Troubleshooting inalámbrico del módulo del regulador LAN

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Antecedentes
Troubleshooting
ISR no reconoce el WLCM
¿Puedo actualizar el flash en el WLCM?
¿Es el WLCM Caliente-intercambiable?
Revestimientos utilizados en el WLCM
Incapaz de tener acceso a los Ethernetes rápidos en el WLCM
Controle el estatus del WLCM
Cómo hacemos las correcciones en el Asisitente de la configuración CLI
El REVESTIMIENTO no se registra con ISR WLCM - WLCM enviado con los Certificados incorrectos
El REVESTIMIENTO no se registra con el WLCM - Tiempo del sistema no fijado
Recuperación de contraseña para el WLCM
Cisco WLCM LED
La mejora del firmware del controlador falla
No puede activar el CDP
Utilice ayuda IP el direccionamiento y los comandos protocol IP-delanteros a los revestimientos del registro con el WLCM
Comandos de Troubleshooting WLCM
Información Relacionada

Introducción

Este documento proporciona procedimientos de troubleshooting para problemas básicos con Cisco Wireless LAN Controller Module (WLCM).

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de Lightweight Access Point Protocol (LWAPP).
- El conocimiento básico de cómo configurar el módulo WLCM para participar en Cisco unificó la red inalámbrica.**Nota:** Si usted es usuario nuevo y no ha trabajado en un WLCM, refiera a la guía de funciones del módulo de red del regulador de la red inalámbrica (WLAN) de Cisco.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- El Router de servicios integrados Cisco 2811 (ISR) ese funciona con la versión 12.4(11)T con WLCM que funcione con la versión 3.2.116.21
- AG APs ligeros (revestimientos) de Cisco 1030 y de Cisco 1232
- Adaptador del cliente LAN de la Tecnología inalámbrica de Cisco 802.11a/b/g (red inalámbrica (WLAN)) que funciona con la versión 2.5
- El Cisco Secure Access Control Server (ACS) ese funciona con la versión 3.2

Nota: Los componentes enumerados aquí son solamente los dispositivos que fueron utilizados para escribir este documento. La información sobre la lista completa del ISRs que utilizan los WLCM y los revestimientos que se utilizan en los WLCM se proporciona en la sección del Troubleshooting de este documento.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Cisco WLCM se diseña para proveer de las pequeñas y medianas empresas (SMB) y de los clientes de la Sucursal corporativa las soluciones de la red inalámbrica del 802.11 para las Cisco 2800 y Cisco 3800 Series ISRs y los Cisco 3700 Series Router.

Cisco WLCM permite a Cisco ISRs y Cisco 3700 Series Router manejar hasta seis puntos de acceso VLAN (APs), y simplifica el despliegue y la Administración de las redes inalámbricas (WLAN). El sistema operativo maneja a todo el cliente de los datos, las comunicaciones, y las funciones de la administración del sistema, realiza las funciones del Administración de recursos de radio (RRM), maneja las directivas sistema-anchas de la movilidad usando la Seguridad del sistema operativo (OSS), y coordina todas las funciones de la Seguridad usando el marco OSS.

Cisco WLCM trabaja conjuntamente con los revestimientos de Cisco Aironet, el Cisco Wireless Control System (WCS), y el Cisco Wireless Location Appliance para utilizar los datos, la Voz, y los aplicación de video inalámbricos misión-críticos.

Troubleshooting

Esta sección discute el resolver problemas de los procedimientos por problemas básicos con el WLCM.

ISR no reconoce el WLCM

El WLCM se utiliza solamente en estas Plataformas ISR:

- Cisco 3725 y 3745 Router
- Cisco 2811, 2821, y 2851 ISRs
- Cisco 3825 y 3845 ISRs

Si aparece cualquier otro ISR que los que está especificados en esta lista, después el WLCM no se detecta. Asegúrese de que usted utilice la dotación física correcta.

Nota: El WLCM se utiliza solamente en los slots de módulo de red. No se utiliza en las ranuras EVM disponibles en Cisco 2821 y Cisco 2851 ISRs.

Nota: Usted puede instalar solamente un Cisco WLCM en un chasis del único router.

Hay también algunos requisitos mínimos de software para el WLCM.

El ISR debe utilizar la versión 12.4(2)XA1 (software del router) del Cisco IOS ® Software o para que el ISR reconozca más adelante el WLCM.

¿Puedo actualizar el flash en el WLCM?

Cisco WLCM envía con y arranca de una placa de memoria instalada 256-MB CompactFlash. La placa de memoria de CompactFlash contiene el cargador de arranque, archivo ejecutable del núcleo de Linux, de Cisco WLCM y APs, y la configuración de Cisco WLCM.

La placa de memoria de CompactFlash en Cisco WLCM no es reemplazable en el terreno.

¿Es el WLCM Caliente-intercambiable?

El WLCM no es caliente-intercambiable en todas las Plataformas ISR. La inserción y el retiro en línea (OIR) del módulo del regulador se utiliza solamente en el Cisco 3745 Router y Cisco 3845 ISR.

Revestimientos utilizados en el WLCM

Se utiliza todo el Cisco LWAPP-activado Aironet APs, que incluye Cisco Aironet 1000, 1100, y las 1200 Series. Los indicadores luminosos LED amarillo de la placa muestra gravedad menor de interfaz HWIC-AP no se utilizan.

Incapaz de tener acceso a los Ethernetes rápidos en el WLCM

Ésta es la conducta esperada. El puerto Ethernet rápido externo en la placa frontal de Cisco WLCM no se utiliza. El NM-WLC (módulo WLCM) tiene solamente un puerto Ethernet rápido internamente conectado con el router del host, y el puerto Ethernet rápido externo en la placa frontal nanómetro está inhabilitado e inutilizable.

Controle el estatus del WLCM

Publique el **comando show version del** ISR para controlar si el WLCM es reconocido por el router y instalado correctamente.

```
2800-ISR-TSWEB#show version

Cisco IOS Software, 2800 Software (C2800NM-ADVSECURITYK9-M), Version 12.4(11)T,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Sat 18-Nov-06 17:16 by prod_rel_team

ROM: System Bootstrap, Version 12.4(1r) [hqluong 1r], RELEASE SOFTWARE (fc1)

2800-ISR-TSWEB uptime is 50 minutes
System returned to ROM by power-on
System 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-part y 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 FTX1014A34X
2 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
```

Publique la **ranura/el comando port status del WLAN-regulador del servicio-módulo** para encontrar el estatus del 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
```

Usted puede también publicar el **comando statistics del WLAN-regulador 1/0 del servicio-módulo** para encontrar las estadísticas del reinicio de módulo del 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
```

En algunos casos, usted ve este error:

```
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 razón de este error pudo ser problemas del hardware. Abre un caso TAC para resolver problemas más lejos este problema. Para abrir un caso TAC, necesitas tener un contrato válido con Cisco. Consulte el soporte técnico para entrar en contacto el TAC de Cisco.

Publique el comando del **sysinfo de la demostración** para recibir más información sobre el 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
Bootloader Version............................... 3.2.116.21
Build Type....................................... DATA + WPS

System Name...................................... WLCM
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
State of 802.11a Network......................... Enabled
Number of WLANs.................................. 1
3rd Party Access Point Support................... Disabled
Number of Active Clients......................... 0
```

Cómo hacemos las correcciones en el Asisitente de la configuración CLI

Cuando usted configura el WLCM por primera vez (o después de reajustar a los valores por defecto) usando el Asisitente de la configuración CLI, **- la** clave se utiliza para hacer las correcciones a las configuraciones. Aquí tiene un ejemplo:

Aquí, en vez de ingresar el **admin**, el usuario ingresa el **adminn** para corregirlo. En la guía siguiente, ingrese **-**, después haga clic ingresan. Las devoluciones del sistema al mensaje anterior.

```
(Cisco Controller)

Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System 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.
```

El REVESTIMIENTO no se registra con ISR WLCM - WLCM enviado con los Certificados incorrectos

Los NM-AIR-WLC6-K9 y los *NM-AIR-WLC6-K9=* WLCMs se envían con los Certificados incorrectos. Esto hace el WLCNM no ser autenticada por Cisco/Airespace APs. El WLCMs enviado entre el 1 de febrero de 2006 y de marzo el 22 de 2006 es afectado. Un error del proceso de fabricación no copió los Certificados correctos a los dispositivos WLCNM. El certificado incorrecto crea una discrepancia de clave RSA, que hace los APs LWAPP-basados fallar unirse a/socio/registro a WLCNM.

Consulte Notificación: El FN - 62379 - módulo de red inalámbrico del regulador LAN no autentica con Cisco/los Puntos de acceso de Airespace - actualización de hardware para más información sobre esto. Este Field Notice contiene la solución alternativa, así como los numeros de parte y los números de serie afectados del módulo de red.

El REVESTIMIENTO no se registra con el WLCM - Tiempo del sistema no fijado

El WLCM tiene que ser configurado con el Tiempo del sistema y la fecha. Puede o ser hecho manualmente, o el WLCM se puede configurar para utilizar al servidor NTP. Si la Fecha y hora no se fija, los revestimientos no se registran con el WLCM. En el Asisitente CLI, le incitan ingresar el Tiempo del sistema y la fecha. Si usted no ingresa la fecha y hora, usted ve este mensaje de advertencia:

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

Publique este comando del WLCM CLI para configurar el tiempo manualmente:

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

Publique este comando si usted quisiera que el WLCM utilizara al servidor NTP:

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

Recuperación de contraseña para el WLCM

Cuando la contraseña a abrirse una sesión al WLCM se pierde, la única forma de conseguir en el WLCM es reajustar el WLCM de nuevo a las configuraciones por defecto. Esto también significa que la configuración entera en el WLCM está reajustada y tiene que ser configurada a partir de cero.

Refiérase reajustan el WLCM a las configuraciones por defecto para la información sobre cómo reajustar el WLCM a los valores por defecto de la fábrica.

Cisco WLCM LED

Esta tabla enumera Cisco WLCM LED y los significados:

LED	Significado
CF	La placa de memoria de CompactFlash es activa.
EN	El módulo ha pasado el autoexamen y está disponible para el router.
PWR	La potencia está disponible para el módulo del regulador.

La mejora del firmware del controlador falla

Durante el proceso de actualización, usted puede parecer algunos errores que afecten al proceso de actualización. Esta sección explica lo que el medio de los mensajes de error y cómo eliminar los errores y actualizar el regulador.

- **Transferencia de archivo de código fallar-ninguna contestación del servidor TFTP** — usted recibe este mensaje de error si el servidor TFTP no es activo. Verifique si el servicio TFTP está habilitado en el servidor.
- **Code file transfer failed - Error from server: El fichero no fue encontrado. Abortando la transferencia** — Usted recibe este mensaje de error si el fichero OS no está presente en el directorio de valor por defecto del servidor TFTP. Para eliminar este error, copie el archivo de imagen al directorio de valor por defecto en el servidor TFTP.
- **TFTP Failure while storing in flash!** — Usted recibe este error cuando hay un problema con el servidor TFTP. Algunos servidores TFTP limitan el tamaño de los archivos que se pueden transferir. Utilice una diversa utilidad del servidor TFTP. Hay muchas utilidades libres del servidor TFTP que están disponibles. Cisco recomienda el uso Tftpd32 del servidor de la versión 2.0 TFTP. Refiera a Tftpd32 para descargar este servidor TFTP.
- **Se destruyen las divisiones del instalar o se corrompe la imagen** — si usted es todavía fracasado después de que una tentativa de actualizar el software, hay una posibilidad que su imagen está corrompida. Entre en contacto con el Soporte técnico de Cisco para la ayuda.

Refiera a actualizar el software del módulo del regulador de la red inalámbrica (WLAN) de Cisco

para más información sobre cómo actualizar los firmwares en el WLCM.

No puede activar el CDP

El usuario no puede activar el Cisco Discovery Protocol (CDP) en el WLCM instalado en los 3750 ISR. Este mensaje aparece:

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

El usuario publica el **comando cdp enable de los config** para activar el CDP, pero todavía ve este mismo mensaje:

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

Esto está debido al ID de bug CSCsg67615 de Cisco. Aunque el regulador inalámbrico integrado 3750G LAN no utilice el CDP, los comandos CLI CDP están disponibles para este regulador. Esto se resuelve en 4.0.206.0.

Utilice ayuda IP el direccionamiento y los comandos protocol IP-delanteros a los revestimientos del registro con el WLCM

Con el WLCM, es difícil que un REVESTIMIENTO descubra el WLCM con el broadcast de subred IP. Esto está debido a cómo el WLCM integra en la Placa posterior del ISR y cómo el REVESTIMIENTO está típicamente en una diversa subred IP (que sea también una buena recomendación). Si usted quiere realizar el descubrimiento del broadcast de subred IP con el éxito, publique los comandos **UDP 12223 del ayudante-direccionamiento IP** y del delantero-**protocolo IP**.

El propósito de estos comandos es generalmente remitir o retransmitir cualquier trama de broadcast IP del potencial. Esta retransmisión y la dirección de él a la interfaz de administración WLC deben ser adecuadas asegurarse de que el WLC responde de nuevo al REVESTIMIENTO.

El comando ip helper-address debe ser dado bajo interfaz con con el cual el REVESTIMIENTO está conectado, y el **comando ip helper-address** debe señalar a la interfaz de administración del WLC.

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

El comando ip forward-protocol es comando global configuration.

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

Comandos de Troubleshooting WLCM

Esta sección proporciona a los **comandos debug que** usted puede utilizar para resolver problemas la configuración WLCM.

Comandos Debug de verificar el REVESTIMIENTO que se registra con el regulador:

Utilice estos **comandos debug** para verificar si los revestimientos se registran con el WLCM:

- **ponga a punto el <AP-MAC-direccionamiento xx addr del mac: xx: xx: xx: xx: xx>** — Configura el depuración de la dirección MAC para el REVESTIMIENTO.
- **permiso de los eventos del lwapp de la depuración** — Configura la depuración de los eventos LWAPP y de los mensajes de error.
- **permiso del pki de la depuración P.M.** — Configura la depuración del módulo del encargado de la política de seguridad.

Aquí está una salida de ejemplo del **comando debug lwapp events enable** cuando el REVESTIMIENTO se registra con el 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
```

Aquí está una salida de ejemplo del **comando debug pm pki enable** cuando el REVESTIMIENTO se registra con el 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: ssphmUserCertVerify: calling x509_decode()
 Mon Mar 12 16:30:40 2007: ssphmUserCertVerify: 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: ssphmUserCertVerify: calling x509_decode()
 Mon Mar 12 16:30:40 2007: ssphmUserCertVerify: user cert verfied 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 <cscoDefaultIdCert>
 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
>cscoDefaultNewRootCaCert<
 Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 5, CA cert >cscoDefaultMfgCaCert<
```

```
 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 >cscoDefaultIdCert<
 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
>cscoDefaultNewRootCaCert<
 Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 5, certname
>cscoDefaultMfgCaCert<
 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
>cscoDefaultIdCert<
 Mon Mar 12 16:30:44 2007: ssphmPublicKeyEncrypt: called to encrypt 16 bytes
 Mon Mar 12 16:30:44 2007: ssphmPublicKeyEncrypt: 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
>cscoDefaultIdCert<
 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
```

Comandos Debug de verificar la autenticación Web:

Utilice estos **comandos debug** para verificar si la autenticación Web trabaja como se esperaba en el WLCM:

- **ponga a punto el aaa todo el permiso** — Configura la depuración de todos los mensajes AAA.
- **permiso del estado PEM de la depuración** — Configura la depuración de la máquina de estado del encargado de la directiva.
- **permiso de los eventos PEM de la depuración** — Configura la depuración de los eventos del encargado de la directiva.
- **permiso de la depuración P.M. SSH-appgw** — Configura la depuración de los gatewayes de aplicación.
- **permiso de la depuración P.M. SSH-TCP** — Configura la depuración de la dirección tcp del encargado de la directiva.

Aquí están las salidas de muestra de algunos de estos **comandos debug**:

```
(Cisco Controller) >debug aaa all enable

User user1 authenticated
00:40:96:ac:e6:57 Returning AAA Error 'Success' (0) for mobile 00:40:96:ac:e6:57
AuthorizationResponse: 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-Identifier......0x00000001 (1) (4 bytes)
00:40:96:ac:e6:57 Applying new AAA override for station 00:40:96:ac:e6:57
00:40:96: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: -1
dataAvgC: -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-Identifier....................0x574c4331 (1464615729) (4 bytes)
      AVP[05] Airespace / WLAN-Identifier......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-Identifier....................0x574c4331 (1464615729) (4 bytes)
      AVP[05] Airespace / WLAN-Identifier......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 enable
```

```
Fri 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 stateto 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 stateto 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 stateto WEBAUTH_REQD (8)

(Cisco Controller) >debug pem events enable

Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
START (0) Initializing policy
Fri 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:d0
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8) Adding TMP rule
Fri 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 = 1506
Fri 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 27
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57
Adding Web RuleID 28 for mobile 00:40:96:ac:e6:57
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8)Adding TMP rule
Fri 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 = 1506
Fri 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 8
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Added NPU entry of type 8
```

Comandos Debug de verificar la operación DHCP:

Utilice estos **comandos debug** para controlar el Cliente de DHCP y las actividades del servidor:

- **ponga a punto el permiso del mensaje DHCP** — Información de debugging de las visualizaciones sobre las actividades del Cliente de DHCP y vigilar el estatus de los paquetes del DHCP.
- **permiso del paquete DHCP de la depuración** — Información del nivel del paquete del DHCP de las visualizaciones.

Aquí están las salidas de muestra de estos **comandos debug**:

```
(Cisco Controller) >debug dhcp message enable
00:40:96:ac:e6:57 dhcp option len,including the magic cookie = 64
00:40:96:ac:e6:57 dhcp option: received DHCP REQUEST msg
00:40:96:ac:e6:57 dhcp option: skipping option 61, len 7
00:40:96:ac:e6:57 dhcp option: requested ip = 10.0.0.1
00:40:96:ac:e6:57 dhcp option: skipping option 12, len 3
00:40:96:ac:e6:57 dhcp option: skipping option 81, len 7
00:40:96:ac:e6:57 dhcp option: vendor class id = MSFT5.0 (len 8)
00:40:96:ac:e6:57 dhcp option: skipping option 55, len 11
00:40:96:ac:e6:57 dhcpParseOptions: options end, len 64, actual 64
00:40:96: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 10.0.0.50
00:40:96:ac:e6:57 dhcp option len, including the magic cookie = 64
00:40:96:ac:e6:57 dhcp option: received DHCP ACK msg
00:40:96:ac:e6:57 dhcp option: server id = 10.0.0.50
00:40:96:ac:e6:57 dhcp option: lease time (seconds) =86400
00:40:96:ac:e6:57 dhcp option: skipping option 58, len 4
00:40:96:ac:e6:57 dhcp option: skipping option 59, len 4
00:40:96:ac:e6:57 dhcp option: skipping option 81, len 6
00:40:96:ac:e6:57 dhcp option: netmask = 255.0.0.0
00:40:96:ac:e6:57 dhcp option: gateway = 10.0.0.50
00:40:96:ac:e6:57 dhcpParseOptions: options end, len 64, actual 64

(Cisco Controller) >debug dhcp packet enable

Fri 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: 0xec03
Fri 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: 1
Fri 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: 30
Fri 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: 1
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP Message Type received: DHCP REQUEST msg
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   op: BOOTREQUEST,
```

```
htype: Ethernet,hlen: 6, hops: 1
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   xid: 1674228912, secs: 0, flags: 0
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   chaddr: 00:40:96:ac:e6:57
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   ciaddr: 10.0.0.1,  yiaddr: 0.0.0.0
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   siaddr: 0.0.0.0,  giaddr: 10.0.0.10
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57 DHCP request to 10.0.0.50,
len 350,switchport 1, vlan 30
Fri 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: 0xec00
Fri Mar  2 16:06:35 2007: DHCP Reply to AP client: 00:40:96:ac:e6:57,
frame len412, switchport 1
Fri 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: 0
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   xid: 1674228912, secs: 0, flags: 0
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   chaddr: 00:40:96:ac:e6:57
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   ciaddr: 10.0.0.1,  yiaddr: 10.0.0.1
Fri Mar  2 16:06:35 2007: 00:40:96:ac:e6:57   siaddr: 0.0.0.0,  giaddr: 0.0.0.0
Fri 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
```

Comandos Debug de verificar la mejora TFTP:

- **msglog de la demostración** — Visualiza los registros de mensajes escritos a la base de datos inalámbrica del regulador LAN de Cisco. Si hay más de 15 entradas, le incitan visualizar los mensajes mostrados en el ejemplo.
- **rastro de la transferencia de la depuración** — Configura la depuración de la transferencia o de la mejora.

Aquí está un ejemplo del **comando trace de la transferencia de la depuración**:

```
Cisco Controller) >debug transfer trace enable

(Cisco Controller) >transfer download start

Mode..................................... TFTP
Data Type................................ Code
TFTP Server IP........................... 172.16.1.1
TFTP Packet Timeout...................... 6
TFTP Max Retries......................... 10
TFTP Path................................ d:\WirelessImages/
TFTP Filename............................ AIR-WLC2006-K9-3-2-78-0.aes

This may take some time.
Are you sure you want to start? (y/n) y
Mon Feb 13 14:06:56 2006: RESULT_STRING: TFTP Code transfer starting.
Mon Feb 13 14:06:56 2006: RESULT_CODE:1

TFTP Code transfer starting.
Mon Feb 13 14:06:59 2006: Still waiting!  Status = 2
Mon Feb 13 14:07:00 2006: Locking tftp semaphore, pHost=172.16.1.1
pFilename=d:\WirelessImages/AIR-WLC2006-K9-3-2-78-0.aes
Mon 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.aes
Mon Feb 13 14:07:00 2006: Semaphore successfully unlocked, pHost=172.16.1.1
pFilename=d:\WirelessImages/AIR-WLC2006-K9-3-2-78-0.aes
Mon Feb 13 14:07:02 2006: Still waiting!  Status = 1
Mon Feb 13 14:07:05 2006: Still waiting!  Status = 1
Mon Feb 13 14:07:08 2006: Still waiting!  Status = 1
Mon Feb 13 14:07:11 2006: Still waiting!  Status = 1
Mon Feb 13 14:07:14 2006: Still waiting!  Status = 1
```

```
Mon Feb 13 14:07:17 2006: Still waiting!  Status = 1
Mon 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.tgz
Mon Feb 13 14:07:19 2006: tftp = 6, file_name=d:\WirelessImages/
AIR-WLC2006-K9-3-2-78-0.aes, ip_address=172.16.1.1
Mon 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:6

TFTP receive complete... extracting components.
Mon Feb 13 14:07:20 2006: Still waiting!  Status = 2
Mon Feb 13 14:07:23 2006: Still waiting!  Status = 1
Mon Feb 13 14:07:23 2006: Still waiting!  Status = 1
Mon Feb 13 14:07:23 2006: Still waiting!  Status = 1
Mon 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 = 2
Mon Feb 13 14:07:29 2006: Still waiting!  Status = 1
Mon 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 = 2
Mon 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 = 2
Mon 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 = 2
Mon Feb 13 14:07:41 2006: Still waiting!  Status = 1
Mon 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 = 2
Mon Feb 13 14:07:47 2006: Still waiting!  Status = 1
Mon 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 = 2
Mon 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 = 2
Mon Feb 13 14:07:53 2006: Still waiting!  Status = 1
Mon Feb 13 14:07:53 2006: Still waiting!  Status = 1
Mon Feb 13 14:07:53 2006: Still waiting!  Status = 1
Mon Feb 13 14:07:53 2006: Still waiting!  Status = 1
Mon 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 = 2
Mon 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 = 2
Mon 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 = 2
Mon 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 = 2
Mon Feb 13 14:08:08 2006: ummounting: <umount /mnt/download/>  cwd  = /mnt/application
Mon Feb 13 14:08:08 2006: finished umounting
```

Comandos Debug para ocultar 802.1X/WPA/RSN/PMK:

- **la depuración dot1x todo activa** — Visualiza la información de debugging del 802.1x.Aquí está una salida de muestra de este comando:

```
(Cisco Controller) >debug dot1x all enable

Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_USER_NAME(1) index=0
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_CALLING_STATION_ID(31) index=1
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_CALLED_STATION_ID(30) index=2
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_PORT(5) index=3
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_IDENTIFIER(32) index=5
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_VAP_ID(1) index=6
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_SERVICE_TYPE(6) index=7
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_FRAMED_MTU(12) index=8
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_EAP_MESSAGE(79) index=10
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_MESS_AUTH(80) index=11
Fri 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:e6:57
Fri 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:e6:57
Fri 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                          EAPUSER1
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Skipping AVP (0/80) for mobile 00:40:96:ac:e6:57
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_USER_NAME(1) index=0
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_CALLING_STATION_ID(31) index=1
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_CALLED_STATION_ID(30) index=2
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_PORT(5) index=3
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
```

```
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_IDENTIFIER(32) index=5
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_VAP_ID(1) index=6
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_SERVICE_TYPE(6) index=7
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_FRAMED_MTU(12) index=8
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_EAP_MESSAGE(79) index=10
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_MESS_AUTH(80) index=11
Fri 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:e6:57
Fri 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:e6:57
Fri 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:e6:57
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_USER_NAME(1) index=0
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_CALLING_STATION_ID(31) index=1
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_CALLED_STATION_ID(30) index=2
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_PORT(5) index=3
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_IDENTIFIER(32) index=5
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_VAP_ID(1) index=6
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_SERVICE_TYPE(6) index=7
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_FRAMED_MTU(12) index=8
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_EAP_MESSAGE(79) index=10
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_MESS_AUTH(80) index=11
Fri 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
```

- la depuración dot11 todo activa — Activa el depuración de las funciones de radio.
- muestre a cliente el *<mac>* sumario — Las visualizaciones resumieron la información para el cliente por la dirección MAC.Aquí está una salida de muestra de este comando:

```
(Cisco Controller) >show client summary

Number of Clients.............................. 1

MAC Address        AP Name            Status         WLAN  Auth  Protocol  Port
-----------------  -----------------  -------------  ----  ----  --------  ----
```

```
00:40:96:ac:e6:57  AP0015.63e5.0c7e   Associated     1     Yes   802.11a   1
```

Información Relacionada

- Referencia inalámbrica del comando controller LAN de Cisco
- Guía de funciones del módulo de red del regulador de la red inalámbrica (WLAN) de Cisco
- Ejemplos inalámbricos de la configuración del módulo del regulador LAN (WLCM)
- Ejemplo de Configuración de la Autenticación Web del Controlador LAN Inalámbrico
- Ejemplo de Configuración de Autenticación de EAP con Controladores de WLAN (WLC)
- Soporte Técnico y Documentación - Cisco Systems