

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Dépannez](#)

[L'ISR n'identifie pas le WLCM](#)

[Est-ce que je peux améliorer l'éclair sur le WLCM ?](#)

[Le WLCM est-il remplaçable à chaud ?](#)

[Recouvrements pris en charge sur le WLCM](#)

[Incapable d'accéder à Fast Ethernet sur le WLCM](#)

[Vérifiez l'état du WLCM](#)

[Comment nous faisons des corrections dans l'assistant de configuration CLI](#)

[Le RECOUVREMENT ne s'inscrit pas à ISR WLCM - WLCM expédié avec les Certificats incorrects](#)

[Le RECOUVREMENT ne s'inscrit pas au WLCM - heure système non réglée](#)

[Reprise de mot de passe pour le WLCM](#)

[Cisco WLCM LED](#)

[La mise à jour du micrologiciel de contrôleur échoue](#)

[Ne peut pas activer le CDP](#)

[Utilisez l'adresse d'ip-helper et les commandes IP-en avant de protocole aux recouvrements de registre avec le WLCM](#)

[Commandes de dépannage WLCM](#)

[Informations connexes](#)

[Introduction](#)

Ce document fournit à des procédures de dépannage pour des problèmes de base le module du contrôleur LAN sans fil (WLCM).

[Conditions préalables](#)

[Conditions requises](#)

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance du protocole Lightweight Access Point Protocol (LWAPP).
- Connaissance de base de la façon configurer le module WLCM pour participer à un réseau sans fil unifié Cisco.**Remarque:** Si vous êtes un nouvel utilisateur et n'avez pas travaillé à un WLCM, référez-vous au [guide de fonctionnalité de module réseau de contrôleur de WLAN Cisco](#).

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Le Routeur à services intégrés Cisco 2811 (ISR) ce exécute la version 12.4(11)T avec WLCM qui exécute la version 3.2.116.21
- AG aps légers (recouvrements) de Cisco 1030 et de Cisco 1232
- Adaptateur de client réseau local de radio de Cisco 802.11a/b/g (WLAN) qui exécute la version 2.5
- Le Cisco Secure Access Control Server (ACS) ce exécute la version 3.2

Remarque: Les composants répertoriés ici sont seulement les périphériques qui ont été utilisés pour écrire ce document. Les informations sur la liste complète des ISR qui prennent en charge les WLCM et les recouvrements qui sont pris en charge sur le WLCM sont fournies dans la section de [dépannage de](#) ce document.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Informations générales

Cisco WLCM est conçu pour fournir aux entreprises petites et moyennes (PME) et aux clients de succursale des solutions réseau sans fil de 802.11 pour les gammes Cisco 2800 et Cisco 3800 ISR et les Routeurs de gamme Cisco 3700.

Cisco WLCM permet à Cisco ISR et à Routeurs de gamme Cisco 3700 de gérer jusqu'à six points d'accès WLAN (aps), et simplifie le déploiement et la Gestion des WLAN. Le système d'exploitation gère tout le client de données, des transmissions, et des fonctions d'administration système, remplit des fonctions de Gestion des ressources radio (RRM), gère au niveau système des stratégies de mobilité utilisant la Sécurité du système d'exploitation (SYSTÈMES D'EXPLOITATION), et coordonne toutes les fonctions de Sécurité utilisant le cadre de SYSTÈMES D'EXPLOITATION.

Cisco WLCM fonctionne en même temps que les recouvrements de Cisco Aironet, le Système de contrôle sans fil Cisco (WCS), et le Dispositif de localisation sans fil Cisco pour prendre en charge des données Sans fil critiques, la Voix, et des applications vidéo.

Dépannez

Cette section discute des procédures de dépannage pour des problèmes de base avec le WLCM.

L'ISR n'identifie pas le WLCM

Le WLCM est pris en charge seulement sur ces Plateformes ISR :

- Routeurs de Cisco 3725 et 3745
- ISR de Cisco 2811, 2821, et 2851

- ISR de Cisco 3825 et 3845

Si n'importe quel autre ISR que celui spécifié dans cette liste apparaît, alors le WLCM n'est pas détecté. Assurez-vous que vous utilisez le matériel correct.

Remarque: Le WLCM est pris en charge seulement dans des emplacements de module réseau. Il n'est pas pris en charge dans des emplacements EVM disponibles à Cisco 2821 et à Cisco 2851 ISR.

Remarque: Vous pouvez installer seulement un Cisco WLCM dans un châssis de routeur unique.

Il y a également quelques configurations logicielles requises minimales pour le WLCM.

L'ISR doit utiliser la version de logiciel 12.4(2)XA1 de Cisco IOS® (logiciel du routeur) ou plus tard pour que l'ISR identifie le WLCM.

[Est-ce que je peux améliorer l'éclair sur le WLCM ?](#)

Cisco WLCM se transporte avec et démarre d'une carte mémoire installée 256-MB CompactFlash. La carte mémoire de CompactFlash contient le programme de démarrage, fichier exécutable de kernel Linux, de Cisco WLCM et aps, et la configuration de Cisco WLCM.

La carte mémoire de CompactFlash à Cisco WLCM n'est pas remplaçable sur place.

[Le WLCM est-il remplaçable à chaud ?](#)

Le WLCM n'est pas remplaçable à chaud sur toutes les Plateformes ISR. La mise en place et la suppression en ligne (OIR) du module de contrôleur est prise en charge seulement sur le routeur et le Cisco 3845 ISR de Cisco 3745.

[Recouvrements pris en charge sur le WLCM](#)

Tout le Cisco Aironet LWAPP-activé aps sont pris en charge, qui inclut Cisco Aironet 1000, 1100, et gamme 1200. Les cartes d'interface HWIC-AP ne sont pas prises en charge.

[Incapable d'accéder à Fast Ethernet sur le WLCM](#)

C'est le comportement prévu. Le port Fast Ethernet externe sur la plaque de Cisco WLCM n'est pas pris en charge. Le NM-WLC (module WLCM) a seulement un port Fast Ethernet intérieurement connecté au routeur hôte, et le port Fast Ethernet externe sur la plaque nanomètre est désactivé et inutilisable.

[Vérifiez l'état du WLCM](#)

Émettez la commande de **show version** de l'ISR afin de vérifier si le WLCM est identifié par le routeur et est installé correctement.

```
2800-ISR-TSWEB#show versionCisco IOS Software, 2800 Software (C2800NM-ADVSECURITYK9-M), Version
12.4(11)T, RELEASE SOFTWARE (fc2)Technical Support: http://www.cisco.com/techsupportCopyright (c) 1986-
2006 by Cisco Systems, Inc.Compiled Sat 18-Nov-06 17:16 by prod_rel_teamROM: System Bootstrap, Version
12.4(1r) [hqluong 1r], RELEASE SOFTWARE (fc1)2800-ISR-TSWEB uptime is 50 minutesSystem returned to ROM by
power-onSystem image file is "flash:c2800nm-advsecurityk9-mz.124-11.T.bin"This product contains
```

cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately. A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html> If you require further assistance please contact us by sending email to export@cisco.com. Cisco 2811 (revision 53.50) with 249856K/12288K bytes of memory. Processor board ID FTX1014A34X2 FastEthernet interfaces 1 terminal line 1 Virtual Private Network (VPN) Module 1 **cisco Wireless LAN Controller(s)** DRAM configuration is 64 bits wide with parity enabled. 239K bytes of non-volatile configuration memory. 62720K bytes of ATA CompactFlash (Read/Write) Configuration register is 0x2102

Émettez la commande d'état d'emplacement/port de WLAN-contrôleur de module de service afin de trouver l'état du WLCM.

```
2800-ISR-TSWEB#service-module wlan-controller 1/0 status
Service Module is Cisco wlan-controller1/0
Service Module supports session via TTY line 66
Service Module is in Steady state
Getting status from the Service Module, please wait..
Cisco WLAN Controller 3.2.116.21
```

Vous pouvez également émettre la commande de **statistiques du WLAN-contrôleur 1/0 de module de service** afin de trouver les statistiques de remise de module du WLCM.

```
2800-ISR-TSWEB#service-module wlan-controller 1/0 statistics
Module Reset Statistics: CLI reset count = 0
CLI reload count = 0 Registration request timeout reset count = 0
Error recovery timeout reset count = 0
Module registration count = 4
```

Dans certains cas, vous voyez cette erreur :

```
Router#service-module wlan-controller 4/0 status
Service Module is Cisco wlan-controller4/0
Service Module supports session via TTY line 258
Service Module is trying to recover from error
Service Module status is not available
Or this: Router#service-module wlan-controller 1/0 status
Service Module is Cisco wlan-controller1/0
Service Module supports session via TTY line 66
Service Module is failed
Service Module status is not available
```

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.

Émettez la commande de **show sysinfo** afin de recevoir plus d'informations sur le WLCM.

```
(Cisco Controller) >show sysinfo
Manufacturer's Name..... Cisco Systems, Inc
Product Name..... Cisco Controller
Product Version..... 3.2.116.21
RTOS Version..... 3.2.116.21
Build 3.2.116.21
Bootloader Version..... 3.2.116.21
Type..... DATA + WP
System Name..... WLC
System Location..... System
Contact..... System ObjectID..... 1.3.6.1.4.1.14179.1.1.4.5
IP Address..... 60.0.0.2
System Up Time..... 0 days 0 hrs 39 mins 18 secs
Configured Country..... United States
State of 802.11b Network..... Enabled
Number of WLANs..... 13
rd Party Access Point Support..... Disabled
Number of Active Clients..... 0
```

[Comment nous faisons des corrections dans l'assistant de configuration CLI](#)

Quand vous configurez le WLCM pour la première fois (ou après remise à l'état initial aux par défaut) utilisant l'assistant de configuration CLI, - la clé est utilisée afin de faire des corrections aux configurations. Voici un exemple :

Ici, au lieu d'entrer dans l'**admin**, l'utilisateur écrit l'**adminn** pour le corriger. À la prochaine demande, entrez -, puis cliquez sur entrent. Le système revient à la demande précédente.

(Cisco Controller>Welcome to the Cisco Wizard Configuration ToolUse the '-' character to backupSystem Name [Cisco_e8:38:c0]: **adminn!**--- The user enters **adminn** instead of admin.Enter Administrative User Name (24 characters max): **-!**--- In order to make the corrections, the user enters **-**.System Name [Cisco_e8:38:c0] (31 characters max): **admin!**--- The user is again prompted for the system name and **!**--- then enters the correct system name **admin**.

[Le RECOUVREMENT ne s'inscrit pas à ISR WLCM - WLCM expédié avec les Certificats incorrects](#)

Les NM-AIR-WLC6-K9 et les NM-AIR-WLC6-K9= WLCMs sont expédiés avec les Certificats incorrects. Ceci cause le WLCNM de ne pas être authentifié par Cisco/Airespace aps. Le WLCMs expédié entre le 1er février 2006 et mars 22, 2006 sont affectés. Une défaillance de processus de fabrication n'a pas copié les Certificats corrects sur des périphériques WLCNM. Le certificat incorrect crée une non-concordance de clé RSA, qui les causes aps basés sur LWAPP à échouer pour se joindre/associé/registre à WLCNM.

Référez-vous aux [notes de terrain : F-N - 62379 - module réseau Sans fil de contrôleur LAN n'authentifie pas avec Cisco/Points d'accès d'Airespace - mise à niveau matérielle](#) pour plus d'informations sur ceci. Cette note de terrain contient le contournement, aussi bien que les numéros de pièce et les numéros de série affectés de module réseau.

[Le RECOUVREMENT ne s'inscrit pas au WLCM - heure système non réglée](#)

Le WLCM doit être configuré avec l'heure système et la date. Il peut ou être fait manuellement, ou le WLCM peut être configuré pour utiliser le serveur de NTP. Si la date et heure n'est pas placée, les recouvrements ne s'inscrivent pas au WLCM. Dans l'assistant CLI, vous êtes incité à écrire l'heure système et la date. Si vous n'écrivez pas la date et l'heure, vous voyez ce message d'avertissement :

Warning! No AP will come up unless the time is setPlease see documentation for more details.

Émettez cette commande du WLCM CLI afin de configurer le temps manuellement :

Warning! No AP will come up unless the time is setPlease see documentation for more details.

Émettez cette commande si vous voulez que le WLCM utilise le serveur de NTP :

Warning! No AP will come up unless the time is setPlease see documentation for more details.

[Reprise de mot de passe pour le WLCM](#)

Quand le mot de passe à ouvrir une session au WLCM est perdu, la seule manière d'entrer dans le WLCM est de remettre à l'état initial le WLCM de nouveau aux valeurs par défaut. Ceci également signifie que la configuration entière sur le WLCM est remise à l'état initial et doit être à partir de zéro configuré.

Référez-vous [remettent à l'état initial le WLCM aux valeurs par défaut](#) pour les informations sur la façon dont remettre à l'état initial le WLCM aux par défaut d'usine.

[Cisco WLCM LED](#)

Ce tableau présente Cisco WLCM LED et les significations :

DEL	Signification
CF	La carte mémoire de CompactFlash est en activité.

En	Le module a passé l'autotest et est à la disposition du routeur.
PWR	L'alimentation est disponible au module de contrôleur.

[La mise à jour du micrologiciel de contrôleur échoue](#)

Pendant le processus de mise à niveau, vous pouvez trouver quelques erreurs par hasard qui affectent le processus de mise à niveau. Cette section explique ce qui le moyen de messages d'erreur et comment éliminer les erreurs et améliorer le contrôleur.

- **Codez le transfert de fichiers échouer-aucune réponse du serveur TFTP ?** Vous recevez ce message d'erreur si le serveur TFTP n'est pas en activité. Vérifiez si le service TFTP est activé sur le serveur.
- **Code file transfer failed - Error from server: Le fichier n'a pas été trouvé. Abandonner le transfert ?** Vous recevez ce message d'erreur si le fichier de SYSTÈME D'EXPLOITATION n'est pas présent dans le répertoire par défaut du serveur TFTP. Afin d'éliminer cette erreur, copiez le fichier d'image sur le répertoire par défaut sur le serveur TFTP.
- **Panne TFTP tout en entreposé dans l'éclair ! ?** Vous recevez cette erreur quand il y a un problème avec le serveur TFTP. Certains serveurs TFTP ont une limitation quant à la taille des fichiers que vous pouvez transférer. Utilisez un utilitaire différent de serveur TFTP. Il y a beaucoup d'utilitaires libres de serveur TFTP qui sont disponibles. Cisco recommande l'utilisation Tftpd32 du serveur de la version 2.0 TFTP. Référez-vous à [Tftpd32](#) afin de télécharger ce serveur TFTP.
- **Les partitions d'installer sont détruites ou l'image est-elle corrompue ?** Si vous êtes encore infructueux après qu'une tentative d'améliorer le logiciel, il y a une possibilité que votre image est corrompue. [Support technique de Cisco de](#) contact pour l'assistance.

Référez-vous à [améliorer le logiciel du module de contrôleur de WLAN Cisco](#) pour plus d'informations sur la façon améliorer le micrologiciel sur le WLCM.

[Ne peut pas activer le CDP](#)

L'utilisateur ne peut pas activer le Protocole CDP (Cisco Discovery Protocol) sur le WLCM installé sur les 3750 ISR. Ce message apparaît :

```
Warning! No AP will come up unless the time is setPlease see documentation for more details.
```

L'utilisateur émet la commande de **cdp enable de config** afin d'activer le CDP, mais voit toujours ce même message :

```
Warning! No AP will come up unless the time is setPlease see documentation for more details.
```

C'est en raison de l'ID de bogue Cisco CSCsg67615. Bien que le contrôleur sans fil LAN intégré 3750G ne prenne en charge pas le CDP, les commandes CLI de CDP sont disponibles pour ce contrôleur. Ceci est résolu dans 4.0.206.0.

[Utilisez l'adresse d'ip-helper et les commandes IP-en avant de protocole aux recouvrements de registre avec le WLCM](#)

Avec le WLCM, il est difficile que un RECOUVREMENT découvre le WLCM par l'émission d'IP de sous-réseau. C'est en raison de la façon dont le WLCM intègre sur le plan arrière de l'ISR et de la

façon dont le RECOUVREMENT est typiquement sur un différent IP de sous-réseau (qui est également une bonne recommandation). Si vous voulez exécuter la détection d'émission d'IP de sous-réseau avec le succès, émettez le **helper-address d'IP** et l'**UDP d'ip forward-protocol 12223** commandes.

Généralement le but de ces commandes est d'expédier ou transmettre par relais n'importe quelle trame potentielle de diffusion IP. Ce relais et la direction de lui vers l'interface de gestion WLC devraient être adéquats pour s'assurer que le WLC répond de nouveau au RECOUVREMENT.

L'instruction de **helper-address d'IP** doit être donnée sous l'interface à la laquelle on connecte le RECOUVREMENT, et la commande de **helper-address d'IP** doit indiquer l'interface de gestion du WLC.

Warning! No AP will come up unless the time is setPlease see documentation for more details.

La commande d'**ip forward-protocol** est une commande de configuration globale.

Warning! No AP will come up unless the time is setPlease see documentation for more details.

Commandes de dépannage WLCM

Cette section fournit les commandes de **débugage** que vous pouvez employer afin de dépanner la configuration WLCM.

Commandes de debug de vérifier le RECOUVREMENT s'inscrivant au contrôleur :

Employez ces commandes de **débugage** afin de vérifier si les recouvrements s'inscrivent au WLCM :

- **<AP-MAC-adresse xx d'adr de debug mac : xx : xx : xx : xx : xx> ?** Configure l'élimination des imperfections d'adresse MAC pour le RECOUVREMENT.
- **enable d'événements de debug lwapp ?** Configure mettent au point des événements et des messages d'erreur LWAPP.
- **enable de PKI de debug pm ?** Configure mettent au point du module de gestionnaire de stratégie de sécurité.

Voici un exemple de sortie de la **commande debug lwapp events enable** quand le RECOUVREMENT s'inscrit au WLCM :

```
Mon Mar 12 16:23:39 2007: Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0 to 00:15:2c:e8:38:c0
on port '1' Mon Mar 12 16:23:39 2007: Successful transmission of LWAPP Discovery-Response to AP
00:0b:85:51:5a:e0 on Port 1 Mon Mar 12 16:23:52 2007: Received LWAPP JOIN REQUEST from AP
00:0b:85:51:5a:e0 to 00:15:2c:e8:38:c0 on port '1' Mon Mar 12 16:23:52 2007: LWAPP Join-Request MTU path
from AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0 Mon Mar 12 16:23:52 2007: Successfully added
NPU Entry for AP 00:0b:85:51:5a:e0 (index 49)Switch IP: 60.0.0.3, Switch Port: 12223, intIfNum 1, vlanId
0 AP IP: 10.77.244.221, AP Port: 5550, next hop MAC: 00:17:94:06:62:98 Mon Mar 12 16:23:52 2007:
Successfully transmission of LWAPP Join-Reply to AP 00:0b:85:51:5a:e0 Mon Mar 12 16:23:52 2007: Register
LWAPP event for AP 00:0b:85:51:5a:e0 slot 0 Mon Mar 12 16:23:52 2007: Register LWAPP event for AP
00:0b:85:51:5a:e0 slot 1 Mon Mar 12 16:23:53 2007: Received LWAPP CONFIGURE REQUEST from AP
00:0b:85:51:5a:e0 to 00:15:2c:e8:38:c0 Mon Mar 12 16:23:53 2007: Updating IP info for AP
00:0b:85:51:5a:e0 -- static 0, 10.77.244.221/255.255.255.224, gtw 10.77.244.220 Mon Mar 12 16:23:53 2007:
Updating IP 10.77.244.221 ==> 10.77.244.221 for AP 00:0b:85:51:5a:e0 Mon Mar 12 16:23:53 2007:
spamVerifyRegDomain RegDomain set for slot 0 code 0 regstring -A regDfromCb -A Mon Mar 12 16:23:53 2007:
spamVerifyRegDomain RegDomain set for slot 1 code 0 regstring -A regDfromCb -A Mon Mar 12 16:23:53 2007:
spamEncodeDomainSecretPayload:Send domain secret WLCM-
Mobility<bc,73,45,ec,a2,c8,55,ef,14,1e,5d,99,75,f2,f9,63,af,74,d9,02> to AP 00:0b:85:51:5a:e0 Mon Mar 12
16:23:53 2007: Successfully transmission of LWAPP Config-Message to AP 00:0b:85:51:5a:e0 Mon Mar 12
16:23:53 2007: Running spamEncodeCreateVapPayload for SSID 'WLCM-TSWEB' Mon Mar 12 16:23:53 2007: Running
```

spamEncodeCreateVapPayload for SSID 'WLCM-TSWEB' Mon Mar 12 16:23:53 2007: AP 00:0b:85:51:5a:e0 associated. Last AP failure was due to AP reset Mon Mar 12 16:23:53 2007: Received LWAPP CHANGE_STATE_EVENT from AP 00:0b:85:51:5a:e0 Mon Mar 12 16:23:53 2007: Successfully transmission of LWAPP Change-State-Event Response to AP 00:0b:85:51:5a:e0 Mon Mar 12 16:23:53 2007: Received LWAPP Up event for AP 00:0b:85:51:5a:e0 slot 0! Mon Mar 12 16:23:53 2007: Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:51:5a:e0 Mon Mar 12 16:23:53 2007: Received LWAPP CHANGE_STATE_EVENT from AP 00:0b:85:51:5a:e0 Mon Mar 12 16:23:53 2007: Successfully transmission of LWAPP Change-State-Event Response to AP 00:0b:85:51:5a:e0 Mon Mar 12 16:23:53 2007: Received LWAPP Up event for AP 00:0b:85:51:5a:e0 slot 1! Mon Mar 12 16:23:54 2007: Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:51:5a:e0 Mon Mar 12 16:23:54 2007: Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:51:5a:e0 Mon Mar 12 16:23:54 2007: Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:51:5a:e0 Mon Mar 12 16:23:54 2007: Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:51:5a:e0 Mon Mar 12 16:23:54 2007: Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:51:5a:e0 Mon Mar 12 16:23:54 2007: Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:51:5a:e0

Voici un exemple de sortie de la commande d'enable de PKI de debug pm quand le RECOUVREMENT s'inscrit au WLCM :

Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: locking ca cert table Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: calling x509_alloc() for user cert Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: calling x509_decode() Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: <subject> C=US, ST=California, L=San Jose, O=airespace Inc, CN=000b85515ae0, MAILTO=support@airespace.com Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: <issuer> C=US, ST=California, L=San Jose, O=airespace Inc, OU=none, CN=ca, MAILTO=support@airespace.com Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: Mac Address in subject is 00:0b:85:51:5a:e0 Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: Cert is issued by Airespace Inc. Mon Mar 12 16:30:40 2007: sshpmGetCID: called to evaluate <bsnDefaultCaCert> Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert< Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 1, CA cert >bsnDefaultRootCaCert< Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 2, CA cert >bsnDefaultCaCert< Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: called to get cert for CID 2816f436 Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 0, certname >bsnOldDefaultCaCert< Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 1, certname >bsnDefaultRootCaCert< Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 2, certname >bsnDefaultCaCert< Mon Mar 12 16:30:40 2007: sshpmUserCertVerify: calling x509_decode() Mon Mar 12 16:30:40 2007: sshpmUserCertVerify: failed to verify AP cert >bsnDefaultCaCert< Mon Mar 12 16:30:40 2007: sshpmGetCID: called to evaluate <bsnOldDefaultCaCert> Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert< Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: called to get cert for CID 226b9636 Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 0, certname >bsnOldDefaultCaCert< Mon Mar 12 16:30:40 2007: sshpmUserCertVerify: calling x509_decode() Mon Mar 12 16:30:40 2007: sshpmUserCertVerify: user cert verified using >bsnOldDefaultCaCert< Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: ValidityString (current): 2007/03/12/16:30:40 Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: **AP sw version is 0x3027415, send a Cisco cert to AP.** Mon Mar 12 16:30:40 2007: sshpmGetCID: called to evaluate <cscsDefaultIdCert> Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert< Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 1, CA cert >bsnDefaultRootCaCert< Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 2, CA cert >bsnDefaultCaCert< Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 3, CA cert >bsnDefaultBuildCert< Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 4, CA cert >cscsDefaultNewRootCaCert< Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 5, CA cert >cscsDefaultMfgCaCert< Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 0, ID cert >bsnOldDefaultIdCert< Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 1, ID cert >bsnDefaultIdCert< Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 2, ID cert >cscsDefaultIdCert< Mon Mar 12 16:30:40 2007: sshpmGetCertFromHandle: calling sshpmGetCertFromCID() with CID 0x15b4c76e Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: called to get cert for CID 15b4c76e Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 0, certname >bsnOldDefaultCaCert< Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 1, certname >bsnDefaultRootCaCert< Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 2, certname >bsnDefaultCaCert< Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 3, certname >bsnDefaultBuildCert< Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 4, certname >cscsDefaultNewRootCaCert< Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 5, certname >cscsDefaultMfgCaCert< Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 0, certname >bsnOldDefaultIdCert< Mon Mar 12 16:30:44 2007: sshpmGetCertFromCID: comparing to row 1, certname >bsnDefaultIdCert< Mon Mar 12 16:30:44 2007: sshpmGetCertFromCID: comparing to row 2, certname >cscsDefaultIdCert< Mon Mar 12 16:30:44 2007: **sshpmPublicKeyEncrypt: called to encrypt 16 bytes** Mon Mar 12 16:30:44 2007: **sshpmPublicKeyEncrypt: successfully encrypted, out is 192 bytes** Mon Mar 12 16:30:44 2007: sshpmPrivateKeyEncrypt: called to encrypt 196 bytes Mon Mar 12 16:30:44 2007: sshpmGetOpensslPrivateKeyFromCID: called to get key for CID


```

15b4c76e Mon Mar 12 16:30:44 2007: sshpmGetOpensslPrivateKeyFromCID: comparing to row 0, certname
>bsnOldDefaultIdCert< Mon Mar 12 16:30:44 2007: sshpmGetOpensslPrivateKeyFromCID: comparing to row 1,
certname >bsnDefaultIdCert< Mon Mar 12 16:30:44 2007: sshpmGetOpensslPrivateKeyFromCID: comparing to row
2, certname >ciscoDefaultIdCert< Mon Mar 12 16:30:44 2007: sshpmGetOpensslPrivateKeyFromCID: match in row
2 Mon Mar 12 16:30:44 2007: sshpmPrivateKeyEncrypt: calling RSA_private_encrypt with 196 bytes Mon Mar 12
16:30:44 2007: sshpmPrivateKeyEncrypt: RSA_private_encrypt returned 256 Mon Mar 12 16:30:44 2007:
sshpmPrivateKeyEncrypt: encrypted bytes: 256

```

Commandes de debug de vérifier l'authentification Web :

Employez ces commandes de **débogage** afin de vérifier si l'authentification Web fonctionne comme prévu sur le WLCM :

- **le debug aaa tout actifent ?** Configures mettent au point de tous les messages d'AAA.
- **enable d'état de debug pem ?** Configures mettent au point de l'ordinateur d'état de gestionnaire de stratégie.
- **enable d'événements de debug pem ?** Configures mettent au point des événements de gestionnaire de stratégie.
- **enable de ssh-appgw de debug pm ?** Configures mettent au point des passerelles d'application.
- **enable de ssh-TCP de debug pm ?** Configures mettent au point de la manipulation de TCP de gestionnaire de stratégie.

Voici les sorties témoin de certaines de ces commandes de **débogage** :

```

(Cisco Controller) >debug aaa all enableUser user1 authenticated00:40:96:ac:e6:57 Returning AAA Error
'Success' (0) for mobile 00:40:96:ac:e6:57AuthorizationResponse: 0xbadff97c
structureSize.....70      resultCode.....0
protocolUsed.....0x00000008
proxyState.....00:40:96:AC:E6:57-00:00      Packet contains 2 AVPs:
AVP[01] Service-Type.....0x00000001 (1) (4 bytes)      AVP[02] Airespace /
WLAN-Identifler.....0x00000001 (1) (4 bytes)00:40:96:ac:e6:57 Applying new AAA override for
station 00:40:96:ac:e6:5700:40:96:ac:e6:57 Override values for station 00:40:96:ac:e6:57 source: 48,
valid bits: 0x1 qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1dataAvgC: -1,
rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: '', aclName:00:40:96:ac:e6:57 Unable to apply
override policy for station 00:40:96:ac:e6:57 - VapAllowRadiusOverride is FALSE      AccountingMessage
Accounting Start: 0xa62700c      Packet contains 13 AVPs:      AVP[01] User-
Name.....user1 (5 bytes)      AVP[02] Nas-
Port.....0x00000001 (1) (4 bytes)      AVP[03] Nas-Ip-
Address.....0x0a4df4d2 (172881106) (4 bytes)      AVP[04] NAS-
Identifler.....0x574c4331 (1464615729) (4 bytes)      AVP[05] Airespace / WLAN-
Identifler.....0x00000001 (1) (4 bytes)      AVP[06] Acct-Session-
Id.....45e84f50/00:40:96:ac:e6:57/9 (28 bytes)      AVP[07] Acct-
Authentic.....0x00000002 (2) (4 bytes)      AVP[08] Tunnel-
Type.....0x0000000d (13) (4 bytes)      AVP[09] Tunnel-Medium-
Type.....0x00000006 (6) (4 bytes)      AVP[10] Tunnel-Group-
Id.....0x3330 (13104) (2 bytes)      AVP[11] Acct-Status-
Type.....0x00000001 (1) (4 bytes)      AVP[12] Calling-Station-
Id.....10.0.0.1 (8 bytes)      AVP[13] Called-Station-
Id.....10.77.244.210 (13 bytes)when web authentication is closed by user:(Cisco
Controller) >      AccountingMessage Accounting Stop: 0xa627c78      Packet contains 20 AVPs:
AVP[01] User-Name.....user1 (5 bytes)      AVP[02] Nas-
Port.....0x00000001 (1) (4 bytes)      AVP[03] Nas-Ip-
Address.....0x0a4df4d2 (172881106) (4 bytes)      AVP[04] NAS-
Identifler.....0x574c4331 (1464615729) (4 bytes)      AVP[05] Airespace / WLAN-
Identifler.....0x00000001 (1) (4 bytes)      AVP[06] Acct-Session-
Id.....45e84f50/00:40:96:ac:e6:57/9 (28 bytes)      AVP[07] Acct-
Authentic.....0x00000002 (2) (4 bytes)      AVP[08] Tunnel-
Type.....0x0000000d (13) (4 bytes)      AVP[09] Tunnel-Medium-
Type.....0x00000006 (6) (4 bytes)      AVP[10] Tunnel-Group-
Id.....0x3330 (13104) (2 bytes)      AVP[11] Acct-Status-

```

```

Type.....0x00000002 (2) (4 bytes) AVP[12] Acct-Input-
Octets.....0x0001820e (98830) (4 bytes) AVP[13] Acct-Output-
Octets.....0x00005206 (20998) (4 bytes) AVP[14] Acct-Input-
Packets.....0x000006ee (1774) (4 bytes) AVP[15] Acct-Output-
Packets.....0x00000041 (65) (4 bytes) AVP[16] Acct-Terminate-
Cause.....0x00000001 (1) (4 bytes) AVP[17] Acct-Session-
Time.....0x000000bb (187) (4 bytes) AVP[18] Acct-Delay-
Time.....0x00000000 (0) (4 bytes) AVP[19] Calling-Station-
Id.....10.0.0.1 (8 bytes) AVP[20] Called-Station-
Id.....10.77.244.210 (13 bytes) (Cisco Controller) >debug pem state enableFri Mar 2
16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Change state to START (0)Fri Mar 2 16:27:39
2007: 00:40:96:ac:e6:57 10.0.0.1 START (0) Change state to AUTHCHECK (2)Fri Mar 2 16:27:39 2007:
00:40:96:ac:e6:57 10.0.0.1 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)Fri Mar 2 16:27:39 2007:
00:40:96:ac:e6:57 10.0.0.1 L2AUTHCOMPLETE (4) Change state to WEBAUTH_REQD (8)Fri Mar 2 16:28:16 2007:
00:16:6f:6e:36:2b 0.0.0.0 START (0) Change state to AUTHCHECK (2)Fri Mar 2 16:28:16 2007:
00:16:6f:6e:36:2b 0.0.0.0 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)Fri Mar 2 16:28:16 2007:
00:16:6f:6e:36:2b 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)Fri Mar 2 16:28:19 2007:
00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Change state to WEBAUTH_NOL3SEC (14)Fri Mar 2 16:28:19 2007:
00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_NOL3SEC (14) Change state to RUN (20)Fri Mar 2 16:28:20 2007:
00:16:6f:6e:36:2b 0.0.0.0 START (0) Change state to AUTHCHECK (2)Fri Mar 2 16:28:20 2007:
00:16:6f:6e:36:2b 0.0.0.0 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)Fri Mar 2 16:28:20 2007:
00:16:6f:6e:36:2b 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)Fri Mar 2 16:28:24 2007:
00:40:96:af:a3:40 0.0.0.0 START (0) Change state to AUTHCHECK (2)Fri Mar 2 16:28:24 2007:
00:40:96:af:a3:40 0.0.0.0 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)Fri Mar 2 16:28:24 2007:
00:40:96:af:a3:40 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)Fri Mar 2 16:28:25 2007:
00:40:96:af:a3:40 40.0.0.1 DHCP_REQD (7) Change state to RUN (20)Fri Mar 2 16:28:30 2007:
00:16:6f:6e:36:2b 0.0.0.0 START (0) Change state to AUTHCHECK (2)Fri Mar 2 16:28:30 2007:
00:16:6f:6e:36:2b 0.0.0.0 AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)Fri Mar 2 16:28:30 2007:
00:16:6f:6e:36:2b 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)Fri Mar 2 16:28:34 2007:
00:16:6f:6e:36:2b 30.0.0.2 DHCP_REQD (7) Change state to WEBAUTH_REQD (8) (Cisco Controller) >debug pem
events enableFri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 START (0) Initializing policyFri Mar 2
16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 L2AUTHCOMPLETE (4) Plumbed mobile LWAPP rule on AP
00:0b:85:5b:fb:d0Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Adding TMP ruleFri
Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8) Replacing Fast Path rule type =
Temporary Entry on AP 00:0b:85:5b:fb:d0, slot 0, interface = 1 ACL Id = 255, Jumbo Frames = NO, 802.1P =
0, DSCP = 0, TokenID = 1506Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8)
Successfully plumbed mobile rule (ACL ID 255)Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8) Deleting mobile policy rule 27Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 Adding Web
RuleID 28 for mobile 00:40:96:ac:e6:57Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD
(8)Adding TMP ruleFri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD (8)ReplacingFast Path
rule type = Temporary Entry on AP 00:0b:85:5b:fb:d0, slot 0, interface = 1 ACL Id = 255, Jumbo Frames =
NO, 802.1P = 0, DSCP = 0, TokenID = 1506Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 WEBAUTH_REQD
(8)Successfully plumbed mobile rule (ACL ID 255)Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
Removed NPU entry.Fri Mar 2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Added NPU entry of type 8Fri Mar
2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Added NPU entry of type 8

```

Commandes de debug de vérifier le fonctionnement de DHCP :

Employez ces commandes de **débugage** afin de vérifier le DHCP Client et les activités de serveur :

- **enable de message de debug dhcp** ? Les informations de débogage d'affichages au sujet des activités de DHCP Client et pour surveiller l'état des paquets DHCP.
- **enable de paquet de debug dhcp** ? Les informations de niveau de paquet DHCP d'affichages.

Voici les sorties témoin de ces commandes de **débugage** :

```

(Cisco Controller) >debug dhcp message enable00:40:96:ac:e6:57 dhcp option len,including the magic cookie
= 6400:40:96:ac:e6:57 dhcp option: received DHCP REQUEST msg00:40:96:ac:e6:57 dhcp option: skipping
option 61, len 700:40:96:ac:e6:57 dhcp option: requested ip = 10.0.0.100:40:96:ac:e6:57 dhcp option:
skipping option 12, len 300:40:96:ac:e6:57 dhcp option: skipping option 81, len 700:40:96:ac:e6:57 dhcp
option: vendor class id = MSFT5.0 (len 8)00:40:96:ac:e6:57 dhcp option: skipping option 55, len
1100:40:96:ac:e6:57 dhcpParseOptions: options end, len 64, actual 6400:40:96:ac:e6:57 Forwarding DHCP

```

```

packet (332 octets)from 00:40:96:ac:e6:57-- packet received on direct-connect port requires forwarding to
external DHCP server. Next-hop is 10.0.0.5000:40:96:ac:e6:57 dhcp option len, including the magic
cookie = 6400:40:96:ac:e6:57 dhcp option: received DHCP ACK msg00:40:96:ac:e6:57 dhcp option: server id =
10.0.0.5000:40:96:ac:e6:57 dhcp option: lease time (seconds) =8640000:40:96:ac:e6:57 dhcp option:
skipping option 58, len 400:40:96:ac:e6:57 dhcp option: skipping option 59, len 400:40:96:ac:e6:57 dhcp
option: skipping option 81, len 600:40:96:ac:e6:57 dhcp option: netmask = 255.0.0.000:40:96:ac:e6:57 dhcp
option: gateway = 10.0.0.5000:40:96:ac:e6:57 dhcpParseOptions: options end, len 64, actual 64(Cisco
Controller) >debug dhcp packet enableFri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: Received
packet: Client 00:40:96:ac:e6:57 DHCP Op: BOOTREQUEST(1), IP len: 300, switchport: 1, encap: 0xec03Fri
Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: dhcp request, client: 00:40:96:ac:e6:57: dhcp op: 1,
port: 1, encap 0xec03, old mscb port number: 1Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 Determing relay
for 00:40:96:ac:e6:57 dhcpServer: 10.0.0.50, dhcpNetmask: 255.0.0.0, dhcpGateway: 10.0.0.50, dhcpRelay:
10.0.0.10 VLAN: 30Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 Relay settings for 00:40:96:ac:e6:57 Local
Address: 10.0.0.10, DHCP Server: 10.0.0.50, Gateway Addr: 10.0.0.50, VLAN: 30, port: 1Fri Mar 2 16:06:35
2007: 00:40:96:ac:e6:57 DHCP Message Type received: DHCP REQUEST msgFri Mar 2 16:06:35 2007:
00:40:96:ac:e6:57 op: BOOTREQUEST, htype: Ethernet,hlen: 6, hops: 1Fri Mar 2 16:06:35 2007:
00:40:96:ac:e6:57 xid: 1674228912, secs: 0, flags: 0Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57
chaddr: 00:40:96:ac:e6:57Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 ciaddr: 10.0.0.1, yiaddr:
0.0.0.0Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 siaddr: 0.0.0.0, giaddr: 10.0.0.10Fri Mar 2
16:06:35 2007: 00:40:96:ac:e6:57 DHCP request to 10.0.0.50, len 350,switchport 1, vlan 30Fri Mar 2
16:06:35 2007: 00:40:96:ac:e6:57 dhcpProxy: Received packet: Client 00:40:96:ac:e6:57 DHCP Op:
BOOTREPLY(2), IP len: 300, switchport: 1, encap: 0xec00Fri Mar 2 16:06:35 2007: DHCP Reply to AP client:
00:40:96:ac:e6:57, frame len412, switchport 1Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP Message
Type received: DHCP ACK msg Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 op: BOOTREPLY, htype: Ethernet,
hlen: 6, hops: 0Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 xid: 1674228912, secs: 0, flags: 0Fri Mar
2 16:06:35 2007: 00:40:96:ac:e6:57 chaddr: 00:40:96:ac:e6:57Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57
ciaddr: 10.0.0.1, yiaddr: 10.0.0.1Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 siaddr: 0.0.0.0,
giaddr: 0.0.0.0Fri Mar 2 16:06:35 2007: 00:40:96:ac:e6:57 server id: 1.1.1.1 rcvd server id:
10.0.0.50

```

Commandes de debug de vérifier la mise à jour TFTP :

- **show msglog ?** Affiche les journaux des messages écrits à la base de données Sans fil de contrôleur LAN de Cisco. S'il y a plus de 15 entrées, vous êtes incité à afficher les messages affichés dans l'exemple.
- **suivi de debug transfer ?** Configure mettent au point du transfert ou de la mise à jour.

Voici un exemple de la commande trace de debug transfer :

```

Cisco Controller) >debug transfer trace enable(Cisco Controller) >transfer download
startMode..... TFTPData
Type..... CodeTFTP Server IP.....
172.16.1.1TFTP Packet Timeout..... 6TFTP Max
Retries..... 10TFTP Path.....
d:\WirelessImages\TFTP Filename..... AIR-WLC2006-K9-3-2-78-0.aesThis may
take some time.Are you sure you want to start? (y/n) yMon Feb 13 14:06:56 2006: RESULT_STRING: TFTP Code
transfer starting.Mon Feb 13 14:06:56 2006: RESULT_CODE:1TFTP Code transfer starting.Mon Feb 13 14:06:59
2006: Still waiting! Status = 2Mon Feb 13 14:07:00 2006: Locking tftp semaphore, pHost=172.16.1.1
pFilename=d:\WirelessImages\AIR-WLC2006-K9-3-2-78-0.aesMon Feb 13 14:07:00 2006: Semaphore locked, now
unlocking, pHost=172.16.1.1 pFilename=d:\WirelessImages\AIR-WLC2006-K9-3-2-78-0.aesMon Feb 13 14:07:00
2006: Semaphore successfully unlocked, pHost=172.16.1.1 pFilename=d:\WirelessImages\AIR-WLC2006-K9-3-2-
78-0.aesMon Feb 13 14:07:02 2006: Still waiting! Status = 1Mon Feb 13 14:07:05 2006: Still waiting!
Status = 1Mon Feb 13 14:07:08 2006: Still waiting! Status = 1Mon Feb 13 14:07:11 2006: Still waiting!
Status = 1Mon Feb 13 14:07:14 2006: Still waiting! Status = 1Mon Feb 13 14:07:17 2006: Still waiting!
Status = 1Mon Feb 13 14:07:19 2006: tftp rc=0, pHost=172.16.1.1 pFilename=d:\WirelessImages\AIR-WLC2006-
K9-3-2-78-0.aes pLocalFilename=/mnt/download/local.tgzMon Feb 13 14:07:19 2006: tftp = 6,
file_name=d:\WirelessImages\AIR-WLC2006-K9-3-2-78-0.aes, ip_address=172.16.1.1Mon Feb 13 14:07:19 2006:
upd_get_code_via_tftp = 6 (target=268435457)Mon Feb 13 14:07:19 2006: RESULT_STRING: TFTP receive
complete... extracting components.Mon Feb 13 14:07:19 2006: RESULT_CODE:6TFTP receive complete...
extracting components.Mon Feb 13 14:07:20 2006: Still waiting! Status = 2Mon Feb 13 14:07:23 2006: Still
waiting! Status = 1Mon Feb 13 14:07:23 2006: Still waiting! Status = 1Mon Feb 13 14:07:23 2006: Still
waiting! Status = 1Mon Feb 13 14:07:25 2006: RESULT_STRING: Executing init script.Mon Feb 13 14:07:25
2006: RESULT_STRING: Executing backup script.Executing backup script.Mon Feb 13 14:07:26 2006: Still

```

```

waiting! Status = 2Mon Feb 13 14:07:29 2006: Still waiting! Status = 1Mon Feb 13 14:07:31 2006:
RESULT_STRING: Writing new bootloader to flash disk.Writing new bootloader to flash disk.Mon Feb 13
14:07:32 2006: Still waiting! Status = 2Mon Feb 13 14:07:33 2006: RESULT_STRING: Executing
install_bootloader script.Executing install_bootloader script.Mon Feb 13 14:07:35 2006: Still waiting!
Status = 2Mon Feb 13 14:07:35 2006: RESULT_STRING: Writing new RTOS to flash disk.Mon Feb 13 14:07:36
2006: RESULT_STRING: Executing install_rtos script.Mon Feb 13 14:07:36 2006: RESULT_STRING: Writing new
Code to flash disk.Writing new Code to flash disk.Mon Feb 13 14:07:38 2006: Still waiting! Status = 2Mon
Feb 13 14:07:41 2006: Still waiting! Status = 1Mon Feb 13 14:07:42 2006: RESULT_STRING: Executing
install_code script.Executing install_code script.Mon Feb 13 14:07:44 2006: Still waiting! Status = 2Mon
Feb 13 14:07:47 2006: Still waiting! Status = 1Mon Feb 13 14:07:48 2006: RESULT_STRING: Writing new APIB
to flash disk.Writing new APIB to flash disk.Mon Feb 13 14:07:50 2006: Still waiting! Status = 2Mon Feb
13 14:07:51 2006: RESULT_STRING: Executing install_apib script.Executing install_apib script.Mon Feb 13
14:07:53 2006: Still waiting! Status = 2Mon Feb 13 14:07:53 2006: Still waiting! Status = 1Mon Feb 13
14:07:53 2006: Still waiting! Status = 1Mon Feb 13 14:07:53 2006: Still waiting! Status = 1Mon Feb 13
14:07:53 2006: Still waiting! Status = 1Mon Feb 13 14:07:54 2006: RESULT_STRING: Writing new APIB to
flash disk.Mon Feb 13 14:07:56 2006: RESULT_STRING: Executing install_apib script.Executing install_apib
script.Mon Feb 13 14:07:56 2006: Still waiting! Status = 2Mon Feb 13 14:07:59 2006: RESULT_STRING:
Writing new APIB to flash disk.Writing new APIB to flash disk.Mon Feb 13 14:08:00 2006: Still waiting!
Status = 2Mon Feb 13 14:08:00 2006: RESULT_STRING: Executing install_apib script.Executing install_apib
script.Mon Feb 13 14:08:03 2006: Still waiting! Status = 2Mon Feb 13 14:08:03 2006: RESULT_STRING:
Writing new Cert-patch to flash disk.Mon Feb 13 14:08:03 2006: RESULT_STRING: Executing
install_cert_patch script.Mon Feb 13 14:08:03 2006: RESULT_STRING: Executing fini script.Mon Feb 13
14:08:04 2006: RESULT_STRING: TFTP File transfer is successful.Reboot the switch for update to
complete.Mon Feb 13 14:08:06 2006: Still waiting! Status = 2Mon Feb 13 14:08:08 2006: ummounting:
<umount /mnt/download/> cwd = /mnt/applicationMon Feb 13 14:08:08 2006: finished umounting

```

Commandes de debug pour la mise en cache 802.1X/WPA/RSN/PMK :

- le debug dot1x tout activent ? Affiche les informations de débogage de 802.1X.Voici un

```

résultat témoin de cette commande : (Cisco Controller) >debug dot1x all enableFri Mar 23 21:35:01
2007: 00:40:96:ac:e6:57 Adding AAA_ATT_USER_NAME(1) index=0Fri Mar 23 21:35:01 2007:
00:40:96:ac:e6:57 Adding AAA_ATT_CALLING_STATION_ID(31) index=1Fri Mar 23 21:35:01 2007:
00:40:96:ac:e6:57 Adding AAA_ATT_CALLED_STATION_ID(30) index=2Fri Mar 23 21:35:01 2007:
00:40:96:ac:e6:57 Adding AAA_ATT_NAS_PORT(5) index=3Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Adding
AAA_ATT_NAS_IDENTIFIER(32) index=5Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Adding
AAA_ATT_VAP_ID(1) index=6Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Adding AAA_ATT_SERVICE_TYPE(6)
index=7Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Adding AAA_ATT_FRAMED_MTU(12) index=8Fri Mar 23
21:35:01 2007: 00:40:96:ac:e6:57 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9Fri Mar 23 21:35:01 2007:
00:40:96:ac:e6:57 Adding AAA_ATT_EAP_MESSAGE(79) index=10Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_MESS_AUTH(80) index=11Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 AAA EAP Packet
created request = 0xbbdfe944.. !!!!Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 AAA Message 'Interim
Response' received for mobile 00:40:96:ac:e6:57Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Received
EAP Attribute (code=1, length=24,id=1, dot1xcb->id = 1) for mobile 00:40:96:ac:e6:57Fri Mar 23
21:35:01 2007: 00000000: 01 01 00 18 11 01 00 08 38 93 8c 47 64 99 e1 d0 .....8..Gd...00000010:
45 41 50 55 53 45 52 31 EAPUSER1Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Skipping AVP (0/80) for mobile 00:40:96:ac:e6:57Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Adding
AAA_ATT_USER_NAME(1) index=0Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Adding
AAA_ATT_CALLING_STATION_ID(31) index=1Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Adding
AAA_ATT_CALLED_STATION_ID(30) index=2Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Adding
AAA_ATT_NAS_PORT(5) index=3Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Adding
AAA_ATT_NAS_IP_ADDRESS(4) index=4Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Adding
AAA_ATT_NAS_IDENTIFIER(32) index=5Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Adding
AAA_ATT_VAP_ID(1) index=6Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Adding AAA_ATT_SERVICE_TYPE(6)
index=7Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Adding AAA_ATT_FRAMED_MTU(12) index=8Fri Mar 23
21:35:01 2007: 00:40:96:ac:e6:57 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9Fri Mar 23 21:35:01 2007:
00:40:96:ac:e6:57 Adding AAA_ATT_EAP_MESSAGE(79) index=10Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_MESS_AUTH(80) index=11Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 AAA EAP Packet
created request = 0xbbdfe944.. !!!!Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 AAA Message 'Interim
Response' received for mobile 00:40:96:ac:e6:57Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Received
EAP Attribute (code=3, length=4,id=1, dot1xcb->id = 1) for mobile 00:40:96:ac:e6:57Fri Mar 23
21:35:01 2007: 00000000: 03 01 00 04 .....Fri Mar 23 21:35:01
2007: 00:40:96:ac:e6:57 Skipping AVP (0/80) for mobile 00:40:96:ac:e6:57Fri Mar 23 21:35:01 2007:

```

```

00:40:96:ac:e6:57 Adding AAA_ATT_USER_NAME(1) index=0Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_CALLING_STATION_ID(31) index=1Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Adding
AAA_ATT_CALLED_STATION_ID(30) index=2Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Adding
AAA_ATT_NAS_PORT(5) index=3Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Adding
AAA_ATT_NAS_IP_ADDRESS(4) index=4Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Adding
AAA_ATT_NAS_IDENTIFIER(32) index=5Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Adding
AAA_ATT_VAP_ID(1) index=6Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Adding AAA_ATT_SERVICE_TYPE(6)
index=7Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Adding AAA_ATT_FRAMED_MTU(12) index=8Fri Mar 23
21:35:01 2007: 00:40:96:ac:e6:57 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9Fri Mar 23 21:35:01 2007:
00:40:96:ac:e6:57 Adding AAA_ATT_EAP_MESSAGE(79) index=10Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_MESS_AUTH(80) index=11Fri Mar 23 21:35:05 2007: 00:40:96:ac:e6:57 AAA EAP Packet
created request = 0xbbdfe944.. !!!!Fri Mar 23 21:35:05 2007: 00:40:96:ac:e6:57 AAA Message 'Success'
received for mobile 00:40:96:ac:e6:57

```

- **le debug dot11 tout activent ?** Active l'élimination des imperfections des fonctions par radio.
- **<mac> de show client summary ?** Les affichages ont récapitulé les informations pour le client par l'adresse MAC. Voici un résultat témoin de cette commande : (Cisco Controller) >**show client summary**

Status	WLAN	Auth	Protocol	Port	MAC Address	AP Name
---	-----	----	00:40:96:ac:e6:57	AP0015.63e5.0c7e	Associated	1 Yes 802.11a 1

Informations connexes

- [Références des commandes du contrôleur de réseau local sans fil Cisco](#)
- [Guide de fonctionnalité de module réseau de contrôleur de WLAN Cisco](#)
- [Exemples de configuration d'un module contrôleur de réseau local sans fil \(WLCM\)](#)
- [Exemple de configuration de l'authentification Web sur un contrôleur de réseau local sans fil](#)
- [Exemple de configuration de l'authentification EAP avec des contrôleurs de réseau local sans fil \(WLC\)](#)
- [Support et documentation techniques - Cisco Systems](#)