Risoluzione dei problemi del modulo Wireless LAN Controller

Sommario

Introduzione

In questo documento vengono descritte le procedure di risoluzione dei problemi di base relativi al modulo Cisco Wireless LAN Controller Module (WLCM).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza del protocollo LWAPP (Lightweight Access Point Protocol).

- Conoscenze base di come configurare il modulo WLCM per partecipare a una rete wireless unificata Cisco.**Nota:** se si è un nuovo utente e non si è lavorato su un WLCM, consultare la guida alle funzionalità del modulo di rete del controller WLAN Cisco.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco 2811 Integrated Services Router (ISR) con versione 12.4(11)T e WLCM con versione 3.2.16.21
- Cisco 1030 e Cisco 1232 AG Lightweight AP (LAP)
- Cisco 802.11a/b/g Wireless LAN (WLAN) Client Adapter con versione 2.5
- Cisco Secure Access Control Server (ACS) con versione 3.2

Nota: i componenti elencati sono solo i dispositivi utilizzati per scrivere il documento. Le informazioni contenute nell'elenco completo degli ISR che supportano WLCM e i LAP supportati da WLCM sono disponibili nella sezione Risoluzione dei problemi di questo documento.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Il WLCM di Cisco è progettato per fornire alle piccole e medie imprese (PMI) e alle aziende che operano nelle filiali soluzioni di rete wireless 802.11 per Cisco serie 2800 e 3800 ISR e router Cisco serie 3700.

Cisco WLCM consente agli ISR Cisco e ai router Cisco serie 3700 di gestire fino a sei access point WLAN (AP) e semplifica l'installazione e la gestione delle WLAN. Il sistema operativo gestisce tutte le funzioni di gestione dei client di dati, delle comunicazioni e del sistema, esegue le funzioni RRM (Radio Resource Management), gestisce le policy di mobilità a livello di sistema utilizzando la sicurezza del sistema operativo e coordina tutte le funzioni di sicurezza utilizzando la struttura OSS.

Il WLCM di Cisco funziona in combinazione con i Cisco Aironet LAP, Cisco Wireless Control System (WCS) e Cisco Wireless Location Appliance per supportare applicazioni dati, voce e video mission-critical.

Risoluzione dei problemi

In questa sezione vengono descritte le procedure di risoluzione dei problemi di base relativi a WLCM.

ISR non riconosce WLCM

WLCM è supportato solo sulle seguenti piattaforme ISR:

- Router Cisco 3725 e 3745
- Cisco 2811, 2821 e 2851 ISR
- Cisco 3825 e 3845 ISR

Se viene visualizzato un ISR diverso da quelli specificati nell'elenco, WLCM non viene rilevato. Assicurarsi di utilizzare l'hardware corretto.

Nota: WLCM è supportato solo negli slot dei moduli di rete. Non è supportato negli slot EVM disponibili nei Cisco 2821 e Cisco 2851 ISR.

Nota: è possibile installare solo un Cisco WLCM in un singolo chassis del router.

Per WLCM sono inoltre previsti alcuni requisiti software minimi.

Affinché l'ISR riconosca WLCM, deve usare il software Cisco IOS® versione 12.4(2)XA1 (software router) o successive.

È possibile aggiornare Flash su WLCM?

Il WLCM di Cisco viene fornito con una scheda di memoria CompactFlash da 256 MB e si avvia da tale scheda. La scheda di memoria CompactFlash contiene il bootloader, il kernel Linux, il file eseguibile Cisco WLCM e AP e la configurazione Cisco WLCM.

La scheda di memoria CompactFlash in Cisco WLCM non può essere sostituita sul campo.

WLCM è sostituibile a caldo?

WLCM non è sostituibile a caldo su tutte le piattaforme ISR. L'inserimento e la rimozione online (OIR) del modulo controller è supportato solo sui router Cisco 3745 e Cisco 3845 ISR.

LAP supportati su WLCM

Sono supportati tutti i Cisco Aironet AP abilitati per LWAPP, compresi i Cisco Aironet serie 1000, 1100 e 1200. Le schede di interfaccia HWIC-AP non sono supportate.

Impossibile accedere a Fast Ethernet su WLCM

Si tratta di un comportamento previsto. La porta Fast Ethernet esterna sul pannello anteriore del Cisco WLCM non è supportata. L'NM-WLC (modulo WLCM) ha solo una porta Fast Ethernet collegata internamente al router host e la porta Fast Ethernet esterna sul pannello frontale dell'NM è disabilitata e inutilizzabile.

Controllare lo stato di WLCM

Utilizzare il comando **show version** dall'ISR per verificare se WLCM è riconosciuto dal router e installato correttamente.

```
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
```

Per individuare lo stato del WLCM, usare il comando **service-module wlan-controller slot/port status**.

```
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
```

èpossibile anche usare il comando **service-module wlan-controller 1/0 statistics** per trovare le statistiche di ripristino del modulo di WLCM.

```
2800-ISR-TSWEB#service-module wlan-controller 1/0 statistics
Module Reset Statistics:
  CLI reset count = 0
  CLI reload count = 0
```

```
  Registration request timeout reset count = 0
  Error recovery timeout reset count = 0
  Module registration count = 4
```

In alcuni casi viene visualizzato il seguente errore:

```
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
```

Questo errore potrebbe essere dovuto a un problema hardware. Apri una richiesta TAC per risolvere ulteriormente il problema. Per aprire una richiesta TAC, è necessario avere un contratto valido con Cisco. Per contattare il centro TAC Cisco, consultare il supporto tecnico.

Per ricevere ulteriori informazioni su WLCM, usare il comando **show sysinfo**.

```
(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
```

Come apportare correzioni nella Configurazione guidata CLI

Quando si configura WLCM per la prima volta (o dopo il ripristino dei valori predefiniti) utilizzando la Configurazione guidata CLI, viene utilizzata la chiave **-** per apportare le correzioni alle configurazioni. Questo è un esempio:

In questo caso, invece di immettere **admin**, l'utente immette **admin** per correggerlo. Al prompt successivo, immettere **-**, quindi fare clic su Invio. Il sistema torna al prompt precedente.

```
(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.
```

Il LAP non si registra presso l'ISR WLCM - WLCM fornito con certificati non corretti

I modelli *NM-AIR-WLC6-K9* e *NM-AIR-WLC6-K9=* WLCM vengono spediti con certificati errati. In questo modo, il WLCNM non verrà autenticato dai Cisco/Airespace AP. I WLCM spediti tra il 1° febbraio 2006 e il 22 marzo 2006 sono interessati. Errore del processo di produzione. Impossibile copiare i certificati corretti nei dispositivi WLCNM. Il certificato errato crea una mancata corrispondenza della chiave RSA, che impedisce agli access point basati su LWAPP di unirsi/associare/registrarsi a WLCNM.

Per ulteriori informazioni, fare riferimento al documento sulla comunicazione dei prodotti: FN - 62379 - Wireless LAN Controller Network Module non esegue l'autenticazione con i Cisco/Airespace Access Point - Aggiornamento hardware per ulteriori informazioni su questo argomento. Questo avviso contiene la soluzione alternativa e i numeri di parte e di serie del modulo di rete interessati.

Il LAP non si registra nel WLCM - Ora di sistema non impostata

WLCM deve essere configurato con la data e l'ora di sistema. È possibile eseguire questa operazione manualmente oppure configurare WLCM per l'utilizzo del server NTP. Se l'ora e la data non sono impostate, i LAP non si registrano con WLCM. Nella procedura guidata CLI, viene richiesto di immettere la data e l'ora del sistema. Se non si immettono la data e l'ora, verrà visualizzato questo messaggio di avviso:

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

Utilizzare questo comando dalla CLI di WLCM per configurare manualmente l'ora:

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

Utilizzare questo comando se si desidera che WLCM utilizzi il server NTP:

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

Recupero password per WLCM

Quando la password di accesso a WLCM viene persa, l'unico modo per accedere a WLCM è ripristinare le impostazioni predefinite. Ciò significa anche che l'intera configurazione di WLCM

viene reimpostata e deve essere configurata da zero.

Per informazioni su come ripristinare WLCM ai valori predefiniti, fare riferimento a Ripristino delle impostazioni predefinite di WLCM.

LED Cisco WLCM

Nella tabella seguente vengono elencati i LED di Cisco WLCM e i relativi significati:

LED	Significato
CF	La scheda di memoria CompactFlash è attiva.
IT	Il modulo ha superato la verifica automatica ed è disponibile per il router.
PWR	L'alimentazione è disponibile per il modulo controller.

Aggiornamento del firmware del controller non riuscito

Durante il processo di aggiornamento, è possibile riscontrare alcuni errori che influiscono sul processo di aggiornamento. In questa sezione viene illustrato il significato dei messaggi di errore e viene spiegato come eliminare gli errori e aggiornare il controller.

- **Trasferimento del file di codice non riuscito-Nessuna risposta dal server TFTP**—Questo messaggio di errore viene visualizzato se il server TFTP non è attivo. Verificare se il servizio TFTP è abilitato sul server.
- **Trasferimento file di codice non riuscito - Errore dal server: Impossibile trovare il file. Interruzione del trasferimento**: questo messaggio di errore viene visualizzato se il file del sistema operativo non è presente nella directory predefinita del server TFTP. Per eliminare questo errore, copiare il file immagine nella directory predefinita sul server TFTP.
- **Errore TFTP durante l'archiviazione nella memoria flash!** - Questo errore si verifica quando si verifica un problema con il server TFTP. Alcuni server TFTP hanno un limite alle dimensioni dei file che è possibile trasferire. Utilizzare una Server Utility TFTP diversa. Sono disponibili molte utilità server TFTP gratuite. Cisco consiglia di utilizzare il server TFTP Tftpd32 versione 2.0. Fare riferimento a Tftpd32 per scaricare questo server TFTP.
- **Le partizioni di installazione vengono distrutte o l'immagine è danneggiata**. Se il tentativo di aggiornare il software non riesce, l'immagine potrebbe essere danneggiata. Per assistenza, contattare il supporto tecnico Cisco.

Per ulteriori informazioni su come aggiornare il firmware sul WLCM, fare riferimento a Aggiornamento del software Cisco WLAN Controller Module.

Impossibile abilitare CDP

L'utente non può abilitare Cisco Discovery Protocol (CDP) sul WLCM installato sull'ISR 3750. Viene visualizzato questo messaggio:

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

L'utente usa il comando **config cdp enable** per abilitare il CDP, ma visualizza ancora questo

messaggio:

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

Questo problema è dovuto all'ID bug Cisco CSCsg67615. Sebbene il controller LAN wireless integrato 3750G non supporti il CDP, per questo controller sono disponibili i comandi CLI di CDP. Questa condizione viene risolta nella versione 4.0.206.0.

Per registrare i LAP sul WLCM, usare i comandi ip-helper address e ip-forward protocol

Con il WLCM, è difficile per un LAP scoprire il WLCM attraverso la trasmissione della subnet IP. Ciò è dovuto al modo in cui il WLCM si integra sul backplane dell'ISR e a come il LAP si trovi in genere su una subnet IP diversa (il che è anche una buona raccomandazione). Se si desidera eseguire correttamente il rilevamento della trasmissione della subnet IP, usare i comandi **ip helper-address** e **ip forward-protocol udp 1223**.

In generale, lo scopo di questi comandi è inoltrare o inoltrare qualsiasi frame di broadcast IP potenziale. Questo relay e il suo indirizzamento all'interfaccia di gestione del WLC devono essere adeguati a garantire che il WLC risponda nuovamente al LAP.

Il comando **ip helper-address** deve essere inviato sotto l'interfaccia a cui è connesso il LAP e il comando **ip helper-address** deve puntare all'interfaccia di gestione del WLC.

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

Il comando **ip forward-protocol** è un comando di configurazione globale.

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

Comandi per la risoluzione dei problemi di WLCM

In questa sezione vengono forniti i comandi di **debug** che è possibile utilizzare per risolvere i problemi relativi alla configurazione di WLCM.

Comandi di debug per verificare la registrazione dei LAP sul controller:

Per verificare se i LAP si registrano su WLCM, usare i seguenti comandi di **debug**:

- **debug mac addr <AP-MAC-address xx:xx:xx:xx:xx:xx>**—Configura il debug dell'indirizzo MAC per il LAP.
- **debug lwapp events enable**: configura il debug di eventi LWAPP e messaggi di errore.
- **debug pm pki enable**: configura il debug del modulo security policy manager.

Di seguito è riportato un output di esempio del comando **debug lwapp events enable** quando il LAP si registra su 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, 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
```

Di seguito è riportato un esempio di output del comando **debug pm pki enable** quando il LAP si registra con WLCM:

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

```
 Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert<
 Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 1, CA cert >bsnDefaultRootCaCert<
 Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 2, CA cert >bsnDefaultCaCert<
 Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: called to get cert for CID 2816f436
 Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 0, certname
>bsnOldDefaultCaCert<
 Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 1, certname
>bsnDefaultRootCaCert<
 Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 2, certname
>bsnDefaultCaCert<
 Mon Mar 12 16:30:40 2007: ssphmUserCertVerify: calling x509_decode()
 Mon Mar 12 16:30:40 2007: ssphmUserCertVerify: failed to verify AP cert
>bsnDefaultCaCert<
 Mon Mar 12 16:30:40 2007: sshpmGetCID: called to evaluate <bsnOldDefaultCaCert>
 Mon Mar 12 16:30:40 2007: sshpmGetCID: comparing to row 0, CA cert
>bsnOldDefaultCaCert<
 Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: called to get cert for CID 226b9636
 Mon Mar 12 16:30:40 2007: sshpmGetCertFromCID: comparing to row 0, certname
>bsnOldDefaultCaCert<
 Mon Mar 12 16:30:40 2007: ssphmUserCertVerify: calling x509_decode()
 Mon Mar 12 16:30:40 2007: ssphmUserCertVerify: user cert 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
```

Comandi di debug per verificare l'autenticazione Web:

Utilizzare questi comandi **debug** per verificare se l'autenticazione Web funziona come previsto in WLCM:

- **debug aaa all enable**: configura il debug di tutti i messaggi AAA.
- **debug pem state enable**: configura il debug della macchina a stati di policy manager.
- **debug pem events enable**: configura il debug degli eventi di policy manager.
- **debug pm ssh-appgw enable**: configura il debug dei gateway dell'applicazione.
- **debug pm ssh-tcp enable**: configura il debug della gestione tcp di policy manager.

Di seguito vengono riportati alcuni output di esempio di alcuni di questi comandi **debug**:

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

User user1 authenticated
00:40:96:ac:e6:57 Returning AAA Error 'Success' (0) for mobile 00:40:96:ac:e6:57
AuthorizationResponse: 0xbadff97c
      structureSize.............................70
      resultCode................................0
      protocolUsed..............................0x00000008
      proxyState................................00:40:96:AC:E6:57-00:00
      Packet contains 2 AVPs:
          AVP[01] Service-Type.........................0x00000001 (1) (4 bytes)
          AVP[02] Airespace / WLAN-Identifier..........0x00000001 (1) (4 bytes)
00:40:96:ac:e6:57 Applying new AAA override for station 00:40:96:ac:e6:57
00:40:96:ac:e6:57 Override values for station 00:40:96:ac:e6:57 source: 48,
valid bits: 0x1 qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: '', aclName:
00:40:96:ac:e6:57 Unable to apply override policy for
station 00:40:96:ac:e6:57 - VapAllowRadiusOverride is FALSE
      AccountingMessage Accounting Start: 0xa62700c
      Packet contains 13 AVPs:
      AVP[01] User-Name............................user1 (5 bytes)
      AVP[02] Nas-Port.............................0x00000001 (1) (4 bytes)
      AVP[03] Nas-Ip-Address.......................0x0a4df4d2 (172881106) (4 bytes)
      AVP[04] NAS-Identifier.......................0x574c4331 (1464615729) (4 bytes)
      AVP[05] Airespace / WLAN-Identifier..........0x00000001 (1) (4 bytes)
      AVP[06] Acct-Session-Id......................45e84f50/00:40:96:ac:e6:57/9 (28 bytes)
      AVP[07] Acct-Authentic.......................0x00000002 (2) (4 bytes)
      AVP[08] Tunnel-Type..........................0x0000000d (13) (4 bytes)
      AVP[09] Tunnel-Medium-Type...................0x00000006 (6) (4 bytes)
      AVP[10] Tunnel-Group-Id......................0x3330 (13104) (2 bytes)
      AVP[11] Acct-Status-Type.....................0x00000001 (1) (4 bytes)
      AVP[12] Calling-Station-Id...................10.0.0.1 (8 bytes)
      AVP[13] Called-Station-Id....................10.77.244.210 (13 bytes)


when web authentication is closed by user:
```

```
(Cisco Controller) >

      AccountingMessage Accounting Stop: 0xa627c78
      Packet contains 20 AVPs:
      AVP[01] User-Name.............................user1 (5 bytes)
      AVP[02] Nas-Port..............................0x00000001 (1) (4 bytes)
      AVP[03] Nas-Ip-Address........................0x0a4df4d2 (172881106) (4 bytes)
      AVP[04] NAS-Identifier........................0x574c4331 (1464615729) (4 bytes)
      AVP[05] Airespace / WLAN-Identifier...........0x00000001 (1) (4 bytes)
      AVP[06] Acct-Session-Id.......................45e84f50/00:40:96:ac:e6:57/9 (28 bytes)
      AVP[07] Acct-Authentic........................0x00000002 (2) (4 bytes)
      AVP[08] Tunnel-Type...........................0x0000000d (13) (4 bytes)
      AVP[09] Tunnel-Medium-Type....................0x00000006 (6) (4 bytes)
      AVP[10] Tunnel-Group-Id.......................0x3330 (13104) (2 bytes)
      AVP[11] Acct-Status-Type......................0x00000002 (2) (4 bytes)
      AVP[12] Acct-Input-Octets.....................0x0001820e (98830) (4 bytes)
      AVP[13] Acct-Output-Octets....................0x00005206 (20998) (4 bytes)
      AVP[14] Acct-Input-Packets....................0x000006ee (1774) (4 bytes)
      AVP[15] Acct-Output-Packets...................0x00000041 (65) (4 bytes)
      AVP[16] Acct-Terminate-Cause..................0x00000001 (1) (4 bytes)
      AVP[17] Acct-Session-Time.....................0x000000bb (187) (4 bytes)
      AVP[18] Acct-Delay-Time.......................0x00000000 (0) (4 bytes)
      AVP[19] Calling-Station-Id....................10.0.0.1 (8 bytes)
      AVP[20] Called-Station-Id.....................10.77.244.210 (13 bytes)

(Cisco Controller) >debug pem state enable

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

```
AUTHCHECK (2) Change state to L2AUTHCOMPLETE (4)
Fri Mar  2 16:28:30 2007: 00:16:6f:6e:36:2b 0.0.0.0
L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7)
Fri Mar  2 16:28:34 2007: 00:16:6f:6e:36:2b 30.0.0.2
DHCP_REQD (7) Change stateto WEBAUTH_REQD (8)

(Cisco Controller) >debug pem events enable

Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
START (0) Initializing policy
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
L2AUTHCOMPLETE (4)Plumbed mobile LWAPP rule on AP 00:0b:85:5b:fb:d0
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8) Adding TMP rule
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8) Replacing Fast Path rule
  type = Temporary Entry on AP 00:0b:85:5b:fb:d0, slot 0,
interface = 1 ACL Id = 255,
Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 1506
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8) Successfully plumbed mobile rule (ACL ID 255)
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8) Deleting mobile policy rule 27
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57
Adding Web RuleID 28 for mobile 00:40:96:ac:e6:57
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8)Adding TMP rule
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8)ReplacingFast Path rule type = Temporary Entry
on AP 00:0b:85:5b:fb:d0, slot 0, interface = 1 ACL Id = 255,
Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 1506
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1
WEBAUTH_REQD (8)Successfully plumbed mobile rule (ACL ID 255)
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Removed NPU entry.
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Added NPU entry of type 8
Fri Mar  2 16:31:06 2007: 00:40:96:ac:e6:57 10.0.0.1 Added NPU entry of type 8
```

Comandi di debug per verificare il funzionamento DHCP:

Utilizzare questi comandi **debug** per controllare le attività del client e del server DHCP:

- **debug dhcp message enable**: visualizza le informazioni di debug sulle attività del client DHCP e per monitorare lo stato dei pacchetti DHCP.
- **debug dhcp packet enable**: visualizza le informazioni a livello di pacchetto DHCP.

Di seguito sono riportati alcuni output di esempio dei seguenti comandi di **debug**:

```
(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
```

Comandi di debug per verificare l'aggiornamento TFTP:

- **show msglog**: visualizza i log dei messaggi scritti nel database dei controller LAN wireless Cisco. Se sono presenti più di 15 voci, verrà richiesto di visualizzare i messaggi illustrati nell'esempio.
- **debug transfer trace**: configura il debug del trasferimento o dell'aggiornamento.

Di seguito è riportato un esempio del comando **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
```

Comandi di debug per la memorizzazione nella cache 802.1X/WPA/RSN/PMK:

- **debug dot1x all enable**: visualizza le informazioni di debug 802.1X.Di seguito è riportato un output di esempio di questo comando:

```
(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**: abilita il debug delle funzioni radio.
- **show client summary** *<mac>* : visualizza le informazioni di riepilogo per il client in base all'indirizzo MAC.Di seguito è riportato un output di esempio di questo comando:

```
(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
```

Informazioni correlate

- Guida di riferimento ai comandi di Cisco Wireless LAN Controller
- Guida alle funzionalità di Cisco WLAN Controller Network Module
- Esempi di configurazione del modulo WLCM (Wireless LAN Controller Module)
- Esempio di configurazione dell'autenticazione Web del controller LAN wireless
- Esempio di configurazione dell'autenticazione EAP con i controller WLAN (WLC)
- Documentazione e supporto tecnico – Cisco Systems