Fehlerbehebung für Wireless LAN Controller-Module

Inhalt

Einführung

Dieses Dokument enthält Verfahren zur Fehlerbehebung bei grundlegenden Problemen mit dem Cisco Wireless LAN Controller Module (WLCM).

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnis des LWAPP (Lightweight Access Point Protocol)
- Grundkenntnisse der Konfiguration des WLCM-Moduls für die Teilnahme an einem Cisco Unified Wireless Network.**Hinweis:** Wenn Sie ein neuer Benutzer sind und noch nicht an einem WLCM gearbeitet haben, lesen Sie den Cisco WLAN Controller Network Module Feature Guide.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco 2811 Integrated Services Router (ISR) mit Version 12.4(11)T und WLCM, auf dem Version 3.2.116.21 ausgeführt wird
- Lightweight APs (LAPs) Cisco 1030 und Cisco 1232 AG
- Cisco 802.11a/b/g Wireless LAN (WLAN) Client-Adapter mit Version 2.5
- Cisco Secure Access Control Server (ACS) mit Version 3.2

Hinweis: Die hier aufgeführten Komponenten sind nur die Geräte, die zum Schreiben dieses Dokuments verwendet wurden. Die vollständige Liste der ISRs, die den WLCM und die vom WLCM unterstützten LAPs unterstützen, finden Sie im Abschnitt Fehlerbehebung dieses Dokuments.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Der Cisco WLCM wurde entwickelt, um kleinen und mittelständischen Unternehmen (KMU) und Zweigstellen-Kunden 802.11-Wireless-Netzwerklösungen für die Cisco ISRs der Serien 2800 und 3800 und Cisco Router der Serie 3700 bereitzustellen.

Der Cisco WLCM ermöglicht Cisco ISRs und Cisco Routern der Serie 3700 die Verwaltung von bis zu sechs WLAN Access Points (APs) und vereinfacht die Bereitstellung und Verwaltung von WLANs. Das Betriebssystem verwaltet alle Daten-Client-, Kommunikations- und Systemverwaltungsfunktionen, führt Radio Resource Management (RRM)-Funktionen durch, verwaltet systemweite Mobilitätsrichtlinien mithilfe der Betriebssystemsicherheit (OSS) und koordiniert alle Sicherheitsfunktionen mithilfe des OSS-Frameworks.

Der Cisco WLCM unterstützt in Verbindung mit Cisco Aironet LAPs, dem Cisco Wireless Control System (WCS) und der Cisco Wireless Location Appliance geschäftskritische Wireless-Daten-, Sprach- und Videoanwendungen.

Fehlerbehebung

In diesem Abschnitt werden Verfahren zur Fehlerbehebung bei grundlegenden Problemen mit dem WLCM erläutert.

ISR erkennt den WLCM nicht.

Der WLCM wird nur auf den folgenden ISR-Plattformen unterstützt:

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

Wenn ein anderer als der in dieser Liste angegebenen ISR angezeigt wird, wird der WLCM nicht erkannt. Stellen Sie sicher, dass Sie die richtige Hardware verwenden.

Hinweis: Der WLCM wird nur in Netzwerkmodulsteckplätzen unterstützt. Die EVM-Steckplätze der Cisco 2821 und Cisco 2851 ISR werden nicht unterstützt.

Hinweis: Sie können nur einen Cisco WLCM in einem Gehäuse mit einem Router installieren.

Es gibt auch einige Mindestsoftwareanforderungen für den WLCM.

Der ISR muss die Cisco IOS® Software Release 12.4(2)XA1 (Router-Software) oder höher verwenden, damit der ISR den WLCM erkennen kann.

Kann ich das Flash-Upgrade auf dem WLCM durchführen?

Der Cisco WLCM wird mit einer installierten 256-MB-CompactFlash-Speicherkarte geliefert und wird von dieser gestartet. Die CompactFlash-Speicherkarte enthält den Bootloader, den Linux-Kernel, die ausführbare Datei Cisco WLCM und APs sowie die Cisco WLCM-Konfiguration.

Die CompactFlash-Speicherkarte im Cisco WLCM kann nicht vor Ort ausgetauscht werden.

Ist der WLCM Hot-Swap-fähig?

Der WLCM kann nicht auf allen ISR-Plattformen im laufenden Betrieb ausgetauscht werden. Online Insertion and Removal (OIR) des Controllermoduls wird nur auf dem Cisco 3745 Router und dem Cisco 3845 ISR unterstützt.

Auf dem WLCM unterstützte LAPs

Alle LWAPP-fähigen Cisco Aironet APs werden unterstützt, einschließlich der Serien Cisco Aironet 1000, 1100 und 1200. Die HWIC-AP-Schnittstellenkarten werden nicht unterstützt.

Zugriff auf Fast Ethernet auf dem WLCM nicht möglich

Dies ist das erwartete Verhalten. Der externe Fast Ethernet-Port auf der Frontplatte des Cisco WLCM wird nicht unterstützt. Das NM-WLC (WLCM-Modul) verfügt nur über einen Fast Ethernet-Port, der intern mit dem Host-Router verbunden ist. Der externe Fast Ethernet-Port auf der NM-Frontblende ist deaktiviert und nicht verwendbar.

Überprüfen Sie den Status des WLCM.

Geben Sie den Befehl **show version** vom ISR aus ein, um zu überprüfen, ob der WLCM vom Router erkannt und korrekt installiert wird.

```
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
```

Geben Sie den Befehl **service-module wlan-controller slot/port status** ein, um den Status des WLCM zu ermitteln.

```
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
```

Sie können auch den Befehl **service-module wlan-controller 1/0 statistics** ausgeben, um die Modulrücksetzstatistiken des WLCM zu finden.

```
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 einigen Fällen tritt dieser Fehler auf:

```
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
```

Der Grund für diesen Fehler kann ein Hardwareproblem sein. Öffnen Sie ein TAC-Ticket, um dieses Problem weiter zu beheben. Um ein TAC-Ticket zu erstellen, benötigen Sie einen gültigen Vertrag mit Cisco. Wenden Sie sich an den technischen Support, um das Cisco TAC zu kontaktieren.

Geben Sie den Befehl **show sysinfo** ein, um weitere Informationen zum WLCM zu erhalten.

```
(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
```

Wie werden Korrekturen im CLI-Konfigurationsassistenten vorgenommen?

Wenn Sie den WLCM zum ersten Mal (oder nach dem Zurücksetzen auf die Standardeinstellungen) mithilfe des CLI-Konfigurationsassistenten konfigurieren, wird der **-** Schlüssel verwendet, um Konfigurationsänderungen vorzunehmen. Dies ist ein Beispiel:

Anstatt **admin** einzugeben, gibt der Benutzer **admin** ein, um es zu korrigieren. Geben Sie bei der nächsten Eingabeaufforderung **-** ein **-** und klicken Sie dann auf "Eingeben". Das System kehrt zur vorherigen Eingabeaufforderung zurück.

```
(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 lässt sich nicht mit ISR WLCM registrieren - WLCM wird mit falschen Zertifikaten geliefert

Die *NM-AIR-WLC6-K9* und *NM-AIR-WLC6-K9=* WLCMs werden mit falschen Zertifikaten geliefert. Dadurch wird der WLCNM nicht von den Cisco/Air-APs authentifiziert. Die zwischen dem 1. Februar 2006 und dem 22. März 2006 ausgelieferten WLCMs sind betroffen. Bei einem Ausfall des Herstellungsprozesses wurden die richtigen Zertifikate nicht auf WLCNM-Geräte kopiert. Das falsche Zertifikat verursacht eine RSA-Schlüsselungleichheit, wodurch LWAPP-basierte APs nicht in WLCNM eingebunden/zugeordnet/registriert werden können.

Siehe Problemhinweis: FN - 62379 - Wireless LAN Controller Network Module authentifiziert sich nicht bei Cisco/Air Access Points - Hardware-Upgrade für weitere Informationen hierzu. Dieser Problemhinweis enthält die Problemumgehung sowie die betroffenen Teilenummern und Seriennummern von Netzwerkmodulen.

LAP lässt sich nicht beim WLCM registrieren - "Systemzeit nicht festgelegt"

Der WLCM muss mit der Systemzeit und dem Systemdatum konfiguriert werden. Sie kann entweder manuell durchgeführt werden, oder der WLCM kann für die Verwendung des NTP-Servers konfiguriert werden. Wenn Uhrzeit und Datum nicht festgelegt sind, registrieren die LAPs nicht beim WLCM. Im CLI-Assistenten werden Sie aufgefordert, die Systemzeit und das Systemdatum einzugeben. Wenn Sie Datum und Uhrzeit nicht eingeben, wird folgende Warnmeldung angezeigt:

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

Geben Sie diesen Befehl über die WLCM-CLI aus, um die Zeit manuell zu konfigurieren:

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

Geben Sie diesen Befehl ein, wenn der WLCM den NTP-Server verwenden soll:

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

Kennwortwiederherstellung für den WLCM

Wenn das Kennwort für die Anmeldung am WLCM verloren geht, können Sie nur noch den WLCM auf die Standardeinstellungen zurücksetzen. Dies bedeutet auch, dass die gesamte Konfiguration auf dem WLCM zurückgesetzt wird und von Grund auf konfiguriert werden muss.

Unter Zurücksetzen des WLCM auf Standardeinstellungen finden Sie Informationen zum Zurücksetzen des WLCM auf die Werkseinstellungen.

Cisco WLCM-LEDs

In dieser Tabelle sind die Cisco WLCM-LEDs und die Bedeutungen aufgeführt:

LED	Bedeutung
CF	Die CompactFlash-Speicherkarte ist aktiv.
DE	Das Modul hat den Selbsttest bestanden und ist für den Router verfügbar.
PWR	Das Controllermodul wird mit Strom versorgt.

Upgrade der Controller-Firmware fehlgeschlagen

Während des Upgrade-Vorgangs können einige Fehler auftreten, die sich auf den Upgrade-Prozess auswirken. In diesem Abschnitt wird erläutert, was Fehlermeldungen bedeuten und wie die Fehler behoben und der Controller aktualisiert werden können.

- **Codedateiübertragung fehlgeschlagen-Keine Antwort vom TFTP-Server** - Sie erhalten diese Fehlermeldung, wenn der TFTP-Server nicht aktiv ist. Überprüfen Sie, ob der TFTP-Dienst auf dem Server aktiviert ist.
- **Dateiübertragung fehlgeschlagen - Fehler vom Server: Datei wurde nicht gefunden. Aborting transfer** - Sie erhalten diese Fehlermeldung, wenn die Betriebssystemdatei nicht im Standardverzeichnis des TFTP-Servers vorhanden ist. Um diesen Fehler zu vermeiden, kopieren Sie die Bilddatei in das Standardverzeichnis auf dem TFTP-Server.
- **TFTP-Fehler beim Speichern im Flash!** - Sie erhalten diesen Fehler, wenn ein Problem mit dem TFTP-Server auftritt. Bei einigen TFTP-Servern ist die Größe der Dateien, die Sie übertragen können, beschränkt. Verwenden Sie ein anderes Dienstprogramm für den TFTP-Server. Es gibt viele kostenlose TFTP-Server-Dienstprogramme, die verfügbar sind. Cisco empfiehlt die Verwendung des Tftpd32-TFTP-Servers der Version 2.0. Informationen zum Herunterladen dieses TFTP-Servers finden Sie unter Tftpd32.
- **Die installierten Partitionen werden zerstört oder das Image beschädigt** - Wenn Sie nach einem Versuch, die Software zu aktualisieren, immer noch nicht erfolgreich sind, besteht die Möglichkeit, dass Ihr Image beschädigt wird. Wenden Sie sich an den technischen Support von Cisco.

Unter Upgrade der Cisco WLAN Controller Module Software finden Sie weitere Informationen zum Aktualisieren der Firmware auf dem WLCM.

CDP kann nicht aktiviert werden

Der Benutzer kann das Cisco Discovery Protocol (CDP) auf dem auf dem 3750 ISR installierten WLCM nicht aktivieren. Diese Meldung wird angezeigt:

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

Der Benutzer gibt den Befehl **config cdp enable** aus, um CDP zu aktivieren, sieht jedoch weiterhin die folgende Meldung:

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

Grund hierfür ist die Cisco Bug-ID CSCsg67615. Obwohl der integrierte Wireless LAN-Controller 3750G CDP nicht unterstützt, sind für diesen Controller die CDP-CLI-Befehle verfügbar. Dies wurde in Version 4.0.206.0 behoben.

Verwenden der Befehle ip-helper address und ip-forward-Protokoll, um LAPs mit dem WLCM zu registrieren

Beim WLCM ist es für eine LAP schwierig, den WLCM über IP-Subnetz-Broadcast zu erkennen. Dies liegt daran, wie der WLCM in die Backplane des ISR integriert wird und wie sich die LAP in der Regel in einem anderen IP-Subnetz befindet (eine gute Empfehlung). Wenn Sie die IP-Subnetz-Broadcast-Erkennung erfolgreich durchführen möchten, geben Sie die Befehle **ip helper-address** und **ip forward-Protokoll udp 12223 ein**.

Im Allgemeinen dient der Zweck dieser Befehle dazu, einen beliebigen potenziellen IP-Broadcast-Frame weiterzuleiten oder weiterzuleiten. Diese Weiterleitung und die Weiterleitung an die WLC-Verwaltungsschnittstelle sollten ausreichend sein, um sicherzustellen, dass der WLC auf die LAP zurückantwortet.

Der Befehl **ip helper-address** muss unter der Schnittstelle angegeben werden, mit der die LAP verbunden ist, und der Befehl **ip helper-address** muss auf die Verwaltungsschnittstelle des WLC zeigen.

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

Der Befehl **ip forward-protocol** ist ein globaler Konfigurationsbefehl.

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

Befehle zur Fehlerbehebung für WLCM

Dieser Abschnitt enthält die **Debug-**Befehle, die Sie zur Fehlerbehebung bei der WLCM-Konfiguration verwenden können.

Debuggen von Befehlen zum Überprüfen der LAP-Registrierung beim Controller:

Verwenden Sie diese **Debug-**Befehle, um zu überprüfen, ob sich die LAPs beim WLCM registrieren:

- **debug mac addr <AP-MAC-address xx:xx:xx:xx:xx:xx>** - Konfiguriert das MAC-Adressen-Debugging für die LAP.

- **debug lwapp events enable**: Konfiguriert das Debuggen von LWAPP-Ereignissen und -Fehlermeldungen.
- **debug pm pki enable**: Konfiguriert das Debuggen des Sicherheitsrichtlinien-Managementmoduls.

Im Folgenden finden Sie ein Beispiel für die Ausgabe des Befehls **debug lwapp events enable**, wenn die LAP beim WLCM registriert ist:

```
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
```

Im Folgenden finden Sie ein Beispiel für die Ausgabe des Befehls **debug pm pki enable**, wenn die LAP beim WLCM registriert wird:

```
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
```

Debuggen von Befehlen zur Überprüfung der Webauthentifizierung:

Verwenden Sie diese **Debug-**Befehle, um zu überprüfen, ob die Webauthentifizierung wie erwartet auf dem WLCM funktioniert:

- **debug aaa all enable**: Konfiguriert das Debuggen aller AAA-Nachrichten.
- **debug pem state enable**: Konfiguriert das Debuggen des State Machine des Richtlinienmanagers.
- **debug pem events enable**: Konfiguriert das Debuggen von Richtlinienmanager-Ereignissen.
- **debug pm ssh-appgw enable**: Konfiguriert das Debuggen von Anwendungs-Gateways.
- **debug pm ssh-tcp enable**: Konfiguriert das Debuggen der Richtlinienmanager-TCP-Verarbeitung.

Hier sind einige Beispielausgaben von einigen der folgenden **Debugbefehle**:

```
(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
```

Debuggen von Befehlen zur Überprüfung des DHCP-Vorgangs:

Verwenden Sie die folgenden **Debug-**Befehle, um DHCP-Client- und Serveraktivitäten zu überprüfen:

- **debug dhcp message enable**: Zeigt Debuginformationen über die DHCP-Client-Aktivitäten an und überwacht den Status von DHCP-Paketen.
- **debug dhcp packet enable**: Zeigt Informationen auf der DHCP-Paketebene an.

Hier sind einige Beispielausgaben dieser Debugbefehle:

```
(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
```

Debug-Befehle zum Überprüfen des TFTP-Upgrades:

- **show msglog**: Zeigt die in die Cisco Wireless LAN Controller-Datenbank geschriebenen Meldungsprotokolle an. Wenn mehr als 15 Einträge vorhanden sind, werden Sie aufgefordert, die im Beispiel angezeigten Meldungen anzuzeigen.
- **debug transfer trace** - Konfiguriert das Debuggen der Übertragung oder Aktualisierung.

Im Folgenden finden Sie ein Beispiel für den Befehl **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
```

Debug-Befehle für 802.1X/WPA/RSN/PMK-Caching:

- **debug dot1x all enable**: Zeigt Debuginformationen zu 802.1X an.Hier eine Beispielausgabe dieses Befehls:

```
(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**: Aktiviert das Debuggen von Funkfunktionen.
- **show client summary *<mac>*: Zeigt zusammengefasste Informationen für den Client nach MAC-Adresse an.**Hier eine Beispielausgabe dieses Befehls:

```
(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
```

Zugehörige Informationen

- Cisco Wireless LAN Controller - Befehlsreferenz
- Funktionsleitfaden für das Cisco WLAN-Controller-Netzwerkmodul
- Konfigurationsbeispiele für Wireless LAN Controller Module (WLCM)
- Konfigurationsbeispiel für die Webauthentifizierung des Wireless LAN-Controllers
- Konfigurationsbeispiel für EAP-Authentifizierung mit WLAN-Controllern (WLC)
- Technischer Support und Dokumentation - Cisco Systems