

Problemen oplossen voor draadloze LAN-controllers

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Problemen oplossen](#)

[ISR herkent de WLCM niet](#)

[Kan ik de Flash op de WLCM upgraden?](#)

[Is de WLCM Hot-swappable?](#)

[LAP's die op de WLCM worden ondersteund](#)

[Kan geen toegang tot Fast Ethernet op de WLCM](#)

[De status van de WLCM controleren](#)

[Hoe maken we correcties in de CLI Configuration Wizard](#)

[LAP registreert niet bij ISR WLCM - WLCM verzonden met onjuiste certificaten](#)

[LAP registreert niet bij WLCM - De tijd voor het systeem is niet ingesteld](#)

[Wachtwoordherstel voor de WLCM](#)

[Cisco WLCM-LEDs](#)

[upgrade van controllerfirmware mislukt](#)

[Kan CDP niet inschakelen](#)

[Gebruik het IP-adres en de IP-voorwaartse protocolopdrachten om LAP's te registreren bij de WLCM](#)

[Opdrachten voor WLCM-probleemoplossing](#)

[Gerelateerde informatie](#)

Inleiding

Dit document bevat procedures voor het opsporen en verhelpen van basisproblemen met de Cisco draadloze LAN-controllerkaart (WLCM).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van Lichtgewicht Access Point Protocol (LWAPP).
- Basiskennis van de manier om de module van WLCM te vormen om aan een Cisco Unified Wireless Network deel te nemen. **N.B.:** Als u een nieuwe gebruiker bent en niet aan een WLCM hebt gewerkt, raadpleegt u de [Functiehandleiding](#) voor [Cisco WLAN-controllers](#).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 2811 geïntegreerde services router (ISR) met versie 12.4(11)T met WLCM die versie 3.2.16.21 uitvoert
- Cisco 1030 en Cisco 1232AG lichtgewicht AP's (LAP's)
- Cisco 802.11a/b/g clientadapter voor draadloos LAN (WLAN) die versie 2.5 uitvoert
- Cisco Secure Access Control Server (ACS) met versie 3.2

N.B.: De hier genoemde onderdelen zijn alleen de apparaten die gebruikt werden om dit document te schrijven. De informatie over de volledige lijst van de ISR's die de WLCM ondersteunen en de LAP's die op de WLCM worden ondersteund, wordt geleverd in het gedeelte [Problemen oplossen](#) van dit document.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\) voor meer informatie over documentconventies](#).

Achtergrondinformatie

Cisco WLCM is ontworpen om kleine en middelgrote ondernemingen (MKB's) en ondernemingen filiaalklanten te voorzien van 802.11 draadloze netwerkoplossingen voor Cisco 2800 en Cisco 3800 Series ISR's en Cisco 3700 Series routers.

De Cisco WLCM stelt Cisco ISR's en Cisco 3700 Series routers in staat om tot zes WLAN-access points (AP's) te beheren, en de implementatie en het beheer van WLAN's te vereenvoudigen. Het besturingssysteem beheert alle functies voor gegevensclient, communicatie en systeembeheer, voert de functies Radio Resource Management (RRM) uit, beheert systeembreed mobiliteitsbeleid met behulp van de OSS (besturingssysteem security) en coördineert alle beveiligingsfuncties met behulp van het OSS-kader.

De Cisco WLCM werkt in combinatie met Cisco Aironet LAP's, Cisco Wireless Control System (WCS) en de Cisco draadloze locatie-applicatie ter ondersteuning van missie-cruciale draadloze gegevens, spraak- en videotoeepassingen.

Problemen oplossen

In dit gedeelte worden procedures voor het oplossen van problemen besproken voor

fundamentele problemen met de WLCM.

[ISR herkent de WLCM niet](#)

De WLCM wordt alleen op deze ISR-platforms ondersteund:

- Cisco 3725 en 3745 routers
- Cisco 2811, 2821 en 2851 ISR's
- Cisco 3825 en 3845 ISR's

Als er een andere ISR dan die welke in deze lijst gespecificeerd is, wordt de WLCM niet gedetecteerd. Zorg ervoor dat u de juiste hardware gebruikt.

Opmerking: De WLCM wordt alleen ondersteund in netwerkmodulesleuven. Het wordt niet ondersteund in EVM-sleuven die beschikbaar zijn in Cisco 2821 en Cisco 2851 ISR's.

Opmerking: u kunt slechts één Cisco WLCM-chassis in één routerchassis installeren.

Er zijn ook een aantal minimale softwarevereisten voor de WLCM.

ISR moet Cisco IOS-software release 12.4(2)XA1 (routersoftware) of hoger gebruiken om de WLCM te herkennen.

[Kan ik de Flash op de WLCM upgraden?](#)

De Cisco WLCM schepen met en start vanaf een geïnstalleerde 256-MB CompactFlash geheugenkaart. De compactFlash-geheugenkaart bevat de lader voor de laars, de Linux-punten, het WLCM- en het APs-uitvoerbaar bestand en de Cisco WLCM-configuratie.

De compactFlash-geheugenkaart in Cisco WLCM is niet in het veld vervangbaar.

[Is de WLCM Hot-swappable?](#)

De WLCM is niet hot-swappable op alle ISR-platforms. Online insertie en verwijdering (OIR) van de controller-module wordt alleen ondersteund op Cisco 3745 router en Cisco 3845 ISR.

[LAP's die op de WLCM worden ondersteund](#)

Alle LWAPP-enabled Cisco Aironet AP's worden ondersteund, wat de Cisco Aironet 1000, 1100 en 1200 Series omvat. De HWIC-AP interfacekaarten worden niet ondersteund.

[Kan geen toegang tot Fast Ethernet op de WLCM](#)

Dit is het verwachte gedrag. De externe Fast Ethernet-poort op de voorplaat van Cisco WLCM wordt niet ondersteund. De NM-WLC (WLCM-module) heeft slechts één Fast Ethernet-poort die intern op de host-router is aangesloten, en de externe Fast Ethernet-poort op de NM-typeplaat is uitgeschakeld en niet meer bruikbaar.

[De status van de WLCM controleren](#)

Geef de opdracht **Versie op** van de ISR om te controleren of het WLCM door de router wordt herkend en correct geïnstalleerd is.

```
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
```

Geef de opdracht **sleuf/poortstatus** van de servicemodule af om de status van de WLCM te vinden.

```
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
```

U kunt ook de opdracht **Service-Module WLAN-controller 1/0 statistieken** uitgeven om de module-reset statistieken van de WLCM te vinden.

```
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 sommige gevallen ziet u deze fout:

```
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
```

De reden voor deze fout kan een hardwarekwestie zijn. Open een TAC-case om dit probleem verder op te lossen. Om een TAC-case te openen, moet u een geldig contract met Cisco hebben. Raadpleeg [Technische ondersteuning](#) om contact op te nemen met Cisco TAC.

Geef de opdracht **show sysinfo** uit om meer informatie over de WLCM te ontvangen.

```
(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
```

[Hoe maken we correcties in de CLI Configuration Wizard](#)

Wanneer u de WLCM voor het eerst configureren (of nadat u de standaardinstellingen hebt hersteld) middels de wizard CLI Configuration, **wordt** de-toets gebruikt om de configuraties te corrigeren. Dit is een voorbeeld:

In plaats van **admin** in te voeren, **voert** de gebruiker **adminn** in om het te corrigeren. Voer bij de

volgende melding - in **en** klik vervolgens op Invoegen. Het systeem keert terug naar de vorige melding.

(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 registreert niet bij ISR WLCM - WLCM verzonden met onjuiste certificaten](#)

De *NM-AIR-WLC6-K9* en *NM-AIR-WLC6-K9=* WLCMs worden verzonden met onjuiste certificaten. Dit zorgt ervoor dat het WLCNM niet wordt geauthentiseerd door Cisco/Aironet APs. De WLCM's die tussen 1 februari 2006 en 22 maart 2006 zijn verzonden, worden aangetast. Een storing in het productieproces heeft de juiste certificaten niet naar WLCNM-inrichtingen gekopieerd. Het onjuiste certificaat creëert een RSA zeer belangrijke mismatch, wat op LWAPP gebaseerde APs ertoe brengt om niet aan te sluiten/te associëren/te registreren aan WLCNM.

Raadpleeg de [melding uit het veld: FN - 62379 - Netwerkmodule voor draadloze LAN-controllers vormt geen verificatie met Cisco/Airespace Access Point - hardware-upgrade](#) voor meer informatie hierover. Deze melding uit het veld bevat de tijdelijke versie, evenals de getroffen nummers voor netwerkmodule en seriële nummers.

[LAP registreert niet bij WLCM - De tijd voor het systeem is niet ingesteld](#)

De WLCM moet met de systeemtijd en -datum worden ingesteld. U kunt deze functie handmatig uitvoeren, of de WLCM kan worden ingesteld om de NTP-server te gebruiken. Als de tijd en datum niet zijn ingesteld, registreren de LAP's niet bij de WLCM. In de wizard CLI wordt u gevraagd de systeemtijd en -datum in te voeren. Als u de datum en het tijdstip niet invoert, ziet u dit waarschuwingsbericht:

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

Geef deze opdracht uit van de WLCM CLI om de tijd handmatig te configureren:

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

Geef deze opdracht uit als u wilt dat de WLCM de NTP-server gebruikt:

config time ntp server <index> <IP Address>

[Wachtwoordherstel voor de WLCM](#)

Wanneer het wachtwoord voor inloggen op de WLCM is kwijtgeraakt, kan de WLCM alleen worden hersteld door de standaardinstellingen van de WLCM te herstellen. Dit betekent ook dat de gehele configuratie op de WLCM wordt hersteld en vanaf nul moet worden ingesteld.

Raadpleeg [De WLCM opnieuw instellen op standaardinstellingen](#) voor informatie over het herstellen van de standaardinstellingen van de WLCM naar de fabriek.

[Cisco WLCM-LEDs](#)

Deze tabel toont de Cisco WLCM-LEDs en de betekenis:

LED	Betekenis
CF	De CompactFlash geheugenkaart is actief.
NL	De module is geslaagd voor zelftest en is beschikbaar voor de router.
PWR	De controllermodule beschikt over de nodige energie.

[upgrade van controllerfirmware mislukt](#)

Tijdens het upgradeproces kunt u bepaalde fouten tegenkomen die het upgradeproces beïnvloeden. In deze sectie wordt uitgelegd wat de foutmeldingen betekenen en hoe de fouten worden geëlimineerd en de controller wordt verbeterd.

- **Geen antwoord van de TFTP-server op de code is mislukt** - U ontvangt deze foutmelding als de TFTP-server niet actief is. Controleer of de TFTP-service op de server is ingeschakeld.
- **Bestandsoverdracht van code mislukt - fout vanaf server: Bestand is niet gevonden.**
Verwijking - U ontvangt deze foutmelding als het OS-bestand niet in de standaardmap van de TFTP-server staat. Om deze fout te elimineren, kopieert u het beeldbestand naar de standaardmap op de TFTP-server.
- **TFTP-fout bij opslaan in flitser!** - U ontvangt deze fout wanneer er een probleem is met de TFTP-server. Sommige TFTP-servers hebben een beperking op de omvang van de bestanden die u kunt overdragen. Gebruik een ander TFTP-serverprogramma. Er zijn veel gratis TFTP-serverhulpprogramma's beschikbaar. Cisco raadt het gebruik van de Tftpd32 versie 2.0 TFTP-server aan. Raadpleeg [Tftpd32](#) om deze TFTP-server te downloaden.
- **De installatiepartities worden vernietigd of de afbeelding is beschadigd** - Als u na een poging om de software te verbeteren nog steeds niet hebt gefunctioneerd, bestaat de mogelijkheid dat de afbeelding beschadigd is. Neem contact op met [Cisco technische ondersteuning](#) voor ondersteuning.

Raadpleeg het gedeelte [Upacteren van de Cisco WLAN-controlemodule-software](#) voor meer informatie over het upgraden van de firmware op de WLCM.

[Kan CDP niet inschakelen](#)

De gebruiker kan Cisco Discovery Protocol (CDP) niet inschakelen op de WLCM die op de 3750 ISR is geïnstalleerd. Dit bericht verschijnt:

```
(Cisco Controller) >show cdp neighbors
```

```
% CDP is not enabled
```

De gebruiker geeft de **configuratie cdp uit**, laat opdracht toe om CDP in te schakelen, maar ziet nog steeds hetzelfde bericht:

```
(Cisco Controller) >show cdp neighbors
```

```
% CDP is not enabled
```

Dit komt door Cisco bug-ID CSC67615. Hoewel de 3750G geïntegreerde draadloze LAN-controller CDP niet ondersteunt, zijn de CDP CLI-opdrachten beschikbaar voor deze controller. Dit besluit wordt op 4.0.2006 opgelost.

[Gebruik het IP-adres en de IP-voorwaartse protocolopdrachten om LAP's te registreren bij de WLCM](#)

Met de WLCM, is het voor een LAP lastig om de WLCM door IP-subnetuitzending te ontdekken. Dit komt door de manier waarop het WLCM op het achtervlak van ISR integreert en hoe de LAP doorgaans op een ander IP-net is (wat ook een goede aanbeveling is). Als u de IP SUBNET uitzending ontdekking met succes wilt uitvoeren, geef de **ip helper-adres** en **ip voorwaarts-protocol uit udp 1223** opdrachten.

In het algemeen, is het doel van deze opdrachten om elk potentieel IP-uitzendingsframe door te sturen of door te geven. Dit relais en de focus op de WLC beheerinterface moet voldoende zijn om te zorgen dat de WLC op de LAP reageert.

De opdracht **Help-adres voor IP** moet worden gegeven onder de interface waarmee de LAP is verbonden en de opdracht **ip-adres** moet verwijzen naar de beheerinterface van de WLC.

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

De **ip forward-protocol** opdracht is een wereldwijde configuratie opdracht.

```
ip forward-protocol udp 1223
```

[Opdrachten voor WLCM-probleemoplossing](#)

Deze sectie verschaft de opdrachten **debug** die u kunt gebruiken om problemen op te lossen met de WLCM-configuratie.

Debug-opdrachten om de LAP-registratie bij de controller te controleren:

Gebruik deze opdrachten **debug** om te controleren of de LAP's zich bij de WLCM registreren:

- **debug hoofdadres <AP-MAC-adres xx:xx:xx:xx:xx:xx>**—hiermee wordt MAC-adresdebugging voor de LAP ingesteld.
- **debug van lwapp gebeurtenissen** configuratie-debug van LWAPP gebeurtenissen en foutmeldingen.
- **debug pm laat pki toe**-configureren debug van de module van de veiligheidsbeleidsbeheerder.

Hier is een voorbeelduitvoer van de **debug lwapp gebeurtenissen** die opdracht **geven** wanneer de LAP zich registreert bij de 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

```

Hier is een voorbeelduitvoer van het debug pm-toestel om opdracht in te schakelen wanneer de LAP bij de WLCM registreert:

```

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
>cscscoDefaultIdCert<
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 opdrachten om webverificatie te controleren:

Gebruik deze **debug** opdrachten om te controleren of de webverificatie werkt zoals verwacht op de WLCM:

- **debug van alle** volgende AAA-berichten: hiermee wordt het debug van alle AAA-berichten hersteld.
- **debug pem state wellicht**— Configuration debug of policy Manager State Machine.
- **debug van pem gebeurtenissen**: configuratie debug van beleidsbeheergebeurtenissen.
- **debug pm ssh-appgw laat toe**-Configureert debug van toepassingsgateways.
- **debug pm ssh-tcp activeren**—hiermee wordt het debug van de tcp-behandeling van beleidsmanager ingesteld.

Hier zijn voorbeelduitgangen van sommige van deze **debug** opdrachten:

```
(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)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
```

Debug opdrachten om de DHCP-werking te controleren:

Gebruik deze **debug** opdrachten om DHCP-client- en serveractiviteiten te controleren:

- **debug dhcp bericht stelt u in staat**—displays om de informatie te zuiveren over de DHCP-clientactiviteiten en de status van DHCP-pakketten te controleren.
- **debug DHCP-pakket: schakelt-DHCP-pakketinformatie op.**

Hier zijn voorbeelduitgangen van deze **debug**-opdrachten:

```
(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 opdrachten om TFTP-upgrade te controleren:

- **Geeft het logbestand weer**—hiermee worden de berichtenlogbestanden weergegeven die zijn geschreven in de database van Cisco draadloze LAN-controllen. Als er meer dan 15 items zijn, wordt u gevraagd de in het voorbeeld weergegeven berichten weer te geven.
- **debug van overdrachtspoorlijn-configuratie debug van de overdracht of upgrade.**

Hier is een voorbeeld van de opdracht **debug transfersporen**:

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 opdrachten voor 802.1X/WAP/RSN/PMK-caching:

- debug dot1x allen activeren-displays 802.1X zuiverende informatie.Hier is een voorbeelduitvoer van deze opdracht:

```
(Cisco Controller) >debug dot1x all enable
```

```

Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_USER_NAME(1) index=0
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_CALLING_STATION_ID(31) index=1
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_CALLED_STATION_ID(30) index=2
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_PORT(5) index=3
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_IDENTIFIER(32) index=5
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_VAP_ID(1) index=6
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_SERVICE_TYPE(6) index=7

```


Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_FRAMED_MTU(12) index=8
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_EAP_MESSAGE(79) index=10
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_MESS_AUTH(80) index=11
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
AAA EAP Packet created request = 0xbbdfe944.. !!!!
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
AAA Message 'Interim Response' received for mobile 00:40:96:ac:e6:57
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Received EAP Attribute (code=1, length=24,id=1, dot1xcb->id = 1)
for mobile 00:40:96:ac:e6:57
Fri Mar 23 21:35:01 2007: 00000000: 01 01 00 18 11 01 00 08 38 93 8c 47 64 99
e1 d08..Gd...
00000010: 45 41 50 55 53 45 52 31 **EAPUSER1**
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Skipping AVP (0/80) for mobile 00:40:96:ac:e6:57
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_USER_NAME(1) index=0
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_CALLING_STATION_ID(31) index=1
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_CALLED_STATION_ID(30) index=2
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_PORT(5) index=3
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_IDENTIFIER(32) index=5
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_VAP_ID(1) index=6
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_SERVICE_TYPE(6) index=7
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_FRAMED_MTU(12) index=8
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_EAP_MESSAGE(79) index=10
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_MESS_AUTH(80) index=11
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
AAA EAP Packet created request = 0xbbdfe944.. !!!!
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
AAA Message 'Interim Response' received for mobile 00:40:96:ac:e6:57
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Received EAP Attribute (code=3, length=4,id=1, dot1xcb->id = 1)
for mobile 00:40:96:ac:e6:57
Fri Mar 23 21:35:01 2007: 00000000: 03 01 00 04
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57 Skipping AVP (0/80)
for mobile 00:40:96:ac:e6:57
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_USER_NAME(1) index=0
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_CALLING_STATION_ID(31) index=1
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_CALLED_STATION_ID(30) index=2
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_PORT(5) index=3
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4

```

Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_IDENTIFIER(32) index=5
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_VAP_ID(1) index=6
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_SERVICE_TYPE(6) index=7
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_FRAMED_MTU(12) index=8
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_EAP_MESSAGE(79) index=10
Fri Mar 23 21:35:01 2007: 00:40:96:ac:e6:57
Adding AAA_ATT_MESS_AUTH(80) index=11
Fri Mar 23 21:35:05 2007: 00:40:96:ac:e6:57
AAA EAP Packet created request = 0xbbdfe944.. !!!!
Fri Mar 23 21:35:05 2007: 00:40:96:ac:e6:57
AAA Message 'Success' received for mobile 00:40:96:ac:e6:57

```

- **debug dot11 allen toelaat**-het zuiveren van radiofuncties.
- **Laat client summier <mac>**-Hiermee geeft u samengevatte informatie weer voor client door MAC-adres.Hier is een voorbeelduitvoer van deze opdracht:

```
(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

[Gerelateerde informatie](#)

- [Cisco draadloze LAN-controllers - handleiding](#)
- [Functiehandleiding voor Cisco WLAN-controllers](#)
- [Configuratievoorbeelden van draadloze LAN-controllers \(WLCM\)](#)
- [Configuratievoorbeeld van draadloze LAN-controllers](#)
- [PPP-verificatie met WLAN-controllers \(WLC\) - configuratievoorbeeld](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)