

无线局域网控制器模块故障排除

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[背景信息](#)

[故障排除](#)

[ISR无法识别WLCM](#)

[能否升级WLCM上的闪存？](#)

[WLCM是否可热插拔？](#)

[WLCM上支持的LAP](#)

[无法访问WLCM上的快速以太网](#)

[检查WLCM的状态](#)

[如何在CLI配置向导中进行更正](#)

[LAP不向ISR WLCM注册 — WLCM随附不正确的证书](#)

[LAP未注册到WLCM — 系统时间未设置](#)

[WLCM的口令恢复](#)

[思科WLCM LED](#)

[控制器固件升级失败](#)

[无法启用CDP](#)

[使用ip-helper address和ip-forward protocol命令向WLCM注册LAP](#)

[WLCM故障排除命令](#)

[相关信息](#)

简介

本文档提供思科无线局域网控制器模块(WLCM)基本问题的故障排除步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 了解轻量接入点协议 (LWAPP)。
- 有关如何配置WLCM模块以参与思科统一无线网络的基本知识。**注：**如果您是新用户，并且尚未使用WLCM，请参阅《[思科WLAN控制器网络模块功能指南](#)》。

[使用的组件](#)

本文档中的信息基于以下软件和硬件版本：

- 运行版本12.4(11)T的思科2811集成多业务路由器(ISR)和运行版本3.2.116.21的WLCM
- Cisco 1030和Cisco 1232 AG轻量AP(LAP)
- 运行版本2.5的思科802.11a/b/g无线局域网(WLAN)客户端适配器
- 运行版本3.2的思科安全访问控制服务器(ACS)

注意：此处列出的组件仅是用于编写本文档的设备。本文档的故障排除部分提供了支持WLCM的ISR和WLCM支持的LAP的完整列表信息。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

[规则](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

[背景信息](#)

Cisco WLCM旨在为中小型企业(SMB)和企业分支机构客户提供适用于Cisco 2800和Cisco 3800系列ISR和Cisco 3700系列路由器的802.11无线网络解决方案。

Cisco WLCM使Cisco ISR和Cisco 3700系列路由器能够管理最多六个WLAN接入点(AP)，并简化WLAN的部署和管理。操作系统管理所有数据客户端、通信和系统管理功能，执行无线电资源管理(RRM)功能，使用操作系统安全(OSS)管理系统范围的移动策略，并使用OSS框架协调所有安全功能。

Cisco WLCM与Cisco Aironet LAP、思科无线控制系统(WCS)和思科无线位置设备配合使用，可支持任务关键型无线数据、语音和视频应用。

[故障排除](#)

本节讨论WLCM基本问题的故障排除步骤。

[ISR无法识别WLCM](#)

WLCM仅在以下ISR平台上受支持：

- Cisco 3725 和 3745 路由器
- Cisco 2811、2821 和 2851 ISR
- Cisco 3825 和 3845 ISR

如果显示除此列表中指定的ISR之外的任何其他ISR，则不会检测到WLCM。确保使用正确的硬件。

注意： WLCM仅在网络模块插槽中受支持。Cisco 2821 和 Cisco 2851 ISR 中的 EVM 插槽不支持此模块。

注意： 在单个路由器机箱中只能安装一个Cisco WLCM。

WLCM还有一些最低软件要求。

ISR必须使用Cisco IOS[®]软件版本12.4(2)XA1 (路由器软件) 或更高版本 , ISR才能识别WLCM。

能否升级WLCM上的闪存 ?

Cisco WLCM随附并从已安装的256 MB闪存卡启动。CompactFlash内存卡包含启动加载器、Linux内核、Cisco WLCM和AP可执行文件以及Cisco WLCM配置。

Cisco WLCM中的CompactFlash内存卡不可现场更换。

WLCM是否可热插拔 ?

WLCM不能在所有ISR平台上热插拔。仅Cisco 3745路由器和Cisco 3845 ISR支持控制器模块的在线插拔(OIR)。

WLCM上支持的LAP

支持所有支持LWAPP的Cisco Aironet AP , 包括Cisco Aironet 1000、1100和1200系列。不支持HWIC-AP接口卡。

无法访问WLCM上的快速以太网

这是预料之中的行为。Cisco WLCM面板上的外部快速以太网端口不受支持。NM-WLC (WLCM模块) 只有一个快速以太网端口在内部连接到主机路由器 , 并且NM面板上的外部快速以太网端口被禁用且不可用。

检查WLCM的状态

从ISR发出**show version**命令 , 以检查路由器是否识别WLCM并正确安装。

```
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-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/wvl/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

发出**service-module wlan-controller slot/port status**命令以查找WLCM的状态。

```
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

您还可以发出**service-module wlan-controller 1/0 statistics**命令以查找WLCM的模块重置统计信息。

```
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
```

在某些情况下，您会看到以下错误：

```
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
```

出现此错误的原因也许是硬件问题。打开TAC案例以进一步排除此问题。要提交TAC案例，您需要与思科签订有效的合同。要联系Cisco TAC，请参阅[技术支持](#)。

发出**show sysinfo**命令以接收有关WLCM的详细信息。

(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
```

[如何在CLI配置向导中进行更正](#)

使用CLI配置向导首次（或重置为默认值后）配置WLCM时，使用-key对配置进行更正。示例如下：

在此，用户不输入admin，而是输入admin进行更正。在下一个提示符下，输入—，然后单击Enter。系统将返回上一个提示符。

(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.

[LAP不向ISR WLCM注册 — WLCM随附不正确的证书](#)

NM-AIR-WLC6-K9和NM-AIR-WLC6-K9=WLCM随附不正确的证书。这会导致WLCNM不由Cisco/Airespace AP进行身份验证。2006年2月1日至2006年3月22日之间发货的WLCM受到影响。制造流程故障未将正确的证书复制到WLCNM设备。不正确的证书会导致RSA密钥不匹配，这会导致基于LWAPP的AP无法加入/关联/注册到WLCNM。

有关此问题的示例，请参阅 [Field Notice : FN - 62379 — 无线LAN控制器网络模块不通过Cisco/Airespace接入点进行身份验证 — 硬件升级](#)，以了解有关此的详细信息。本“现场通知”包含解决方法以及受影响的网络模块部件号和序列号。

[LAP未注册到WLCM — 系统时间未设置](#)

WLCM必须配置系统时间和日期。可以手动完成，也可以将WLCM配置为使用NTP服务器。如果未设置时间和日期，则LAP不向WLCM注册。在CLI向导中，系统会提示您输入系统时间和日期。如果不输入日期和时间，您将看到以下警告消息：

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

从WLCM CLI发出以下命令以手动配置时间：

```
(Cisco Controller) >config time manual <MM/DD/YY> <HH:MM:SS>
```

如果希望WLCM使用NTP服务器，请发出以下命令：

```
config time ntp server <index> <IP Address>
```

WLCM的口令恢复

丢失 WLCM 的登录口令时，进入 WLCM 的唯一方法是将 WLCM 重置回默认设置。这也意味着将重置 WLCM 中的整个配置，并且必须从头开始配置。

有关如何[将WLCM重置为出厂默认](#)值的信息，请参阅[将WLCM重置为默认设置](#)。

思科WLCM LED

下表列出了Cisco WLCM LED及其含义：

LED	含义
CF	CompactFlash内存卡处于活动状态。
企业	该模块已通过自检，可供路由器使用。
电源	控制器模块可用电源。

控制器固件升级失败

在升级过程中，您可能会遇到一些影响升级过程的错误。本节介绍错误消息的含义以及如何消除错误并升级控制器。

- **代码文件传输失败 - No reply from the TFTP server** — 如果TFTP服务器不活动，您会收到此错误消息。请检查以确定是否在服务器上启用了TFTP服务。
- **Code file transfer failed - Error from server:找不到文件。Aborting transfer** — 如果OS文件不在TFTP服务器的默认目录中，您会收到此错误消息。要消除此错误，请将映像文件复制到TFTP服务器上的默认目录。
- **TFTP Failure while storing in flash!** — 当TFTP服务器出现问题时，您会收到此错误。一些TFTP服务器对于可以传输的文件大小有限制。使用其他TFTP服务器实用程序。有许多免费的TFTP服务器实用程序可用。思科建议使用Tftpd32 2.0版TFTP服务器。要下载此TFTP服务器，请参阅[Tftpd32](#)。
- **安装分区已销毁或映像已损坏** — 如果在尝试升级软件后仍未成功，则可能是映像已损坏。请[联系思科技术支持](#)。

有关如何[升级WLCM上的固件的详细信息](#)，请参阅升级Cisco WLAN控制器模块软件。

[无法启用CDP](#)

用户无法在3750 ISR上安装的WLCM上启用思科发现协议(CDP)。将显示以下消息：

```
(Cisco Controller) >show cdp neighbors
% CDP is not enabled
```

用户发出`config cdp enable`命令以启用CDP，但仍然看到以下相同消息：

```
(Cisco Controller) >show cdp neighbors
% CDP is not enabled
```

这是由于Cisco Bug ID CSCsg67615。尽管3750G集成无线局域网控制器不支持CDP，但CDP CLI命令可用于此控制器。这在4.0.206.0中解决。

[使用ip-helper address和ip-forward protocol命令向WLCM注册LAP](#)

使用WLCM时，LAP很难通过IP子网广播发现WLCM。这是因为WLCM如何集成在ISR的后面板上，以及LAP通常位于不同的IP子网上（这也是一个很好的建议）。如果要成功执行IP子网广播发现，请发出`ip helper-address`和`ip forward-protocol udp 12223`命令。

通常，这些命令的目的是转发或中继任何潜在的IP广播帧。此中继并将其定向到WLC管理接口应足以确保WLC回复到LAP。

必须在LAP所连接的接口下提供`ip helper-address`命令，并且`ip helper-address`命令必须指向WLC的管理接口。

```
ip helper-address <Management Interface of the WLC>
```

`ip forward-protocol`命令是全局配置命令。

```
ip forward-protocol udp 12223
```

[WLCM故障排除命令](#)

本部分提供可用于排除WLCM配置故障的`debug`命令。

用于验证LAP向控制器注册的调试命令：

使用以下`debug`命令验证LAP是否向WLCM注册：

- `debug mac addr <AP-MAC-address xx:xx:xx:xx:xx:xx>` — 配置LAP的MAC地址调试。
- `debug lwapp events enable` — 配置LWAPP事件和错误消息的调试。
- `debug pm pki enable` — 配置安全策略管理器模块的调试。

以下是当LAP向WLCM注册时`debug lwapp events enable`命令的示例输出：

```
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, gw 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

以下是当LAP向WLCM注册时debug pm pki enable命令的输出示例：

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 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: **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
>cscsDefaultIdCert<
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

```

用于验证Web身份验证的调试命令：

使用以下debug命令验证Web身份验证在WLCM上是否按预期工作：

- debug aaa all enable - 配置所有 AAA 消息的调试。
- debug pem state enable — 配置策略管理器状态机的调试。
- debug pem events enable — 配置策略管理器事件的调试。
- debug pm ssh-appgw enable — 配置应用程序网关的调试。
- debug pm ssh-tcp enable — 配置策略管理器 tcp 处理的调试。

下面是其中一些 debug 命令的输出范例：

```
(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 state to 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
```

用于检验DHCP运行的调试命令：

使用以下**debug**命令检查DHCP客户端和服务端活动：

- **debug dhcp message enable** — 显示有关DHCP客户端活动的调试信息并监控DHCP数据包的状态。
- **debug dhcp packet enable** — 显示DHCP数据包级别信息。

以下是这些debug命令的示例输出：

```
(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
```

用于检验TFTP升级的调试命令：

- **show msglog** — 显示写入思科无线局域网控制器数据库的消息日志。如果有15个以上的条目，系统会提示您显示示例中显示的消息。
- **debug transfer trace** — 配置传输或升级的调试。

以下是debug transfer trace命令的示例：

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

```

用于802.1X/WPA/RSN/PMK缓存的调试命令：

- **debug dot1x all enable** — 显示802.1X调试信息。以下是此命令的输出示例：

```
(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 d08..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
```

- **debug dot11 all enable** — 启用无线电功能的调试。
- **show client summary<mac>** — 按MAC地址显示客户端的汇总信息。以下是此命令的输出示例

```
:
(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
```

[相关信息](#)

- [Cisco 无线 LAN 控制器命令参考](#)
- [Cisco WLAN 控制器网络模块功能指南](#)
- [无线局域网控制器模块\(WLCM\)配置示例](#)
- [无线局域网控制器 Web 身份验证配置示例](#)
- [WLAN 控制器 \(WLC\) 中 EAP 身份验证的配置示例](#)
- [技术支持和文档 - Cisco Systems](#)