Troubleshooting do módulo do controlador do Wireless LAN

Índice

Introdução

Este documento fornece procedimentos para o troubleshooting de problemas básicos com o Cisco Wireless LAN Controller Module (WLCM).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do Lightweight Access Point Protocol (LWAPP).
- Conhecimento básico de como configurar o módulo WLCM para participar em uma rede de Cisco Unified Wireless.**Nota:** Se você é um novo usuário e não trabalhou em um WLCM, refira o guia de função do módulo de rede do controlador de WLAN de Cisco.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- O Roteador de serviços integrados Cisco 2811 (ISR) esse executa a versão 12.4(11)T com WLCM que executa a versão 3.2.116.21
- AG AP de pouco peso de Cisco 1030 e de Cisco 1232 (regaços)
- Adaptador cliente do Wireless LAN de Cisco 802.11a/b/g (WLAN) que executa a versão 2.5
- O Serviço de controle de acesso Cisco Secure (ACS) esse executa a versão 3.2

Nota: Os componentes alistados aqui são somente os dispositivos que foram usados para redigir este documento. A informação na lista completa dos ISR que apoiam os WLCM e os regaços que são apoiados no WLCM é fornecida na seção da pesquisa de defeitos deste documento.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Cisco WLCM é projetado fornecer as pequenas e médias empresas (SMB) e os clientes do escritório da filial de empreendimento as soluções da rede de comunicação Wireless do 802.11 para o Cisco 2800 e Cisco 3800 Series ISR e os Cisco 3700 Series Router.

Cisco WLCM permite Cisco ISR e Cisco 3700 Series Router de controlar até seis pontos de acesso a WLAN (AP), e simplifica o desenvolvimento e o Gerenciamento dos WLAN. O sistema operacional controla todo o cliente dos dados, comunicações, e funções da administração do sistema, executa funções do Radio Resource Management (RRM), controla políticas sistema-largas da mobilidade usando a Segurança do sistema operacional (OSS), e coordena todas as funções da Segurança usando a estrutura OSS.

Cisco WLCM trabalha conjuntamente com regaços do Cisco Aironet, Sistema de controle sem fio da Cisco (WCS), e a Aplicação de localização sem fio da Cisco para apoiar dados wireless, Voz, e aplicativos de vídeo da missão crítica.

Troubleshooting

Esta seção discute procedimentos de Troubleshooting para problemas básicos com o WLCM.

O ISR não reconhece o WLCM

O WLCM é apoiado somente nestas plataformas ISR:

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

Se qualquer outro ISR do que esses especificados nesta lista aparece, a seguir o WLCM não está detectado. Assegure-se de que você use o hardware correto.

Nota: O WLCM é apoiado somente nos slots de módulo de rede. Não é apoiado nos entalhes EVM disponíveis em Cisco 2821 e em Cisco 2851 ISR.

Nota: Você pode instalar somente um Cisco WLCM em um chassi do roteador único.

Há igualmente alguns requisitos de software mínimo para o WLCM.

O ISR deve usar a liberação 12.4(2)XA1 do Cisco IOS ® Software (software do roteador) ou mais tarde para que o ISR reconheça o WLCM.

Posso eu promover o flash no WLCM?

Cisco WLCM envia com e botas de uma placa de memória instalada do CompactFlash 256-MB. A placa de memória do CompactFlash contém o Boot Loader, arquivo executável do kernel (centro) de Linux, do Cisco WLCM e AP, e a configuração de Cisco WLCM.

A placa de memória do CompactFlash em Cisco WLCM não é campo-substituível.

É o WLCM swappable recente?

O WLCM não é swappable recente em todas as plataformas ISR. O Online Insertion and Removal (OIR) do módulo do controlador é apoiado somente no Cisco 3745 Router e no Cisco 3845 ISR.

Regaços apoiados no WLCM

Todo o Cisco Aironet LWAPP-permitido AP é apoiado, que inclui o Cisco Aironet 1000, 1100, e 1200 Series. As placas de interface HWIC-AP não são apoiadas.

Incapaz de alcançar o Fast Ethernet no WLCM

Este é o comportamento esperado. A porta de Ethernet rápida externo na placa dianteira de Cisco WLCM não é apoiada. O NM-WLC (módulo WLCM) tem somente uma porta de Ethernet rápida conectada internamente ao roteador host, e a porta de Ethernet rápida externo na placa dianteira NM é desabilitado e inusável.

Verifique o estado do WLCM

Emita o **comando show version do** ISR a fim verificar se o WLCM é reconhecido pelo roteador e instalado corretamente.

```
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
```

Emita o comando status da /porta do entalhe do WLAN-controlador do módulo de serviço a fim encontrar o estado do WLCM.

```
2800-ISR-TSWEB#service-module wlan-controller 1/0 status
Service Module is Cisco wlan-controller1/0
Service Module supports session via TTY line 66
Service Module is in Steady state
Getting status from the Service Module, please wait..

Cisco WLAN Controller 3.2.116.21
```

Você pode igualmente emitir o comando statistics do WLAN-controlador 1/0 do módulo de serviço a fim encontrar as estatísticas da reinicialização de módulo do 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
```

Em alguns casos, você vê este erro:

```
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
```

O motivo desse erro pode ser um problema de hardware. Abra uma ocorrência do TAC para fazer troubleshooting adicional deste problema. Para abrir uma ocorrência do TAC, você precisa de um contrato válido com Cisco. [Consulte o Suporte Técnico para saber como entrar em contato com o TAC Cisco.]

Emita o comando do **sysinfo da mostra** a fim receber mais informação no WLCM.

```
(Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems, Inc
Product Name..................................... Cisco Controller
Product Version.................................. 3.2.116.21
RTOS Version..................................... 3.2.116.21
Bootloader Version............................... 3.2.116.21
Build Type....................................... DATA + WPS

System Name...................................... WLCM
System Location..................................
System Contact...................................
System ObjectID.................................. 1.3.6.1.4.1.14179.1.1.4.5
IP Address....................................... 60.0.0.2
System Up Time................................... 0 days 0 hrs 39 mins 18 secs

Configured Country............................... United States

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled
Number of WLANs.................................. 1
3rd Party Access Point Support................... Disabled
Number of Active Clients......................... 0
```

Como nós fazemos correções no assistente da configuração de CLI

Quando você configurar o WLCM pela primeira vez (ou após a restauração aos padrões) que usa o assistente da configuração de CLI, **- a** chave é usada a fim fazer correções às configurações. Este é um exemplo:

Aqui, em vez de incorporar o **admin**, o usuário incorpora o **adminn** para corrigi-lo. Na alerta seguinte, entre **-**, a seguir clique entram. O sistema retorna à alerta 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.
```

O REGAÇO não se registra com ISR WLCM - WLCM enviado com Certificados incorretos

Os NM-AIR-WLC6-K9 e os *NM-AIR-WLC6-K9=* WLCMs são enviados com Certificados incorretos. Isto faz com que o WLCNM não seja autenticado por Cisco/Airespace AP. O WLCMs enviado entre o 1º de fevereiro de 2006 e março o 22, 2006 é afetado. Uma falha do processo de fabricação não copiou os Certificados corretos aos dispositivos WLCNM. O certificado incorreto cria uma incompatibilidade de chave RSA, que faça com que os AP LWAPP-baseados falhem se juntar/associado/registro a WLCNM.

Consulte Field Notice: O FN - 62379 - módulo de rede do controlador do Wireless LAN não autentica com Cisco/Access point de Airespace - upgrade de hardware para obter mais informações sobre deste. Este Field Notice contém a ação alternativa, assim como os part numbers e os números de série afetados do módulo de rede.

O REGAÇO não se registra com o WLCM - tempo de sistema não ajustado

O WLCM tem que ser configurado com o tempo de sistema e a data. Pode ou ser feito manualmente, ou o WLCM pode ser configurado para usar o servidor de NTP. Se as horas e data não são ajustadas, os regaços não se registram com o WLCM. No assistente CLI, você é alertado incorporar o tempo de sistema e a data. Se você não incorpora a data e hora, você vê este mensagem de advertência:

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

Emita este comando do WLCM CLI a fim configurar manualmente o tempo:

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

Emita este comando se você quer o WLCM usar o servidor de NTP:

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

Recuperação de senha para o WLCM

Quando a senha a entrar ao WLCM é perdida, a única maneira de obter no WLCM é restaurar o WLCM de volta às configurações padrão. Isto igualmente significa que a configuração completa no WLCM está restaurada e tem que ser configurado a partir do zero.

Consulte para restaurar o WLCM às configurações padrão para obter informações sobre de como restaurar o WLCM aos padrões de fábrica.

Diodo emissor de luz de Cisco WLCM

Esta tabela alista o diodo emissor de luz de Cisco WLCM e os significados:

LED	Significado
CF	A placa de memória do CompactFlash é ativa.
EN	O módulo passou o self-test e está disponível ao roteador.
PWR	A potência está disponível ao módulo do controlador.

A elevação do firmware de controlador falha

Durante o processo de upgrade, você pode vir através de alguns erros que afetam o processo de upgrade. Esta seção explica que o meio dos Mensagens de Erro e como eliminar os erros e promover o controlador.

- **Transferência de arquivo de código falhar-nenhuma resposta do servidor TFTP** — você recebe este Mensagem de Erro se o servidor TFTP não é ativo. Verifique se o serviço TFTP está habilitado no server.
- **Code file transfer failed - Error from server: O arquivo não foi encontrado. Abortando transferência** — Você recebe este Mensagem de Erro se o arquivo do OS não está atual no diretório padrão do servidor TFTP. A fim eliminar este erro, copie o arquivo de imagem ao diretório padrão no servidor TFTP.
- **TFTP Failure while storing in flash!** — Você recebe este erro quando há um problema com o servidor TFTP. Alguns servidores TFTP têm uma limitação no tamanho dos arquivos que você pode transferir. Use uma utilidade diferente do servidor TFTP. Há muitas utilidades livres do servidor TFTP que estão disponíveis. Cisco recomenda o uso do servidor TFTP da versão 2.0 de Tftpd32. Refira Tftpd32 a fim transferir este servidor TFTP.
- **As separações da instalação estão destruídas ou a imagem está corrompida** — se você é ainda mal sucedido depois que uma tentativa de promover o software, há uma possibilidade que sua imagem está corrompida. Contacte o Suporte técnico de Cisco para o auxílio.

Refira o melhoramento do software do módulo do controlador de WLAN de Cisco para obter mais informações sobre de como promover o firmware no WLCM.

Não pode permitir o CDP

O usuário não pode permitir o Cisco Discovery Protocol (CDP) no WLCM instalado nos 3750 ISR. Esta mensagem aparece:

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

O usuário emite o **comando cdp enable da configuração** a fim permitir o CDP, mas ainda vê esta mesma mensagem:

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

Isto é devido à identificação de bug Cisco CSCsg67615. Embora o controlador integrado 3750G do Wireless LAN não apoie o CDP, os comandos CLI CDP estão disponíveis para este controlador. Isto é resolvido em 4.0.206.0.

Use o endereço do ajudante de IP e os comandos protocol IP-dianteiros aos regaços do registro com o WLCM

Com o WLCM, é difícil para um REGAÇO descobrir o WLCM com o broadcast de sub-rede IP. Isto é devido a como o WLCM integra no back plane do ISR e a como o REGAÇO está tipicamente em uma sub-rede diferente IP (que é igualmente uma boa recomendação). Se você quer executar a descoberta do broadcast de sub-rede IP com o sucesso, emita os comandos **UDP 12223 do endereço auxiliar IP** e do dianteiro-**protocolo IP**.

Geralmente, a finalidade destes comandos é enviar ou retransmitir todo o quadro potencial da transmissão IP. Este relé e a direção dela à interface de gerenciamento WLC devem ser adequados certificar-se que o WLC responde de volta ao REGAÇO.

O comando ip helper-address deve ser dado sob a relação a que o REGAÇO é conectado, e o **comando ip helper-address** deve apontar à interface de gerenciamento do WLC.

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

O comando ip forward-protocol é um comando global configuration.

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

Comandos de Troubleshooting WLCM

Esta seção fornece os **comandos debug que** você pode se usar a fim pesquisar defeitos a configuração WLCM.

Comandos Debug verificar o REGAÇO que registra-se com o controlador:

Use estes **comandos debug** a fim verificar se os regaços se registram com o WLCM:

- **debugar o <AP-MAC-endereço xx do ADDR do Mac: xx: xx: xx: xx: xx>** — Configura a eliminação de erros do MAC address para o REGAÇO.
- **debugar eventos do lwapp permitem** — Configures debuga de eventos e de Mensagens de Erro LWAPP.
- **debugar o pki pm permitem** — Configures debuga do módulo do gerente da política de segurança.

Estão aqui umas saídas de exemplo do **comando debug lwapp events enable** quando o REGAÇO se registra com o 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
```

Estão aqui umas saídas de exemplo do **comando debug pm pki enable** quando o REGAÇO se registra com o 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
```

Comandos Debug verificar a autenticação da Web:

Use estes **comandos debug** a fim verificar se a autenticação da Web trabalha como esperado no WLCM:

- **debugar o aaa que todos permitem** — Configures debuga de todos os mensagens AAA.
- **debugar o estado PEM permitem** — Configures debuga da máquina de estado do gerente da política.
- **debugar eventos PEM permitem** — Configures debuga de eventos do gerente da política.
- **debugar pm SSH-appgw permitem** — Configures debuga dos gateway de aplicativo.
- **debugar pm SSH-TCP permitem** — Configures debuga da manipulação tcp do gerente da política.

Estão aqui os exemplos de saída de alguns destes **comandos 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
```

Comandos Debug verificar a operação de DHCP:

Use estes **comandos debug** a fim verificar o DHCP Client e as atividades do servidor:

- **debugar o mensagem DHCP permitem** — Informação sobre debugging dos indicadores sobre as atividades DHCP Client e para monitorar o estado dos pacotes DHCP.
- **debugar o pacote DHCP permite** — Informação do nível do pacote DHCP dos indicadores.

Estão aqui os exemplos de saída destes **comandos 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
```

Comandos Debug verificar a elevação TFTP:

- **msglog da mostra** — Indica os log de mensagens escritos ao base de dados do controlador de LAN do Cisco Wireless. Se há mais de 15 entradas, você está alertado indicar as mensagens mostradas no exemplo.
- **debugar o traço de transferência** — Configures debuga de transferência ou da elevação.

Está aqui um exemplo do **comando trace de transferência debugar**:

```
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
```

Comandos Debug para pôr em esconderijo 802.1X/WPA/RSN/PMK:

- **debugar o dot1x que todos permitem** — Indica a informação sobre debugging do 802.1X.Está aqui um exemplo de saída deste 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
```

- **debugar o dot11 que todos permitem** — Permite a eliminação de erros das funções de rádio.
- **mostre a cliente o *<mac>* sumário** — Os indicadores resumiram a informação para o cliente

pelo MAC address.Está aqui um exemplo de saída deste 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
```

Informações Relacionadas

- Referência de comandos do controlador de LAN do Cisco Wireless
- Guia de função do módulo de rede do controlador de WLAN de Cisco
- Exemplos de configuração do módulo do controlador do Wireless LAN (WLCM)
- Exemplo de configuração da autenticação da Web do controlador do Wireless LAN
- Autenticação de EAP com exemplo de configuração dos controladores de WLAN (WLC)
- Suporte Técnico e Documentação - Cisco Systems