Exemplo de configuração da rede de malha do controlador do Wireless LAN

Índice

Introdução

Este documento fornece um exemplo da configuração básica que mostra como estabelecer um link ponto a ponto usando a solução de rede de malha. Este exemplo usa dois pontos de acesso leves (LAP). Um LAP opera como um ponto de acesso de telhado (RAP), o outro LAP opera como um ponto de acesso de montagem em poste (PAP), e são conectados a um Controlador de LAN Wireless (WLC) da Cisco. O RAP é conectado ao WLC através de um switch Cisco Catalyst.

Refira por favor o exemplo de configuração da rede de malha do controlador do Wireless LAN para as liberações 5.2 e mais atrasado para a liberação 5.2 WLC e umas versões mais atrasadas

Pré-requisitos

- O WLC é configurado para a operação básica.
- O WLC é configurado no modo da camada 3.
- O interruptor para o WLC é configurado.

Requisitos

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

- Conhecimento básico da configuração dos LAPs e dos WLCs da Cisco
- Conhecimento básico do protocolo de pouco peso AP (LWAPP).
- Conhecimento da configuração de um servidor de DHCP externo e/ou do Domain Name Server (DNS)
- Conhecimento da configuração básica dos switch Cisco

Componentes Utilizados

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

- Cisco 4402 Series WLC que executa o firmware 3.2.150.6
- Dois (2) regaços do 1510 Series do Cisco Aironet
- Switch de Camada 2 de Cisco

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

Malha exterior de pouco peso AP do 1510 Series do Cisco Aironet

A malha exterior de pouco peso AP do 1510 Series do Cisco Aironet é um dispositivo Wireless projetado para o acesso de cliente Wireless e a construção de uma ponte sobre ponto a ponto, a construção de uma ponte sobre point-to-multipoint, e a conectividade Wireless point-to-multipoint da malha. O Access point exterior é uma unidade autônoma que possa ser montada em uma parede ou em uma saliência, em um polo do telhado, ou em um polo claro de rua.

O AP1510 opera-se com controladores para fornecer o Gerenciamento centralizado e escalável, a segurança elevada, e a mobilidade. Projetou apoiar facilmente disposições da zero-configuração, o AP1510 e junta-se firmemente à rede de malha e está-se disponível controlar e monitorar a rede através do controlador GUI ou CLI.

O AP1510 é equipado com os dois rádios simultaneamente de funcionamento: um 2.4-GHz transmite por rádio usado para o acesso do cliente e um 5-GHz transmite por rádio usado para o regresso dos dados ao outro AP1510s. O tráfego do cliente do Wireless LAN passa através do rádio do regresso do AP ou está retransmitido com o outro AP1510s até que alcance a conexão Ethernet do controlador.

Access point da Telhado-parte superior (RAP)

As batidas têm uma conexão ligada com fio a Cisco WLC. Usam a relação wireless do regresso para comunicar-se com os PAP vizinhos. As batidas são o nó do pai a toda a construção de uma ponte sobre ou rede de malha e conectam uma ponte ou uma rede de malha à rede ligada com fio. Consequentemente, pode haver somente um RAP para qualquer segmento em bridge ou de rede em malha.

Nota: Quando você usa a solução de rede de comunicação da malha para o LAN para LAN que constrói uma ponte sobre, não conecte um RAP diretamente a Cisco WLC. Um interruptor ou um roteador entre Cisco WLC e o RAP são exigidos porque Cisco WLC não envia o tráfego Ethernet que vem de uma porta LWAPP-permitida. As batidas podem trabalhar no modo LWAPP da camada 2 ou da camada 3.

Access point da Polo-parte superior (PAP)

Os PAP não têm nenhuma conexão ligada com fio a Cisco WLC. Podem ser completamente wireless, e apoiam os clientes que se comunicam com outras PAP ou batidas, ou podem ser usados para conectar aos dispositivos periféricos ou a uma rede ligada com fio. A porta Ethernet é desabilitar por padrão por razões de segurança, mas você deve habilitá-la para os PAPs.

Nota: O Cisco Aironet 1030 regaços da borda do telecontrole apoia disposições do salto único quando o Cisco Aironet série 1500 AP exteriores de pouco peso apoiar disposições únicas e do multi-salto. Como tal, o Cisco Aironet série 1500 AP exteriores de pouco peso pode ser usado como o telhado AP e como PAP para uns ou vários saltos de Cisco WLC.

Características não apoiadas em redes de malha

Estas características do controlador não são apoiadas em redes de malha:

- apoio do Multi-país
- CAC Carga-baseado (apoio das redes de malha largura de banda-baseado somente, ou estática, CAC.)
- Alta disponibilidade (a pulsação do coração rápida e a descoberta preliminar se juntam ao temporizador)
- Autenticação EAP-FASTv1 e de 802.1X
- Autenticação EAP-FASTv1 e de 802.1X
- Localmente - certificado significativo
- Serviços com base na localização

Sequência de inicialização do Access point

Esta lista descreve o que acontece quando o RAP e o PAP começam acima:

- Todo o tráfego viaja através do RAP e do Cisco WLC antes que esteja enviado ao LAN.
- Quando o RAP vem acima, os PAP conectam-lhe automaticamente.
- O link conectado usa um segredo compartilhado para gerar uma chave que seja usada para fornecer o Advanced Encryption Standard (AES) para o link.
- Uma vez que o PAP remoto conecta ao RAP, a malha AP pode passar o tráfego de dados.
- Os usuários podem mudar o segredo compartilhado ou configurar a malha AP usando a interface de linha do comando cisco (CLI), a relação de usuário de web de Cisco do controlador, ou o Sistema de controle sem fio da Cisco (Cisco WCS). Cisco recomenda que

você altera o segredo compartilhado.

Configurar

Termine estas etapas a fim configurar o WLC e os AP para a construção de uma ponte sobre ponto a ponto.

1. Permita a configuração zero do toque no WLC.
2. Adicionar o MIC à lista da autorização AP.
3. Configure que constrói uma ponte sobre parâmetros para os AP.
4. Verifique a configuração.

Permita a configuração zero do toque (permitida à revelia)

Configuração de GUI

Permita a configuração zero do toque permite os AP de obter a chave secreta compartilhada do controlador quando se registra com o WLC. Se você desmarca esta caixa, o controlador não fornece a chave secreta compartilhada, e os AP usam uma chave pré-compartilhada do padrão para uma comunicação segura. O valor padrão é permitido (ou verificado). Termine estas etapas do WLC GUI:

Nota: Não há nenhuma disposição para a configuração do Zero-toque na versão 4.1 e mais recente WLC.

1. Escolha o **Sem fio > construindo uma ponte sobre** e o clique **permite a configuração zero do toque**.
2. Selecione o formato chave.
3. Incorpore a chave secreta compartilhada de construção de uma ponte sobre.
4. Incorpore a chave secreta compartilhada de construção de uma ponte sobre outra vez à chave secreta compartilhada confirmação.

Configuração de CLI

Termine estas etapas do CLI:

1. Emita o **comando enable da zero-configuração da rede da configuração** a fim permitir a configuração zero do toque.`(Cisco Controller) >`**`config network zero-config enable`**
2. Emita o comando do **<string> do construir uma ponte sobre-compartilhar-segredo da rede da configuração** a fim adicionar a chave secreta compartilhada de construção de uma ponte sobre.`(Cisco Controller) >`**`config network bridging-shared-secret Cisco`**

Adicionar o MIC à lista da autorização AP

A próxima etapa é adicionar o AP à lista da autorização no WLC. A fim fazer isto, para escolher a **Segurança > as políticas AP**, para incorporar o MAC address AP adicionar abaixo o AP à lista da autorização e o clique **adiciona**.

Neste exemplo, ambos os AP (o RAP e o PAP) são adicionados à lista da autorização AP no controlador.

Configuração de CLI

Emita a autêntico-**lista da configuração adicionam o** comando do **mac> mic <AP** a fim adicionar o MIC à lista da autorização.

```
(Cisco Controller) >config auth-list add mic 00:0b:85:5e:40:00 (Cisco Controller) >config auth-list add mic 00:0b:85:5e:5a:80
```

Configuração

Este documento utiliza esta configuração:

Cisco WLC 4402

```
(Cisco Controller) >show run-config Press Enter to
continue... System Inventory Switch
Description..............................  Cisco
Controller Machine
Model.................................... WLC4402-12
Serial Number.....................................
FLS0943H005 Burned-in MAC
Address.......................... 00:0B:85:40:CF:A0
Crypto Accelerator 1............................ Absent
Crypto Accelerator 2............................ Absent
Power Supply 1.................................. Absent
Power Supply 2...................................
Present, OK Press Enter to continue Or <Ctl Z> to abort
System Information Manufacturer's
Name............................ Cisco Systems, Inc
Product Name.................................... Cisco
Controller Product
Version................................. 3.2.150.6 RTOS
Version..................................... 3.2.150.6
Bootloader Version...............................
3.2.150.6 Build
Type..................................... DATA + WPS
System Name.....................................
lab120wlc4402ip100 System
Location................................. System
Contact.................................. System
ObjectID.................................
1.3.6.1.4.1.14179.1.1.4.3 IP
Address.....................................
192.168.120.100 System Up
Time................................. 0 days 1 hrs 4
mins 6 secs Configured
Country............................. United States
Operating Environment...........................
Commercial (0 to 40 C) Internal Temp Alarm
Limits...................... 0 to 65 C Internal
Temperature............................ +42 C State of
802.11b Network....................... Disabled State
of 802.11a Network...................... Disabled
Number of WLANs................................. 1 3rd
Party Access Point Support................... Disabled
Number of Active Clients........................ 0
Press Enter to continue Or <Ctl Z> to abort Switch
Configuration 802.3x Flow Control
```

```
Mode..................... Disable Current LWAPP
Transport Mode..................... Layer 3 LWAPP
Transport Mode after next switch reboot.... Layer 3 FIPS
prerequisite features..................... Disabled
Press Enter to continue Or <Ctl Z> to abort Network
Information RF-Network Name.............................
airespacerf Web Mode....................................
Enable Secure Web Mode..............................
Enable Secure Shell (ssh)...........................
Enable Telnet.......................................
Enable Ethernet Multicast Mode.....................
Disable Mode: Ucast User Idle
Timeout.......................... 300 seconds ARP Idle
Timeout.......................... 300 seconds ARP
Unicast Mode............................ Disabled Cisco
AP Default Master..................... Disable Mgmt Via
Wireless Interface.................. Enable Bridge AP
Zero Config...................... Enable Bridge Shared
Secret....................... youshouldsetme Allow Old
Bridging Aps To Authenticate...... Disable Over The Air
Provisioning of AP's........... Disable Mobile Peer to
Peer Blocking................. Disable Apple Talk
................................ Disable AP Fallback
................................ Enable Web Auth
Redirect Ports ..................... 80 Fast SSID Change
........................... Disabled Press Enter to
continue Or <Ctl Z> to abort Port Summary STP Admin
Physical Physical Link Link Mcast Pr Type Stat Mode Mode
Status Status Trap Appliance POE -- ------- ---- -------
---------- ---------- ------ ------- --------- ------- 1
Normal Forw Enable Auto 1000 Full Up Enable Enable N/A 2
Normal Forw Enable Auto 1000 Full Up Enable Enable N/A
Mobility Configuration Mobility Protocol
Port........................... 16666 Mobility Security
Mode........................... Disabled Default
Mobility Domain........................... airespacerf
Mobility Group members configured................. 3
Switches configured in the Mobility Group MAC Address IP
Address Group Name 00:0b:85:33:a8:40 192.168.5.70
<local> 00:0b:85:40:cf:a0 192.168.120.100 <local>
00:0b:85:43:8c:80 192.168.5.40 airespacerf Interface
Configuration Interface
Name................................... ap-manager IP
Address.....................................
192.168.120.101 IP
Netmask.....................................
255.255.255.0 IP
Gateway.....................................
192.168.120.1
VLAN........................................
untagged Active Physical
Port............................ 1 Primary Physical
Port............................ 1 Backup Physical
Port............................ Unconfigured Primary
DHCP Server.............................. 192.168.1.20
Secondary DHCP Server...........................
Unconfigured
ACL.........................................
Unconfigured AP
Manager..................................... Yes
Interface Name..................................
management MAC
Address.....................................
00:0b:85:40:cf:a0 IP
```

```
Address.....................................
192.168.120.100 IP
Netmask.....................................
255.255.255.0 IP
Gateway.....................................
192.168.120.1
VLAN........................................
untagged Active Physical
Port........................... 1 Primary Physical
Port........................... 1 Backup Physical
Port........................... Unconfigured Primary
DHCP Server............................. 192.168.1.20
Secondary DHCP Server.......................
Unconfigured
ACL.........................................
Unconfigured AP
Manager..................................... No
Interface Name..............................
service-port MAC
Address.....................................
00:0b:85:40:cf:a1 IP
Address.....................................
192.168.250.100 IP
Netmask.....................................
255.255.255.0 DHCP
Protocol.................................. Disabled AP
Manager..................................... No
Interface Name..............................
virtual IP
Address..................................... 1.1.1.1
Virtual DNS Host Name.......................
Disabled AP
Manager..................................... No WLAN
Configuration WLAN
Identifier.................................. 1 Network
Name (SSID).............................
lab120wlc4402ip100
Status......................................
Enabled MAC
Filtering................................... Enabled
Broadcast SSID..............................
Enabled AAA Policy
Override.............................. Disabled Number
of Active Clients....................... 0
Exclusionlist Timeout.......................... 60
seconds Session
Timeout................................. 1800 seconds
Interface...................................
management WLAN
ACL.....................................
unconfigured DHCP
Server..................................... Default
Quality of Service............................. Silver
(best effort)
WMM.........................................
Disabled
802.11e.....................................
Disabled Dot11-Phone Mode
(7920)........................ Disabled Wired
Protocol.................................. None IPv6
Support................................... Disabled
Radio Policy.................................. All
Radius Servers
Authentication.............................
```

```
192.168.1.20 1812 Security 802.11
Authentication:..................... Open System
Static WEP Keys.............................. Enabled
Key Index:..................................... 1
Encryption:.................................... 104-bit
WEP 802.1X.....................................
Disabled Wi-Fi Protected Access (WPA1).................
Disabled Wi-Fi Protected Access v2 (WPA2).............
Disabled IP Security...................................
Disabled IP Security Passthru..........................
Disabled L2TP..........................................
Disabled Web Based Authentication......................
Disabled Web-Passthrough...............................
Disabled Auto Anchor...................................
Disabled Cranite Passthru..............................
Disabled Fortress Passthru.............................
Disabled RADIUS Configuration Vendor Id Backward
Compatibility................. Disabled Credentials
Caching............................. Disabled Call
Station Id Type............................. IP Address
Administrative Authentication via RADIUS.........
Enabled
Keywrap........................................
Disabled Load Balancing Info Aggressive Load
Balancing....................... Enabled Aggressive
Load Balancing Window................. 0 clients
Signature Policy Signature
Processing........................... Enabled Spanning
Tree Switch Configuration STP
Specification...................... IEEE 802.1D STP Base
MAC Address................... 00:0B:85:40:CF:A0
Spanning Tree Algorithm................. Disable STP
Bridge Priority................... 32768 STP Bridge
Max. Age (seconds).......... 20 STP Bridge Hello Time
(seconds)........ 2 STP Bridge Forward Delay
(seconds)..... 15 Spanning Tree Port Configuration STP
Port ID................................ 8001 STP Port
State............................. Forwarding STP Port
Administrative Mode................ 802.1D STP Port
Priority.......................... 128 STP Port Path
Cost........................... 4 STP Port Path Cost
Mode..................... Auto STP Port
ID................................. 8002 STP Port
State............................. Forwarding STP Port
Administrative Mode................ 802.1D STP Port
Priority.......................... 128 STP Port Path
Cost........................... 4 STP Port Path Cost
Mode..................... Auto
```

Configurar a construção de uma ponte sobre de parâmetros para os AP

Esta seção fornece instruções em como configurar o papel do AP na rede de malha e relativo construindo uma ponte sobre parâmetros. Você pode configurar estes parâmetros usando o GUI ou o CLI.

1. Clique **Sem fio** e então **todos os AP** sob Access point. Toda a página AP publica-se.
2. Clique o link do **detalhe** para seu AP1510 a fim alcançar o todo o página AP > de detalhes

Nesta página, o modo AP sob o general é ajustado automaticamente para construir uma ponte sobre para os AP que têm a funcionalidade da ponte, tal como o AP1510. Esta página igualmente mostra esta informação sob a construção de uma ponte sobre da informação. Sob a construção

de uma ponte sobre da informação, escolha uma destas opções a fim especificar o papel deste AP na rede de malha:

- **MeshAP** — Escolha esta opção se o AP1510 tem uma conexão Wireless ao controlador.
- **RootAP** — Escolha esta opção se o AP1510 tem uma conexão ligada com fio ao controlador.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Depois que os AP se registram com o WLC, você pode vê-los sob a aba wireless na parte superior do GUI do WLC:

No CLI, você pode usar o **comando show ap summary** a fim verificar que os AP se registraram com o WLC:

```
(Cisco Controller) >show ap summary AP Name Slots AP Model Ethernet MAC Location Port ----------
-------- ----- ---------- ----------------- ---------------- ---- lab120br1510ip152 2 OAP1500
00:0b:85:5e:5a:80 default_location 1 lab120br1510ip150 2 OAP1500 00:0b:85:5e:40:00
default_location 1 (Cisco Controller) >
```

Clique a **construção de uma ponte sobre de detalhes no** GUI a fim verificar o papel do AP:

No CLI, você pode usar o **<Cisco AP> do trajeto da malha da mostra** e a **malha da mostra relincha** comandos do **<Cisco AP>** a fim verificar que os AP se registraram com o WLC:

```
(Cisco Controller) >show mesh path lab120br1510ip152 00:0B:85:5E:5A:80 is RAP (Cisco Controller)
>show mesh neigh lab120br1510ip152 AP MAC : 00:0B:85:5E:40:00 FLAGS : 160 CHILD worstDv 255, Ant
0, channel 0, biters 0, ppiters 10 Numroutes 0, snr 0, snrUp 0, snrDown 26, linkSnr 0
adjustedEase 0, unadjustedEase 0 txParent 0, rxParent 0 poorSnr 0 lastUpdate 1150103792 (Mon Jun
12 09:16:32 2006) parentChange 0 Per antenna smoothed snr values: 0 0 0 0 Vector through
00:0B:85:5E:40:00 (Cisco Controller) >
```

Troubleshooting

`A malha AP não associa ao WLC` é um da maioria de problemas comuns considerados no desenvolvimento da malha. Termine estas verificações:

1. Certifique-se do MAC address do Access point esteja adicionado na lista de filtro do Mac no WLC. Isto pode ser visto sob a **Segurança > a filtração do Mac**.
2. Verifique o segredo compartilhado entre o RAP e o MAPA. Você pode ver esta mensagem no WLC quando há uma má combinação na chave.`“Juntar-pedido AUTH_STRING_PAYLOAD LWAPP, mistura inválida AP 00:0b:85:68:c1:d0" da chave da PONTE` **Nota:** Tente sempre usar a **possibilidade zero opções de configuração do toque** se disponível para uma versão. Isto configura automaticamente a chave para a malha AP e evita configurações incorretas.
3. As batidas não encaminham nenhuns mensagens de transmissão em sua interface de rádio. Configurar assim o servidor DHCP para enviar endereços IP de Um ou Mais Servidores Cisco ICM NT com o unicast de modo que o MAPA possa obter seus endereços IP de Um ou Mais Servidores Cisco ICM NT encaminhados pelo RAP. Se não use um IP Estático para o MAPA.
4. Deixe o nome de grupo de bridge em valores padrão ou certifique-se de que os nomes de grupo de bridge estão configurados exatamente o mesmos em mapas e no RAP

correspondente.

Estas são as edições que são específicas engrenar Access point. Para os problemas de conectividade que são comuns entre o WLC e um Access point, consulte para pesquisar defeitos um Access point de pouco peso que não se junta a um controlador do Wireless LAN.

Comandos para Troubleshooting

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

Você pode usar estes comandos debug pesquisar defeitos o WLC:

- debugar o estado PEM permitem — Usado para configurar o gerente da política de acesso debugar opções.
- debugar eventos PEM permitem — Usado para configurar o gerente da política de acesso debugar opções.
- debugar o mensagem DHCP permitem — Mostra debugar dos mensagens DHCP que são trocados a e do servidor DHCP.
- debugar o pacote DHCP permitem — Mostra debugar dos detalhes do pacote DHCP que são enviados a e do servidor DHCP.

Alguns **comandos debug** adicionais que você pode usar para pesquisar defeitos são:

- **debugar erros de lwapp permitem** — Mostra debugar dos erros de lwapp.
- **debugar o pki pm permitem** — Mostra debugar das mensagens do certificado que são passadas entre o AP e o WLC.

Isto **debuga eventos do lwapp permite o** comando WLC de output mostra que o REGAÇO obtém registrado ao WLC:

```
(Cisco Controller) >debug lwapp events enable Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00
Received LWAPP JOIN REQUEST from AP 00:0b:85:5e:40:00 to 06:0a:10:10:00:00 on port '1' Mon Jun
12 09:04:57 2006: 00:0b:85:5e:40:00 AP lab120br1510ip150: txNonce 00:0B:85:40:CF:A0 rxNonce
00:0B:85:5E:40:00 Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00 LWAPP Join-Request MTU path from
AP 00:0b:85:5e:40:00 is 1500, remote debug mode is 0 Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00
Successfully added NPU Entry for AP 00:0b:85:5e:40:00 (index 1) Switch IP: 192.168.120.101,
Switch Port: 12223, intIfNum 1, vlanId 0 AP IP: 192.168.120.150, AP Port: 58368, next hop MAC:
00:0b:85:5e:40:00 Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP
Join-Reply to AP 00:0b:85:5e:40:00 Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Register LWAPP
event for AP 00:0b:85:5e:40:00 slot 0 Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Register LWAPP
event for AP 00:0b:85:5e:40:00 slot 1 Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP
CONFIGURE REQUEST from AP 00:0b:85:5e:40:00 to 00:0b:85:40:cf:a3 Mon Jun 12 09:04:59 2006:
00:0b:85:5e:40:00 Updating IP info for AP 00:0b:85:5e:40:00 -- static 1,
192.168.120.150/255.255.255.0, gtw 192.168.120.1 Mon Jun 12 09:04:59 2006: spamVerifyRegDomain
RegDomain set for slot 0 code 0 regstring -A regDfromCb -A Mon Jun 12 09:04:59 2006:
spamVerifyRegDomain RegDomain set for slot 1 code 0 regstring -A regDfromCb -A Mon Jun 12
09:04:59 2006: spamEncodeDomainSecretPayload:Send domain secret
airespacerf<65,4d,c3,6f,88,35,cd,4d,3b,2b,bd,95,5b,42,6d,ac,b6,ab,f7,3d> to AP 00:0b:85:5e:40:00
Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP Config-Message to
AP 00:0b:85:5e:40:00 Mon Jun 12 09:04:59 2006: Running spamEncodeCreateVapPayload for SSID
'lab120wlc4402ip100' Mon Jun 12 09:04:59 2006: Running spamEncodeCreateVapPayload for SSID
'lab120wlc4402ip100' Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 AP 00:0b:85:5e:40:00
associated. Last AP failure was due to Link Failure, reason: STATISTICS_INFO_RES Mon Jun 12
09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CHANGE_STATE_EVENT from AP 00:0b:85:5e:40:00 Mon
Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP Change-State-Event
Response to AP 00:0b:85:5e:40:00 Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00
apfSpamProcessStateChangeInSpamContext: Down LWAPP event for AP 00:0b:85:5e:40:00 slot 0 Mon Jun
```

```
12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP Down event for AP 00:0b:85:5e:40:00 slot 0!
Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE COMMAND RES from AP
00:0b:85:5e:40:00 Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CHANGE_STATE_EVENT
from AP 00:0b:85:5e:40:00 Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission
of LWAPP Change-State-Event Response to AP 00:0b:85:5e:40:00 Mon Jun 12 09:04:59 2006:
00:0b:85:5e:40:00 apfSpamProcessStateChangeInSpamContext: Down LWAPP event for AP
00:0b:85:5e:40:00 slot 1 Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP Down event
for AP 00:0b:85:5e:40:00 slot 1! Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP
CONFIGURE COMMAND RES from AP 00:0b:85:5e:40:00 Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00
Received LWAPP CONFIGURE COMMAND RES from AP 00:0b:85:5e:40:00
```

Informações Relacionadas

- Cisco engrena o guia de distribuição da solução de rede de comunicação
- Guia de início rápido: Access point exteriores de pouco peso da malha do Cisco Aironet série 1500
- Guia de Configuração da Cisco Wireless LAN Controller Release 4.0
- Página de Suporte Wireless
- Suporte Técnico e Documentação - Cisco Systems