FAQ sur les messages d'erreur et les messages système du contrôleur LAN sans fil (WLC)

Table des matières

Introduction

Ce document décrit les questions fréquemment posées (FAQ) sur les messages d'erreur et les messages système pour les contrôleurs de réseau local sans fil (WLAN) Cisco (WLC).

Conventions

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. La conversion de plus de 200 points d'accès (AP) du logiciel Cisco IOS® au protocole LWAPP (Lightweight AP Protocol) avec un WLC Cisco 4404 a commencé. La conversion de 48 AP a été effectuée et le message reçu sur le WLC a déclaré : `[ERREUR] spam_lrad.c 4212 : le point d'accès ne peut pas se joindre car le nombre maximal de points d'accès sur l'interface 1 est atteint.` Pourquoi l'erreur se produit-elle ?

R.Vous devez créer des interfaces de gestionnaire d'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 seconde interface de gestionnaire d'AP afin d'activer des AP supplémentaires. Mais assurez-vous que vos configurations de port principal et de port de secours pour chaque gestionnaire ne se chevauchent 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. Je dispose d'un contrôleur LAN sans fil (WLC) 4402 et j'utilise 1 240 points d'accès légers (LAP). J'ai activé le cryptage 128 bits sur le WLC. Lorsque je sélectionne le cryptage WEP 128 bits sur le WLC, je reçois un message d'erreur indiquant que le cryptage 128 bits n'est pas pris en charge sur les 1240s : `[ERROR] spam_lrad.c 12839 : Not creation SSID mode on CISCO AP xx:xx:xx:xx:xx:xx, car le cryptage WEP128 bit n'est pas pris en charge.` Pourquoi est-ce que je

reçois cette erreur ?

R.Les longueurs de clé indiquées 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 obtenir la **taille de clé WEP de 128 bits n'est pas pris en charge sur les AP de modèles 11xx, 12xx et 13xx. Le WLAN ne peut pas être envoyé vers ces points d'accès.** Message d'erreur lorsque j'essaie de configurer le WEP sur un WLC ?

R. Sur un contrôleur LAN sans fil, lorsque vous choisissez la méthode de sécurité de couche 2 Static WEP, vous disposez de ces options ou de 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 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 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 s'authentifier auprès d'un WLAN configuré pour WPA2 et le contrôleur affiche le message d'erreur **apf_80211.c:1923 APF-1-PROC_RSN_WARP_IE_FAILED: Could not process the RSN and WARP IE. station not using RSN (WPA2) on WLAN require RSN.MobileStation:00:0c:f1:0c:51:22, SSID:<>.** Pourquoi est-ce que je reçois cette erreur ?

R. Cela se produit principalement en raison d'incompatibilité côté 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 WPA2. Consultez le support Microsoft pour plus d'informations.
- Mettez à niveau le pilote et le micrologiciel client.
- Désactivez les extensions Aironet sur le WLAN.

Q. Une fois que j'ai redémarré le WLC, j'obtiens le **Lun Jul 17 15:23:28 2006 MFP Anomaly Detected -**

3023 Invalid MIC event(s) found as viole by the radio 00:XX:XX:XX:XX et detected by the dot11 interface at slot 0 of AP 00:XX:XX:XX:XX in 300 seconds when observing Probe response, Beacon Frames error message. Pourquoi cette erreur se produit-elle et comment est-ce que je me débarrasse d'elle ?

R.Ce message d'erreur s'affiche lorsque des trames avec des valeurs MIC incorrectes sont détectées par des LAP compatibles MFP. Référez-vous àExemple de configuration de la protection de trame de gestion d'infrastructure (MFP) 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. Référez-vous àFAQ sur les groupes de mobilité des contrôleurs LAN 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 à un point d'accès avec le protocole EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling). Cependant, quand l'AP associé est éteint, le client ne se déplace pas à un autre AP. Ce message apparaît en permanence dans le journal des messages du contrôleur : "ven juin 2 14:48:49 2006 [SECURITY] 1x_auth_page.c 1922 : Unable to allow user into the system - may the user is already connected to the system ? Ven juin 2 14:48:49 2006 [SECURITY] apf_ms.c 2557 : Impossible de supprimer le nom d'utilisateur pour le mobile 00:40:96:ad:75:f4". Pourquoi ?

R.Lorsque la carte client a besoin d'itinérance, elle envoie une demande d'authentification, mais elle ne gère pas correctement les clés (n'informe pas le point d'accès/contrôleur, ne répond pas à la réauthentification).

Ceci est documenté dans le bogue Cisco IDCSCsd02837. Ce bogue a été réparé avec l'Assistant d'installation 3.5 des adaptateurs client de Cisco Aironet 802.11a/b/g.

En général, `le message Impossible de supprimer le nom d'utilisateur pour` mobilemessage se produit également pour l'une des raisons suivantes :

- 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.

  Remarque : seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations et aux outils internes relatifs aux bogues Cisco.

Q. Lorsque j'installe la nouvelle lame Wireless Services Module (WiSM) dans le commutateur 6509 et que j'implémente le protocole PEAP (Protected Extensible Authentication Protocol) 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 required 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 et 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 required by LWAPP CLIENT. . Pourquoi ?

A.RADIUS et les débogages dot1x montrent que le WLC envoie une demande d'accès, mais il n'y a pas de réponse du serveur 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 légers (LAP) ne sont pas enregistrés auprès du contrôleur. Quel peut être le problème ? Je vois ces messages d'erreur sur le contrôleur : **Jeu 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. Jeu 3 fév 03:20:47 2028: Impossible de libérer la clé publique pour AP 00:0B:85:68:F4:F0.**

R.Lorsque le point d'accès (AP) envoie la requête de jonction LWAPP (Lightweight Access Point Protocol) au WLC, il intègre 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. Lorsque le WLC reçoit la demande de jointure LWAPP, il valide la signature du certificat X.509 avec la clé publique des AP et vérifie que le certificat a été émis par une autorité de certification approuvée. Il examine également la date et l'heure de début de l'intervalle de validité du certificat AP et compare cette date et cette heure à sa propre 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, émettez la commande show time et config time de l'assistant.

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 celui-ci : **LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP 00:0b:85:68:ab:01.** Pourquoi ?

R.Vous pouvez recevoir ce message d'erreur si le tunnel LWAPP entre le point d'accès et le WLC traverse un chemin de réseau avec un MTU inférieur à 1500 octets. Ceci entraîne la fragmentation des paquets LWAPP. C'est un bogue connu dans le contrôleur. Référez-vous au bogue Cisco IDCSCsd39911.

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

> **Remarque** : seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations et aux outils internes relatifs aux bogues Cisco.

Q. Je souhaite 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>. Requête d'exportation d'ancrage à partir de l'adresse IP du commutateur : <adresse IP du contrôleur> ignorée.** Quel est le problème ?

A.La transmission tunnel invité offre une sécurité supplémentaire pour l'accès invité-utilisateur au réseau sans fil de l'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 le résultat de la commande debugcommand l'indique, le problème peut être lié à la non-concordance dans n'importe laquelle des politiques de sécurité configurées pour ce WLAN particulier dans les contrôleurs internes ainsi 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 commune à 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 LAN sans fil (WLC) 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 ?

R. Étant donné que la multidiffusion est désactivée sur les contrôleurs, les messages à l'origine de cette alarme peuvent être des messages ARP (Address Resolution Protocol). 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_foreign_ap.c 763 : STA [00:0A:E4:36:1F:9B] Received a packet on port 1 but no Foreign AP configured for this port." dans l'un de mes contrôleurs. Que signifie cette erreur et quelles mesures dois-je prendre pour la résoudre ?

A.Ce message s'affiche lorsque 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 atténuer ce message est d'autoriser seulement les VLAN qui sont utilisés sur le contrôleur sur l'agrégation qui va au contrôleur avec **la commande switchport vlan** allow sur le commutateur.

Q. Pourquoi ce message d'erreur s'affiche-t-il sur la console : Échec de la commande Msg « Set Default Gateway » de la table système, ID = 0x0050b986 valeur d'erreur = 0xfffffffc ?

R. Cela peut être dû à une charge CPU élevée. 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.

Pour plus d'informations, référez-vous à Contrôleurs LAN sans fil Cisco.

Q. Je reçois ces messages d'erreur de clé WEP (Wired Equivalent Privacy) sur mon système de contrôle sans fil (WCS) : `la clé WEP configurée sur la station peut être incorrecte. L'adresse MAC de la station est « xx:xx:xx:xx:xx:xx », l'adresse MAC de la radio de base du point d'accès est « xx:xx:xx:xx:xx » et l'ID de logement est « 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 ?

R.Si toutes vos configurations liées à la sécurité sont parfaites, les messages que vous recevez maintenant sont à cause de bogues. Il y a quelques bogues identifiés dans le contrôleur. Référez-vous au bogue Cisco IDCSCse17260 et Cisco mais ID CSCse1202, qui indique « La clé WEP configurée sur la station peut être incorrecte **avec les clients WPA et TKIP respectivement** ». En fait, l'ID de bogue Cisco **CSCse17260** est un doublon de l'ID de bogue Cisco **CSCse1202**. Le correctif pour Cisco, mais l'ID **CSCse1202**est déjà disponible avec la version 3.2.171.5 du WLC.

> **Remarque** : les dernières versions de WLC ont un correctif pour ces bogues.

> **Remarque** : seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations de bogue et aux outils internes de Cisco.

Q. J'utilise un serveur RADIUS externe pour authentifier les clients sans fil via le contrôleur. Le contrôleur envoie régulièrement ce message d'erreur : `aucun serveur RADIUS ne répond`. Pourquoi ces messages d'erreur s'affichent-ils ?

R. Lorsqu'une requête sort du WLC vers le serveur RADIUS, chaque paquet a un numéro de séquence auquel le WLC attend une réponse. En l'absence de réponse, un message `indique` que `radius-server ne répond pas`.

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 du WLC **sous Security > authentication-server**. Le maximum est de 30 secondes. Par conséquent, il peut être utile de définir cette valeur de temporisation à son maximum afin de résoudre ce problème.

Parfois, les serveurs RADIUS effectuent des **'rejets silencieux'** 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, dans de tels cas, le contrôleur peut marquer le serveur RADIUS comme ne répondant pas

Afin de surmonter le problème des rejets silencieux, désactivez **la fonctionnalité de basculement agressif** dans le WLC.

Si **la fonctionnalité de basculement agressif** est activée dans le WLC, le WLC est trop agressif pour marquer le serveur AAA comme ne répondant pas. Cependant, cela ne doit pas être fait parce que le serveur AAA ne peut pas répondre seulement à ce client particulier (il ne supprime pas silencieusement). Cela peut être une réponse à d'autres clients valides (avec des certificats valides). Cependant, le WLC peut toujours marquer le serveur AAA comme ne répondant pas et

ne fonctionnant pas.

Pour remédier à ce problème, désactivez **la fonction de** basculement **agressif**. Émettez **la commande config radius agressif-failover** disable à partir de l'interface de ligne de commande du contrôleur afin d'effectuer 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 enregistre le message d'erreur `IAPP-3-MSGTAG015 : iappSocketTask : iappRecvPkt renvoyé`. Que se passe-t-il ?

R.Cela se produit principalement en raison d'un problème avec les cartes Intel qui prennent en charge CCX v4, mais qui exécutent une version du bundle 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. Référez-vous au bogue Cisco IDCSCsi91347 pour plus d'informations sur ce message d'erreur.

> **Remarque** : seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations de bogue et aux outils internes de Cisco.

Q. Ce message d'erreur s'affiche sur le contrôleur de réseau local sans fil (WLC) : `Retries Max EAP-Identity Request Retries (21) atteintes pour STA 00:05:4e:42:ad:c5`. Pourquoi ?

R.Ce message d'erreur se produit lorsque l'utilisateur tente de se connecter à un réseau WLAN protégé par EAP et a échoué au nombre préconfiguré de tentatives EAP. Lorsque l'utilisateur ne parvient pas à s'authentifier, le contrôleur exclut le client et le client ne peut pas se connecter au réseau tant que le compteur d'exclusion n'expire pas ou n'est pas remplacé manuellement 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) : `Une alerte de commutateur de catégorie 1 est générée avec la gravité 1 par le commutateur WLCSCH01/10.0.16.5 Le message de l'alerte est le contrôleur « 10.0.16.5 ». RADIUS server(s) are not responding to authentication requests`. Quel est le problème ?

R. Cela 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.

> **Remarque** : seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations de bogue et aux outils internes de Cisco.

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

R.L'état du profil de bruit ÉCHEC/RÉUSSI est défini après le résultat du test effectué par le WLC et en comparaison avec le seuil actuellement défini. 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 ajuster les paramètres dans le profil, mais il est recommandé de modifier les paramètres après avoir bien compris la conception du réseau et comment elle peut affecter les performances du réseau.

Les seuils PASSED/FAILED de la gestion des ressources radio (RRM) sont globalement définis pour tous les points d'accès sur les pages **802.11a Global Parameters > Auto** RF et **802.11b/g Global Parameters > Auto** RF. Les seuils PASSED/FAILED RRM sont définis individuellement pour ce point d'accès sur la page **802.11 AP Interfaces > Performance** Profilepage.

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 ?

R.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 seul gestionnaire AP doit être configuré sur chaque port (pas de sauvegarde). 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 : `L'AP '00:0b:85:67:6b:b0' a reçu une erreur WPA MIC sur le protocole '1' de la station '00:13:02:8d:f6:41'. Counter measures have been activated and traffic has been suspended for 60 seconds.` Pourquoi ?

A.Message Integrity Check (MIC) incorporé dans Wi-Fi Protected Access (WPA) inclut un compteur de trames qui empêche une attaque man-in-the-middle. Cette erreur signifie qu'une personne du réseau souhaite relire le message envoyé par le client d'origine ou 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 défaillance MIC ultérieure se produit dans les 60 secondes qui suivent la défaillance précédente la plus récente, alors un STA dont l'entité IEEE 802.1X a agi en tant que demandeur doit s'invalider lui-même ou invalider tous les STA avec une association de sécurité si son entité IEEE 802.1X a

agi en tant qu'authentificateur.*

En outre, le périphérique ne reçoit ni ne transmet aucune trame de données cryptée TKIP et ne reçoit ni ne transmet aucune trame de données non cryptée autre que les messages IEEE 802.1X, en provenance ou à destination d'un homologue pendant une période d'au moins 60 secondes après avoir détecté la seconde défaillance. Si le périphérique est un point d'accès, il interdit les nouvelles associations avec TKIP pendant cette période de 60 secondes ; à la fin de la période de 60 secondes, le point d'accès reprend le fonctionnement normal et permet aux STA de (re)s'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 **isconfig 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.

*Invalidé : fin de l'authentification.

Q. Ce message d'erreur apparaît dans les journaux de mon contrôleur : `[ERROR] dhcp_support.c 357 : dhcp_bind() : servPort dhcpstate failed.` Pourquoi ?

R.Ces messages d'erreur apparaissent surtout lorsque le port de service du contrôleur a 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 LAN 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 00:00:00:00:00:00:00.` Qu'est-ce que cela signifie ?

R. 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 la durée nécessaire à l'envoi de la trame en fonction de la longueur de trame et du débit de données. 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 (ce qui peut constituer une véritable attaque) et vous devez la confirmer par une capture de paquets.

Q. Après avoir configuré le contrôleur et l'avoir redémarré, je ne peux pas accéder au contrôleur en mode Web sécurisé (https). Ce message d'erreur est reçu alors que j'essaie d'accéder au mode web sécurisé du contrôleur : `Web sécurisé : Certificat d'authentification Web introuvable (erreur).` Quelle est la raison de ce problème ?

R. Plusieurs raisons peuvent être associées 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 pouvez voir le message suivant : `Le certificat d'authentification Web a été généré.`

Vous pouvez maintenant 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 dissociation IDS contre des clients valides dans lesquels l'adresse MAC de l'attaquant est celle d'un point d'accès (AP) joint à ce contrôleur : `Alerte : Attaque de signature d'inondation de dissociation IDS détectée sur le protocole AP « <nom AP> » « 802.11b/g » sur le contrôleur « x.x.x.x ». The Signature description is 'Disassociation flood', with precedence 'x'. L'adresse MAC du pirate est « hh:hh:hh:hh:hh:hh », le numéro de canal est « x » et le nombre de détections est « x ».` Pourquoi est-ce que ceci se produit ?

R.Ceci est dû au bogue Cisco IDCSCsg81953 .

> **Remarque** : seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations de bogue et aux outils internes de Cisco.

Les attaques par inondation de dissociation IDS contre des clients valides sont parfois signalées

lorsque l'adresse MAC de l'attaquant est celle d'un point d'accès joint à ce contrôleur.

Lorsqu'un client est associé au point d'accès mais arrête les communications en raison du retrait de la carte, il se déplace hors de portée, et ainsi de suite, vers le point d'accès, le point d'accès attend 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 ?

R. En fait, les messages `Missing Supported Rate` indiquent que le WLC est configuré pour certains débits de données requis dans les paramètres sans fil, mais que la carte réseau ne dispose pas du 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 ?

R. Ce message est diffusé par les LAP. Cela se produit lorsque vous avez configuré une fonction de remplacement de WLAN pour un WLAN et que ce WLAN particulier n'est pas annoncé.

`Configureconfig 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 syslog afin que ce message soit diffusé au serveur seul.

Q. Je reçois ce message d'erreur sur mon contrôleur LAN sans fil (WLC) : **`[ERROR] Fichier : apf_mm.c : Line: 581 : Announce collision for mobile 00:90:7a:05:56:8a, delete.`** Pourquoi ?

R.Généralement, ce message d'erreur indique que le contrôleur avait annoncé des collisions pour un client sans fil (c'est-à-dire que des points d'accès distincts annoncent qu'ils ont le client), et le contrôleur n'a pas reçu de transfert d'un point d'accès au suivant. Il n'y a aucun état de réseau à mettre à jour. Supprimez le client sans fil et demandez au client de réessayer. Si ce problème se produit fréquemment, il peut y avoir un problème avec la configuration de la mobilité. Sinon, il peut s'agir d'une anomalie liée à un client ou à une condition spécifique.

Q. Mon contrôleur déclenche ce message d'alarme : **`le seuil de couverture de '12' a été violé.`** Quelle est cette erreur et comment peut-elle être résolue ?

A.Ce message d'alarme est déclenché lorsqu'un rapport signal/bruit (SNR) client tombe à une valeur inférieure à la valeur de seuil SNR pour la radio particulière. 12 est la valeur de seuil SNR

par défaut pour la détection des trous de couverture.

L'algorithme de détection et de correction des trous de couverture détermine s'il existe un trou de couverture lorsque les niveaux SNR des clients sont inférieurs à un seuil SNR donné. Ce seuil SNR varie en fonction de deux valeurs : la puissance de transmission du point d'accès et la valeur du profil de couverture du contrôleur.

En détail, le seuil SNR du client est défini par la puissance de transmission de chaque point d'accès (représentée en dBm), moins la valeur constante de 17dBm, moins la valeur du profil de couverture configurable par l'utilisateur (cette valeur est par défaut de 12dB).

- **Valeur de coupure SNR du client (|dB|) = [Puissance d'émission AP (dBm) - Constante (17 dBm) - Profil de couverture (dB)]**

Cette valeur de profil de couverture configurable par l'utilisateur est accessible de la manière suivante :

1. Dans l'interface graphique utilisateur du WLC, allez à l'en-tête principal de Wireless et sélectionnez l'option **Network** pour la norme WLAN de choix sur le côté gauche (802.11a ou 802.11b/g). Sélectionnez ensuite **Auto RF** dans le coin supérieur droit de la fenêtre.
2. Dans la page Paramètres généraux RF automatiques, recherchez la section Seuils de profil. Dans cette section, vous trouverez la valeur de la couverture (3 à 50 dbm). Cette valeur est la valeur du profil de couverture configurable par l'utilisateur.
3. Cette valeur peut être modifiée pour influencer la valeur du seuil SNR du client. L'autre façon 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 LAN sans fil (WLC) 4402. Lorsque le WLC tente d'authentifier MAC un client sans fil auprès d'ACS 4.1, l'ACS ne répond pas avec l'ACS et signale ce message d'erreur : " *Une erreur interne s'est produite* ". Toutes mes configurations sont correctes. Pourquoi cette erreur interne se produit-elle ?

R.Il y a un bogue Cisco IDCSCsh62641 lié à l'authentification dans ACS 4.1, où ACS donne `le message d'erreur Internal error has` occrederror.

Ce bogue peut être le problème. Il y a un correctif disponible pour ce bogue sur le site de téléchargements d'ACS 4.1 qui peut résoudre le problème.

> **Remarque** : seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations de bogue et aux outils internes de Cisco.

Q. Le contrôleur LAN sans fil (WLC) de la gamme Cisco 4400 ne peut pas démarrer. Ce message d'erreur est reçu sur le contrôleur : `** Unable to use ide 0:4 for fatload ** Error (no IRQ) dev 0 blk 0 : status 0x51 Error reg : 10 ** Cannot read from device 0.` Pourquoi ?

R. La raison de cette erreur peut être un problème matériel. Ouvrez un dossier TAC pour résoudre ce problème. Pour ouvrir un dossier TAC, vous devez disposer d'un contrat valide avec Cisco. Reportez-vous au support technique pour contacter le centre d'assistance technique Cisco.

Q. Le contrôleur LAN sans fil (WLC) rencontre des problèmes de mémoire tampon. Une fois que les mémoires tampons sont pleines, le contrôleur tombe en panne et doit être redémarré pour le remettre en ligne. Ces messages d'erreur sont affichés dans le journal des messages : `Mon Apr 9`

10:41:03 2007 [ERROR] dtl_net.c 506 : Out of System buffers Mon Apr 9 10:41:03 2007 [ERROR] sysapi_if_net.c 537 : Cannot allocate new Mbuf. Lun Apr 9 10:41:03 2007 [ERREUR] sysapi_if_net.c 2019 : MbufGet : no free Mbufs. Pourquoi ?

R. Cela est dû au bogue Cisco IDCSCsh93980. Ce bogue a été résolu dans WLC version 4.1.185.0. Mettez à niveau votre contrôleur vers cette version du logiciel ou une version ultérieure afin de surmonter ce message.

> **Remarque** : seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations de bogue et aux outils internes de Cisco.

Q. J'ai effectué la mise à niveau de notre contrôleur LAN sans fil (WLC) 4400 vers le code 4.1 et notre Syslog a été bombardé par des messages, tels que celui-ci : May**03 03:55:49.591 dtl_net.c:1191 DTL-1-ARP_POISON_DETECTED: STA [00:17:f2:43:26:93, 0.0.0.0] ARP (op 1) reçu avec SPA 192.168.1.233/TPA 192.168.1.233 non valide.** **Qu'indiquent ces messages ?**

R. Cela peut se produire lorsque le WLAN est marqué comme DHCP requis . Dans ce cas, seules les stations qui reçoivent une adresse IP via DHCP sont autorisées à s'associer. Les clients statiques n'ont pas l'autorisation de s'associer à ce WLAN. WLC agit comme un agent de relais DHCP et enregistre l'adresse IP de toutes les stations. Ce message d'erreur est généré lorsque le WLC reçoit une requête ARP d'une station avant que le WLC n'ait reçu des paquets DHCP de la station et enregistré son adresse IP.

Q. Lorsque vous utilisez la technologie PoE (Power over Ethernet) sur le contrôleur LAN sans fil Cisco 2106, les points d'accès radio ne sont pas activés. Le point d'accès ne peut pas vérifier une alimentation en ligne suffisante. Emplacement radio désactivé. **Un message d'erreur apparaît. Comment est-ce que je peux résoudre cela ?**

A.Ce message d'erreur se produit lorsque le commutateur, qui met le point d'accès sous tension, est un commutateur pré-standard, mais que le point d'accès ne prend pas en charge le mode pré-standard d'alimentation en entrée.

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

Vous devez activer **le** mode **pré-**standard d'alimentation sur l'AP qui est soumis à ce message d'erreur. Pour ce faire, utilisez l'interface de ligne de commande du contrôleur avec **la prénorme config ap power {enable | désactiver} {all | Cisco_AP}**.

Cette commande doit déjà être configurée, si nécessaire, si vous effectuez une mise à niveau vers la version logicielle 4.1 à partir d'une version précédente. Mais, il est possible que vous ayez besoin d'entrer cette commande pour les nouvelles installations, ou si vous réinitialisez l'AP aux valeurs d'usine par défaut.

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 : Impossible d'ajouter une entrée ARP pour xx : xx.-xxx.x au processeur réseau. Cette entrée n'existe pas.` Message syslog similaire à celui-ci. Que signifie ce message syslog ?

R. Bien que certains clients sans fil envoient une réponse ARP, l'unité NPU (Network Processor Unit) doit connaître cette réponse. Ainsi, la réponse ARP est transmise à NPU, mais le logiciel WLC ne doit pas essayer d'ajouter cette entrée au processeur réseau. Dans ce cas, ces messages sont générés. Il n'y a pas d'impact de fonctionnalité sur le WLC en raison de cela, mais le WLC ne génère pas ce message syslog.

Q. J'ai installé et configuré un nouveau WLC Cisco 2106. Le WLC indique que le capteur de température est défaillant. Lorsque vous vous connectez à l'interface Web sous « controller summary », il est écrit « `sensor failed` » à côté de la température interne. Tout le reste semble fonctionner normalement.

R. La défaillance du capteur de température interne est cosmétique et peut être résolue par une mise à niveau vers la version 4.2.61.0 du WLC.

WLC 2106 et WLC 526**construits le 01/07/2007 ou après** peuvent utiliser la puce de capteur de température d'un autre fournisseur. Ce nouveau capteur fonctionne correctement mais n'est pas compatible avec les logiciels ultérieurs à la version 4.2. Par conséquent, un logiciel plus ancien ne peut pas lire la température et montre cette erreur. Toutes les autres fonctionnalités du contrôleur ne sont pas affectées par ce défaut.

Un bogue Cisco IDCSCsk97299 connu est lié à ce problème. Ce bogue est mentionné dans la note de version de WLC version 4.2.

> **Remarque** : seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations de bogue et aux outils internes de Cisco.

Q. J'obtiens le message `radius_db.c:1823 AAA-5-RADSERVER_NOT_FOUND: Could not find approprié RADIUS server for WLAN <WLAN ID> - Unable to find a default server"` pour ALL SSIDs. Ce message apparaît même pour les SSID qui n'utilisent pas de serveurs AAA.

R. Ce message d'erreur signifie que le contrôleur n'a pas pu contacter le serveur RADIUS par défaut ou qu'un serveur RADIUS n'a pas été défini.

L'une des raisons possibles de ce comportement est le bogue Cisco IDCSCsk08181, qui a été résolu dans la version 4.2. Mettez à jour votre contrôleur à la version 4.2.

Q. Le `message : Jul 10 17:55:00.725 sim.c:1061 SIM-3-MACADDR_GET_FAIL: Interface 1 source MAC address is not found.` message d'erreur apparaît sur le contrôleur LAN sans fil (WLC). Qu'est-ce que cela indique?

R. Cela signifie que le contrôleur a eu une erreur lors de l'envoi d'un paquet provenant du CPU.

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

- 10 juil 14:52:21.902 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: échec de la lecture du fichier de configuration 'cliWebInitParms.cfg'
- 10 juil 14:52:21.624 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: échec de la lecture du fichier de configuration « rfidInitParms.cfg »
- 10 juil 14:52:21.610 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: échec de la lecture du fichier de configuration « dhcpParms.cfg »
- 10 juil 14:52:21.287 nvstore.c:304 SYSTEM-3-FILE_READ_FAIL: échec de la lecture du fichier de configuration « bcastInitParms.cfg »
- 18 mars 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED : échec de la suppression du fichier : sshpmInitParms.cfg. échec de la suppression du fichier. -Process : Name:fp_main_task, Id:11ca7618
- 18 mars 16:05:56.753 osapi_file.c:274 OSAPI-5-FILE_DEL_FAILED : échec de la suppression du fichier : bcastInitParms.cfg. échec de la suppression du fichier. -Process : Name:fp_main_task, Id:11ca7618

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

R. Ces messages sont des messages d'information et font partie de la procédure normale de démarrage. Ces messages apparaissent en raison d'une erreur de lecture ou de suppression de plusieurs fichiers de configuration différents. Lorsque des fichiers de configuration particuliers sont introuvables ou si le fichier de configuration ne peut pas être lu, la séquence de configuration de chaque processus envoie ce message, par exemple, no DHCP server config, no tags (RF ID) config, etc. Il s'agit de messages de faible gravité qui peuvent être ignorés en toute sécurité. Ces messages n'interrompent pas le fonctionnement du contrôleur.

Q. Le message d'erreur **HE6-WLC01,local0,alert,2008-07-25,12:48:18,apf_rogue.c:740 APF-1-UNABLE_TO_KEEP_ROUGE_CONTAIN: Unable to keep rogue 00:14:XX:02:XX:XX dans l'état contenu - aucun point d'accès disponible à contenir.** apparaît. Qu'est-ce que cela indique?

R. Cela signifie que le point d'accès qui a exécuté la fonction de confinement des systèmes non fiables n'est plus disponible, et le contrôleur ne peut pas trouver de point d'accès approprié pour exécuter le confinement des systèmes non fiables.

Q. Le message système **DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] ARP (op 1) reçu avec SPA 192.168.1.152/TPA 192.168.0.206 non valide** apparaît sur le contrôleur LAN sans fil. Qu'implique ce message ?

R. Il est possible que le système ait détecté une usurpation ou un empoisonnement ARP. Mais ce message n'implique pas nécessairement qu'une usurpation ARP malveillante se soit produite. Le message apparaît quand ces conditions sont vraies :

- Un WLAN est configuré avec DHCP Required et un périphérique client, après s'être associé à ce WLAN, transmet un message ARP sans exécuter DHCP au préalable. Cela peut être un comportement normal ; cela peut se produire, par exemple, lorsque le client est adressé de manière statique, ou lorsque le client détient un bail DHCP valide d'une association antérieure. Le message d'erreur peut ressembler à cet exemple :

```
DTL-1-ARP_POISON_DETECTED: STA [00:01:02:0e:54:c4, 0.0.0.0] ARP (op 1) received with invalid SPA 192.168.1.152/TPA 192.168.0.206
```

Cette condition a pour effet que le client est incapable d'envoyer ou de recevoir du trafic de données, jusqu'à ce qu'il DHCP via le WLC.

Référez-vous à la section Messages DTL du Cisco Wireless LAN Controller System Message Guide pour plus d'informations.

Q. Les LAP n'utilisent pas la technologie Power over Ethernet (POE) pour la mise sous tension. Les journaux du contrôleur LAN sans fil s'affichent :

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

Q. Quel est le problème ?

R. Cela peut se produire si les paramètres PoE (Power over Ethernet) ne sont pas configurés correctement. Lorsqu'un point d'accès qui a été converti en mode léger, par exemple un point d'accès AP1131 ou AP1242, ou un point d'accès de la gamme 1250 est alimenté par un injecteur de puissance connecté à un commutateur Cisco de gestion de l'alimentation pré-intelligente (pré-IPM), vous devez configurer la technologie Power over Ethernet (PoE), également appelée alimentation en ligne.

Référez-vous à Configurer Power over Ethernet, Prise en charge Ethernet pour plus d'informations.

Q. Vous voyez ce message sur le contrôleur LAN 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
```

Q. Qu'est-ce que cela indique ?

R. Les points d'accès légers suivent un certain algorithme pour trouver un contrôleur. Le processus de détection et de jointure est expliqué en détail dans Enregistrement de point d'accès léger (LAP) à un contrôleur de réseau local sans fil (WLC).

Ce message d'erreur s'affiche sur le WLC, quand il reçoit une requête de détection après avoir atteint sa capacité maximale d'AP.

Si le contrôleur principal d'un LAP n'est pas configuré ou s'il s'agit d'un nouveau LAP prêt à l'emploi, il envoie des requêtes de détection LWAPP à tous les contrôleurs accessibles. Si les demandes de détection atteignent un contrôleur qui fonctionne à sa capacité d'AP complète, le WLC obtient les demandes et se rend compte qu'il est à sa capacité d'AP maximale et ne répond pas à la demande et donne cette erreur.

Q. Où puis-je trouver plus d'information sur les messages du système LWAPP ?

R. Reportez-vous au Cisco Wireless LAN Controller System Message Guide, 4.2 (Retrait) pour plus d'informations sur les messages système LWAPP.

Q. Le message d'erreur `Error extrecting webauth files` apparaît sur le contrôleur LAN sans fil (WLC). Qu'est-ce que cela indique?

A.WLC ne parvient pas à charger une offre groupée d'authentification Web personnalisée/Passthrough si l'un des fichiers groupés a plus de 30 caractères dans le nom de fichier, ce qui inclut l'extension de fichier. Le bundle d'authentification Web personnalisé peut contenir jusqu'à 30 caractères pour les noms de fichiers. Assurez-vous qu'aucun nom de fichier dans le bundle ne dépasse 30 caractères.

Q. Les contrôleurs LAN sans fil (WLC), qui exécutent le code 5.2 ou 6.0 avec un grand nombre de groupes AP, l'interface utilisateur graphique Web n'affiche pas tous les groupes AP configurés. Quel est le problème ?

R. Les groupes de points d'accès manquants sont visibles si vous utilisez l'interface de ligne de commande **show wlan ap-groups**erasecat4000_flash:.

Essayez d'ajouter un groupe AP supplémentaire à la liste. Par exemple, 51 groupes de points d'accès sont déployés et le 51e est manquant (page 3). Ajoutez le 52e groupe et la page 3 doit apparaître dans l'interface utilisateur graphique Web.

Afin de résoudre ce problème, mettez à niveau vers la version WLC 7.0.220.0.

Informations connexes

- Dépannage de WiSM - Forum Aux Questions
- Page de prise en charge du mode sans fil
- Assistance technique et téléchargements Cisco

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

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