Exemplo de configuração de autorização de um ponto de acesso leve (LAP) em uma rede sem fio unificada da Cisco

Índice

Introdução

Este documento explica como configurar os Controllers de LAN Wireless (WLC) para autorizar os Lightweight Access Points (LAPs) com base no endereço MAC dos LAPs.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento básico de como configurar um Serviço de controle de acesso Cisco Secure (ACS) para autenticar clientes Wireless
- Conhecimento da configuração dos regaços do Cisco Aironet e do Cisco WLC
- Conhecimento de soluções da Segurança do Cisco Unified Wireless

Componentes Utilizados

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

- Cisco 4400 Series WLC que executa a versão 5.0.148.0

- Regaços do Cisco Aironet série 1000
- Regaços do Cisco Aironet série 1200
- Versão de servidor 4.2 do Cisco Secure ACS

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.

Autorização de pouco peso do Access point (REGAÇO)

Durante o processo de registro do REGAÇO, os regaços e os WLC autenticam mutuamente usando os Certificados X.509.

Os Certificados X.509 são queimados no flash protegido no Access Point (AP) e no WLC na fábrica por Cisco. No AP, a fábrica Certificados instalados é chamada fabricação os Certificados instalados (MIC). Todo o Cisco AP fabricou depois de julho 18, 2005 tem MIC.

1130, e 1240 os AP do Cisco Aironet 1200, fabricaram antes de julho 18, 2005, que foram promovidos dos IO autônomos ao protocolo de pouco peso do Access point (LWAPP) IO, gerenciem um certificado auto-assinado (SSC) durante o processo de upgrade. Para obter informações sobre de como controlar AP com SSCs, refira o melhoramento de Access point autônomos do Cisco Aironet ao modo leve.

Além do que esta autenticação mútua que ocorre durante o processo de registro, os WLC podem igualmente restringir os regaços que se registram com eles basearam no MAC address do REGAÇO.

A falta de uma senha elaborada pelo uso do MAC address do REGAÇO não deve ser uma edição porque o controlador usa o MIC para autenticar o AP antes de autorizar o AP através do servidor Radius. O uso do MIC fornece a autenticação forte.

A autorização do REGAÇO pode ser executada em duas maneiras:

- Usando a autorização interna aliste no WLC
- Usando o base de dados do MAC address em um servidor AAA

Os comportamentos dos regaços diferem baseado no certificado usado:

- Dobra com SSCs — O WLC usará somente a lista interna da autorização e não enviará um pedido a um servidor Radius para estes regaços.
- Dobra com MIC — O WLC pode usar a lista interna da autorização configurada no WLC ou usar um servidor Radius para autorizar os regaços

Este documento discute a autorização do REGAÇO usando a lista interna da autorização e o servidor AAA.

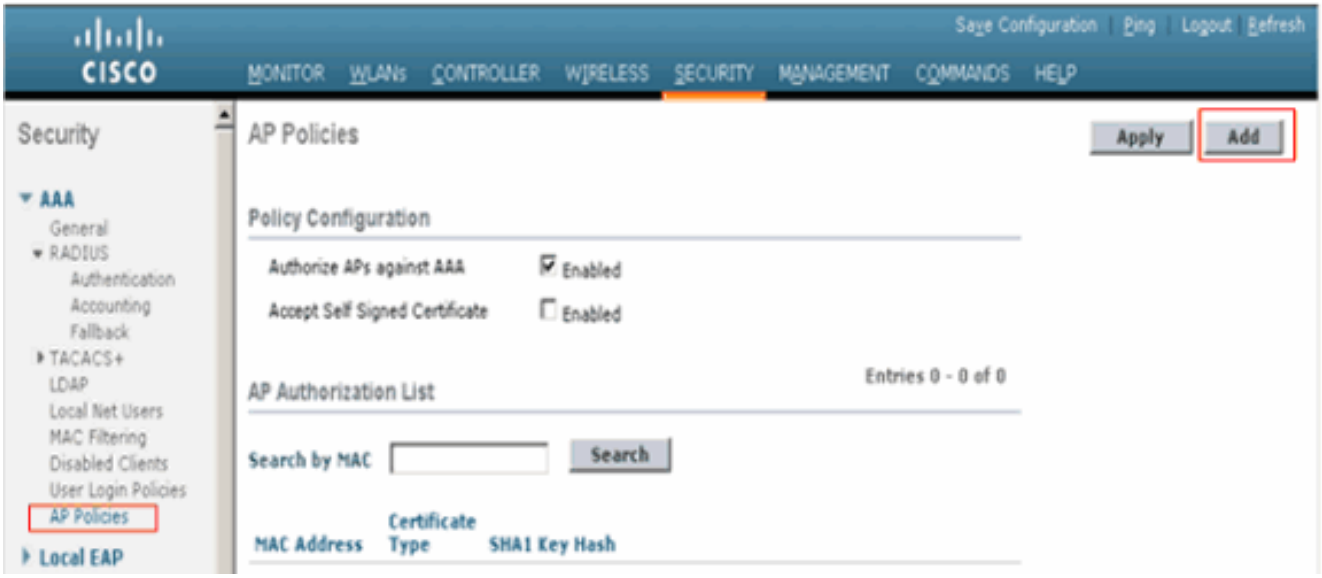
Usando a lista interna da autorização no WLC

No WLC, use a lista da autorização AP para restringir os regaços baseados em seu MAC address. A lista da autorização AP está disponível sob a **Segurança > as políticas AP no** WLC GUI.

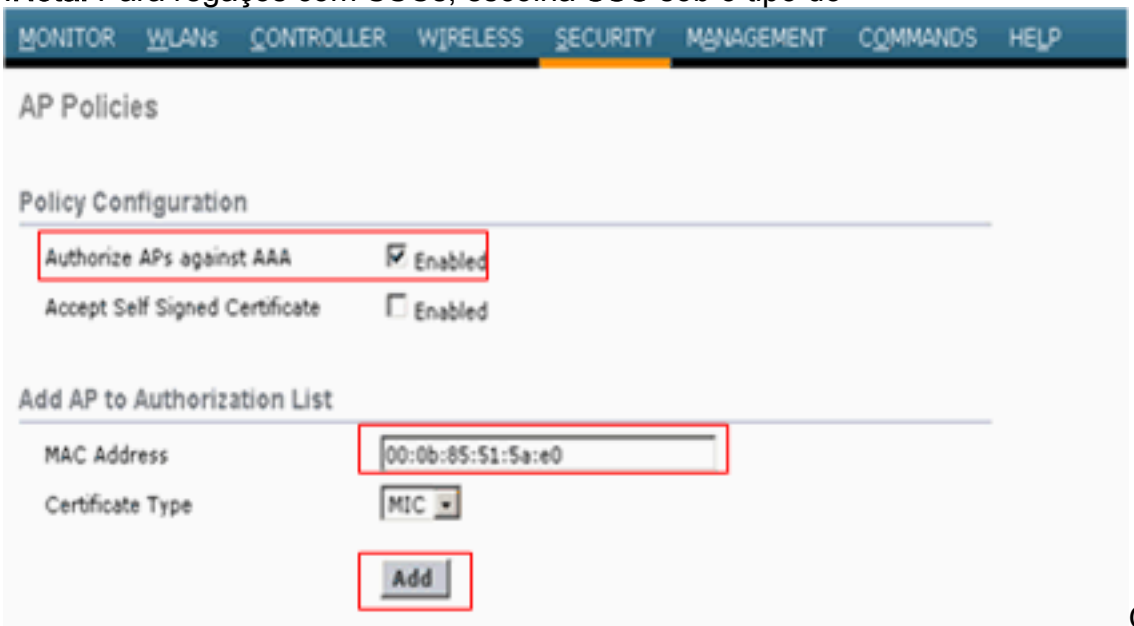
Este exemplo mostra como adicionar o REGAÇO com MAC address **00:0b:85:5b:fb:d0**.

Conclua estes passos:

1. Do controlador GUI WLC, clique a **Segurança > as políticas AP**.A página das políticas AP publica-se.
2. Sob a configuração das normas, verifique a caixa para ver se há **Authorize AP contra o AAA**.Quando este parâmetro é selecionado, o WLC verifica a lista da autorização local primeiramente. Se o MAC do REGAÇO não está atual, verifica o servidor Radius.
3. Clique o **botão Add no** lado direito da tela.

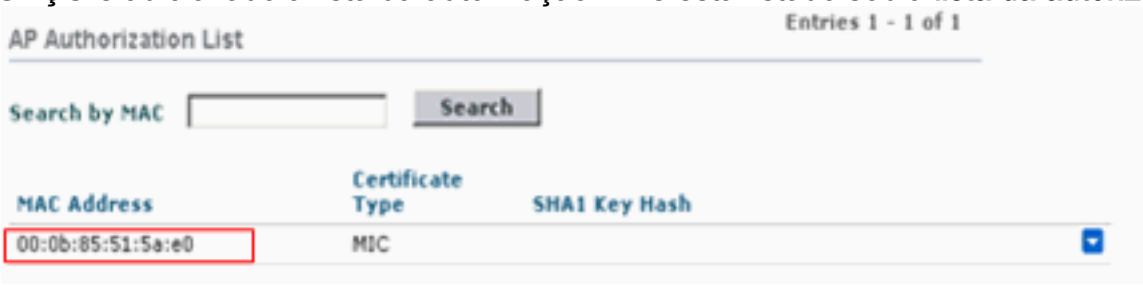


4. Sob adicionar o AP à lista da autorização, incorporam o MAC address AP. Então, escolha o tipo do certificado e o clique **adiciona**.Neste exemplo, um REGAÇO com certificado MIC é adicionado.**Nota:** Para regaços com SSCs, escolha **SSC** sob o tipo do certificado.



O

REGAÇO é adicionado à lista da autorização AP e está listado sob a **lista da autorização AP**.



Verificar

A fim verificar esta configuração, você precisa de conectar o REGAÇO com o MAC address 00:0b:85:51:5a:e0 à rede e ao monitor. Use os **eventos do lwapp debugar permitem** e **comandos debug aaa all enable** executar isto.

Esta saída mostra que debuga quando o MAC address do REGAÇO não está atual na lista da autorização AP:

Nota: Algumas das linhas na saída foram movidas para a segunda linha devido às limitações do espaço.

```
debug lwapp events enable Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY
REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1' Wed Sep 12 17:42:39 2007:
00:0b:85:51:5a:e0 Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on
Port 1 Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST from AP
00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1' Wed Sep 12 17:42:39 2007: 00:0b:85:51:5a:e0
Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1 Wed Sep 12
17:42:50 2007: 00:0b:85:51:5a:e0 Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0 to
00:0b:85:33:52:80 on port '1' Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0:
txNonce 00:0B:85:33:52:80 rxNonce 00:0B:85:51:5A:E0 Wed Sep 12 17:42:50 2007: 00:0b:85:51:5a:e0
LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0 Wed Sep 12
17:42:50 2007: spamRadiusProcessResponse: AP Authorization failure for 00:0b:85:51:5a:e0 debug
aaa all enable Wed Sep 12 17:56:26 2007: Unable to find requested user entry for 000b85515ae0
Wed Sep 12 17:56:26 2007: AuthenticationRequest: 0xac476e8 Wed Sep 12 17:56:26 2007:
Callback.....0x8108e2c Wed Sep 12 17:56:26 2007:
protocolType.....0x00000001 Wed Sep 12 17:56:26 2007:
proxyState.....00:0B:85:51:5A:E0-00:00 Wed Sep 12 17:56:26 2007: Packet
contains 8 AVPs (not shown) Wed Sep 12 17:56:26 2007: 00:0b:85:51:5a:e0 Returning AAA Error 'No
Server' (-7) for mobile 00:0b:85:51:5a:e0 Wed Sep 12 17:56:26 2007: AuthorizationResponse:
0xbadff7d4 Wed Sep 12 17:56:26 2007: structureSize.....28 Wed Sep 12 17:56:26
2007: resultCode.....-7 Wed Sep 12 17:56:26 2007:
protocolUsed.....0xffffffff Wed Sep 12 17:56:26 2007:
proxyState.....00:0B:85:51:5A:E0-00:00 Wed Sep 12 17:56:26 2007: Packet
contains 0 AVPs: Wed Sep 12 17:56:31 2007: Unable to find requested user entry for 000b85515ae0
Wed Sep 12 17:56:31 2007: AuthenticationRequest: 0xac476e8 Wed Sep 12 17:56:31 2007:
Callback.....0x8108e2c Wed Sep 12 17:56:31 2007:
protocolType.....0x00000001 Wed Sep 12 17:56:31 2007:
proxyState.....00:0B:85:51:5A:E0-00:00 Wed Sep 12 17:56:31 2007: Packet
contains 8 AVPs (not shown) Wed Sep 12 17:56:31 2007: 00:0b:85:51:5a:e0 Returning AAA Error 'No
Server' (-7) for mobile 00:0b:85:51:5a:e0
```

Esta mostra da saída debuga quando o MAC address do REGAÇO é adicionado à lista da autorização AP:

Nota: Algumas das linhas na saída foram movidas para a segunda linha devido às limitações do espaço.

debug lwapp events enable Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0 **Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'** Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0 **Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1** Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0 **Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0 to ff:ff:ff:ff:ff:ff on port '1'** Wed Sep 12 17:43:59 2007: 00:0b:85:51:5a:e0 **Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1** Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 **Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:52:80 on port '1'** Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0: txNonce 00:0B:85:33:52:80 rxNonce 00:0B:85:51:5A:E0 Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 **LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0** Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 Successfully added NPU Entry for AP 00:0b:85:51:5a:e0 (index 58)Switch IP: 10.77.244.213, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 10.77.244.221, AP Port: 5550, next hop MAC: 00:0b:85:51:5a:e0 Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 **Successfully transmission of LWAPP Join-Reply to AP 00:0b:85:51:5a:e0** Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 0 Wed Sep 12 17:44:10 2007: 00:0b:85:51:5a:e0 **Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 1 debug aaa all enable** Wed Sep 12 17:57:44 2007: **User 000b85515ae0 authenticated** Wed Sep 12 17:57:44 2007: **00:0b:85:51:5a:e0 Returning AAA Error 'Success' (0) for mobile 00:0b:85:51:5a:e0** Wed Sep 12 17:57:44 2007: AuthorizationResponse: 0xbadff96c Wed Sep 12 17:57:44 2007: structureSize.....70 Wed Sep 12 17:57:44 2007: resultCode.....0 Wed Sep 12 17:57:44 2007: protocolUsed.....0x00000008 Wed Sep 12 17:57:44 2007: proxyState.....00:0B:85:51:5A:E0-00:00 Wed Sep 12 17:57:44 2007: Packet contains 2 AVPs: Wed Sep 12 17:57:44 2007: AVP[01] Service-Type..... 0x00000065 (101) (4 bytes) Wed Sep 12 17:57:44 2007: AVP[02] Airespace / WLAN-Identifier..... 0x00000000 (0) (4 bytes)

Autorização AP contra um servidor AAA

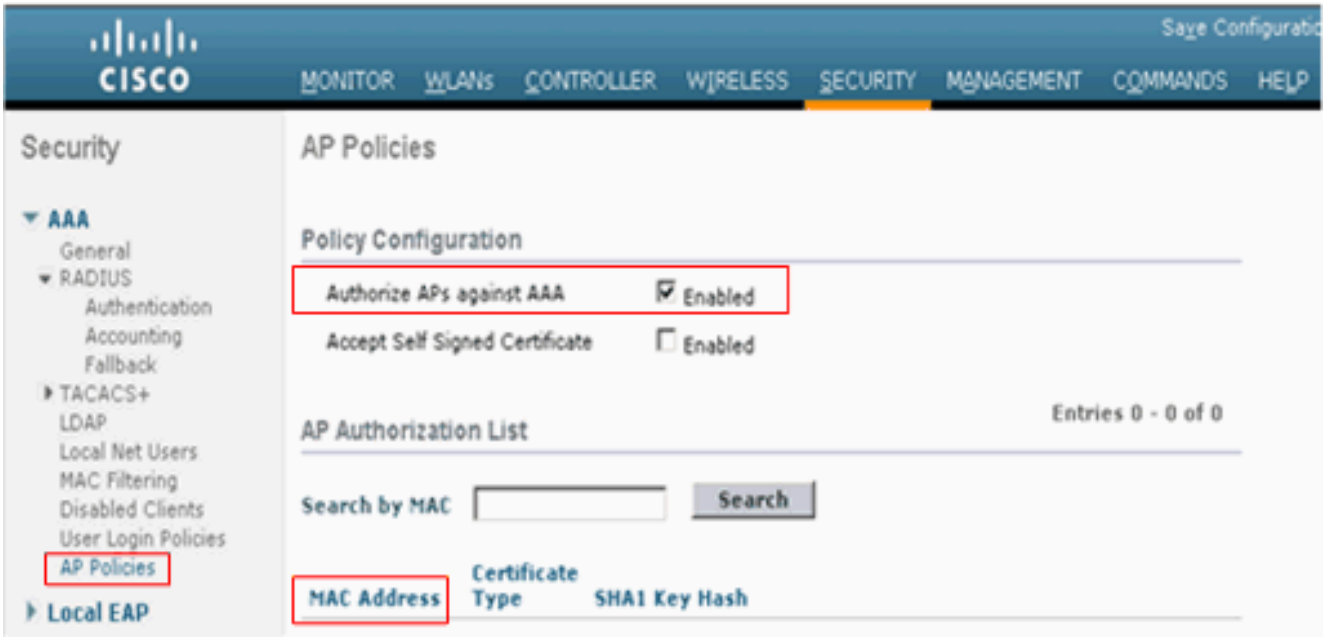
Você pode igualmente configurar WLC para usar servidores Radius para autorizar AP usando MIC. O WLC usa o MAC address de um REGAÇO como ambos o nome de usuário e senha ao enviar a informação a um servidor Radius. Por exemplo, se o MAC address do AP é 000b85229a70, ambos o nome de usuário e senha usado pelo controlador para autorizar o AP são 000b85229a70.

Nota: Se você usa o MAC address como o nome de usuário e senha para a autenticação AP em um servidor AAA do RAIO, não use o mesmo servidor AAA para a authenticação do cliente. A razão para esta é se os hacker encontram o MAC address AP, a seguir podem usar esse MAC como as credenciais do nome de usuário e senha para obter na rede.

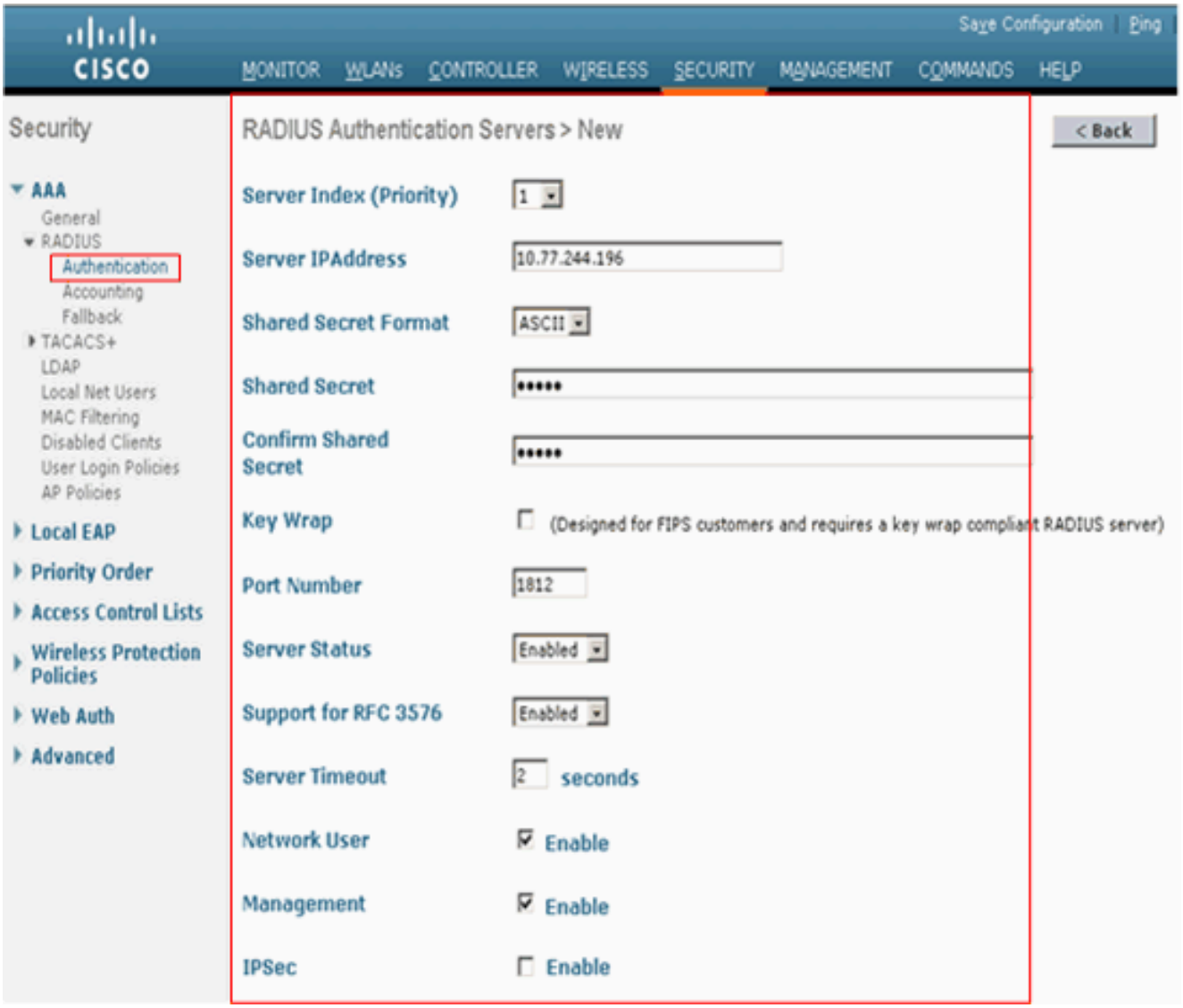
Este exemplo mostra como configurar os WLC para autorizar regaços usando o Cisco Secure ACS.

Termine estas etapas no WLC:

1. Do controlador GUI WLC, clique a **Segurança > as políticas AP**.A página das políticas AP publica-se.
2. Sob a configuração das normas, verifique a caixa para ver se há **Authorize AP contra o AAA**.Quando este parâmetro é selecionado, o WLC verifica o base de dados do MAC local primeiramente. Por este motivo, certifique-se que o base de dados local está vazio cancelando os endereços MAC sob a lista da autorização AP. Se o MAC address do REGAÇO não está atual, verifica então o servidor Radius.



3. Clique a **Segurança** e a **autenticação RADIUS do** controlador GUI para indicar a página dos servidores de autenticação RADIUS. Então, clique **novo** a fim definir um servidor Radius.



4. Defina os parâmetros do servidor Radius nos **servidores de autenticação RADIUS >** página **nova**. Estes parâmetros incluem o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius, o segredo compartilhado, o número de porta, e o status de servidor.Este

exemplo usa o Cisco Secure ACS como o servidor Radius com endereço IP 10.77.244.196.

5. Clique em Apply.

Configurar o Cisco Secure ACS para autorizar regaços

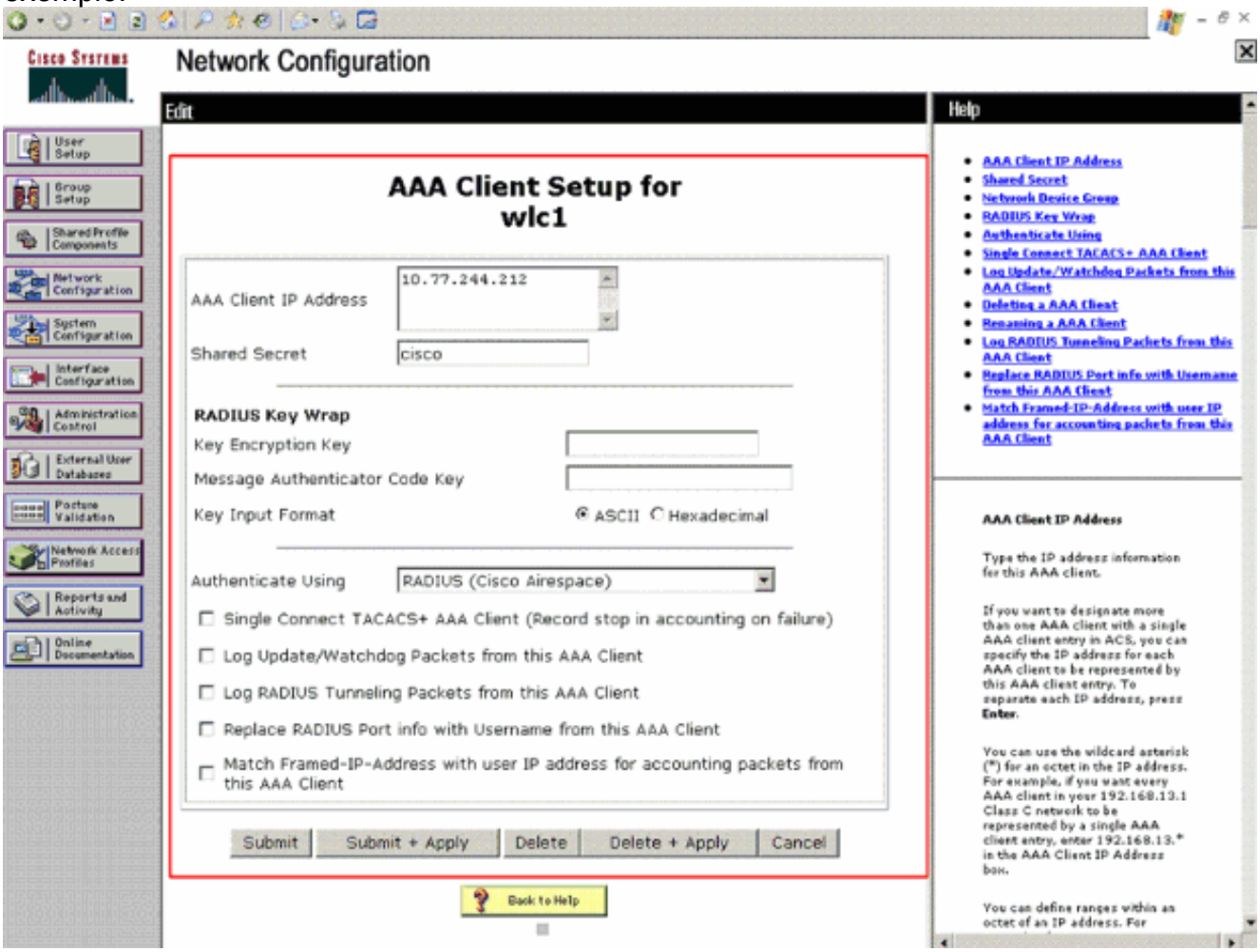
A fim permitir o Cisco Secure ACS de autorizar regaços, você precisa de terminar estas etapas:

1. Configurar o WLC como um cliente de AAA no Cisco Secure ACS
2. Adicionar os endereços do REGAÇO MAC à base de dados de usuário no Cisco Secure ACS

Configurar o WLC como um cliente de AAA no Cisco Secure ACS

Termine estas etapas a fim configurar o WLC como um cliente de AAA no Cisco Secure ACS:

1. Clique o **cliente de AAA do > Add da configuração de rede**.A página do cliente de AAA adicionar publica-se.
2. Nesta página, defina o nome de sistema WLC, endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de gerenciamento, segredo compartilhado, e autentique-o usando o RAIO Airespace.**Nota:** Alternativamente, você pode tentar a opção da autenticação usando o RAIO Aironet.Aqui está um exemplo:

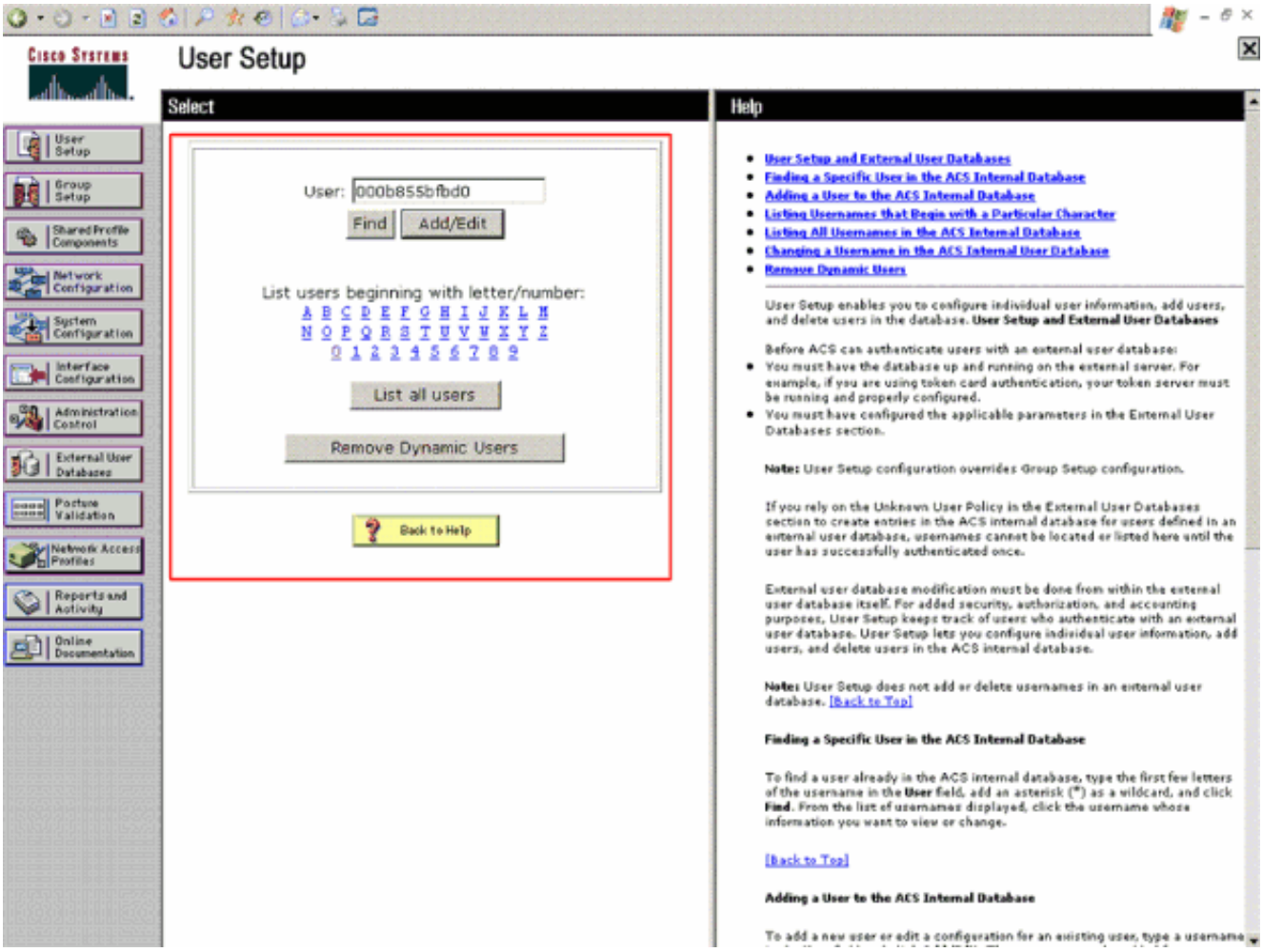


3. O clique **submete-se + aplica-se**.

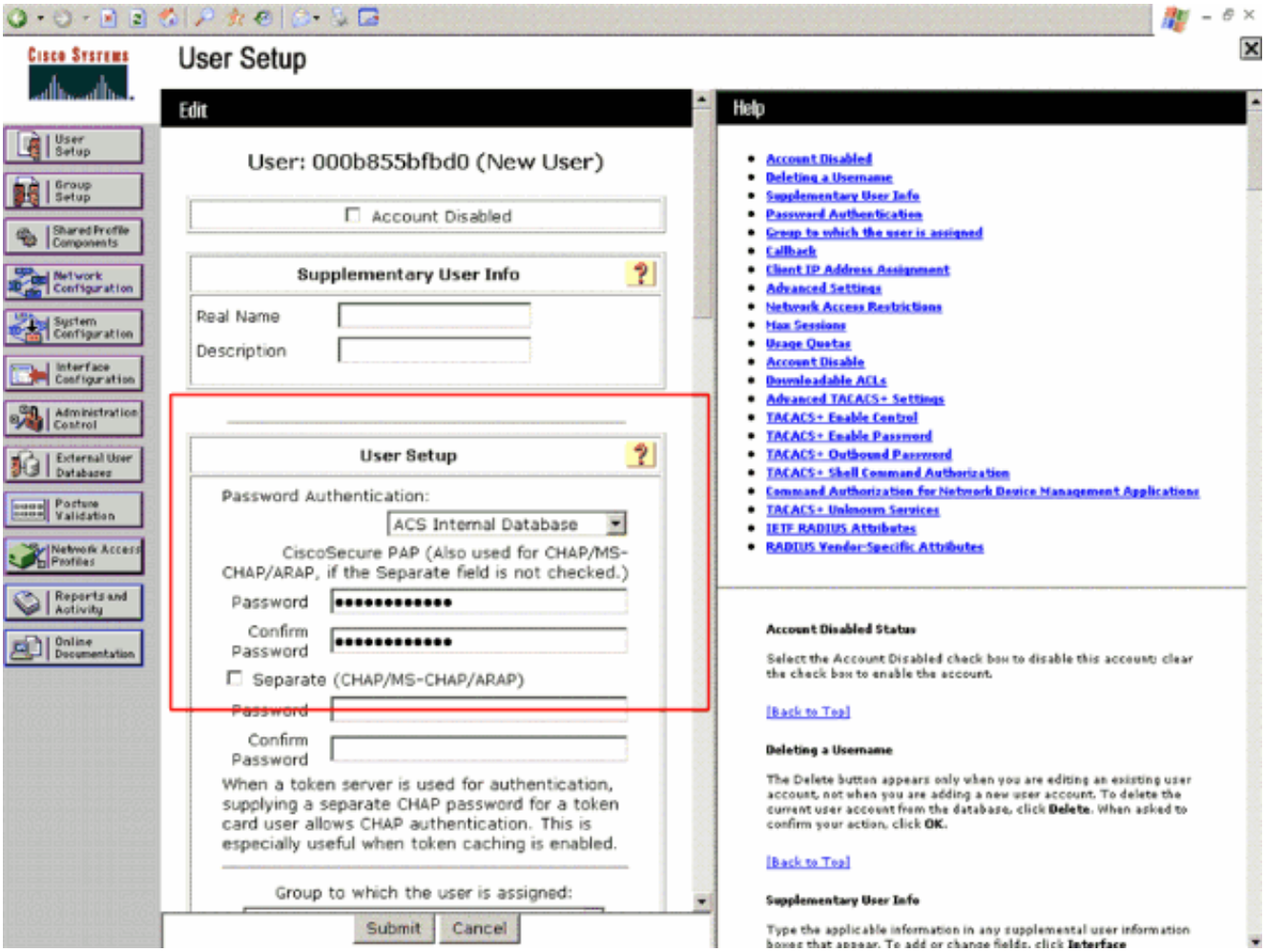
Adicionar os endereços do REGAÇO MAC à base de dados de usuário no Cisco Secure ACS

Termine estas etapas a fim adicionar os endereços do REGAÇO MAC ao Cisco Secure ACS:

1. Escolha a **instalação de usuário do** ACS GUI, incorpore o username, e o clique **adiciona/edita**.O username deve ser o MAC address do REGAÇO que você quer autorizar. O MAC address não deve conter dois pontos ou hífens.Neste exemplo, o REGAÇO é adicionado com MAC address **000b855bfbd0**:



2. Quando a página da instalação de usuário se publica, defina a senha para este REGAÇO no campo de senha como mostrado.A senha deve igualmente ser o MAC address do REGAÇO. Neste exemplo, é **000b855bfbd0**.



3. Clique em Submit.
4. Repita este procedimento para adicionar mais regaços ao base de dados do Cisco Secure ACS.

Verificar

A fim verificar esta configuração, você precisa de conectar o REGAÇO com o MAC address 00:0b:85:51:5a:e0 à rede e ao monitor. Use os **eventos do lwapp debugar permitem** e **comandos debug aaa all enable** a fim executar isto.

Como visto do debuga, o WLC passado no MAC address do REGAÇO ao servidor Radius 10.77.244.196, e o server autenticou com sucesso o REGAÇO. O REGAÇO registra-se então com o controlador.

Nota: Algumas das linhas na saída foram movidas para a segunda linha devido às limitações do espaço.

```
debug aaa all enable Thu Sep 13 13:54:39 2007: AuthenticationRequest: 0xac48778 Thu Sep 13
13:54:39 2007: Callback.....................0x8108e2c Thu Sep 13 13:54:39 2007:
protocolType.....................0x00000001 Thu Sep 13 13:54:39 2007:
proxyState.....................00:0B:85:51:5A:E0-00:00 Thu Sep 13 13:54:39 2007: Packet
contains 8 AVPs (not shown) Thu Sep 13 13:54:39 2007: 00:0b:85:51:5a:e0 Successful transmission
of Authentication Packet (id 123) to 10.77.244.196:1812, proxy state 00:0b:85:51:5a:e0-85:51 Thu
Sep 13 13:54:39 2007: 00000000: 01 7b 00 72 00 00 00 00 00 00 00 00 00 00 00 00 .{.r............
Thu Sep 13 13:54:39 2007: 00000010: 00 00 00 00 01 0e 30 30 30 62 38 35 35 31 35 61
......000b85515a Thu Sep 13 13:54:39 2007: 00000020: 65 30 1e 13 30 30 2d 30 62 2d 38 35 2d 33
33 2d e0..00-0b-85-33- Thu Sep 13 13:54:39 2007: 00000030: 35 32 2d 38 30 1f 13 30 30 2d 30 62
```

```
2d 38 35 2d 52-80..00-0b-85- Thu Sep 13 13:54:39 2007: 00000040: 35 31 2d 35 61 2d 65 30 05 06
00 00 00 01 04 06 51-5a-e0..... Thu Sep 13 13:54:39 2007: 00000050: 0a 4d f4 d4 20 06 77 6c
63 31 02 12 03 04 0e 12 .M....wlc1..... Thu Sep 13 13:54:39 2007: 00000060: 84 9c 03 8f 63 40
2a be 9d 38 42 91 06 06 00 00 ....c@*..8B..... Thu Sep 13 13:54:39 2007: 00000070: 00 0a .. Thu
Sep 13 13:54:40 2007: 00000000: 02 7b 00 30 aa fc 40 4b fe 3a 33 10 f6 5c 30 fd .{.0..@K.:3..\0.
Thu Sep 13 13:54:40 2007: 00000010: 12 f3 6e fa 08 06 ff ff ff ff 19 16 43 41 43 53
..n.........CACS Thu Sep 13 13:54:40 2007: 00000020: 3a 30 2f 39 37 37 2f 61 34 64 66 34 64 34
2f 31 :0/977/a4df4d4/1 Thu Sep 13 13:54:40 2007: ****Enter processIncomingMessages: response
code=2 Thu Sep 13 13:54:40 2007: ****Enter processRadiusResponse: response code=2 Thu Sep 13
13:54:40 2007: 00:0b:85:51:5a:e0 Access-Accept received from RADIUS server 10.77.244.196 for
mobile 00:0b:85:51:5a:e0 receiveId = 0 Thu Sep 13 13:54:40 2007: AuthorizationResponse:
0x9845500 Thu Sep 13 13:54:40 2007: structureSize....................84 Thu Sep 13 13:54:40
2007: resultCode.....................0 Thu Sep 13 13:54:40 2007:
protocolUsed.....................0x00000001 Thu Sep 13 13:54:40 2007:
proxyState.....................00:0B:85:51:5A:E0-00:00 Thu Sep 13 13:54:40 2007: Packet
contains 2 AVPs: Thu Sep 13 13:54:40 2007: AVP[01] Framed-IP-Address.............. 0xffffffff
(-1) (4 bytes) Thu Sep 13 13:54:40 2007: AVP[02] Class.........................
CACS:0/977/a4df4d4/1 (20 bytes) debug lwapp events enable Thu Sep 13 14:01:51 2007:
00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0 to
00:0b:85:33:52:80 on port '1' Thu Sep 13 14:01:51 2007: 00:0b:85:51:5a:e0 Successful
transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1 Thu Sep 13 14:01:51
2007: 00:0b:85:51:5a:e0 Received LWAPP DISCOVERY REQUEST from AP 00:0b:85:51:5a:e0 to
ff:ff:ff:ff:ff:ff on port '1' Thu Sep 13 14:01:51 2007: 00:0b:85:51:5a:e0 Successful
transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1 Thu Sep 13 14:02:02
2007: 00:0b:85:51:5a:e0 Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0 to
00:0b:85:33:52:80 on port '1' Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0:
txNonce 00:0B:85:33:52:80 rxNonce 00:0B:85:51:5A:E0 Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0
LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0 is 1500, remote debug mode is 0 Thu Sep 13
14:02:02 2007: 00:0b:85:51:5a:e0 Successfully added NPU Entry for AP 00:0b:85:51:5a:e0(index
57)Switch IP: 10.77.244.213, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 10.77.244.221, AP
Port: 5550, next hop MAC: 00:0b:85:51:5a:e0 Thu Sep 13 14:02:02 2007: 00:0b:85:51:5a:e0
Successfully transmission of LWAPP Join-Reply to AP 00:0b:85:51:5a:e0 Thu Sep 13 14:02:02 2007:
00:0b:85:51:5a:e0 Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 0 Thu Sep 13 14:02:02 2007:
00:0b:85:51:5a:e0 Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 1
```

Troubleshooting

Use estes comandos pesquisar defeitos sua configuração:

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **debugar eventos do lwapp permitem** — Configures debuga de eventos e de erros LWAPP.
- **debugar o pacote lwapp permitem** — Configures debuga do traço do pacote lwapp.
- **debugar o aaa que todos permitem** — Configures debuga de todos os mensagens AAA.

Informações Relacionadas

- Atualização de Pontos de Acesso Autônomos Cisco Aironet para o Modo Lightweight
- A ferramenta de upgrade LWAPP pesquisa defeitos pontas
- Página de Suporte Wireless
- Suporte Técnico e Documentação - Cisco Systems