

Wireless LAN Controller Module (WLCM) Troubleshooting

[TAC Notice: What's Changing on TAC Web](#)

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Conventions](#)
[Background Information](#)
[Troubleshoot](#)
[ISR Does Not Recognize the WLCM](#)
[Can I Upgrade the Flash on the WLCM?](#)
[Is the WLCM Hot-swappable?](#)
[LAPs Supported on the WLCM](#)
[Unable to Access Fast Ethernet on the WLCM](#)
[Check the Status of the WLCM](#)
[How Do We Make Corrections in the CLI Configuration Wizard](#)
[LAP Does Not Register with ISR WLCM - WLCM Shipped with Incorrect Certificates](#)
[LAP Does Not register with the WLCM - System Time Not Set](#)
[Password Recovery for the WLCM](#)
[Cisco WLCM LEDs](#)
[Upgrade of Controller Firmware Fails](#)
[Cannot Enable CDP](#)
[Use the ip-helper address and ip-forward protocol Commands to Register LAPs with the WLCM](#)
[WLCM Troubleshooting Commands](#)
[NetPro Discussion Forums - Featured Conversations](#)
[Related Information](#)

Help us help you.

Please rate this document.

Excellent
 Good
 Average
 Fair
 Poor

This document solved my problem.

Yes
 No
 Just browsing

Suggestions for improvement:

(256 character limit)

Introduction

This document provides troubleshooting procedures for basic problems with the Cisco Wireless LAN Controller Module (WLCM).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of Lightweight Access Point Protocol (LWAPP).
- Basic knowledge of how to configure the WLCM module to participate in a Cisco Unified Wireless Network.

Note: If you are a new user and have not worked on a WLCM, refer to [Cisco WLAN Controller Network Module Feature Guide](#).

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 2811 Integrated Services Router (ISR) that runs version 12.4(11)T with WLCM that runs version 3.2.116.21
- Cisco 1030 and Cisco 1232 AG Lightweight APs (LAPs)
- Cisco 802.11a/b/g Wireless LAN (WLAN) Client adapter that runs version 2.5
- Cisco Secure Access Control Server (ACS) that runs version 3.2

Note: The components listed here are only the devices that were used to write this document. The information on the complete list of the ISRs that support the WLCM and the LAPs that are supported on the WLCM is provided in the [Troubleshoot](#) section of this document.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to [Cisco Technical Tips Conventions](#) for more information on document conventions.

Background Information

The Cisco WLCM is designed to provide small and medium-sized businesses (SMBs) and enterprise branch office customers with 802.11 wireless networking solutions for Cisco 2800 and Cisco 3800 Series ISRs and Cisco 3700 Series Routers.

The Cisco WLCM enables Cisco ISRs and Cisco 3700 Series Routers to manage up to six WLAN access points (APs), and simplifies the deployment and management

of WLANs. The operating system manages all data client, communications, and system administration functions, performs Radio Resource Management (RRM) functions, manages system-wide mobility policies using the operating system security (OSS), and coordinates all security functions using the OSS framework.

The Cisco WLCM works in conjunction with Cisco Aironet LAPs, Cisco Wireless Control System (WCS), and the Cisco Wireless Location Appliance to support mission-critical wireless data, voice, and video applications.

Troubleshoot

This section discusses troubleshooting procedures for basic problems with the WLCM.

ISR Does Not Recognize the WLCM

The WLCM is supported only on these ISR platforms:

- Cisco 3725 and 3745 Routers
- Cisco 2811, 2821, and 2851 ISRs
- Cisco 3825 and 3845 ISRs

If any other ISR than the ones specified in this list appears, then the WLCM is not detected. Ensure that you use the correct hardware.

Note: The WLCM is supported only in network module slots. It is not supported in EVM slots available in the Cisco 2821 and Cisco 2851 ISRs.

Note: You can install only one Cisco WLCM in a single router chassis.

There are also some minimum software requirements for the WLCM.

The ISR must use Cisco IOS® Software Release 12.4(2)XA1 (router software) or later for the ISR to recognize the WLCM.

Can I Upgrade the Flash on the WLCM?

The Cisco WLCM ships with and boots from an installed 256-MB CompactFlash memory card. The CompactFlash memory card contains the boot loader, Linux kernel, Cisco WLCM and APs executable file, and the Cisco WLCM configuration.

The CompactFlash memory card in the Cisco WLCM is not field-replaceable.

Is the WLCM Hot-swappable?

The WLCM is not hot-swappable on all the ISR platforms. Online insertion and removal (OIR) of the controller module is supported only on the Cisco 3745 Router and the Cisco 3845 ISR.

LAPs Supported on the WLCM

All LWAPP-enabled Cisco Aironet APs are supported, which includes the Cisco Aironet 1000, 1100, and 1200 series. The HWIC-AP interface cards are not supported.

Unable to Access Fast Ethernet on the WLCM

This is the expected behavior. The external Fast Ethernet port on the faceplate of the Cisco WLCM is not supported. The NM-WLC (WLCM module) has only one Fast Ethernet port internally connected to the host router, and the external Fast Ethernet port on the NM faceplate is disabled and unusable.

Check the Status of the WLCM

Issue the show version command from the ISR in order to check if the WLCM is recognized by the router and is installed correctly.

```
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
```

Issue the service-module wlan-controller slot/port status command in order to find the status of the 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
```

You can also issue the service-module wlan-controller 1/0 statistics command in order to find the module reset statistics of the 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
```

In some cases, you see this error:

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

Or this:

```
Router#service-module wlan-controller 1/0 status
Service Module is Cisco wlan-controller1/0
Service Module supports session via TTY line 66
Service Module is failed
Service Module status is not available
```

The reason for this error might be a hardware issue. Open a TAC case to further troubleshoot this problem. In order to open a TAC case, you need to have a valid contract with Cisco. Refer to [Technical Support](#) in order to contact the Cisco TAC.

Issue the show sysinfo command in order to receive more information on the 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
```

How Do We Make Corrections in the CLI Configuration Wizard

When you configure the WLCM for the first time (or after resetting to defaults) using the CLI Configuration wizard, the - key is used in order to make corrections to the configurations. This is an example:

Here, instead of entering admin, the user enters adminn to correct it. At the next prompt, enter -, then click enter. The system returns to the previous prompt.

```
(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 Does Not Register with ISR WLCM - WLCM Shipped with Incorrect Certificates

The *NM-AIR-WLC6-K9* and *NM-AIR-WLC6-K9=* WLCMs are shipped with incorrect certificates. This causes the WLCNM to not be authenticated by Cisco/Airespace APs. The WLCMs shipped between February 1, 2006 and March 22, 2006 are affected. A manufacturing process failure did not copy the correct certificates to WLCNM devices. The incorrect certificate creates an RSA key mismatch, which causes LWAPP-based APs to fail to join/associate/register to WLCNM.

Refer to [Field Notice: FN - 62379 - Wireless LAN Controller Network Module does not Authenticate with Cisco/Airespace Access Points - Hardware Upgrade](#) for more information on this. This Field Notice contains the workaround, as well as the affected Network Module Part Numbers and Serial Numbers.

LAP Does Not register with the WLCM - System Time Not Set

The WLCM has to be configured with the system time and date. It can either be done manually, or the WLCM can be configured to use the NTP server. If the time and date is not set, the LAPs do not register with the WLCM. In the CLI wizard, you are prompted to enter the system time and date. If you do not enter the date and time, you see this warning message:

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

Issue this command from the WLCM CLI in order to configure the time manually:

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

Issue this command if you want the WLCM to use the NTP server:

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

Password Recovery for the WLCM

When the password to login to the WLCM is lost, the only way to get into the WLCM is to reset the WLCM back to default settings. This also means that the entire configuration on the WLCM is reset and has to be configured from scratch.

Refer to [Reset the WLCM to Default Settings](#) for information on how to reset the WLCM to factory defaults.

Cisco WLCM LEDs

This table lists the Cisco WLCM LEDs and the meanings:

LED	Meaning
CF	The CompactFlash memory card is active.
EN	The module has passed self-test and is available to the router.
PWR	Power is available to the controller module.

Upgrade of Controller Firmware Fails

During the upgrade process, you can come across some errors that affect the upgrade process. This section explains what the error messages mean and how to eliminate the errors and upgrade the controller.

- Code file transfer failed-No reply from the TFTP server—You receive this error message if the TFTP server is not active. Check to determine if the TFTP service is enabled on the server.
- Code file transfer failed - Error from server: File was not found. Aborting transfer—You receive this error message if the OS file is not present in the default directory of the TFTP server. In order to eliminate this error, copy the image file to the default directory on the TFTP server.
- TFTP Failure while storing in flash!—You receive this error when there is a problem with the TFTP server. Some TFTP servers have a limitation on the size of the files that you can transfer. Use a different TFTP server utility. There are many free TFTP server utilities that are available. Cisco recommends use of the Tftpd32 version 2.0 TFTP server. Refer to [Tftpd32](#) in order to download this TFTP server.
- The install partitions are destroyed or the image is corrupted—If you are still unsuccessful after an attempt to upgrade the software, there is a possibility that your image is corrupted. Contact [Cisco Technical Support](#) for assistance.

Refer to [Upgrading the Cisco WLAN Controller Module Software](#) for more information on how to upgrade the firmware on the WLCM.

Cannot Enable CDP

The user cannot enable Cisco Discovery Protocol (CDP) on the WLCM installed on the 3750 ISR. This message appears:

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

The user issues the config cdp enable command in order to enable CDP, but still sees this same message:

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

This is because of Cisco bug ID CSCsg67615. Although the 3750G Integrated Wireless LAN Controller does not support CDP, the CDP CLI commands are available for this controller. This is resolved in 4.0.206.0.

Use the ip-helper address and ip-forward protocol Commands to Register LAPs with the WLCM

With the WLCM, it is difficult for a LAP to discover the WLCM through IP subnet broadcast. This is because of how the WLCM integrates on the back plane of the ISR and how the LAP is typically on a different IP subnet (which is also a good recommendation). If you want to perform IP subnet broadcast discovery with success, issue the ip helper-address and ip forward-protocol udp 12223 commands.

In general, the purpose of these commands is to forward or relay any potential IP broadcast frame. This relay and directing it to the WLC management interface should be adequate to make sure the WLC responds back to the LAP.

The ip helper-address command must be given under the interface to which the LAP is connected to, and the ip helper-address command must point to the management interface of the WLC.

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

The ip forward-protocol command is a global configuration command.

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

WLCM Troubleshooting Commands

This section provides the debug commands you can use in order to troubleshoot the WLCM configuration.

Debug commands to verify LAP registering with the controller:

Use these debug commands in order to verify if the LAPs register with the WLCM:

- debug mac addr <AP-MAC-address xx:xx:xx:xx:xx:xx>—Configures MAC address debugging for the LAP.
- debug lwapp events enable—Configures debug of LWAPP events and error messages.
- debug pm pki enable—Configures debug of security policy manager module.

Here is an example output of the debug lwapp events enable command when the LAP registers with the WLCM:

```
Mon Mar 12 16:23:39 2007: Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0
to 00:15:2c:e8:38:c0 on port '1'
Mon Mar 12 16:23:39 2007: Successful transmission of LWAPP Discovery-Response to
AP 00:0b:85:51:5a:e0 on Port 1
Mon Mar 12 16:23:52 2007: Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0 to
00:15:2c:e8:38:c0 on port '1'
Mon Mar 12 16:23:52 2007: LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0
is 1500, remote debug mode is 0
Mon Mar 12 16:23:52 2007: Successfully added NPU Entry for AP 00:0b:85:51:5a:e0
(index 49)Switch IP: 60.0.0.3, Switch Port:
12223, intIfNum 1, vlanId 0 AP IP: 10.77.244.221, AP Port: 5550,
next hop MAC: 00:17:94:06:62:98
Mon Mar 12 16:23:52 2007: Successfully transmission of LWAPP Join-Reply to
AP 00:0b:85:51:5a:e0
Mon Mar 12 16:23:52 2007: Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 0
Mon Mar 12 16:23:52 2007: Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 1
Mon Mar 12 16:23:53 2007: Received LWAPP CONFIGURE REQUEST from AP 00:0b:85:51:5a:e0
to 00:15:2c:e8:38:c0
Mon Mar 12 16:23:53 2007: Updating IP info for AP 00:0b:85:51:5a:e0 --
static 0, 10.77.244.221/255.255.255.224, 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
Mon Mar 12 16:23:54 2007: Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:51:5a:e0
```

Here is an example output of the debug pm pki enable command when the LAP registers with the WLCM:

```
Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: locking ca cert table
Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: calling x509_alloc() for user cert
Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: calling x509_decode()
Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: <subject> C=US, ST=California,
L=San Jose, O=airespace Inc, CN=000b85515ae0,
MAILTO=support@airespace.com
Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: <issuer> C=US, ST=California,
L=San Jose, O=airespace Inc, OU=none, CN=ca,
MAILTO=support@airespace.com
Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: Mac Address in subject is
00:0b:85:51:5a:e0
Mon Mar 12 16:30:40 2007: sshpmGetIssuerHandles: Cert is issued by Airespace Inc.
Mon Mar 12 16:30:40 2007: sshpmGetCID: called to evaluate <bsnDefaultCaCert>
Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 1, CA cert >bsnDefaultRootCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 2, CA cert >bsnDefaultCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: called to get cert for CID 2816f436
Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 0, certname
>bsnOldDefaultCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 1, certname
>bsnDefaultRootCaCert<
```

```

Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 2, certname
>bsnDefaultCaCert<
Mon Mar 12 16:30:40 2007: ssphmUserCertVerify: calling x509_decode()
Mon Mar 12 16:30:40 2007: ssphmUserCertVerify: failed to verify AP cert
>bsnDefaultCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCID: called to evaluate <bsnOldDefaultCaCert>
Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 0, CA cert
>bsnOldDefaultCaCert<
Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: called to get cert for CID 226b9636
Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 0, certname
>bsnOldDefaultCaCert<
Mon Mar 12 16:30:40 2007: ssphmUserCertVerify: calling x509_decode()
Mon Mar 12 16:30:40 2007: ssphmUserCertVerify: user cert 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

```

Debug commands to verify web authentication:

Use these debug commands in order to verify if web authentication works as expected on the WLCM:

- debug aaa all enable—Configures debug of all AAA messages.
- debug pem state enable— Configures debug of policy manager State Machine.
- debug pem events enable—Configures debug of policy manager events.
- debug pm ssh-appgw enable—Configures debug of application gateways.
- debug pm ssh-tcp enable—Configures debug of policy manager tcp handling.

Here are sample outputs from some of these debug commands:

```
(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 state to L2AUTHCOMPLETE (4)
Fri Mar 2 16:27:39 2007: 00:40:96:ac:e6:57 10.0.0.1
L2AUTHCOMPLETE (4) Change state to WEBAUTH_REQD (8)
Fri Mar 2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0
START (0) Change state to AUTHCHECK (2)
Fri Mar 2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0
AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)
Fri Mar 2 16:28:16 2007: 00:16:6f:6e:36:2b 0.0.0.0
L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)
Fri Mar 2 16:28:19 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8) Change state to WEBAUTH_NOL3SEC (14)
Fri Mar 2 16:28:19 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_NOL3SEC (14) Change state to RUN (20)
Fri Mar 2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0
START (0) Change state to AUTHCHECK (2)
Fri Mar 2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0
AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)
Fri Mar 2 16:28:20 2007: 00:16:6f:6e:36:2b 0.0.0.0
L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)
Fri Mar 2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0
START (0) Change state to AUTHCHECK (2)
Fri Mar 2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0
AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)
Fri Mar 2 16:28:24 2007: 00:40:96:af:a3:40 0.0.0.0
L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)
Fri Mar 2 16:28:25 2007: 00:40:96:af:a3:40 40.0.0.1
DHCP_REQD (7) Change state to RUN (20)
Fri Mar 2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0
START (0) Change state to AUTHCHECK (2)
Fri Mar 2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0
AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)
Fri Mar 2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0
L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)
Fri Mar 2 16:28:34 2007: 00:16:6f:6e:36:2b 30.0.0.2
DHCP_REQD (7) Change state to WEBAUTH_REQD (8)

```

(Cisco Controller) >debug pem events 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) Replacing Fast Path rule type = Temporary Entry
on AP 00:0b:85:5b:fb:d0, slot 0, interface = 1 ACL Id = 255,

```

Cisco - Wireless LAN Controller Module (WLCM) Troubleshooting

```
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
```

Debug commands to verify DHCP operation:

Use these debug commands in order to check DHCP client and server activities:

- debug dhcp message enable—Displays debugging information about the DHCP client activities and to monitor the status of DHCP packets.
- debug dhcp packet enable—Displays DHCP packet level information.

Here are sample outputs of these debug commands:

```
(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 Forwaring 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 Determining 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
```

Debug commands to verify TFTP upgrade:

- show msglog—Displays the message logs written to the Cisco Wireless LAN controller database. If there are more than 15 entries, you are prompted to display the messages shown in the example.
- debug transfer trace—Configures debug of the transfer or upgrade.

Here is an example of the debug transfer trace command:

```
(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
```

Debug commands for 802.1X/WPA/RSN/PMK caching:

- debug dot1x all enable—Displays 802.1X debugging information.

Here is a sample output of this command:

```
(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—Enables debugging of radio functions.
- show client summary <mac> —Displays summarized information for client by MAC address.












Here is a sample output of this command:

```

(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

```

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

Wireless - Mobility -General Conversations			
	LAP1131 to autonomous mo...	jordan01060	0 replies Nov 9, 2009, 9:56am PST
	Clients appearing in AP ...	walthowd80	0 replies Nov 9, 2009, 9:26am PST
	How do you Sniff with a ...	scott.hammond	5 replies Nov 5, 2009, 10:52am PST
	Recovery Password AP...	ricardorojas123	2 replies Nov 8, 2009, 5:45pm PST
	1310 Bridges...	bstory	0 replies Nov 9, 2009, 7:06am PST
	AP1242AG - IOS - Wireles...	sven@hruza	0 replies Nov 9, 2009, 5:24am PST
	WLCs loses config after ...	lydia.walther	0 replies Nov 9, 2009, 3:41am PST
	Aironet 1240AG AP...	joe.gowan	2 replies Nov 6, 2009, 12:37pm PST
	AP1242 AG ...	paulo.s	5 replies Oct 30, 2009, 9:15am PST
	WLC mesh upgrade...	massimo.baschieri	2 replies Nov 8, 2009, 12:56am PST
Start a Conversation		Email-Subscribe	
			No.of Conversations: 10

Related Information

- [Cisco Wireless LAN Controller Command Reference](#)
- [Cisco WLAN Controller Network Module Feature Guide](#)
- [Wireless LAN Controller Module \(WLCM\) Configuration Examples](#)
- [Wireless LAN Controller Web Authentication Configuration Example](#)
- [EAP Authentication with WLAN Controllers \(WLC\) Configuration Example](#)
- [Technical Support & Documentation - Cisco Systems](#)

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)