrait être configuré sur chaque port (pas de port de secours). Si vous utilisez l'Agrégation de lien (LAG), il y a un seul gestionnaire AP.

L'interface statique (ou constante) du gestionnaire AP doit être attribuée au port 1 du système de distribution et doit avoir une adresse IP unique. Elle ne peut pas être mise en correspondance avec un port de secours. Elle est habituellement configurée sur le même VLAN ou sous-réseau IP que l'interface de gestion, mais ce n'est pas une condition requise.

Q. Je vois ce message d'erreur : `The AP '00:0b:85:67:6b:b0' received a WPA MIC error on`

protocol '1' from Station '00:13:02:8d:f6:41'. Counter measures have been activated and traffic has been suspended for 60 seconds. Pourquoi ?

A. Le Message Integrity Check (MIC) incorporé dans le Protocole WPA (Wi-Fi Protected Access) inclut un compteur de trame qui empêche une attaque homme-dans-le-moyenne. Cette erreur signifie que quelqu'un dans le réseau essaye de rejouer le message qui a été envoyé par le client initial, ou elle peut signifier que le client est défectueux.

Si un client échoue à plusieurs reprises le contrôle MIC, le contrôleur désactive le WLAN sur l'interface AP où les erreurs sont détectées pendant 60 secondes. La première panne MIC est consignée et un compteur est lancé afin d'activer l'application des contre-mesures. Si une nouvelle panne MIC se produit dans les 60 secondes suivant la panne la plus récente, alors un STA dont l'entité IEEE 802.1X a agi en tant que demandeur se désauthentifie lui-même ou désauthentifie tous les STA ayant une association de sécurité si son entité IEEE 802.1X a agi en tant qu'authentificateur.

En outre, le périphérique ne reçoit ou ne transmet aucune trame de données codée TKIP et ne reçoit ou ne transmet aucune trame de données décryptée autre que les messages IEEE 802.1X, de ou à tout homologue pendant une période d'au moins 60 secondes après qu'il détecte la deuxième panne. Si le périphérique est un AP, il rejette les nouvelles associations avec TKIP au cours de cette période de 60 secondes ; à la fin de la période de 60 secondes, l'AP reprend un fonctionnement normal et permet aux STA de se (ré)associer.

Ceci empêche une attaque possible sur la structure du cryptage. Ces erreurs MIC ne peuvent pas être désactivées dans les versions WLC antérieures à 4.1. Avec les versions 4.1 et ultérieures du contrôleur de réseau local sans fil, il y a une commande pour modifier le moment d'analyse des erreurs MIC. La commande est **config wlan security tkip hold-down <0-60 seconds> <wlan id>**. Utilisez la valeur 0 afin de désactiver la détection de panne MIC pour des contre-mesures.

Q. Je vois ce message d'erreur dans mes journaux du contrôleur : **[[ERROR] dhcp_support.c 357: dhcp_bind(): servPort dhcpstate failed. Pourquoi** ?

A. Ces messages d'erreur apparaissent en grande partie quand le port de service du contrôleur a le DHCP activé mais ne reçoit pas d'adresse IP d'un serveur DHCP.

Par défaut, l'interface du port de service physique a un client DHCP installé et recherche une adresse par l'intermédiaire du DHCP. Le WLC tente de demander une adresse DHCP pour le port de service. Si aucun serveur DHCP n'est disponible, alors une demande de DHCP pour le port de service échoue. Par conséquent, ceci génère les messages d'erreur.

La solution de contournement est de configurer une adresse IP statique au port de service (même si le port de service est déconnecté) ou d'avoir un serveur DHCP disponible pour attribuer une adresse IP au port de service. Puis, rechargez le contrôleur si nécessaire.

Le port de service est réellement réservé pour l'administration hors bande de la restauration du contrôleur et du système et pour la maintenance en cas d'une défaillance du réseau. C'est également le seul port qui est en activité quand le contrôleur est en mode démarrage. Le port de service ne peut pas porter des tags 802.1Q. Par conséquent, il doit être connecté à un port d'accès sur le commutateur voisin. L'utilisation du port de service est facultative.

L'interface du port de service contrôle les communications et est statiquement mise en correspondance par le système avec le port de service. Elle doit avoir une adresse IP sur un sous-

réseau différent de la gestion, du gestionnaire AP et de toutes les interfaces dynamiques. En outre, elle ne peut pas être mise en correspondance avec un port de secours. Le port de service peut utiliser le DHCP afin d'obtenir une adresse IP, ou une adresse IP statique peut lui être attribuée, mais une passerelle par défaut ne peut pas être attribuée à l'interface du port de service. Les routes statiques peuvent être définis par le contrôleur pour avoir un accès réseau distant au port de service.

Q. Mes clients sans fil ne peuvent pas se connecter au réseau local sans fil (WLAN). Le WiSM auquel le point d'accès (AP) est connecté signale ce message : Big NAV Dos attack from AP with Base Radio MAC 00:0g:23:05:7d:d0, Slot ID 0 and Source MAC 00:00:00:00:00:00. Qu'est-ce que cela signifie ?

A. Comme condition pour accéder au support, la couche MAC vérifie la valeur de son vecteur d'allocation réseau (NAV). Le NAV est un compteur qui se trouve à chaque station et qui représente le temps nécessaire à la trame précédente pour envoyer sa trame. Le NAV doit être zéro avant qu'une station puisse essayer d'envoyer une trame. Avant la transmission d'une trame, une station calcule le temps nécessaire pour envoyer la trame en fonction de la longueur et du débit de données de la trame. La station place une valeur qui représente ce temps dans le champ de durée de l'en-tête de la trame. Quand les stations reçoivent la trame, elles examinent cette valeur du champ de durée et l'utilisent comme base pour définir leurs NAV correspondants. Ce processus réserve le support pour la station émettrice.

Un NAV élevé indique la présence d'une valeur exagérée de NAV (mécanisme de détection de porteuse virtuel pour 802.11). Si l'adresse MAC signalée est 00:00:00:00:00:00, elle est probablement usurpée (potentiellement une vraie attaque) et vous devez confirmer ceci avec une capture de paquets.

Q. Après avoir configuré le contrôleur et l'avoir redémarré, nous ne pouvons pas accéder au contrôleur en mode web sécurisé (https). Ce message d'erreur est reçu tout en essayant d'accéder au mode web sécurisé du contrôleur : `Secure Web:` Web Authentication Certificate not found (error). Quelle est la raison de ce problème ?

A. Il peut y avoir plusieurs raisons liées à ce problème. Une raison courante peut être liée à la configuration de l'interface virtuelle du contrôleur. Afin de résoudre ce problème, supprimez l'interface virtuelle et régénérez-la avec cette commande :

```
WLC>config interface address virtual 1.1.1.1
```

Puis, redémarrez le contrôleur. Après que le contrôleur a redémarré, régénérez localement le certificat webauth sur le contrôleur avec cette commande :

```
WLC>config certificate generate webauth
```

Dans le résultat de cette commande, vous devriez voir ce message : Web Authentication certificate has been generated.

Maintenant, vous devriez pouvoir accéder au mode web sécurisé du contrôleur lors du redémarrage.

Q. Les contrôleurs signalent parfois ce message d'alerte d'attaque de signature d'inondation de dissassociation d'ID contre les clients valides dans lesquels l'adresse MAC de l'attaquant est celle d'un Point d'accès (AP) joint à ce contrôleur : **Alerte : IDS 'Disassoc flood' Signature attack detected on AP '<AP name>' protocol '802.11b/g' on Controller 'x.x.x.x'. The Signature description is 'Disassociation flood', with precedence 'x'. The attacker's mac address is 'hh: hh : hh : hh : hh : hh', channel number is 'x', and the number of detections is 'x'.** Pourquoi est-ce que ceci se produit ?

A. C'est en raison de l'ID de bogue Cisco CSCsg81953 (clients enregistrés seulement).

Les attaques par désassociation flottante IDS contre les clients valides sont parfois signalées quand l'adresse MAC de l'attaquant est celle de l'AP connecté à ce contrôleur.

Quand un client est associé à un AP mais cesse de communiquer en raison de l'enlèvement de la carte, de l'itinérance hors de portée, etc. avec l'AP, l'AP attendra jusqu'au délai d'inactivité. Une fois que le délai d'inactivité est atteint, l'AP envoie une trame dissociée à ce client. Quand le client ne reconnaît pas la trame dissociée, l'AP retransmet la trame de nombreuses fois (environ 60 trames). Le sous-système IDS du contrôleur entend ces retransmissions et donne l'alerte avec ce message.

Ce bogue est résolu dans la version 4.0.217.0. Mettez à jour votre version du contrôleur avec cette version afin de maîtriser ce message d'alerte contre les clients valides et les AP.

Q. Je reçois ce message d'erreur dans le syslog du contrôleur : **[[WARNING] apf_80211.c 2408: Received a message with an invalid supported rate from station <xx: xx : xx : xx : xx : xx> [ERROR] apf_utils.c 198: Missing Supported Rate. Pourquoi** ?

A. En fait, les messages Missing Supported Rate indiquent que le WLC est configuré pour certains débits de données requis sous les paramètres sans fil, mais la carte NIC n'a pas le débit requis.

Si vous avez des débits de données, tels que 1 et 2M, requis sur le contrôleur mais que la carte NIC ne communique pas sur ces débits de données, vous pouvez recevoir ce genre de message. C'est conduite incorrecte de la carte NIC. D'autre part, si votre contrôleur 802.11g est activé et que le client est une carte 802.11b(uniquement), ceci est un message légitime. Si ces messages ne posent aucun problème et que les cartes peuvent encore se connecter, ces messages peuvent être ignorés. Si les messages sont spécifique à la carte, alors assurez-vous que le pilote pour cette carte est à jour.

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

WLC>config certificate generate webauth

A. Ce message est diffusé par les LAP. Ceci est vu quand vous avez configuré la caractéristique de priorité WLAN pour un WLAN et ce WLAN particulier n'est pas annoncé.

Configurez le `config ap syslog host global 0.0.0.0` afin de l'arrêter ou vous pouvez mettre une adresse IP spécifique si vous avez un serveur de Syslog de sorte que le message soit émission seul au serveur.

Q. Je reçois ce message d'erreur sur mon contrôleur de réseau local sans fil (WLC) : **[[ERROR] File: apf_mm.c : Ligne : 581 : Annoncez la collision pour 00:90:7a:05:56:8a mobile, supprimant. Pourquoi** ?

A. Généralement, ce message d'erreur indique que le contrôleur avait annoncé des collisions pour un client sans fil (c.-à-d. les aps distincts annoncent qu'ils ont le client), et le contrôleur n'a pas reçu un transfert d'un AP au prochain. Il n'y a aucun état de réseau à mettre à jour. Supprimez le client sans fil et ayez l'essai de client de nouveau. Si ce problème se pose fréquemment, il peut y a un problème avec la configuration de mobilité. Autrement, ce pourrait être une anomalie qui est liée à un client ou à un état spécifique.

Q. Mon contrôleur signale ce message d'alarme : **Seuil de couverture de '12' violé.** Qu'est-ce que c'est cette erreur et comment peut être résolu ?

A. Ce message d'alarme est augmenté quand un rapport signal/bruit de client (SNR) tombe au-dessous de la valeur de seuil SNR pour la radio particulière. 12 est la valeur par défaut de seuil SNR pour la détection de trou de couverture.

L'algorithme de détection et de correction de trou de couverture déterminent si un trou de couverture existe quand les niveaux SNR des clients passent au-dessous d'un seuil SNR indiqué. Ce seuil SNR varie selon deux valeurs : La puissance de transmission AP et la couverture de contrôleur profilent la valeur.

En détail, le seuil SNR de client est défini par la puissance de transmission de chaque AP (représentée dans le dBm), sans la valeur constante de 17dBm, sans la valeur configurable de profil de couverture d'utilisateur (cette valeur est transférée sur 12 dB).

- **Valeur de coupure SNR du client (|dB|) = [puissance de transmission AP (dBm) – constante (dBm 17) – profil de couverture (dB)]**

Cette valeur configurable de profil de couverture d'utilisateur peut être accédée à de cette façon :

1. Dans le GUI WLC, allez au titre principal de la radio et sélectionnez l'**option Network** pour la norme WLAN du choix du côté gauche (802.11a ou 802.11b/g). Puis, **Auto RF** choisie dans le juste de stimulant de la fenêtre.
2. Dans l'Auto RF Global les paramètres paginent, trouvent la section de seuils de profil. Dans cette section, vous trouverez la valeur de la couverture (3 à 50 dbm). Cette valeur est la valeur configurable de profil de couverture d'utilisateur.
3. Cette valeur peut être modifiée pour influencer la valeur du seuil SNR du client. L'autre manière d'influencer ce seuil SNR est d'augmenter la puissance de transmission et de compenser la détection de trou de couverture.

Q. J'utilise ACS v 4.1 et un contrôleur de réseau local sans fil (WLC) 4402. Quand les tentatives WLC MAC-d'authentifier un client sans fil à ACS 4.1, l'ACS échoue pour répondre avec l'ACS et signale ce message d'erreur : La « *erreur interne s'est produite* ». J'ai toutes mes configurations correctes. Pourquoi cette erreur interne se produit-elle ?

A. Il y a un ID de bogue Cisco associé par authentification CSCsh62641 (clients enregistrés seulement) dans l'ACS 4.1, où l'ACS donne l'`erreur interne a le` message d'erreur `produit`.

Ce bogue peut être le problème. Il y a un correctif disponible pour cette bogue à la page de téléchargements ACS 4.1 (clients enregistrés seulement) qui devrait réparer le problème.

Q. Le contrôleur de réseau local sans fil (WLC) de la gamme Cisco 4400 ne démarre pas. Ce message d'erreur est reçu sur le contrôleur : `** Incapable d'utiliser ide 0:4 pour le fatload ** noir 0 du dev 0 de l'erreur (aucun IRQ) : status 0x51 Error reg: 10 ** Ne peut pas lire du périphérique 0.` Pourquoi ?

A. La raison pour cette erreur peut être un problème matériel. Ouvrez une valise TAC pour dépanner plus loin ce problème. Afin d'ouvrir une valise TAC, vous devez avoir un contrat valide avec Cisco. Référez-vous au Soutien technique afin de contacter Cisco TAC.

Q. Le contrôleur de réseau local sans fil (WLC) rencontre des problèmes de mémoire tampon. Une fois que les tampons mémoire sont pleins, le contrôleur tombe en panne et doit être redémarré pour le rapporter en ligne. Ces messages d'erreur apparaissent dans le journal des messages : `Mon Apr 9 10:41:03 2007 [ERROR] dtl_net.c 506: Hors mises en mémoire tampon du système Lun du 9 avril 10:41:03 2007 [ERREUR] sysapi_if_net.c 537 : Ne peut pas allouer nouveau Mbuf. Mon Apr 9 10:41:03 2007 [ERROR] sysapi_if_net.c 219: MbufGet : aucun Mbufs libre. Pourquoi ?`

A. C'est dû à l'ID de bogue Cisco CSCsh93980 (clients enregistrés seulement). Ce bogue a été résolu dans WLC version 4.1.185.0. Améliorez votre contrôleur afin de surmonter à cette version de logiciel ou à plus tard ce message.

Q. Nous avons exécuté la mise à jour de notre contrôleur LAN Sans fil (WLC) 4400s au code 4.1 et notre Syslog a été bombardé par des messages, de ce type : `May 03 03:55:49.591 dtl_net.c:1191 DTL-1-ARP_POISON_DETECTED: STA [00:17:f2:43:26:93, ARP de 0.0.0.0] (1) op reçu avec STATION THERMALE non valide 192.168.1.233/TPA 192.168.1.233.` Que ces messages indiquent-ils ?

A. Ceci peut se produire quand le WLAN est marqué comme requérant DHCP. En pareil cas, on permet seulement aux des stations qui reçoivent une adresse IP par le DHCP pour s'associer. Les clients statiques n'ont pas l'autorisation de s'associer à ce WLAN. WLC agit en tant qu'agent de relais DHCP et enregistre l'adresse IP de toutes les stations. Ce message d'erreur est généré quand WLC reçoit la demande d'ARP d'une station avant que le WLC ait reçu des paquets DHCP de la station et ait enregistré son adresse IP.

Q. Quand vous utilisez l'alimentation au-dessus des Ethernets (PoE) sur le contrôleur LAN sans fil Cisco 2106, les radios AP ne sont pas activées. `AP ne peut pas vérifier l'alimentation intégrée suffisante. Radio slot disabled.` apparaît. Comment est-ce que je peux résoudre cela ?

A. Ce message d'erreur se produit quand le commutateur, qui met le Point d'accès sous tension, est un commutateur pré-standard mais AP ne prend en charge pas le mode Pré-standard de la puissance d'entrée.

Un commutateur pré-standard de Cisco est un qui ne prend en charge pas la gestion de l'alimentation intelligente (IPM) mais a l'alimentation suffisante pour un point d'accès standard.

Vous devez activer le mode Pré-**standard** de mettez sous tension AP qui est soumis à ce

message d'erreur. Ceci peut être fait du contrôleur CLI avec le **config ap power pre-standard {enable | disable} {all | Cisco_AP}**.

Cette commande devrait déjà être configurée, s'il y a lieu, si vous améliorez à la version de logiciel 4.1 d'une version précédente. Mais, il est possible que vous deviez sélectionner cette commande pour de nouvelles installations, ou si vous remettez à l'état initial AP à Factory Defaults.

Les commutateurs 15 watt pré-standard Cisco suivants sont disponibles :

- AIR-WLC2106-K9
- WS-C3550, WS-C3560, WS-C3750
- C1880
- 2600, 2610, 2611, 2621, 2650, 2651
- 2610XM, 2611XM, 2621XM, 2650XM, 2651XM, 2691
- 2811, 2821, 2851
- 3631-telco, 3620, 3640, 3660
- 3725, 3745
- 3825, 3845

Q. Le contrôleur génère un `dtl_arp.c:2003 DTL-3-NPUARP_ADD_FAILED : Unable to add an ARP entry for xx: xx. - xxx.x au processeur de réseau. entry does not exist.` message de `Syslog` semblable à ceci. Qu'est-ce que ce message syslog signifie ?

A. Tandis qu'un certain client sans fil envoie une réponse d'ARP, les besoins de l'unité de processeur de réseau (NPU) de connaître cette réponse. Ainsi la réponse d'ARP est expédiée au logiciel NPU mais WLC ne devrait pas essayer d'ajouter cette entrée au processeur de réseau. S'il fait ainsi, ces messages sont générés. Il n'y a aucune incidence de fonctionnalité sur le WLC dû à ceci mais le WLC génère ce message de Syslog.

Q. J'ai installé et configuré un nouveau WLC 2106 Cisco. Le WLC indique que le capteur de température a manqué. Quand vous vous connectez dans l'interface web sous le « résumé de contrôleur, » il indique que le « `capteur a manqué` » à côté de la température interne. Tout autrement semble fonctionner normalement.

A. La panne interne de capteur de température est cosmétique et peut être résolue avec une mise à jour à la version 4.2.61.0 WLC.

WLC 2106 et WLC 526 **construit sur ou après 07/01/2007** peuvent utiliser la puce de capteur de température d'un autre constructeur. Ce nouveau capteur fonctionne bien, mais n'est pas compatible avec le logiciel plus tard que la release 4.2. Par conséquent, un logiciel plus ancien ne peut pas relever la température et affiche cette erreur. Toutes autres fonctionnalités de contrôleur ne sont pas affectées par ce défaut.

Il y a un ID de bogue Cisco connu CSCsk97299 (clients enregistrés seulement) lié à cette question. Cette bogue est mentionnée dans la note en version de la version 4.2 WLC.

Q. J'obtiens le message radius_db.c:1823 AAA-5-RADSERVER_NOT_FOUND: `N'a pas pu trouver le serveur compétent de RADIUS pour WLAN <WLAN ID> - incapable` message `de trouver serveur par défaut le »` pour TOUT LE SSID. Ce message apparaît même pour

le SSID qui n'utilisent pas des serveurs d'AAA.

A. Ce message d'erreur signifie que le contrôleur ne pouvait pas contacter le serveur par défaut de rayon ou qu'on n'a pas été défini.

Un possible raison pour ce comportement est l'ID de bogue Cisco CSCsk08181 (clients enregistrés seulement), qui a été résolu dans la version 4.2. Mettez à jour votre contrôleur à la version 4.2.

Q. Le message d'erreur : `10 juillet 17:55:00.725 sim.c:1061 SIM-3-MACADDR_GET_FAIL : L'adresse MAC source de l'interface 1 n'est pas trouvée.` le message d'erreur apparaît sur le contrôleur LAN Sans fil (WLC). Qu'est-ce que cela indique?

A. Ceci signifie que le contrôleur a eu une erreur tandis qu'il envoyait à une CPU le paquet originaire.

Q. Ces messages d'erreur apparaissent sur le contrôleur de réseau local sans fil (WLC) :

- `10 juillet 14:52:21.902 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL : Pour lire le fichier de configuration « cliWebInitParms.cfg »`
- `10 juillet 14:52:21.624 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL : Pour lire le fichier de configuration « rfidInitParms.cfg »`
- `10 juillet 14:52:21.610 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL : Pour lire le fichier de configuration « dhcpParms.cfg »`
- `10 juillet 14:52:21.287 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL : Pour lire le fichier de configuration « bcastInitParms.cfg »`
- `18 mars 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED : Failed to delete the file : la suppression de fichier sshpmInitParms.cfg a manqué. - Processus : Nom : fp_main_task, Id:11ca7618`
- `18 mars 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED : Failed to delete the file : la suppression de fichier bcastInitParms.cfg a manqué. - Processus : Nom : fp_main_task, Id:11ca7618`

Qu'est-ce que ces messages d'erreur indiquent ?

A. Ces messages sont des messages d'information et font partie de la procédure normale de démarrage. Ces messages apparaissent en raison d'un manque de lire ou supprimer plusieurs différents fichiers de configuration. Quand des fichiers de configuration particuliers ne sont pas trouvés ou si le fichier de configuration ne peut pas être indiqué, l'ordre de config pour chaque processus envoie ce message, par exemple, aucun config de serveur DHCP, aucun config de balises (ID rf), et ainsi de suite. Ce sont des messages de bas-sévérité qui peuvent sans risque être ignorés. Ces messages n'interrompent pas le fonctionnement du contrôleur.

Q. `Le HE6-WLC01,local0,alert,2008-07-25,12:48:18,apf_rogue.c:740 APF-1-UNABLE_TO_KEEP_ROUGE_CONTAIN : Incapable de maintenir 00:14:XX:02:XX:XX escroc dans l'état contenu - aucun AP disponible pour contenir.` apparaît. Qu'est-ce que cela indique?

A. Ceci signifie qu'AP qui a rempli la fonction escroc de retenue n'est plus disponible, et le contrôleur ne peut trouver aucun AP approprié pour exécuter la retenue escroc.

Q. Le message système DTL-1-ARP_POISON_DETECTED: `STA [00:01:02:0e:54:c4, ARP de 0.0.0.0] (1) op reçu avec le` message système `non valide de la STATION THERMALE 192.168.1.152/TPA 192.168.0.206` apparaît sur le contrôleur LAN Sans fil. Que ce message

implique-t-il ?

A. Il est possible que le système ait détecté un spoofing ou empoisonnement de l'ARP. Mais, ce message n'implique pas nécessairement que n'importe quelle mystification malveillante d'ARP s'est produite. Le message apparaît quand ces conditions sont vraies :

- Un WLAN est configuré avec le DHCP exigé, et un périphérique de client, après avoir associé sur ce WLAN, transmet un message d'ARP sans le premier DHCP se terminant. Ceci peut être comportement normal ; il peut se produire, par exemple, quand le client est statiquement adressé, ou quand le client tient un bail valide DHCP d'une association antérieure. Le message d'erreur peut ressembler à cet exemple :
  `WLC>config certificate generate webauth`

  L'effet de cette condition est que le client ne peut pas envoyer ou recevoir n'importe quel trafic de données, jusqu'à ce qu'il DHCPs par le WLC.Référez-vous à la section de messages DTL de pour en savoir plus Sans fil de guide des messages système de contrôleur LAN de Cisco.

Q. Les LAP n'utilisent pas Power over Ethernet (POE) pour se mettre sous tension. Je vois les logins le contrôleur LAN Sans fil :

AP's Interface:1(802.11a) Operation State Down: Base Radio MAC:XX:1X:XX:AA:VV:CD Cause=Low in-line power

Quel est le problème ?

A. Ceci peut se produire si l'alimentation au-dessus des configurations des Ethernets (POE) ne sont pas configurées correctement. Quand un Point d'accès qui a été converti en mode léger, par exemple, un AP1131 ou un AP1242, ou un Point d'accès de gamme 1250 est actionné par un injecteur de courant qui est connecté à un commutateur pré-intelligent de la Gestion d'alimentation de Cisco (pré-IPM), vous devez configurer l'alimentation au-dessus des Ethernets (PoE), également connus sous le nom d'alimentation en ligne.

Référez-vous à configurer l'alimentation au-dessus des Ethernets pour plus d'informations sur la façon configurer l'alimentation au-dessus des Ethernets (POE).

Q. Vous voyez ce message sur le contrôleur de réseau local sans fil (WLC) :

***Mar 05 10:45:21.778: %LWAPP-3-DISC_MAX_AP2: capwap_ac_sm.c:1924 Dropping primary discovery request from AP XX:1X:XX:AA:VV:CD - maximum APs joined 6/6**

Qu'est-ce que cela indique?

A. Le Point d'accès léger suit un certain algorithme pour trouver un contrôleur. La détection et le processus de jonction est expliquée en détail dans l'enregistrement léger AP (RECOUVREMENT) à un contrôleur LAN Sans fil (WLC)

Ce message d'erreur est vu sur le WLC, quand il reçoit une demande de détection après qu'il ait atteint sa capacité du maximum AP.

Si le contrôleur primaire pour un RECOUVREMENT n'est pas configuré ou si son un nouveau hors du RECOUVREMENT de case, il envoie des demandes de LWAPP discovery à tous les

contrôleurs accessibles. Si les demandes de détection atteint un contrôleur qui fonctionne à sa pleine capacité AP, WLC obtient les demandes et se rend compte qu'il est à sa capacité du maximum AP, et ne répond pas à la demande et donne cette erreur.

Q. Où peux-je trouver plus d'informations sur les messages système LWAPP ?

A. Référez-vous au guide des messages système Sans fil de contrôleur LAN de Cisco, 4.2 pour plus d'informations sur les messages système LWAPP.

Q. `L'erreur extrayant le` message d'erreur de `fichiers de webauth` apparaît sur le contrôleur LAN Sans fil (WLC). Qu'est-ce que cela indique?

A. WLC ne charge pas un paquet fait sur commande d'authentification Web/fonction émulation si des n'importe quels des fichiers empaquetés ont plus considérablement que 30 caractères dans le nom du fichier, qui inclut l'extension de fichier. Le paquet authentique personnalisé de Web a une limite de jusqu'à 30 caractères pour des noms du fichier. Assurez-vous qu'aucun nom du fichier dans le paquet n'est plus grand que 30 caractères.

Q. Les contrôleurs LAN Sans fil (WLCs), exécutant le code 5.2 ou 6.0 avec un grand nombre de groupes AP, GUI de Web peuvent ne pas afficher tous les groupes configurés AP. Quel est le problème ?

A. Les groupes des disparus AP peuvent être vus si vous utilisez les AP-**groupes de show wlan** CLI commandez.

Essayez d'ajouter un groupe supplémentaire AP à la liste. Par exemple, 51 groupes AP déployés, et le cinquante-et-unième manque (page 3). Ajoutez le cinquante-deuxième groupe, et la page 3 devrait paraître dans le GUI de Web.

Afin de résoudre ce problème, mise à jour à la version 7.0.220.0 WLC.

Informations connexes

- Guide de configuration du contrôleur LAN sans fil Cisco, version 4.0
- Dépannage de WiSM - Forum Aux Questions
- Dépannage du contrôleur LAN sans fil (WLC) - FAQ
- Page de prise en charge du mode sans fil
- Support et documentation techniques - Cisco Systems