무선 LAN 컨트롤러 모듈 문제 해결

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[표기 규칙](#)
[배경 정보](#)
[문제 해결](#)
[ISR에서 WLCM을 인식하지 못함](#)
[WLCM에서 플래시를 업그레이드할 수 있습니까?](#)
[WLCM 핫 스왑 가능 여부](#)
[WLCM에서 지원되는 LAP](#)
[WLCM에서 고속 이더넷에 액세스할 수 없음](#)
[WLCM의 상태 확인](#)
[CLI 컨피그레이션 마법사에서 수정하는 방법](#)
[LAP가 ISR WLCM에 등록되지 않음 - 잘못된 인증서로 배송된 WLCM](#)
[LAP가 WLCM에 등록되지 않음 - 시스템 시간이 설정되지 않음](#)
[WLCM의 비밀번호 복구](#)
[Cisco WLCM LED](#)
[컨트롤러 펌웨어 업그레이드 실패](#)
[CDP를 활성화할 수 없음](#)
[ip-helper 주소 및 ip-forward 프로토콜 명령을 사용하여 LDAP를 WLCM에 등록합니다.](#)
[WLCM 문제 해결 명령](#)
[관련 정보](#)

소개

이 문서에서는 Cisco LCM(Wireless LAN Controller Module)의 기본적인 문제에 대한 트러블슈팅 절차를 제공합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- LWAPP(Lightweight Access Point Protocol)에 대한 지식
- Cisco Unified Wireless Network에 참여하도록 WLCM 모듈을 구성하는 방법에 대한 기본적인

지식.**참고:** 새 사용자이고 WLCM에서 작업하지 않은 경우 Cisco WLAN Controller Network Module 기능 가이드를 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 3.2.116.21을 실행하는 WLCM과 함께 버전 12.4(11)T를 실행하는 Cisco 2811 ISR(Integrated Services Router)
- Cisco 1030 및 Cisco 1232 AG LAP(Lightweight AP)
- 버전 2.5를 실행하는 Cisco 802.11a/b/g Wireless LAN(WLAN) Client 어댑터
- 버전 3.2를 실행하는 Cisco ACS(Secure Access Control Server)

참고: 여기에 나열된 구성 요소는 이 문서를 작성하는 데 사용된 디바이스입니다.WLCM을 지원하는 ISR의 전체 목록 및 WLCM에서 지원되는 LAP에 대한 정보는 이 문서의 문제 해결 섹션에 나와 있습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

배경 정보

Cisco WLCM은 중소기업(SMB) 및 대기업 지사 고객에게 Cisco 2800 및 Cisco 3800 Series ISR 및 Cisco 3700 Series 라우터를 위한 802.11 무선 네트워킹 솔루션을 제공하도록 설계되었습니다.

Cisco WLCM을 사용하면 Cisco ISR 및 Cisco 3700 Series 라우터가 최대 6개의 WLAN 액세스 포인트(AP)를 관리하고 WLAN의 배포 및 관리를 간소화할 수 있습니다.운영 체제는 모든 데이터 클라이언트, 통신 및 시스템 관리 기능을 관리하고 RRM(Radio Resource Management) 기능을 수행하고 OSS(Operating System Security)를 사용하여 시스템 전반의 모빌리티 정책을 관리하고 OSS 프레임워크를 사용하여 모든 보안 기능을 조정합니다.

Cisco WLCM은 Cisco Aironet LAP, Cisco WCS(Wireless Control System) 및 Cisco Wireless Location Appliance와 함께 작동하여 미션 크리티컬 무선 데이터, 음성 및 비디오 애플리케이션을 지원합니다.

문제 해결

이 섹션에서는 WLCM의 기본 문제에 대한 문제 해결 절차에 대해 설명합니다.

ISR에서 WLCM을 인식하지 못함

WLCM은 다음 ISR 플랫폼에서만 지원됩니다.

- Cisco 3725 및 3745 Router

- Cisco 2811, 2821 및 2851 ISR
- Cisco 3825 및 3845 ISR

이 목록에 지정된 ISR이 아닌 다른 ISR이 나타나면 WLCM이 검색되지 않습니다.올바른 하드웨어를 사용해야 합니다.

참고: WLCM은 네트워크 모듈 슬롯에서만 지원됩니다.Cisco 2821 및 Cisco 2851 ISR에서 사용할 수 있는 EVM 슬롯에서는 지원되지 않습니다.

참고: 단일 라우터 섀시에 Cisco WLCM을 하나만 설치할 수 있습니다.

또한 WLCM에 대한 몇 가지 최소 소프트웨어 요구 사항도 있습니다.

ISR에서 WLCM을 인식하려면 ISR에서 Cisco IOS® Software Release 12.4(2)XA1(라우터 소프트웨어) 이상을 사용해야 합니다.

WLCM에서 플래시를 업그레이드할 수 있습니까?

Cisco WLCM은 설치된 256MB CompactFlash 메모리 카드와 함께 및 부팅됩니다.CompactFlash 메모리 카드에는 부트 로더, Linux 커널, Cisco WLCM 및 AP 실행 파일 및 Cisco WLCM 구성이 포함되어 있습니다.

Cisco WLCM의 CompactFlash 메모리 카드는 현장 교체가 불가능합니다.

WLCM 핫 스왑 가능 여부

WLCM은 모든 ISR 플랫폼에서 운영중 교체가 불가능합니다.컨트롤러 모듈의 OIR(온라인 삽입 및 제거)은 Cisco 3745 Router 및 Cisco 3845 ISR에서만 지원됩니다.

WLCM에서 지원되는 LAP

Cisco Aironet 1000, 1100 및 1200 시리즈를 포함하는 모든 LWAPP 지원 Cisco Aironet AP가 지원됩니다.HWIC-AP 인터페이스 카드는 지원되지 않습니다.

WLCM에서 고속 이더넷에 액세스할 수 없음

이는 예상 동작입니다.Cisco WLCM 면판에 있는 외부 고속 이더넷 포트는 지원되지 않습니다.NM-WLC(WLCM 모듈)에는 내부적으로 호스트 라우터에 연결된 고속 이더넷 포트가 하나만 있으며, NM 면판의 외부 고속 이더넷 포트는 비활성화되어 사용할 수 없습니다.

WLCM의 상태 확인

ISR에서 **show version** 명령을 실행하여 WLCM이 라우터에서 인식되고 올바르게 설치되었는지 확인합니다.

```
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
```

WLCM의 상태를 찾으려면 **service-module wlan-controller slot/port status** 명령을 실행합니다.

```
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
```

WLCM의 모듈 재설정 통계를 찾기 위해 **service-module wlan-controller 1/0 statistics** 명령을 실행할 수도 있습니다.

```
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
```

경우에 따라 다음과 같은 오류가 표시됩니다.

```
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
```

이 오류의 원인은 하드웨어 문제일 수 있습니다.이 문제를 더 자세히 해결하려면 TAC 케이스를 여십시오.TAC 케이스를 열려면 Cisco와 유효한 계약을 체결해야 합니다.Cisco TAC에 문의하려면 기술 지원을 참조하십시오.

WLCM에 대한 자세한 내용을 수신하려면 **show sysinfo** 명령을 실행합니다.

```
(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
```

CLI 컨피그레이션 마법사에서 수정하는 방법

CLI 컨피그레이션 마법사를 사용하여 WLCM을 처음(또는 기본값으로 재설정한 후)으로 구성할 때 **-**키를 사용하여 컨피그레이션을 수정합니다.예:

여기서 **admin**을 입력하는 대신 사용자가 **adminn**을 입력하여 수정합니다.다음 프롬프트에서 **-**를 입력하고 Enter를 클릭합니다.시스템이 이전 프롬프트로 돌아갑니다.

```
(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.
```

LAP가 ISR WLCM에 등록되지 않음 - 잘못된 인증서로 배송된 WLCM

NM-*AIR-WLC6-K9* 및 *NM-AIR-WLC6-K9=* WLCM에는 잘못된 인증서가 제공됩니다.이로 인해 WLCNM이 Cisco/Airespace AP에서 인증되지 않습니다.2006년 2월 1일부터 2006년 3월 22일까지 배송된 WLCM에 영향이 미칩니다.제조 프로세스 오류가 올바른 인증서를 WLCNM 장치에 복사하지 못했습니다.잘못된 인증서가 RSA 키 불일치를 생성하므로 LWAPP 기반 AP가 WLCNM에 가입/연결/등록하지 못합니다.

필드 알림을 참조하십시오.FN - 62379 - Wireless LAN Controller Network Module이 Cisco/Airespace Access Points로 인증되지 않음 - 하드웨어 업그레이드에 대한 자세한 정보.이 필드 알림에는 해결 방법, 영향을 받는 네트워크 모듈 부품 번호 및 일련 번호가 포함되어 있습니다.

LAP가 WLCM에 등록되지 않음 - 시스템 시간이 설정되지 않음

WLCM은 시스템 시간과 날짜로 구성해야 합니다.수동으로 수행하거나 NTP 서버를 사용하도록 WLCM을 구성할 수 있습니다.시간과 날짜가 설정되지 않은 경우 LAP는 WLCM에 등록되지 않습니다.CLI 마법사에서 시스템 시간 및 날짜를 입력하라는 메시지가 표시됩니다.날짜와 시간을 입력하지 않으면 다음 경고 메시지가 표시됩니다.

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

시간을 수동으로 구성하려면 WLCM CLI에서 이 명령을 실행합니다.

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

WLCM에서 NTP 서버를 사용하도록 하려면 다음 명령을 실행합니다.

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

WLCM의 비밀번호 복구

WLCM에 로그인하기 위한 암호가 손실된 경우 WLCM에 로그인하는 유일한 방법은 WLCM을 기본 설정으로 다시 설정하는 것입니다.이는 WLCM의 전체 컨피그레이션이 재설정되고 처음부터 구성해야 함을 의미합니다.

WLCM을 공장 기본값으로 재설정하는 방법에 대한 자세한 내용은 WLCM을 기본 설정으로 재설정을 참조하십시오.

Cisco WLCM LED

다음 표에는 Cisco WLCM LED와 의미가 나열되어 있습니다.

LED	의미
CF	CompactFlash 메모리 카드가 활성 상태입니다.

EN	모듈이 자체 테스트를 통과했으며 라우터에서 사용할 수 있습니다.
PWR	컨트롤러 모듈에 전원이 공급됩니다.

컨트롤러 펌웨어 업그레이드 실패

업그레이드 프로세스 중에 업그레이드 프로세스에 영향을 미치는 몇 가지 오류가 발생할 수 있습니다.이 섹션에서는 오류 메시지의 의미와 오류를 제거하고 컨트롤러를 업그레이드하는 방법에 대해 설명합니다.

- **코드 파일 전송 실패-TFTP 서버로부터 응답 없음**—TFTP 서버가 활성 상태가 아닌 경우 이 오류 메시지가 표시됩니다.서버에서 TFTP 서비스가 활성화되어 있는지 확인합니다.
- **코드 파일 전송 실패 - 서버의 오류:파일을 찾을 수 없습니다.전송 중단** - OS 파일이 TFTP 서버의 기본 디렉토리에 없는 경우 이 오류 메시지가 표시됩니다.이 오류를 제거하려면 TFTP 서버의 기본 디렉토리에 이미지 파일을 복사합니다.
- **플래시에 저장하는 동안 TFTP Failure!** - TFTP 서버에 문제가 있을 때 이 오류가 발생합니다.일부 TFTP 서버는 전송할 수 있는 파일의 크기에 제한이 있습니다.다른 TFTP 서버 유틸리티를 사용합니다.사용 가능한 많은 무료 TFTP 서버 유틸리티가 있습니다.Cisco에서는 Tftpd32 버전 2.0 TFTP 서버를 사용하는 것이 좋습니다.이 TFTP 서버를 다운로드하려면 Tftpd32를 참조하십시오.
- **설치 파티션이 제거되거나 이미지가 손상되었습니다**. - 소프트웨어를 업그레이드한 후에도 오류가 계속되면 이미지가 손상될 수 있습니다.Cisco 기술 지원에 문의하십시오.

WLCM에서 펌웨어를 업그레이드하는 방법에 대한 자세한 내용은 Cisco WLAN Controller 모듈 소프트웨어 업그레이드를 참조하십시오.

CDP를 활성화할 수 없음

사용자는 3750 ISR에 설치된 WLCM에서 CDP(Cisco Discovery Protocol)를 활성화할 수 없습니다.다음 메시지가 나타납니다.

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

사용자가 CDP를 **활성화하기** 위해 config cdp enable 명령을 실행하지만 여전히 동일한 메시지가 표시됩니다.

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

이는 Cisco 버그 ID CSCsg67615 때문입니다. 3750G 통합 무선 LAN 컨트롤러는 CDP를 지원하지 않지만 이 컨트롤러에 대해 CDP CLI 명령을 사용할 수 있습니다.이 문제는 4.0.206.0에서 해결됩니다.

ip-helper 주소 및 ip-forward 프로토콜 명령을 사용하여 LDAP를 WLCM에 등록합니다.

WLCM을 사용하면 LAP에서 IP 서브넷 브로드캐스트를 통해 WLCM을 검색하기가 어렵습니다.이는 WLCM이 ISR의 뒷면 평면에 통합되는 방식과 일반적으로 LAP가 다른 IP 서브넷에 있는 방식(좋은 권장 사항)이 원인입니다. 성공적으로 IP 서브넷 브로드캐스트 검색을 수행하려면 **ip helper-address** 및 **ip forward-protocol udp 1223** 명령을 실행합니다.

일반적으로 이러한 명령의 목적은 잠재적인 IP 브로드캐스트 프레임을 전달하거나 릴레이하는 것입니다.WLC가 LAP에 다시 응답하도록 하려면 이 릴레이와 WLC 관리 인터페이스로 전달해야 합니다.

ip helper-**address** 명령은 LAP가 연결된 인터페이스 아래에 지정해야 하며, **ip helper-address** 명령은 WLC의 관리 인터페이스를 가리켜야 합니다.

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

ip forward-**protocol** 명령은 전역 컨피그레이션 명령입니다.

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

WLCM 문제 해결 명령

이 섹션에서는 WLCM 컨피그레이션의 문제를 해결하는 데 사용할 수 있는 **debug** 명령을 제공합니다.

디버그 명령을 사용하여 컨트롤러에 LAP 등록을 확인합니다.

다음 **debug** 명령을 사용하여 LAP가 WLCM에 등록되는지 확인합니다.

- **debug mac addr <AP-MAC-address xx:xx:xx:xx:xx:xx>** - LAP에 대한 MAC 주소 디버깅을 구성합니다.
- **debug lwapp events enable** - LWAPP 이벤트 및 오류 메시지의 디버그를 구성합니다.
- **debug pm pki enable** - 보안 정책 관리자 모듈의 디버그를 구성합니다.

다음은 LAP가 WLCM에 등록될 때 **debug lwapp events enable** 명령의 출력 예입니다.

```
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
```

다음은 LAP가 WLCM에 등록될 때 **debug pm pki enable** 명령 출력의 예입니다.

```
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
```

웹 인증을 확인하는 디버그 명령:

WLCM에서 웹 인증이 예상대로 작동하는지 확인하려면 다음 debug 명령을 사용합니다.

- **debug aaa all enable** - 모든 AAA 메시지의 디버그를 구성합니다.
- **debug pem state enable** - 정책 관리자 상태 시스템의 디버그를 구성합니다.
- **debug pem events enable** - 정책 관리자 이벤트의 디버그를 구성합니다.
- **debug pm ssh-appgw enable** - 애플리케이션 게이트웨이의 디버그를 구성합니다.
- **debug pm ssh-tcp enable** - 정책 관리자 tcp 처리의 디버그를 구성합니다.

다음은 다음 **debug** 명령의 샘플 출력입니다.

```
(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
```

DHCP 작업을 확인하는 디버그 명령:

DHCP 클라이언트 및 서버 활동을 확인하려면 다음 debug 명령을 사용합니다.

- **debug dhcp message enable** - DHCP 클라이언트 활동에 대한 디버깅 정보를 표시하고 DHCP 패킷의 상태를 모니터링합니다.
- **debug dhcp packet enable** - DHCP 패킷 레벨 정보를 표시합니다.

다음은 이러한 **debug** 명령의 샘플 출력입니다.

```
(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
```

TFTP 업그레이드를 확인하는 디버그 명령:

- **show msglog** - Cisco Wireless LAN Controller 데이터베이스에 기록된 메시지 로그를 표시합니다.항목이 15개 이상인 경우 예제에 표시된 메시지를 표시하라는 메시지가 표시됩니다.
- **debug transfer trace(디버그 전송 추적)** - 전송 또는 업그레이드의 디버그를 구성합니다.

다음은 debug **transfer trace** 명령의 예입니다.

```
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
```

802.1X/WPA/RSN/PMK 캐싱에 대한 디버그 명령:

- **debug dot1x all enable** - 802.1X 디버깅 정보를 표시합니다.다음은 이 명령의 샘플 출력입니다.

```
(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
```

- **debug dot11 all enable** - 라디오 함수의 디버깅을 활성화합니다.
- **show client summary** *<mac>*—MAC 주소별로 클라이언트에 대한 요약 정보를 표시합니다.다음은 이 명령의 샘플 출력입니다.

```
(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
```

관련 정보

- Cisco Wireless LAN Controller 명령 참조
- Cisco WLAN Controller Network Module 기능 가이드
- WLCM(Wireless LAN Controller Module) 컨피그레이션 예
- 무선 LAN 컨트롤러 웹 인증 컨피그레이션 예
- WLAN 컨트롤러(WLC)를 사용한 EAP 인증 컨피그레이션 예
- 기술 지원 및 문서 – Cisco Systems