

# Registro de AP leve (LAP) em um Wireless LAN Controller (WLC)

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Informações de Apoio](#)

[Registrar o LAP com a WLC](#)

[Algoritmo de Descoberta de WLC LWAPP da Camada 2](#)

[Algoritmo de Descoberta de WLC LWAPP da Camada 3](#)

[Processo de seleção de WLC](#)

[Troubleshooting](#)

[Failover de AP entre Grupos de Mobilidade Diferentes](#)

[Informações Relacionadas](#)

## Introdução

Este documento explica os métodos diferentes que o Lightweight Access Points (regações) usa a fim descobrir WLC. Em uma arquitetura de rede Cisco Unified Wireless, os pontos de acesso (AP) são lightweight. Isso significa que eles não podem atuar independentemente de uma controladora de Wireless LAN (WLC). Os regações têm que primeiramente descobrir que os WLC e para se registrar com eles antes dos regações prestam serviços de manutenção a clientes Wireless. O documento também mostra o processo de registro que acontece entre o LAP e a WLC após a fase de descoberta.

Nota: No Software Release 5.2 ou Mais Recente do controlador, os regações de Cisco usam o controle do padrão de IETF e o abastecimento do protocolo dos pontos de acesso Wireless (CAPWAP) a fim comunicar-se entre o controlador e outros regações na rede. Software release do controlador mais cedo do que o uso da liberação 5.2 o protocolo de pouco peso do Access point (LWAPP) para estas comunicações, que é coberto neste documento. Veja [para pesquisar defeitos um Access point de pouco peso que não se junta a um controlador do Wireless LAN](#) para o registro AP e como pesquisar defeitos com o protocolo CAPWAP.

## Pré-requisitos

### Requisitos

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

- Conhecimento do Lightweight Access Point Protocol (LWAPP).
- Conhecimento de como configurar parâmetros básicos na WLC. Se você é um novo usuário e não configurou o WLC para a operação básica, refira a [utilização da](#) seção do [wizard de configuração do manual de configuração do controlador de LAN do Cisco Wireless, a liberação 6.0](#).
- Conhecimento de como configurar o servidor DHCP e o servidor de Domain Name System (DNS) do Microsoft Windows 2000.

## Componentes Utilizados

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

- Cisco 4400 Series WLC com firmware 4.0.217.0
- Cisco 1000 Series LAPs
- Servidor DHCP do Windows 2000
- Servidor DNS do Windows 2000

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

As WLCs e os Cisco LAPs são parte da arquitetura de rede Cisco Unified Wireless. A arquitetura de rede Cisco Unified Wireless centraliza a configuração e o controle da WLAN na WLC. Os LAPs não podem atuar de forma independente da WLC. A WLC gerencia as configurações e o firmware do LAP. Os LAPs são implantados na forma “toque zero”, e nenhuma configuração individual dos LAPs é necessária.

Para que a WLC seja capa de gerenciar o LAP, o LAP deve descobrir a controladora e se registrar na WLC. Após o LAP se registrar na WLC, as mensagens de LWAPP são trocadas e o AP inicia um download de firmware da WLC (se houver incompatibilidade de versão entre o AP e a WLC). Se o firmware do AP não for o mesmo que o da WLC, o AP baixará o firmware para permanecer em sincronia com a WLC. O mecanismo de download de firmware utiliza o LWAPP. Então, a WLC provisiona o LAP com as configurações que são específicas das WLANs de modo que o LAP possa aceitar associações de clientes. Essas configurações específicas de WLAN incluem:

- Identificador de Conjunto de Serviços (SSID)
- Parâmetros de segurança
- Parâmetros do IEEE 802.11, como: Taxa de dados Canais de rádio Níveis de potência

Há os métodos diferentes que um REGAÇO usa a fim descobrir o WLC. Este documento discute os diferentes métodos que um LAP pode usar para registrar a WLC. Mas primeiramente, o documento explica a sequência de evento que ocorre quando um REGAÇO se registra com o

WLC.

Nota: A interface de gerenciamento é a interface padrão para o Gerenciamento In-Band do WLC e da Conectividade aos serviços de empreendimento tais como servidores AAA. A interface de gerenciamento é usada igualmente para comunicações da camada dois entre o WLC e os Access point. A interface de gerenciamento é o único consistentemente endereço IP de Um ou Mais Servidores Cisco ICM NT da relação da em-faixa do “processo de ping” no WLC.

Nota: Um WLC tem umas ou várias relações do gerente AP que estão usadas para todas as comunicações da camada 3 entre o WLC e o Lightweight Access Points depois que o Access point descobre o controlador. O endereço IP de Um ou Mais Servidores Cisco ICM NT do gerente AP é usado como o origem de túnel para pacotes lwapp do WLC ao Access point, e como o destino para pacotes lwapp do Access point ao WLC. O gerente AP deve ter um endereço IP exclusivo. Isto é configurado geralmente na mesma sub-rede como a interface de gerenciamento, mas esta não é necessariamente uma exigência. Um endereço IP de Um ou Mais Servidores Cisco ICM NT do gerente AP não é processo de ping fora do WLC. Refira a seção [configurando das portas e das relações do guia de configuração de controle do Wireless LAN](#) para mais informação.

## Registrar o LAP com a WLC

Esta sequência de evento deve ocorrer para que um REGAÇO registre-se a um WLC:

1. Os LAPs emitem uma solicitação de descoberta de DHCP para obter um endereço IP, a menos possuam um endereço IP estático pré-configurado.
2. O LAP envia mensagens de solicitação de descoberta LWAPP às WLCs.
3. Toda WLC que receber a solicitação de descoberta LWAPP responde com uma mensagem de resposta de descoberta de LWAPP.
4. Das respostas de descoberta de LWAPP que o LAP recebe, ele seleciona uma WLC para se unir.
5. O LAP envia então uma solicitação de união LWAPP para a WLC e espera uma resposta de união LWAPP.
6. A WLC valida o LAP e envia então uma resposta de união LWAPP a ele.
7. O LAP valida a WLC, o que conclui o processo de descoberta e união. O processo de união LWAPP inclui a derivação da autenticação mútua e da chave de criptografia, usadas para proteger o processo de união e também futuras mensagens de controle do LWAPP.
8. O LAP se registra com a controladora.

O primeiro problema enfrentado pelo LAP é como determinar para onde enviar as solicitações de descoberta LWAPP (etapa 2). O LAP usa um procedimento de caçada e um algoritmo de descoberta para determinar a lista de WLCs para as quais o LAP pode enviar as mensagens de solicitação de descoberta.

Este procedimento descreve o processo de caçada:

1. O LAP emite uma solicitação de DHCP para um servidor DHCP a fim de obter um endereço IP, a menos que uma atribuição tenha sido feita anteriormente com um endereço IP estático.
2. Se o modo LWAPP da camada 2 for aceito pelo LAP, o LAP transmitirá uma mensagem de

descoberta LWAPP em um quadro LWAPP da camada 2. Qualquer WLC que estiver conectada à rede e for configurada para o modo LWAPP da camada 2 responderá com uma resposta de descoberta da camada 2. Se o LAP não oferecer suporte ao modo da camada 2, ou se a WLC ou o LAP falharem ao receber uma resposta de descoberta LWAPP para o broadcast de mensagem de descoberta LWAPP da camada 2, o LAP continuará para etapa 3.

3. Se etapa 1 falhar, ou se o LAP ou a WLC não oferecerem suporte ao modo LWAPP da camada 2, o LAP tentará uma descoberta de WLC LWAPP da camada 3. Consulte a seção [Algoritmo de Descoberta de WLC LWAPP da camada 3](#) deste documento.
4. Se etapa 3 falhar, o LAP será reiniciado e voltará para o passo 1.

Nota: Se você quer especificar um endereço IP de Um ou Mais Servidores Cisco ICM NT para um Access point em vez de ter um atribuído automaticamente por um servidor DHCP, você pode usar o controlador GUI ou CLI para configurar um endereço IP estático para o Access point. Refira [configurar um endereço IP estático em uma seção de pouco peso do Access point do](#) manual de configuração WLC para mais informação. Se o REGAÇO é atribuído um endereço IP estático e não pode alcançar o WLC, cai de volta ao DHCP.

## Algoritmo de Descoberta de WLC LWAPP da Camada 2

A comunicação LWAPP entre o AP e a WLC pode ser feita via frames Ethernet nativos da camada 2. Isso é conhecido como modo LWAPP da camada 2. Embora definido no esboço da RFC, o modo LWAPP da camada 2 é considerado fora de uso na implementação da Cisco. Somente os Cisco 1000 Series LAPs oferecem suporte ao modo LWAPP da camada 2. Além disso, não há suporte ao modo LWAPP da camada 2 nas Cisco 2000 Series WLCs. Essas WLC oferecem suporte somente ao modo LWAPP da camada 3.

Esse é o primeiro método que um LAP usa para descobrir uma WLC. Os LAPs que oferecem suporte ao modo LWAPP da camada 2 fazem o broadcast de uma mensagem de solicitação de descoberta LWAPP em um quadro LWAPP da camada 2. Se houver uma WLC na rede configurada para o modo LWAPP da camada 2, a controladora responderá com uma resposta da descoberta. O LAP avança então para a fase de união (veja o passo 5 da seção [Registrar a LAP com a WLC](#)).

Esta saída do comando **debug lwapp enable** mostra a sequência de eventos que ocorre quando um LAP que usa o modo LWAPP da camada 2 se registra com a WLC:

Nota: As linhas desta saída foram movidas para duas linhas devido a limitações de espaço.

```
Thu Sep 27 00:24:25 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 '2'
Thu Sep 27 00:24:25 2007: 00:0b:85:51:5a:e0 Successful transmission of
LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 2
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Received LWAPP JOIN REQUEST
from AP 00:0b:85:51:5a:e0 to 00:0b:85:48:53:c0 on port '2'
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 AP ap:51:5a:e0:
txNonce 00:0B:85:48:53:C0 rxNonce 00:0B:85:51:5A:E0
Thu Sep 27 00:24:40 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 27 00:24:40 2007: 00:0b:85:51:5a:e0 Successfully added NPU Entry for
AP 00:0b:85:51:5a:e0 (index 48)Switch IP: 0.0.0.0, Switch Port: 0, intIfNum 2,
vlanId 0AP IP: 0.0.0.0, AP Port: 0, next hop MAC: 00:0b:85:51:5a:e0
Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Successfully transmission of
```

LWAPP Join-Reply to AP 00:0b:85:51:5a:e0

Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 0

Thu Sep 27 00:24:40 2007: 00:0b:85:51:5a:e0 Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 1

## Algoritmo de Descoberta de WLC LWAPP da Camada 3

Os LAPs usam o algoritmo de descoberta da camada 3 quando não há suporte ao método heurístico da camada 2 ou se o método de descoberta da camada 2 falha. O algoritmo da descoberta da camada 3 usa opções diferentes para tentar descobrir WLCs. O algoritmo de descoberta de WLC LWAPP da camada 3 é usado para criar uma lista de controladoras. Após a criação de uma lista de controladoras, o AP seleciona uma WLC e tenta juntar-se à WLC.

O algoritmo de descoberta de WLC LWAPP da camada 3 se repete até pelo menos uma WLC ser encontradas e unida.

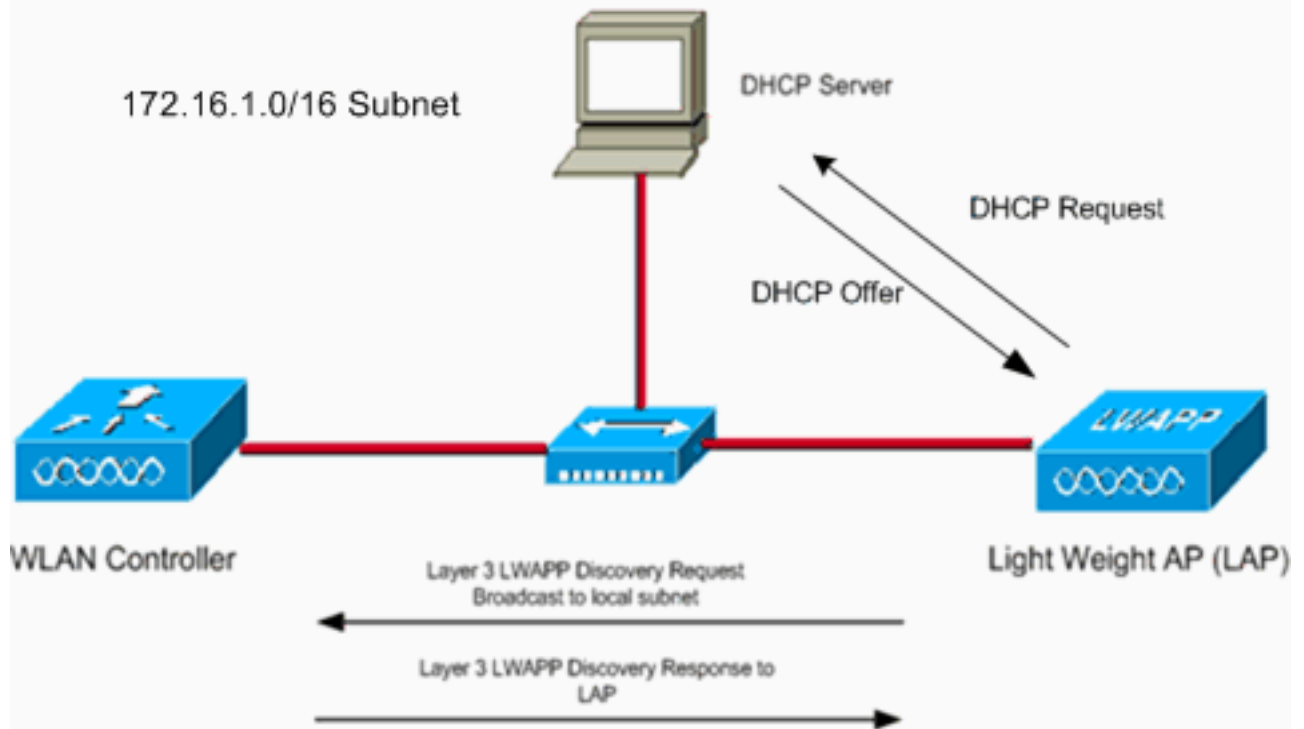
Nota: Durante a descoberta de WLC LWAPP da camada , o AP conclui sempre todos os passos de 1 a 5 desta seção para criar uma das WLCs candidatas. Após o AP concluir todos os passos da descoberta de WLC LWAPP, ele seleciona uma WLC na lista de WLCs candidatas com base em determinados critérios e envia a essa WLC uma solicitação de união LWAPP.

Cada cenário de exemplo explicado nesta seção é independente dos demais e é fornecido somente para auxiliar na compreensão de como cada passo do processo de descoberta funciona. O LAP usa todos os passos da descoberta para encontrar uma lista WLCs candidatas antes de selecionar uma WLC para se unir.

Este procedimento descreve os passos que o algoritmo de descoberta da camada 3 executa na tentativa de descobrir WLCs:

1. Depois que o LAP obtém um endereço IP do servidor DHCP, ele inicia o seguinte processo de descoberta: O LAP transmite um broadcast da mensagem de descoberta LWAPP da camada 3 na sub-rede IP local. Qualquer WLC que esteja configurada para o modo LWAPP da camada 3 e que esteja conectada à mesma sub-rede local recebe a mensagem de descoberta LWAPP da camada 3. Cada uma das WLCs que recebe a mensagem de descoberta LWAPP responde com uma mensagem de resposta de descoberta LWAPP unicast para o LAP.

## Layer 3 Local Subnet Discovery Message Broadcast



Ex

emplo: Supõe que você tem um WLC e um REGAÇO na mesma sub-rede (172.16.1.0/16). Há também uma sub-rede de servidor DHCP. Quando o LAP é ligado, ele envia uma solicitação de DHCP na esperança de um servidor DHCP fornecer um endereço IP. Após o LAP obter um endereço IP do servidor DHCP, ele transmite uma mensagem de descoberta LWAPP da camada 3 para sua sub-rede local. Como a WLC também está na mesma sub-rede, a WLC recebe a solicitação de descoberta LWAPP do LAP e responde com uma resposta de descoberta LWAPP da camada 3. Esta saída de exemplo do **comando debug lwapp events enable** mostra este processo de descoberta:

```
(Cisco Controller) >debug lwapp
events enable
Mon May 22 12:00:21 2006: Received LWAPP DISCOVERY REQUEST from AP
00:0b:85:5b:fb:d0 to ff:ff:ff:ff:ff:ff on port '1'
Mon May 22 12:00:21 2006: Successful transmission of LWAPP Discovery-Response
to AP 00:0b:85:5b:fb:d0 on Port 1
```

A saída do **comando debug lwapp packet enable** para a descoberta via broadcast da sub-rede local é semelhante a:

```
(Cisco Controller) >debug lwapp packet enable
Tue May 23 12:37:50 2006: Start of Packet
Tue May 23 12:37:50 2006: Ethernet Source MAC (LRAD):      00:0B:85:51:5A:E0
Tue May 23 12:37:50 2006: Msg Type                :
Tue May 23 12:37:50 2006:     DISCOVERY_REQUEST
Tue May 23 12:37:50 2006: Msg Length       :   31
Tue May 23 12:37:50 2006: Msg SeqNum      :    0
Tue May 23 12:37:50 2006:
IE                : UNKNOWN IE 58
Tue May 23 12:37:50 2006: IE Length       :    1
Tue May 23 12:37:50 2006: Decode routine not available, Printing Hex Dump
Tue May 23 12:37:50 2006: 00000000: 00
```

Observe as linhas marcadas em negrito. O valor do parâmetro **IE 58** indica o tipo da descoberta:

- 0 - broadcast
- 1 - configured
- 2 - OTAP
- 3 - dhcp server
- 4 - dns

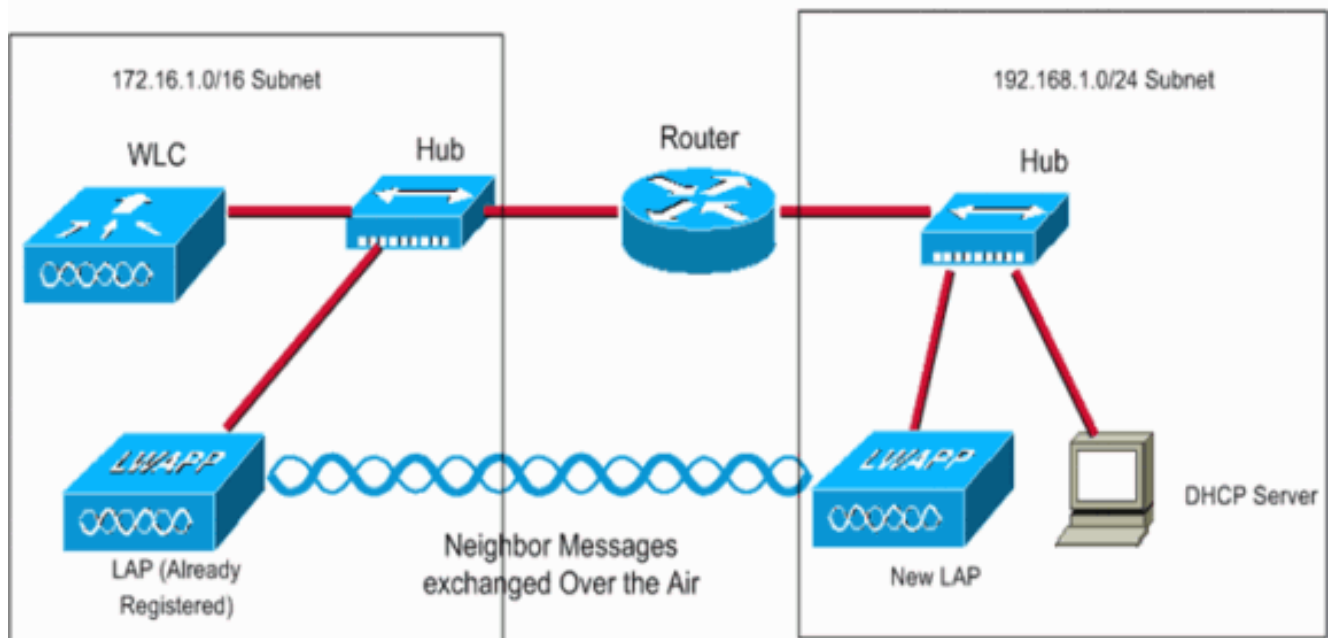
Como este é um broadcast da sub-rede local, o valor do parâmetro **IE 58** é **0** nesta saída do



comando **debug lwapp packet enable**.

- Os LAPs também usam o recurso Over-the-Air Provisioning (OTAP) para descobrir a WLC. A característica OTAP é *desabilitada à revelia em 4.2.39.13, em 5.0.68.0 e em umas versões mais atrasadas WLC*. O OTAP é *permitido à revelia nas versões WLC mais cedo de 4.2.39.13*. Este é o processo de descoberta quando o OTAP está habilitado: Os LAPs que já estão registrados na WLC podem anunciar o endereço IP da WLC para os LAPs (na tentativa de encontrar a WLC) com o uso de mensagens para vizinhos transmitidas no ar. Os LAPs novos que tentam descobrir WLCs ouvem essas mensagens e então enviam mensagens de solicitação de descoberta LWAPP unicast para as WLCs. As WLCs que recebem a mensagem de descoberta LWAPP respondem com uma mensagem de resposta de descoberta LWAPP unicast para o LAP. O OTAP deverá estar habilitado somente durante os intervalos de provisionamento do AP. Após a implantação dos AP, desabilite o OTAP como uma prática recomendada de implantação. Além disso os Cisco Aironet LAPs (1130 AG, 1200, e 1240 AG Séries) saem de fábrica com uma versão simplificada do lightweight Cisco IOS® Software chamada LWAPP Recovery Cisco IOS Image. Não há suporte ao OTAP nos APs prontos para funcionar que executam o LWAPP Cisco IOS Software. Quando você atualiza os Cisco Aironet APs do Cisco IOS Software autônomo para o modo lightweight, o LWAPP Recovery Cisco IOS Image é o software que é carregado. O LWAPP Recovery Cisco IOS Image não oferece suporte ao OTAP. Para oferecerem suporte ao OTAP, os LAPs Aironet devem primeiro se unir a uma WLC para baixar um LWAPP Cisco IOS Image completo.

Using Over the Air Provisioning



Exemplo: Supõe que, na sub-rede 172.16.1.0/16, você tem um REGAÇO que seja registrado já com o WLC, e o OTAP é permitido no WLC. Quando o novo LAP na sub-rede 192.168.1.0/24 é ativado, ele procura um servidor DHCP e obtém um endereço IP (se nenhuma atribuição de endereço IP estático foi feita anteriormente). O LAP envia então uma solicitação de descoberta à sub-rede local. Como neste cenário não há WLC alguma na sub-rede local, o LAP tenta usar o OTAP para descobrir WLCs. O LAP escuta as mensagens de vizinhos que são enviadas no ar pelos LAPs (na sub-rede 172.16.1.0/16) que já estão registrados e procura endereços IP de WLCs. Na lista de endereços IP de WLCs que

aprendem das mensagens de vizinhos, os os novos LAPs enviam uma solicitação de descoberta LWAPP da camada 3 para as WLCs. As WLCs que recebem essa solicitação de descoberta respondem com uma resposta de descoberta LWAPP da camada 3. Esta saída do comando **debug lwapp event enable** ilustra a sequência de mensagens enviada pelas

```
Tue May 23 14:37:10 2006: Received LWAPP DISCOVERY REQUEST from AP
00:0b:85:5b:fb:d0 to 00:0b:85:33:84:a0 on port '1'
Tue May 23 14:37:10 2006: Successful transmission of LWAPP Discovery-Response to
AP 00:0b:85:5b:fb:d0 on Port 1
```

Nota: Como o LAP aprendeu o endereço IP da WLC nas mensagens dos vizinhos, ele envia uma solicitação de descoberta unicast para a WLC. Desta forma, essa passo é o contrário do método do passo 1 deste procedimento, no qual o LAP envia um broadcast na sub-rede local. Nota: O valor do parâmetro **IE 58** na saída do comando **debug lwapp packet enable** mostra que o LAP usou o OTAP como o método de descoberta.

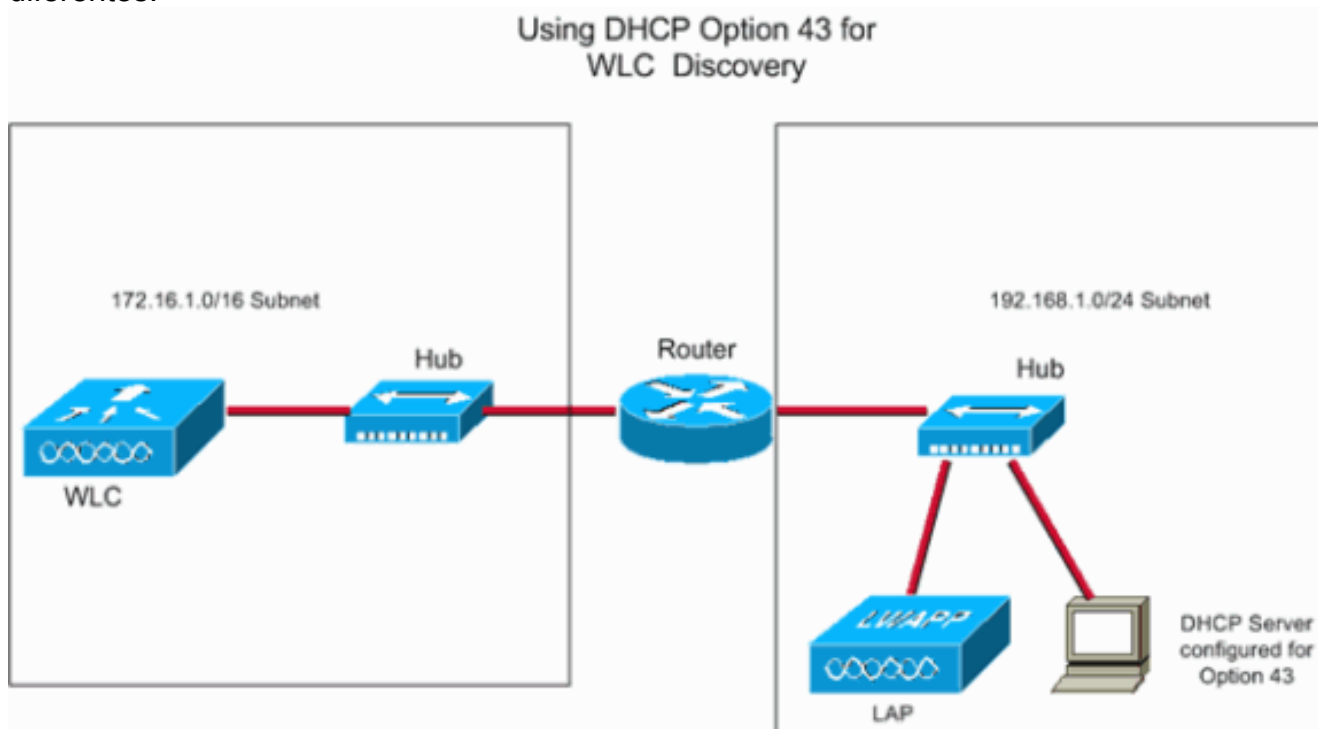
```
Tue May 23 14:21:55 2006:
Start of Packet
Tue May 23 14:21:55 2006: Ethernet Source MAC (LRAD):      00:D0:58:AD:AE:CB
Tue May 23 14:21:55 2006: Msg Type                :
Tue May 23 14:21:55 2006:      DISCOVERY_REQUEST
Tue May 23 14:21:55 2006: Msg Length         :    31
Tue May 23 14:21:55 2006: Msg SeqNum        :     0
Tue May 23 14:21:55 2006:
IE                :   UNKNOWN IE 58
Tue May 23 14:21:55 2006: IE Length         :     1
Tue May 23 14:21:55 2006: Decode routine not available, Printing Hex Dump
Tue May 23 14:21:55 2006: 00000000: 02
Tue May 23 14:21:55 2006:
```

3. Se o LAP foi registrado em uma WLC em uma implantação anterior, o LAP mantém a lista de endereços IP de WLCs localmente na NVRAM. Os endereços IP de WLCs armazenados incluem todas as WLCs que pertencem a "grupos de mobilidade de WLCs unidas previamente. Este é o processo de descoberta: Os LAPs enviam uma solicitação de descoberta LWAPP da camada 3 unicast para cada um dos endereços IP de WLCs armazenados em suas NVRAMs. As WLCs que recebem a mensagem de descoberta LWAPP respondem com uma mensagem de resposta de descoberta LWAPP unicast para o LAP. A seguir são apresentados exemplos de saída dos comandos **debug lwapp events enable** e **debug lwapp packet enable** para este método de descoberta de WLC: Nota: Se você usar o comando **clear ap-config ap\_name** para restaurar o LAP para os padrões de fábrica, todas as configurações do LAP serão redefinidas. As configurações que são redefinidas incluem os endereços IP de WLCs armazenados na NVRAM. Neste caso, o LAP deve usar algum outro método para descobrir a WLC. (Cisco Controller) >**debug lwapp events enable**

```
Tue May 23 14:37:10 2006: Received LWAPP DISCOVERY REQUEST from AP
00:0b:85:5b:fb:d0 to 00:0b:85:33:84:a0 on port '1'
Tue May 23 14:37:10 2006: Successful transmission of LWAPP Discovery-Response to
AP 00:0b:85:5b:fb:d0 on Port 1
(Cisco Controller) >debug lwapp packet enable
Tue May 23 14:45:36 2006: Start of Packet
Tue May 23 14:45:36 2006: Ethernet Source MAC (LRAD):      00:D0:58:AD:AE:CB
Tue May 23 14:45:36 2006: Msg Type                :
Tue May 23 14:45:36 2006:      DISCOVERY_REQUEST
Tue May 23 14:45:36 2006: Msg Length         :    31
Tue May 23 14:45:36 2006: Msg SeqNum        :     0
Tue May 23 14:45:36 2006:
IE                :   UNKNOWN IE 58
Tue May 23 14:45:36 2006: IE Length         :     1
Tue May 23 14:45:36 2006: Decode routine not available, Printing Hex Dump
Tue May 23 14:45:36 2006: 00000000: 01
Tue May 23 14:45:36 2006:
```



4. Você também pode programar servidores DHCP para retornar endereços IP de WLCs na "Opção 43" específica do fornecedor na oferta de DHCP para os LAPs. Este é o processo de descoberta: Quando um REGAÇO obtém um endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor DHCP, o REGAÇO procura endereços IP de Um ou Mais Servidores Cisco ICM NT WLC no campo da opção 43 da oferta de DHCP. O LAP envia um pedido de descoberta LWAPP da camada 3 a cada uma das WLCs relacionadas opção de DHCP 43. As WLCs que recebem a mensagem de descoberta LWAPP respondem com uma mensagem de resposta de descoberta LWAPP unicast para o LAP. Nota: Você pode usar a opção de DHCP 43 quando os LAPs e as WLCs estão em sub-redes diferentes.



Éis um exemplo de cenário. Suponha que haja uma WLC em uma sub-rede (por exemplo, 172.16.1.0/16) e os LAPs e o servidor DHCP estejam em uma sub-rede diferente (por exemplo, 192.168.1.0/24). O roteamento entre as duas sub-redes está habilitado. Você pode configurar o servidor DHCP para retornar os endereços IP de WLCs ao LAP na mensagem da oferta de DHCP. Você pode usar qualquer servidor DHCP que ofereça suporte à opção 43. Nota: Refira a [OPÇÃO DE DHCP 43 para o exemplo de configuração de pouco peso dos Access point do Cisco Aironet](#) para obter informações sobre de como configurar o servidor DHCP do Windows 2000 para a opção 43. Assim, quando o LAP for ligado, ele procurará um servidor DHCP para obter um endereço IP. O servidor DHCP aloca um endereço IP para o LAP e também fornece a lista de endereços IP de WLCs através do uso da opção de DHCP 43. O LAP envia uma solicitação de descoberta unicast para cada uma das WLCs. As WLC que ouvem essas mensagens enviam uma resposta de descoberta, o que inicia o processo de registro. Esta saída do comando **debug lwapp events enable** mostra a sequência de mensagens LWAPP:

```
Tue May 23 14:43:42 2006: Received LWAPP DISCOVERY REQUEST from AP
00:0b:85:5b:fb:d0 to 00:0b:85:33:84:a0 on port '1'
Tue May 23 14:43:42 2006: Successful transmission of LWAPP Discovery-Response to
AP 00:0b:85:5b:fb:d0 on Port 1
```

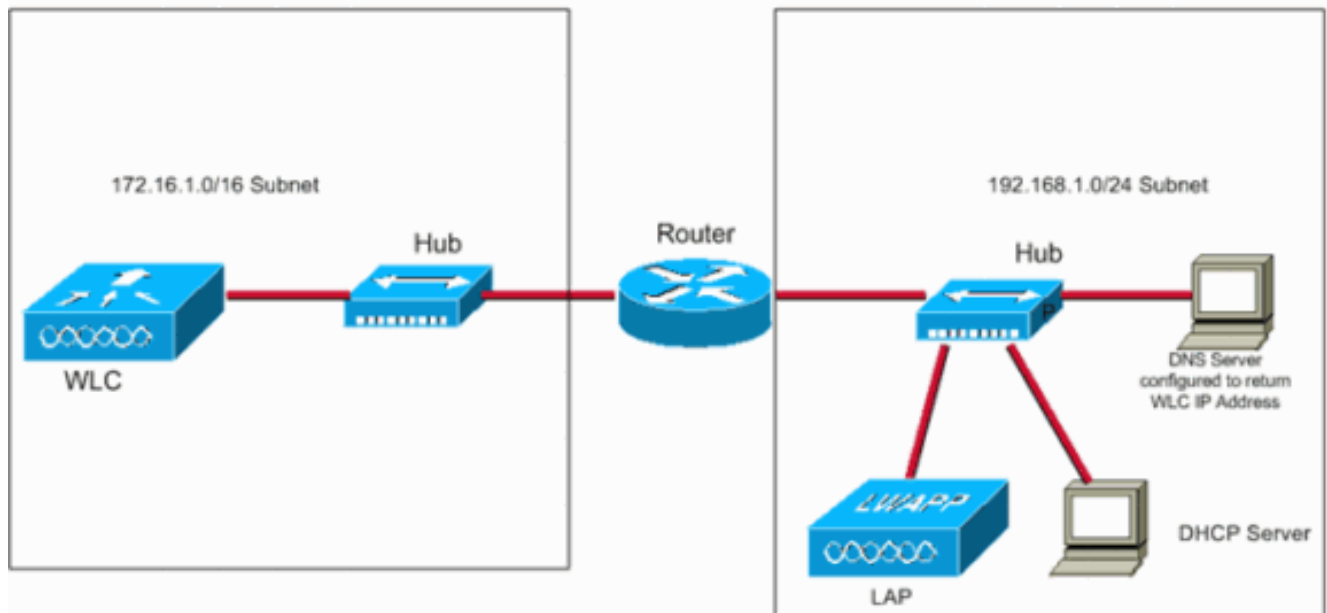
Esta saída do comando **debug lwapp packet enable** indica que a opção de DHCP 43 foi usada como o método de descoberta dos endereços IP de WLCs:

```
Tue May 23 16:14:32 2006:
Start of Packet
Tue May 23 16:14:32 2006: Ethernet Source MAC (LRAD):          00:D0:58:AD:AE:CB
Tue May 23 16:14:32 2006: Msg Type                               :
```

```
Tue May 23 16:14:32 2006:     DISCOVERY_REQUEST
Tue May 23 16:14:32 2006: Msg Length      :    31
Tue May 23 16:14:32 2006: Msg SeqNum       :     0
Tue May 23 16:14:32 2006:
IE           : UNKNOWN IE 58
Tue May 23 16:14:32 2006: IE Length        :     1
Tue May 23 16:14:32 2006: Decode routine not available, Printing Hex Dump
Tue May 23 16:14:32 2006: 00000000: 03
Tue May 23 16:14:32 2006:
```

5. Finalmente, você pode também pode usar o servidor DNS para retornar endereços IP de WLCs para o LAP. Este é o processo de descoberta:O REGAÇO tenta resolver o nome de DNS "CISCO-CAPWAP-CONTROLLER.local-domain" ou "CISCO-LWAPP-CONTROLLER.local-domain". Nota: Nessa sintaxe do nome de DNS, localdomain refere-se ao nome de domínio que precisa ser resolvido. Por exemplo, se o domínio for cisco.com, o nome de DNS será CISCO-LWAPP-CONTROLLER.cisco.com. O AP precisa ser informado sobre o nome de domínio que deve ser resolvido, de modo que o AP possa enviar a solicitação para o servidor DNS que fez a solicitação para resolver esse nome de domínio específico. O AP é informado sobre esse nome de domínio através da opção de DHCP 15. A opção de DHCP 15 especifica o nome de domínio que o AP deve usar para a resolução de DNS. Assim, é necessário que a opção de DHCP 15 esteja configurada com a informação de nome de domínio. Isso permite que o servidor DHCP que envia o endereço IP do servidor DNS envie também essa informação de opção de DHCP 15 (o nome de domínio a ser resolvido) para o AP.Quando o LAP é capaz de resolver esse nome em um ou mais endereços IP de WLCs, ele envia uma solicitação de descoberta LWAPP da camada 3 unicast a cada uma das WLCs.As WLCs que recebem a mensagem de descoberta LWAPP enviam uma resposta de descoberta LWAPP unicast ao AP.Este exemplo usa a mesma configuração que foi usada para a opção de DHCP 43 (passo 3). No entanto, nesse exemplo, o servidor DHCP não usa a opção 43. Em vez disso, o servidor DHCP fornece ao LAP um endereço IP e também o endereço IP do servidor DNS na oferta de DHCP. Depois que o REGAÇO obtém o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor DNS, o REGAÇO manda uma pergunta DNS para o nome de DNS "CISCO-CAPWAP-CONTROLLER.local-domain" ou "CISCO-LWAPP-CONTROLLER.local-domain". O servidor DNS deve ser configurado de forma a retornar o endereço IP da WLC para esta consulta. Quando o LAP obtém o endereço IP da WLC, ele inicia o processo de registro junto à WLC.

## Using DNS Query for WLC Discovery



Esta saída do comando **debug lwapp packet enable** mostra o tipo de descoberta como

```
DNS:Tue May 23 16:14:32 2006: Start of Packet
Tue May 23 16:14:32 2006: Ethernet Source MAC (LRAD):      00:D0:58:AD:AE:CB
Tue May 23 16:14:32 2006: Msg Type                   :
Tue May 23 16:14:32 2006:      DISCOVERY_REQUEST
Tue May 23 16:14:32 2006: Msg Length          : 31
Tue May 23 16:14:32 2006: Msg SeqNum         : 0
Tue May 23 16:14:32 2006:
IE           : UNKNOWN IE 58
Tue May 23 16:14:32 2006: IE Length          : 1
Tue May 23 16:14:32 2006: Decode routine not available, Printing Hex Dump
Tue May 23 16:14:32 2006: 00000000: 04
```

Tue May 23 16:14:32 2006: Nota: Se, após a conclusão dos passos 1 a 5, o LAP não receber uma resposta de descoberta LWAPP, ele redefinirá e reiniciará o algoritmo de caçada.

6. **Use o endereço do IP helper no roteador** Embora não faça parte do algoritmo de descoberta da camada 3, este é um método mais simples que pode ser usado quando a WLC e as LAPs estão em sub-redes diferentes. Após o LAP obter um endereço IP do servidor DHCP, ele transmite uma mensagem de descoberta LWAPP da camada 3 para sua sub-rede local. O endereço IP da WLC é configurado como o endereço de *ip-helper* no roteador. O roteador encaminha esses broadcasts para os endereços IP configurados com o comando *ip-helper* na *interface* em que o broadcast é ouvido. Quando você usa o comando *ip helper-address*, BROADCASTS DIRECIONADOS, bem como unicasts, oito portas UDP diferentes são encaminhadas automaticamente. Essas portas são Trivial File Transfer (TFTP) (Porta 69), Domain Name System (Porta 53), Time Service (Porta 37), NetBIOS Name Server (Porta 137), NetBIOS Datagram Server (Porta 138), Boot Protocol (BOOTP) Cliente e Servidor (Porta 67 e Porta 68), serviço TACACS (Porta 49). Desde que a porta 12223 dos usos UDP da transmissão LWAPP ele deve explicitamente ser encaminhada no roteador. Eis um exemplo de cenário. Suponha que haja uma WLC em uma sub-rede (por exemplo, 172.16.1.0/16) e os LAPs e o servidor DHCP estejam em uma sub-rede diferente (por exemplo, 192.168.1.0/24). O roteamento entre as duas sub-redes está habilitado. Este exemplo mostra a configuração no roteador:
- ```
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip helper-address 172.16.0.1
!--- IP address of the WLC Router(config-if)#exit
Router(config)#ip forward-protocol udp 12223
```

Nota: Se você executa a versão 5.2 ou mais recente WLC, use o número de porta 5246 UDP porque a transmissão CAPWAP usa a porta 5246 UDP.

```
Router(config)#interface
FastEthernet 0/1
Router(config-if)#ip helper-address 172.16.0.1
!--- IP address of the WLC Router(config-if)#exit
Router(config)#ip forward-protocol udp 12223
```

## Processo de seleção de WLC

Depois que o LAP conclui os passos de 1 a 5 do [algoritmo de descoberta de WLC LWAPP da camada 3](#), ele seleciona uma WLC da lista de WLCs candidatas e envia a essa WLC uma solicitação de união LWAPP.

As WLC incorporam estas importantes informações na resposta de descoberta LWAPP:

- O sysName da controladora
- O tipo da controladora
- A capacidade do AP da controladora e sua carga de AP atual
- O sinalizador da controladora mestre
- Um endereço IP de gerenciador de AP

O LAP usa essas informações para fazer uma seleção de controladora através destas regras de precedência:

1. Se o REGAÇO tem sido configurado previamente com um preliminar, secundário, e/ou o controlador terciário, o REGAÇO examina o campo do sysName do controlador (das respostas de descoberta de LWAPP) na tentativa de encontrar o WLC que é configurado como o "preliminar". Se o LAP encontrar um sysName correspondente para a controladora primária, ele enviará uma solicitação de união LWAPP àquela WLC. Se o LAP não encontrar sua controladora primária ou se a união LWAPP falhar, ele tentará corresponder o sysName da controladora secundária às respostas de descoberta LWAPP. Se o LAP encontrar uma correspondência, ele enviará uma solicitação de união LWAPP à controladora secundária. Se a WLC secundária não puder ser encontrada ou a união LWAPP falhar, o LAP repetirá o processo para sua controladora terciária.
2. O LAP verifica o campo de sinalizador da controladora mestre nas respostas de descoberta LWAPP das WLCs candidatas se um destes itens é verdadeiro: Nenhuma controladora primária, secundária e/ou terciária foi configurada para um AP. Essas controladoras não podem ser encontradas na lista de candidatos. As uniões LWAPP a essas controladoras falhou. Se um WLC é configurado como um controlador mestre, o REGAÇO seleciona esse WLC e envia-o que um LWAPP se junta ao pedido.
3. Se o LAP não puder se unir com êxito a uma WLC com base nos critérios dos passos 1 e 2, ele tentará se unir à WLC que tem a maior capacidade excedente.

Depois de selecionar uma WLC, o LAP enviará uma solicitação de união LWAPP à WLC. Na solicitação de união LWAPP, o LAP incorpora um certificado X.509 assinado digitalmente. Quando o certificado é validado, a WLC envia uma resposta de união LWAPP para indicar ao LAP que ele se uniu com êxito à controladora. A WLC incorpora seu próprio certificado X.509 assinado digitalmente na resposta de união LWAPP que deve ser validada pelo LAP. Após o LAP validar o certificado da WLC, o processo de união LWAPP está concluído.

O LAP e a controladora de Wireless LAN gerenciam a fragmentação e a remontagem para o túnel LWAPP. Eles trabalham sob a suposição de uma MTU com 1500 bytes. Esse não é um

parâmetro configurável. No AP ou na WLC, se o MTU for superior a 1500 bytes, o pacote será fragmentado e enviado. O sistema lida com até 4 fragmentos na versão 3.2. As versões anteriores oferecem suporte somente até dois fragmentos.

Está aqui um link a um vídeo na [comunidade do apoio de Cisco](#) que explica o processo de registro do REGAÇO:

[Registro de pouco peso do Access point com controladores do Wireless LAN \(WLC\)](#)



## Troubleshooting

A versão do firmware da controladora é 3.2.78.0. Quando o comando **debug lwapp events** é executado, a seguinte saída é mostrada:

```
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip helper-address 172.16.0.1
!--- IP address of the WLC Router(config-if)#exit
Router(config)#ip forward-protocol udp 12223
```

Esta mensagem de erro significa que a imagem 3.2.78.0 não oferece suporte ao LAP. Essencialmente, a controladora não é capaz de encontrar a imagem para o LAP em sua lista de imagens. Consequentemente, o LAP não pode baixar a imagem da WLC. Para resolver este problema, atualize a controladora para a versão 3.2.116.0 ou posterior. Isso resolve o problema e o LAP une-se à controladora e baixa a imagem necessária.

Às vezes, a seguinte mensagem de erro poderá ser gerada em sua controladora:

```
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip helper-address 172.16.0.1
!--- IP address of the WLC Router(config-if)#exit
```

```
Router(config)#ip forward-protocol udp 12223
```

Essa mensagem de erro significa que a controladora recebeu um pedido de descoberta através de um endereço IP de broadcast que possui um endereço IP de origem (atribuído) que não pertence a nenhuma sub-rede configurada na controladora. Ela também significa que a controladora descartou o pacote. Isto normalmente acontece quando todos os troncos do cliente permitiram VLANs em vez de restringi-las a VLANs wireless.

Você também pode encontrar esta mensagem de erro:

```
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip helper-address 172.16.0.1
!--- IP address of the WLC Router(config-if)#exit
Router(config)#ip forward-protocol udp 12223
```

Ela significa que a controladora recebeu uma solicitação de descoberta em que endereço IP de destino (atribuído) não é seu endereço IP de gerenciamento. Ela também significa que a controladora descartou o pacote.

Há muitas razões que um Access point de pouco peso (REGAÇO) pode não se junta ao WLC. Consulte [para pesquisar defeitos um Access point de pouco peso que não se junta a um controlador do Wireless LAN](#) para obter informações sobre de algumas das razões que um REGAÇO não se junta a um WLC e como pesquisar defeitos as edições.

## Failover de AP entre Grupos de Mobilidade Diferentes

Considere este cenário. O grupo de mobilidade **MG1** contém duas controladoras, C1 e C2. Essas controladoras estão implantadas em um prédio, com balanceamento de carga de LAPs entre ambos. A filial da empresa implanta uma terceira controladora C3 e a configura para o grupo de mobilidade **MG2**. Os LAPs dessa controladora (C3) não executam o failover para uma das outras duas controladoras, mas um dia, quando a controladora C3 reinicializa, os LAPs que estavam originalmente registrados em C3 agora se registram em C1 no grupo de mobilidade **MG1**.

Agora, mesmo que a controladora primária dos LAPs seja C3, e há não secundária ou terciária, os LAPs se uniram a C1; uma reinicialização do LAP não o traz de volta para C3. Qual é o problema?

A razão é que, na implantação inicial, a empresa criou um de dois cenários:

- Uma entrada de DNS para "CISCO-CAPWAP-CONTROLLER.local-domain" ou "CISCO-LWAPP-CONTROLLER.local-domain" a apontar ao C1 ou ao C2.
- A adição de uma opção de DHCP 43 para apontar para C1 ou C2 para facilitar a instalação inicial. Após a conclusão da instalação no primeiro prédio, essas entradas nunca foram removidas.

Nota: O AP também pode descobrir as controladoras C1 ou C2 por qualquer outro método de descoberta, tal como broadcast da camada 3 e o OTAP. Assim certifique-se de que precauções apropriadas sejam tomadas para que o AP possa somente aprender sobre controladoras de um único grupo de mobilidade através de qualquer um dos métodos.

Quando a controladora C3 é desativada, os LAPs que estavam conectados a ela são reinicializados. Eles passam por seus processos de descoberta da forma descrita. Eles não apenas enviam solicitações de descoberta para as controladoras existentes na configuração da NVRAM, mas também para os endereços IP aprendidos via DNS e DHCP que, como resultado,



incluem C1 ou C2.

Como C3 está desativada no momento da descoberta, os LAPs não obtêm uma RESPOSTA DE DESCOBERTA. Assim, eles não podem continuar com a união às suas controladoras principais configuradas e devem se unir à controladora descoberta via DHCP ou DNS.

Ao se unirem a C1 ou C2, os LAPs baixam a nova lista do grupo de mobilidade, a qual inclui endereços IP somente para C1 e C2. Assim, se eles forem reinicializados, não será possível eles aprenderem o endereço IP de C3 para enviarem solicitações de descoberta. Eles não podem se unir a essa controladora. A única maneira de trazer os LAPs de volta para C3 é adicionar C3 à lista do grupo de mobilidade de C1 e C2 ou alterar a opção 43 ou a entrada de DNS.

Há diversas maneiras de evitar esses problemas:

- Recomenda-se usar o DNS e as opções de DHCP somente na implantação inicial e que ambos sejam removidos uma vez que a rede esteja configurada. Desse modo, os APs na rede não terão como aprender sobre outros grupos de mobilidade.
- Separe os escopos de DHCP ou os domínios de DNS. Tenha um escopo para o prédio 1 e outro prédio 2 no servidor DHCP corporativo. O administrador pode configurar endereços IP de opção 43 diferentes para cada escopo. O mesmo se aplica a domínios de DNS: ao usar um nome de host `building1.companyname.com` para um prédio e `building2.companyname.com` para o outro, você pode ter opções diferentes de CISCO-LWAPP-CONTROLLER para cada subdomínio.
- Você também pode usar funções na WLC para controlar alguns comportamentos: No caso dos AP com certificados auto-assinados (SSC), adicione os SSCs somente às controladoras que você deseja que se unam aos APs. No caso dos APs com certificados instalados pelo fabricante (MIC), use a função de **autorização de AP AAA na WLC** (com o comando **config auth-list ap-policy authorize-ap enable**) para informar à controladora para verificar se ela deve aceitar o AP. Para permitir a união dos APs, use uma destas opções: Adicione-os à lista de autorização da WLC: use o comando **config auth-list add mic <MAC-Address>**. Adicione-os como clientes ao servidor RADIUS. Called-Station-ID é o endereço MAC da controladora. Se você separar os AP em grupos, poderá criar políticas para definir quais AP podem se autenticar em quais Called-Station-IDs.

A fim conseguir um REGAÇO juntar-se a um controlador que não seja parte do grupo da mobilidade do controlador atualmente juntado, você precisa de certificar-se de que o nome do controlador principal é aquele do controlador a que você deseja enviar o REGAÇO.

Uma vez que isso seja feito, tudo o que você precisará fazer é dar ao LAP uma maneira de descobrir essa controladora. Isso pode ser feito com alguns dos métodos descritos no algoritmo de descoberta de WLCs explicado neste documento.

## Informações Relacionadas

- [Controlando Pontos de Acesso Lightweight](#)
- [Exemplo de Configuração Básica de Controladoras de Wireless LAN e Pontos de Acesso Lightweight](#)
- [LWAPP \(modo leve\) à conversão autônoma e vice-versa](#)
- [Estudo do tráfego LWAPP](#)
- [Manual de configuração do controlador de LAN do Cisco Wireless, liberação 6.0](#)



- [Suporte Técnico e Documentação - Cisco Systems](#)