

Устранение неполадок модуля контроллера беспроводной LAN

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Общие сведения](#)

[Устранение неполадок](#)

[ISR не распознает WLCM](#)

[Я могу обновить Флэш на WLCM?](#)

[WLCM с возможностью горячего подключения без перезагрузки?](#)

[LAP, поддерживаемые на WLCM](#)

[Неспособный обратиться к Fast Ethernet на WLCM](#)

[Проверьте статус WLCM](#)

[Как делаем мы делаем исправления в мастере настройки CLI](#)

[LAP не регистрирует в ISR WLCM - WLCM, поставленный с неправильными сертификатами](#)

[LAP Не регистрируется в WLCM - "Not set" Системного времени](#)

[Восстановление пароля для WLCM](#)

[Cisco светодиоды WLCM](#)

[Обновление сбоев микропрограммы контроллера](#)

[Не может включить CDP](#)

[Используйте адрес IP-помощника и IP прямой протокол Команды для Регистрации LAP в WLCM](#)

[Команды устранения проблем WLCM](#)

[Дополнительные сведения](#)

Введение

Этот документ излагает порядок устранения типичных проблем с модулем контроллера беспроводной сети Cisco (WLCM).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Знание протокола LWAPP.
- Базовые знания о том, как настроить модуль WLCM для участия в единой беспроводной сети Cisco (UWN). **Примечание:** Если вы - новый пользователь и не работали на WLCM, обратитесь к [Руководству по функциям и свойствам Сетевого модуля контроллера беспроводной локальной сети Cisco](#).

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Маршрутизатор Cisco ISR 2811 (ISR), который выполняет версию 12.4 (11) T с WLCM, который выполняет версию 3.2.116.21
- Cisco 1030 и AP легкого веса AG Cisco 1232 (LAP)
- Беспроводная локальная сеть Cisco 802.11a/b/g (WLAN) Клиентский адаптер, который выполняет версию 2.5
- Сервер Cisco Secure Access Control Server (ACS), который выполняет версию 3.2

Примечание: Компоненты, перечисленные здесь, являются только устройствами, которые использовались для записи этого документа. Информация о полном списке ISR, которые поддерживают WLCM и LAP, которые поддерживаются на WLCM, предоставлена в разделе [Устранения неполадок](#) этого документа.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

Общие сведения

Cisco WLCM разработана для обеспечения малых и средних компаний (SMB) и клиенты филиала организации с решениями для беспроводной сети 802.11 для Cisco 2800 и Cisco ISR серии 3800 и Маршрутизаторы серии Cisco 3700.

Cisco WLCM позволяет ISR Cisco и Маршрутизаторам серии Cisco 3700 управлять до шести Точек доступа WLAN (AP), и упрощает развертывания и управление WLAN. Операционная система управляет всем клиентом данных, связью и функциями администрирования системы, выполняет функции Управления радиоресурсами (RRM), управляет политикой мобильности в масштабе всей системы с помощью защиты операционной системы (OSS) и координирует все функции защиты с помощью платформы OSS.

Cisco WLCM работает в сочетании с LAP Cisco Aironet, Cisco Wireless Control System (WCS) и устройство Cisco Wireless Location Appliance для поддержки критически важных беспроводных данных, голоса и видеоприложений.

Устранение неполадок

В этом разделе рассматриваются процедуры устранения проблем для основных проблем с WLCM.

ISR не распознает WLCM

WLCM поддерживается только на этих платформах ISR:

- Маршрутизаторы Cisco 3725 и 3745
- Маршрутизаторы ISR Cisco 2811, 2821 и 2851
- Маршрутизаторы ISR Cisco 3825 и 3845

Если какой-либо другой ISR, чем те заданные в этом списке появляется, то WLCM не обнаружен. Гарантируйте использование корректных аппаратных средств.

Примечание: WLCM поддерживается только в слотах сетевого модуля. Он не поддерживается в слотах EVM, доступных в маршрутизаторах ISR Cisco 2821 и Cisco 2851.

Примечание: Можно установить только одну Cisco WLCM в шасси одиночного маршрутизатора.

Существуют также некоторые минимальные требования к программному обеспечению для WLCM.

ISR должен использовать Выпуск 12.4 (2) XA1 программного обеспечения Cisco IOS (программное обеспечение маршрутизатора) или позже для ISR для распознавания WLCM.

Я могу обновить Флэш на WLCM?

Cisco WLCM отправляет с и загружается с установленной карты памяти CompactFlash на 256 МБ. Карта памяти CompactFlash содержит программу загрузки, Ядро Linux, Cisco WLCM и исполняемый файл AP и Cisco конфигурация WLCM.

Карта памяти CompactFlash в Cisco WLCM не заменима полем.

WLCM с возможностью горячего подключения без перезагрузки?

WLCM не находится с возможностью горячего подключения без перезагрузки на всех платформах ISR. Оперативная установка и демонтаж модуля контроллера поддерживается только на маршрутизаторе Cisco 3745 и ISR Cisco 3845.

LAP, поддерживаемые на WLCM

Все поддерживающие LWAPP AP Cisco Aironet поддерживаются, который включает Cisco Aironet 1000, 1100, и серии 1200. Интерфейсные карты AP HWIC не поддерживаются.

Неспособный обратиться к Fast Ethernet на WLCM

Это ожидаемое поведение. Внешний Порт Fast Ethernet на заглушке Cisco WLCM не

поддерживается. WLC NM (модуль WLCM) имеет только один Порт Fast Ethernet, внутренне связанный с узловым маршрутизатором, и внешний Порт Fast Ethernet на заглушке NM отключен и неприменим.

[Проверьте статус WLCM](#)

Выполните команду **Show version** от ISR, чтобы проверить, распознан ли WLCM маршрутизатором и установлен правильно.

```
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
```

Выполните команду **service-module wlan-controller slot/port status** для обнаружения статуса 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
```

Можно также выполнить команду **service-module wlan-controller 1/0 statistics** для обнаружения

статистики сброса модуля 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
```

В некоторых случаях вы видите эту ошибку:

```
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
```

Причина для этой ошибки могла бы быть проблемой аппаратных средств. Откройте кейс ТАС (Центра технической поддержки) для дальнейшего устренения этой проблемы. Для открытия кейса ТАС (Центра технической поддержки) у вас должен быть корректный контракт с Cisco. См. [Техническую поддержку](#) для контакта с Центром технической поддержки Cisco.

Выполните команду **show sysinfo** для получения дополнительных сведений о 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
```

[Как делают мы делаем исправления в мастере настройки CLI](#)

При настройке WLCM впервые (или после сброса к настройкам по умолчанию) использование мастера настройки CLI, - ключ используется для создания исправлений к

конфигурациям. Ниже представлен пример:

Здесь, вместо того, чтобы ввести **admin**, пользователь вводит **admin** для исправления его. В следующем приглашении войдите - тогда нажмите, входят. Система возвращается к предыдущему приглашению.

(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 не регистрирует в ISR WLCM - WLCM, поставленный с неправильными сертификатами](#)

NM-AIR-WLC6-K9 и *NM-AIR-WLC6-K9* = WLCMs поставлены с неправильными сертификатами. Это заставляет WLCNM не аутентифицироваться AP Cisco/Airespace. На WLCMs, поставленные между 1 февраля 2006 и 22 марта 2006, влияют. Сбой производственного процесса не скопировал корректные сертификаты к устройствам WLCNM. Неправильный сертификат создает основную несогласованность RSA, которая заставляет основанные на LWAPP AP быть не в состоянии присоединяться/привязывать/регистрировать к WLCNM.

[Для получения дополнительной информации см. следующее уведомление: FN - 62379 - Сетевой модуль Контроллера беспроводной локальной сети не Аутентифицируется с точками доступа Cisco/Airespace - Модернизация оборудования](#) для получения дополнительной информации об этом. Это Уведомление о дефекте содержит обходной путь, а также Номера изделия Сетевого модуля, на которые влияют, и Серийные номера.

[LAP Не регистрируется в WLCM - "Not set" Системного времени](#)

WLCM должен быть настроен с системным временем и датой. Это может или быть сделано вручную, или WLCM может быть настроен для использования сервера NTP. Если время и дата является "not set", LAP не регистрируются в WLCM. В мастере CLI вам предлагают ввести системное время и дату. Если вы не вводите дату и время, вы видите это предупреждающее сообщение:

Warning! No AP will come up unless the time is set

Please see documentation for more details.

Выполните эту команду от CLI WLCM для настройки времени вручную:

Warning! No AP will come up unless the time is set

Please see documentation for more details.

Выполните эту команду, если вы хотите, чтобы WLCM использовал сервер NTP:

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

[Восстановление пароля для WLCM](#)

Когда пароль для входа в систему к WLCM потерян, единственный способ войти в WLCM состоит в том, чтобы перезагрузить WLCM назад к настройкам по умолчанию. Это также означает, что полная конфигурация на WLCM перезагружена и должна быть настроена с нуля.

См. [Сброс WLCM к Настройкам по умолчанию](#) для получения информации о том, как перезагрузить WLCM к заводским настройкам.

[Cisco светодиоды WLCM](#)

Эта таблица приводит Cisco светодиоды WLCM и значения:

СВЕТОДИОД	Значение
CF	Карта памяти CompactFlash активна.
EN	Модуль передал самопроверку и доступен маршрутизатору.
PWR	Питание доступно модулю контроллера.

[Обновление сбоев микропрограммы контроллера](#)

Во время процесса обновления можно столкнуться с некоторыми ошибками, которые влияют на процесс обновления. Этот раздел объясняет, что среднее значение сообщений об ошибках и как устранить ошибки и обновить контроллер.

- **Передача файла кодов отказала - никакой ответ от сервера TFTP** — Вы получаете это сообщение об ошибках, если сервер TFTP не активен. Проверьте, чтобы определить, включен ли Сервис TFTP на сервере.
- **Передача файла кодов отказала - Ошибка от сервера: Файл не был найден.** Если файл ОС не присутствует в каталоге по умолчанию сервера TFTP, **при прерывании передачи** — Вы получаете это сообщение об ошибках. Для устранения этой ошибки скопируйте графический файл к каталогу по умолчанию на сервере TFTP.
- **Сбой TFTP при хранении во флэш-памяти!** Когда существует проблема с сервером TFTP — вы получаете эту ошибку. У некоторых TFTP-серверов могут быть ограничения на размер передаваемых файлов. Используйте другую утилиту сервера TFTP. Существует много свободных утилит сервера TFTP, которые доступны. Cisco рекомендует использование сервера TFTP версии 2.0 Tftpd32. См. [Tftpd32](#) для загрузки этого сервера TFTP.
- **Отделения установки уничтожены, или образ поврежден** — Если вы все еще неуспешны после попытки обновить программное обеспечение, существует возможность, что поврежден ваш образ. [Обратитесь в техническую поддержку Cisco](#) для помощи.

См. [Обновление Программного обеспечения модуля контроллера беспроводной локальной сети Cisco](#) для получения дополнительной информации о том, как обновить

микропрограммное обеспечение на WLCM.

Не может включить CDP

Пользователь не может включить протокол CDP на WLCM, установленном на 3750 ISR. Будет отображено следующее сообщение:

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

Пользователь выполняет команду **config cdp enable**, чтобы включить CDP, но все еще видит это то же сообщение:

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

Это вызвано тем, что идентификатора ошибки Cisco CSCsg67615. Несмотря на то, что 3750G Интегрированный Контроллер беспроводной локальной сети не поддерживает CDP, команды CLI CDP доступны для этого контроллера. Это решено в 4.0.206.0.

Используйте адрес IP-помощника и IP прямой протокол Команды для Регистрации LAP в WLCM

С WLCM для LAP трудно обнаружить WLCM через широковещание IP-подсети. Это вызвано тем, что того, как WLCM интегрируется на соединительной панели ISR и как LAP, как правило, находится на другой IP-подсети (который является также хорошей рекомендацией). Если вы хотите выполнить широковещательное обнаружение IP-подсети с успехом, выполнить команды **ip helper-address** и **ip forward-protocol udp 12223**.

В целом цель этих команд состоит в том, чтобы передать или реле любой потенциальный кадр IP - трансляции. Это реле и направление его к интерфейсу управления WLC должны соответствовать, чтобы удостовериться, что WLC назад отвечает на LAP.

Команда **ip helper-address** должна быть дана под интерфейсом, к которому LAP связан с, и команда **ip helper-address** должна указать к интерфейсу управления WLC.

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

Команда **ip forward-protocol** является командой глобальной конфигурации.

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

Команды устранения проблем WLCM

Этот раздел предоставляет команды отладки, которые можно использовать для устранения проблем конфигурации WLCM.

Команды отладки для проверки LAP, регистрирующегося в контроллере:

Используйте эти команды отладки, чтобы проверить, регистрируются ли LAP в WLCM:

- **адрес debug mac <Mac-address AP xx:xx:xx:xx:xx:xx>** — Настраивает отладку MAC-адреса для LAP.
- **debug lwapp events enable** отладку Событий lwapp и сообщений об ошибках.
- **debug pm pki enable** отладку менеджера политики безопасности модуль.

Когда LAP регистрируется в WLCM, вот пример выходных данных команды **debug lwapp events enable**:

```

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

```

Когда LAP регистрируется в WLCM, вот пример выходных данных команды **debug pm pki enable**:

```

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: 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

```

Команды отладки для проверки web-аутентификации:

Используйте эти команды отладки, чтобы проверить, работает ли web-аутентификация как ожидалось на WLCM:

- **debug aaa all enable** – настраивает отладку сообщений AAA.
- **debug pem state enable** - настраивает отладку конечного автомата менеджера политик.
- **debug pem events enable** - настраивает отладку событий менеджера политик.
- **debug pm ssh-appgw enable** - настраивает отладку шлюзов приложений.
- **debug pm ssh-tcp enable** – настраивает отладку обработки пакетов TCP менеджера политик.

Ниже приведен пример выходных данных некоторых команд 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
```

Команды отладки для проверки операции DHCP:

Используйте эти команды отладки для проверки клиента DHCP и функционирования сервера:

- **сообщение debug dhcp включает** — Отображает информацию об отладке о действиях клиента DHCP и контролировать статус пакетов DHCP.
- **debug dhcp packet enable** — Информация об уровне пакета DHCP Показов.

Вот примеры выходных данных этих команд отладки:

```
(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
```

Команды отладки для проверки обновления TFTP:

- **show msglog** — Отображает журналы сообщений, записанные в базу данных контроллера WLAN Cisco. Если существует больше чем 15 записей, вам предлагают отобразить сообщения, показанные в примере.
- **debug transfer trace** — Настраивает отладку передачи или обновления.

Вот пример команды debug transfer trace:

```
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**

Команды отладки для кэширования 802.1X/WPA/RSN/PMK:

- **debug dot1x**, которого все включают — Отображает информацию об отладке 802.1X. Вот пример выходных данных ЭТОЙ КОМАНДЫ: (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**, которого все включают — Включает отладку радио-функций.
- **show client summary <Mac>** — Отображает обобщенную информацию для клиента MAC-адресом. Вот пример выходных данных этой команды: (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

```

Дополнительные сведения

- [Справочник по командам контроллера беспроводной локальной сети Cisco](#)
- [Руководство по функциям модуля сетевого контроллера WLAN Cisco](#)
- [Примеры конфигурации модуля контроллера беспроводной LAN \(WLCM\)](#)
- [Пример настройки веб-аутентификации контроллера беспроводной LAN](#)
- [Пример конфигурации аутентификации EAP в контроллерах WLAN \(WLC\)](#)
- [Cisco Systems – техническая поддержка и документация](#)