Регистрация облегченных точек доступа у контроллеру беспроводных LAN (WLC)

Содержание

Введение

Этот документ объясняет другие методы это облегченные точки доступа (LAP) используют для обнаружения WLC . В архитектуре единой беспроводной сети Cisco (UWN) точки доступа (AP) являются легковесными. Это означает, что они не могут действовать независимо от контроллера беспроводной локальной сети (WLC). LAP должны сначала обнаружить WLC и зарегистрироваться в них перед беспроводными клиентами сервиса LAP. Документ также объясняет процесс регистрации, который происходит между LAP и WLC после фазы обнаружения.

> **Примечание:** В выпуске ПО контроллера 5.2 или позже, LAP Cisco используют Контроль за стандартом IETF и Инициализацию Точек беспроводного доступа (CAPWAP) протокол для передачи между контроллером и другими LAP в сети. Выпуски ПО контроллера ранее, чем Выпуск 5.2 используют Протокол LWAPP для этой связи, который покрыт этим документом. Посмотрите Устранение неполадок Облегченная точка доступа, Не Присоединяющаяся к Контроллеру беспроводной локальной сети для регистрации AP и как устранить неполадки с протоколом CAPWAP.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Знание протокола LWAPP.
- Знание того, как настроить основные параметры на WLC.Если вы - новый пользователь и не настроили WLC для главной операции, обратитесь к Использованию раздела Мастера настройки *руководства по конфигурированию контроллера Cisco Wireless LAN, Выпуска 6.0*.
- Знание как к Серверу Сервера DHCP и Системы доменных имен (DNS) Microsoft Windows 2000 configure.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco WLC серии 4400, который выполняет микропрограммное обеспечение 4.0.217.0
- Облегченные точки доступа Cisco 1000 серии
- Сервер DHCP Windows 2000
- Сервер DNS Windows 2000

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

WLC и LAP Cisco являются частью архитектуры беспроводной унифицированной сети Cisco (CUWN). Архитектура беспроводной унифицированной сети Cisco (CUWN) централизует конфигурацию WLAN и контроль на WLC. LAP не могут действовать независимо от WLC. WLC управляет конфигурациями LAP и микропрограммным обеспечением. LAP являются "нулевым касанием", развернутым, и никакая отдельная конфигурация LAP не требуется.

Для WLC, чтобы быть в состоянии управлять LAP, LAP должен обнаружить контроллер и зарегистрироваться в WLC. После того, как LAP зарегистрировался к WLC, сообщениями LWAPP обмениваются, и AP инициирует загрузку микропрограммы от WLC (если существует несоответствие версии между AP и WLC). Если встроенное микропрограммное обеспечение AP не будет тем же как WLC, то AP загрузит микропрограммное обеспечение для пребывания в синхронизовании с WLC. Механизм загрузки микропрограммы использует LWAPP. Затем WLC настраивает LAP с конфигурациями, которые являются определенными для WLAN так, чтобы LAP мог принять связывания клиента. Эти специфичные для WLAN конфигурации включают:

- Идентификатор набора служб (SSID)
- Параметры безопасности
- Параметры IEEE 802.11, такие как:Скорость передачи данныхРадио-каналыУровни мощности

Существуют другие методы, которые LAP использует для обнаружения WLC. Этот документ обсуждает другие методы, которые LAP может использовать для регистрации WLC. Но сначала, документ объясняет последовательность событий, которые происходят, когда LAP регистрируется в WLC.

> **Примечание:** Интерфейс управления является интерфейсом по умолчанию для внутриполосного управления WLC и подключения к корпоративному обслуживанию, такому как AAA-серверы. Интерфейс управления также используется для уровня две связи между WLC и точками доступа. Интерфейс управления является единственным последовательно "отвечающим на команду ping" внутриполосным IP-адресом интерфейса на WLC.

> **Примечание:** WLC имеет один или несколько интерфейсов диспетчера точки доступа, которые используются для всей связи Уровня 3 между WLC и облегченными точками доступа после того, как точка доступа обнаруживает контроллер. Менеджер AP IP-адрес используется в качестве точки начала туннеля для Пакетов lwapp от WLC до точки доступа, и как назначение для Пакетов lwapp от точки доступа до WLC. У Менеджера AP должен быть уникальный IP - адрес. Обычно это настроено в той же подсети как Интерфейс управления, но это - не обязательно требование. Менеджер AP IP-адрес не является отвечающим на команду ping снаружи WLC. См. раздел портов и Интерфейсов Настройки Руководства по конфигурации Контроллера беспроводной локальной сети для получения дополнительной информации.

Зарегистрируйте LAP в WLC

Эта последовательность событий должна произойти для LAP для регистрации к WLC:

1. LAP выполняют запрос на обнаружение DHCP для получения IP-адреса, пока этому ранее не настроили статический IP - адрес.
2. LAP передает сообщения запроса обнаружения LWAPP к WLC.
3. Любой WLC, который получает запрос обнаружения LWAPP, отвечает сообщением ответа обнаружения LWAPP.
4. От ответов обнаружения LWAPP, которые получает LAP, LAP выбирает WLC для присоединения.
5. LAP тогда передает Запрос на присоединение LWAPP к WLC и ожидает ответ соединения LWAPP.
6. WLC проверяет LAP и затем передает LWAPP, соединяют ответ на LAP.
7. LAP проверяет WLC, который завершает процесс соединения и обнаружение. Процесс соединения LWAPP включает обоюдную проверку подлинности и деривацию ключа шифрования, которая используется для обеспечения процесса соединения и будущих сообщений управления LWAPP.
8. LAP регистрируется в контроллере.

Первая проблема, с которой стоит LAP, состоит в том, как определить, куда передать (шаг 2) запросов обнаружения LWAPP. LAP использует процедуру поиска и алгоритм обнаружения для определения списка WLC, к которым LAP может передать сообщения запроса на обнаружение.

Эта процедура описывает процесс поиска:

1. LAP выполняет запрос DHCP к серверу DHCP для получения IP-адреса, пока присвоение не было сделано ранее со статическим IP - адресом.
2. Если Режим LWAPP уровня 2 поддерживается на LAP, LAP передает сообщение обнаружения LWAPP в кадре LWAPP Уровня 2. Любой WLC, который связан с сетью и это настроено для Режима LWAPP уровня 2, отвечает ответом обнаружения Уровня 2. Если LAP не делает режима уровня поддержки 2, или если WLC или LAP не в состоянии получать ответ обнаружения LWAPP к радиопередаче сообщений обнаружения LWAPP Уровня 2, LAP продолжается к шагу 3.
3. Если шаг 1 отказывает, или если LAP или WLC не делают режима LWAPP уровня поддержки 2, LAP делает попытку обнаружения WLC LWAPP Уровня 3.Посмотрите раздел Алгоритма Обнаружения WLC LWAPP Уровня 3 этого документа.
4. Если шаг 3 отказывает, LAP перезагружает и возвращается к шагу 1.

Примечание: Если вы хотите задать IP-адрес для точки доступа вместо того, чтобы назначить ту автоматически сервером DHCP, можно использовать графический интерфейс контроллера или CLI для настройки статического IP - адреса для точки доступа. См. Настройку Статический IP - адрес на разделе Облегченной точки доступа Руководства по конфигурации WLC для получения дополнительной информации. Если LAP назначают статический IP - адрес и не может достигнуть WLC, он переключается на DHCP.

Алгоритм обнаружения WLC LWAPP уровня 2

Подключение LWAPP между AP и WLC может быть в собственном компоненте, Фреймах Ethernet Уровня 2. Это известно как Режим LWAPP уровня 2. Несмотря на то, что определенный в проекте RFC, Режим LWAPP уровня 2 считают осуждаемым в реализации Cisco. Только режим LWAPP уровня поддержки 2 облегченных точек доступа Cisco 1000 серии. Кроме того, Режим LWAPP уровня 2 не поддерживается на Cisco WLC серии 2000. Эти WLC поддерживают только режим LWAPP Уровня 3.

Это - первый метод, который LAP использует для обнаружения WLC. LAP, что режим LWAPP уровня поддержки 2 передавал сообщение запроса обнаружения LWAPP в кадре LWAPP Уровня 2. Если существует WLC в сети, настроенной для Режима LWAPP уровня 2, контроллер отвечает ответом обнаружения. LAP тогда перемещается в фазу соединения (см. шаг 5 Регистра LAP с разделом WLC).

Эти выходные данные **команды debug lwapp events enable** показывают последовательность событий, которые происходят, когда LAP с помощью Режима LWAPP уровня 2 регистрируется в WLC:

Примечание: Линии этих выходных данных были перемещены во вторые линии из-за пространственных ограничений.

```
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**

Алгоритм обнаружения WLC LWAPP уровня 3

LAP используют алгоритм обнаружения Уровня 3, если метод обнаружения Уровня 2 не поддерживается или если отказывает метод обнаружения Уровня 2. Алгоритм обнаружения Уровня 3 использует различные варианты, чтобы попытаться обнаружить WLC. Алгоритм обнаружения WLC LWAPP Уровня 3 используется для построения списка контроллеров. После того, как список контроллеров создан, AP выбирает WLC и попытки присоединиться к WLC.

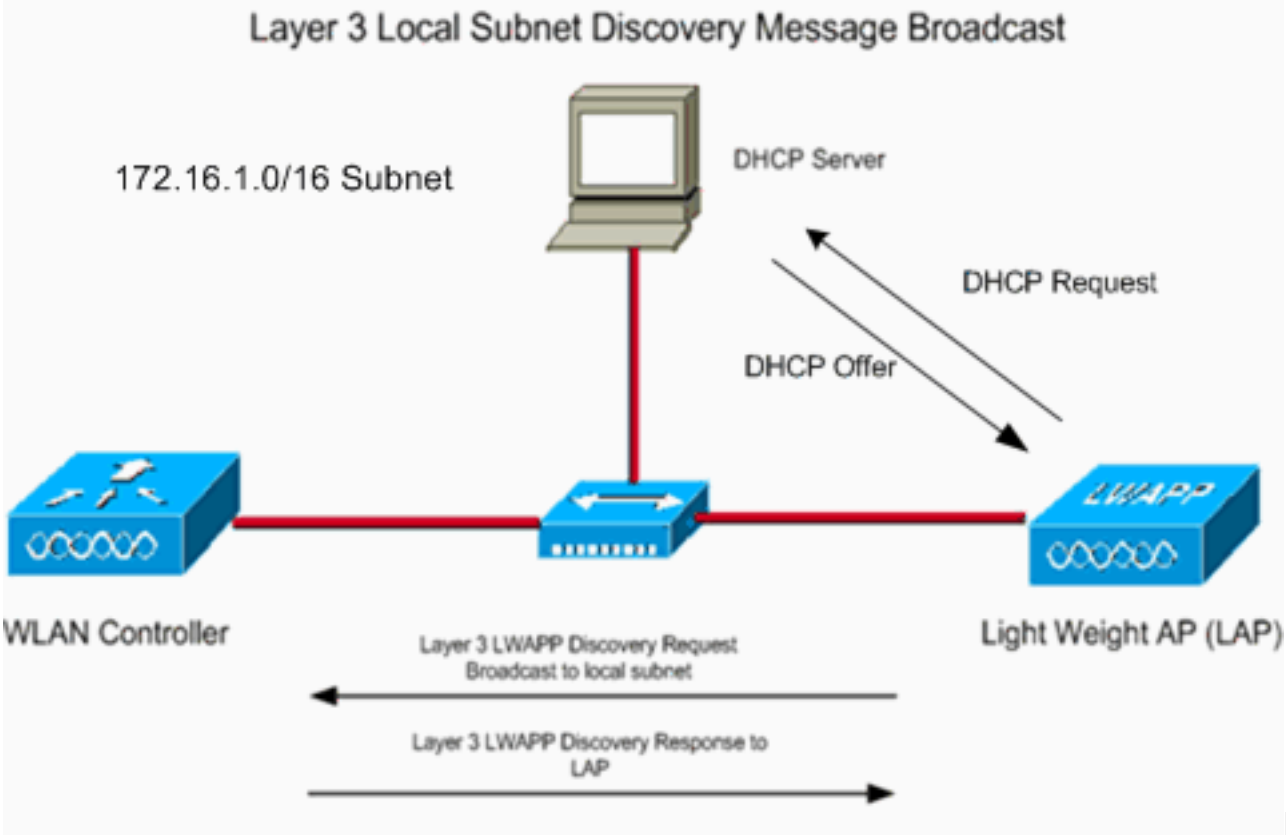
Повторения алгоритма обнаружения WLC Уровня 3 LWAPP по крайней мере до одного WLC находят и присоединяются.

> **Примечание:** Во время обнаружения WLC Уровня 3 LWAPP AP всегда завершает все шаги 1 - 5 в этот раздел для построения списка WLC кандидата. После того, как AP выполнил шаги обнаружения WLC LWAPP, AP выбирает WLC из списка WLC кандидата на основе определенных критериев, и затем передает тому WLC Запрос на присоединение LWAPP.

Каждый пример сценария, который объясняет этот раздел, независим от других и предоставлен только для предоставления понимания того, как работает каждый шаг в процесс обнаружения. LAP использует все шаги обнаружения для обнаружения списка WLC кандидата, прежде чем он выберет WLC для присоединения.

Эта процедура описывает шаги, которые алгоритм обнаружения Уровня 3 проходит в попытке обнаружить WLC:

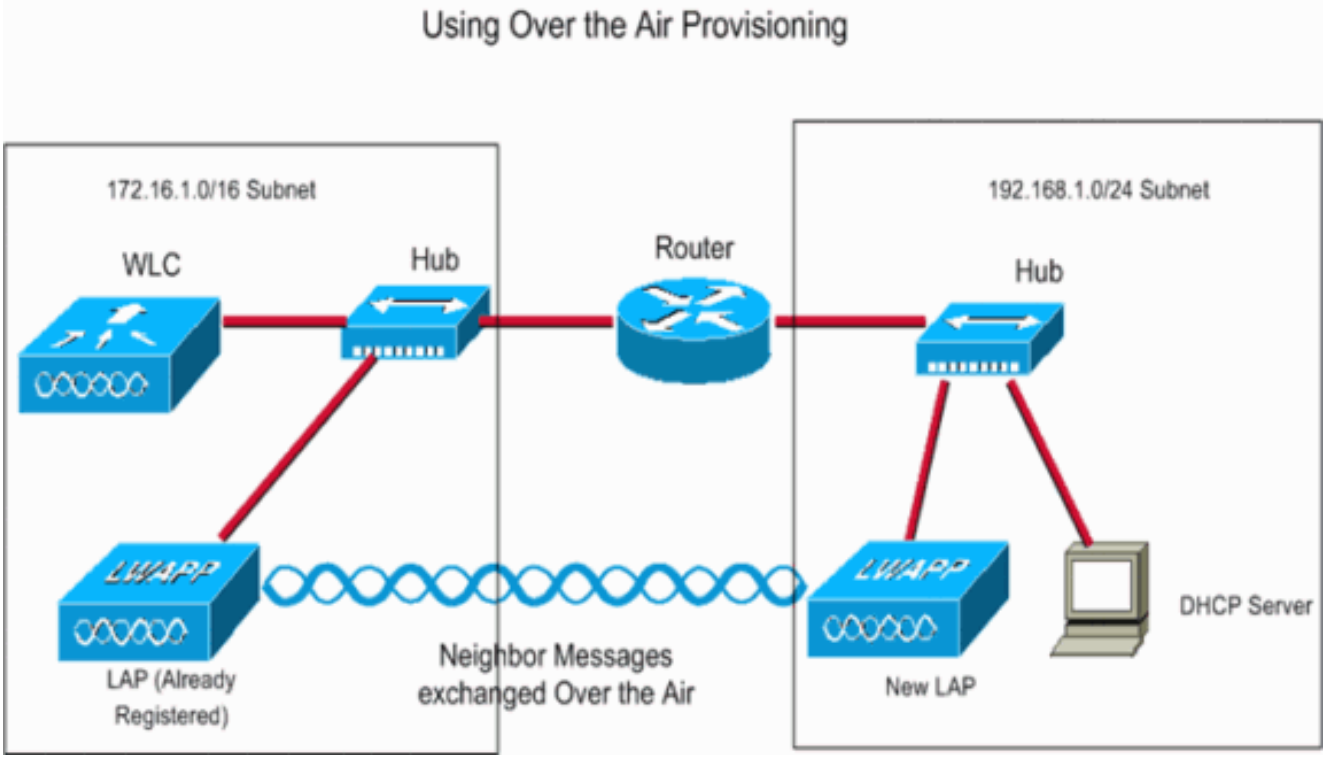
1. После того, как LAP получает IP-адрес от сервера DHCP, LAP начинает этот процесс обнаружения:LAP передает сообщение обнаружения LWAPP Уровня 3 на подсети локального IP. Любой WLC, который настроен для режима LWAPP Уровня 3 и это связано с той же локальной подсетью, получает сообщение обнаружения LWAPP Уровня 3.Каждый из WLC, который получает ответы на сообщение обнаружения LWAPP с сообщением одноадресного ответа обнаружения LWAPP к LAP.



Н
апример. Предположите, что у вас есть WLC и LAP в той же подсети (172.16.1.0/16). У вас также есть подсеть сервера DHCP. Когда LAP включается, он отсылает запрос DHCP с надеждой, что сервер DHCP предоставит IP-адрес. После того, как LAP получает IP-адрес от сервера DHCP, LAP передает сообщение обнаружения LWAPP Уровня 3 на своей локальной подсети. Поскольку WLC находится также в той же подсети, WLC получает запрос обнаружения LWAPP от LAP и отвечает ответом обнаружения LWAPP Уровня 3. Выходные данные данного примера **команды debug lwapp events enable** показывают этот процесс обнаружения:`(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`** Выходные данные **команды debug lwapp packet enable** для широковещательного обнаружения локальной подсети похожи на данный пример:`(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`** Заметьте линии, которые отмечены в полужирном шрифте. **`IE 58 :0 - broadcast 1 - configured 2 - OTAP 3 - dhcp server 4 - dns .. , IE 58 0 debug lwapp packet enable.`**

2. LAP также используют функцию По беспроводной связи инициализации (OTAP) для обнаружения WLC. Опция OTAP *отключена по умолчанию* в 4.2.39.13, 5.0.68.0 и более поздние версии WLC. OTAP *включен по умолчанию* в версиях WLC ранее, чем 4.2.39.13.. Когда OTAP включен, это - процесс обнаружения:LAP, которые уже зарегистрированы к WLC, могут объявить IP-адрес WLC к LAP (в попытке найти WLC) с использованием соседних сообщений, которые передаются по воздуху.Новые LAP, которые пытаются обнаружить WLC, слышат эти сообщения и затем одноадресно передают сообщения запроса обнаружения LWAPP к WLC.WLC, которые получают ответ на сообщение обнаружения LWAPP с сообщением одноадресного ответа

обнаружения LWAPP к LAP.У вас должен быть OTAP, включенный только во время интервалов инициализации AP. После того, как AP развернуты, отключают OTAP как оптимальный метод развертываний. Кроме того, LAP Cisco Aironet (AG 1130, 1200, и серии 1240) отправляют от фабрики с упрощенной версией легковесного программного обеспечения Cisco IOS, которое называют Образом Cisco IOS Восстановления LWAPP. OTAP не поддерживается на тех AP out-of-the-box то программное обеспечение Cisco IOS LWAPP выполнения. При обновлении AP Cisco Aironet от автономного программного обеспечения Cisco IOS до облегченного режима Образ Cisco IOS Восстановления LWAPP является программным обеспечением, которое загружено. Образ Cisco IOS Восстановления LWAPP не поддерживает OTAP. Для поддержки OTAP LAP Aironet должны сначала присоединиться к WLC для загрузки полного Образа Cisco IOS
LWAPP.



Например. Предположите, что, в подсети 172.16.1.0/16, у вас есть LAP, который уже зарегистрирован в WLC, и OTAP включен на WLC. Когда новый LAP в 192.168.1.0/24 подсети подходит, LAP ищет сервер DHCP и получает IP-адрес (если никакое присвоение не было сделано ранее со статическим IP - адресом). LAP тогда отсылает запрос на обнаружение в локальную подсеть. Поскольку в этом сценарии нет никакого WLC в локальной подсети, LAP пытается использовать OTAP для обнаружения WLC. LAP слушает соседние сообщения, которые передаются по воздуху LAP (в 172.16.1.0/16 подсети), которые уже зарегистрированы, и ищет IP-адреса WLC. Из списка IP-адресов WLC, которые новые LAP изучают из соседних сообщений, новые LAP отсылают запрос обнаружения LWAPP Уровня 3 в WLC. WLC, которые получают этот запрос на обнаружение, отвечают ответом обнаружения LWAPP Уровня 3. Эти выходные данные **команды debug lwapp event enable** иллюстрируют последовательность сообщений, что WLC передают:`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`** **Примечание:** Поскольку LAP знает IP-адрес WLC через соседние сообщения, LAP передает запрос на обнаружение индивидуальной рассылки

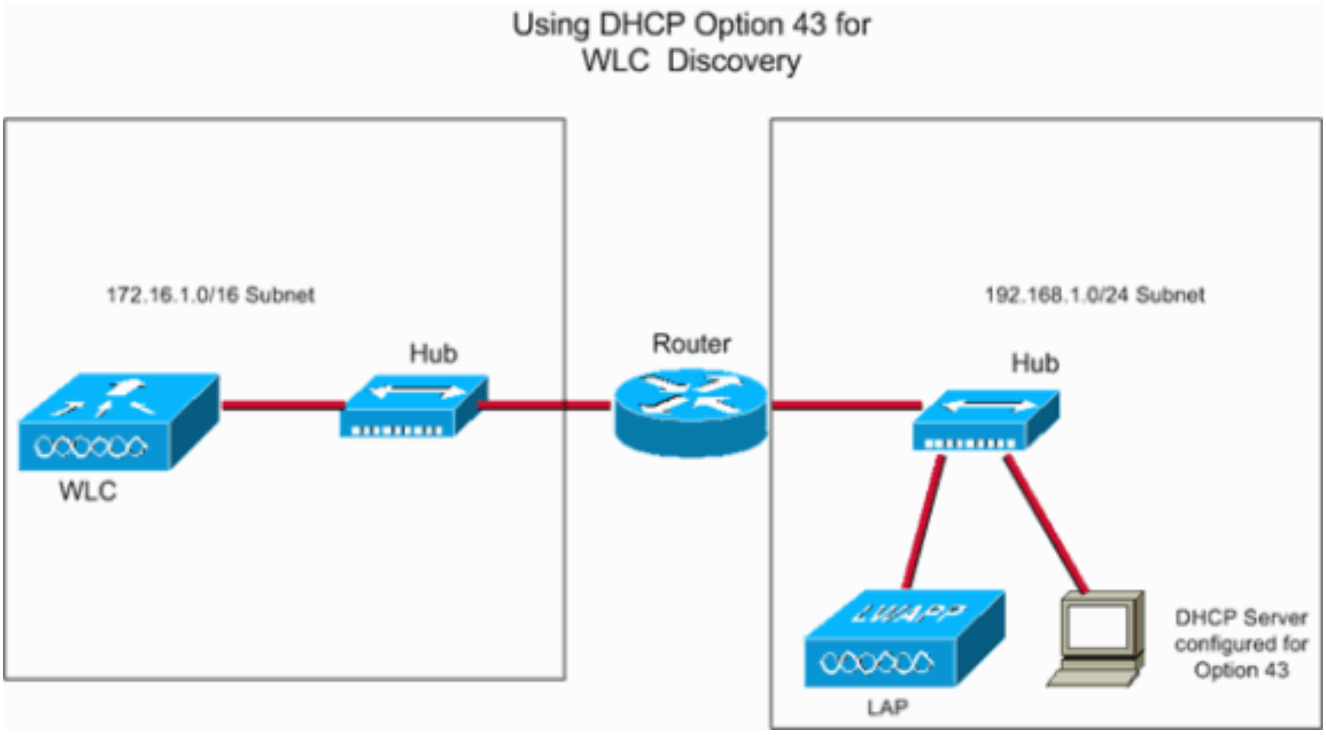
к WLC. Таким образом этот шаг непохож на метод в шаге 1 этой процедуры, в которой LAP отсылает широковещание локальной подсети.**Примечание:** Значение параметра IE 58 в выходных данных команды debug lwapp packet enable показывает, что "облегченная" точка доступа использует функцию OTAP в качестве способа обнаружения.

```
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. Если LAP был зарегистрирован к WLC в предыдущих развертываниях, LAP ведет список IP-адресов WLC локально в NVRAM. Сохраненные IP-адреса WLC включают все WLC, которые находятся в WLC, к которому ранее присоединяются, "группы мобильности". Это - процесс обнаружения:LAP отправляют запрос обнаружения LWAPP Уровня 3 индивидуальной рассылки к каждому из IP-адресов WLC, которые LAP имеет в его NVRAM.WLC, которые получают ответ на сообщение обнаружения LWAPP с сообщением одноадресного ответа обнаружения LWAPP к LAP.Вот пример выходных данных **команды debug lwapp events enable** и **команды debug lwapp packet enable** для этого метода обнаружения WLC: **Примечание:** При использовании **clear ap-config** *ap_name* команда для сброса LAP к заводским настройкам, все конфигурации LAP перезагружены. Конфигурации, которые перезагружены, включают IP-адреса WLC, которые сохранены в NVRAM. В этом случае LAP должен использовать некоторый другой метод для обнаружения 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:
```

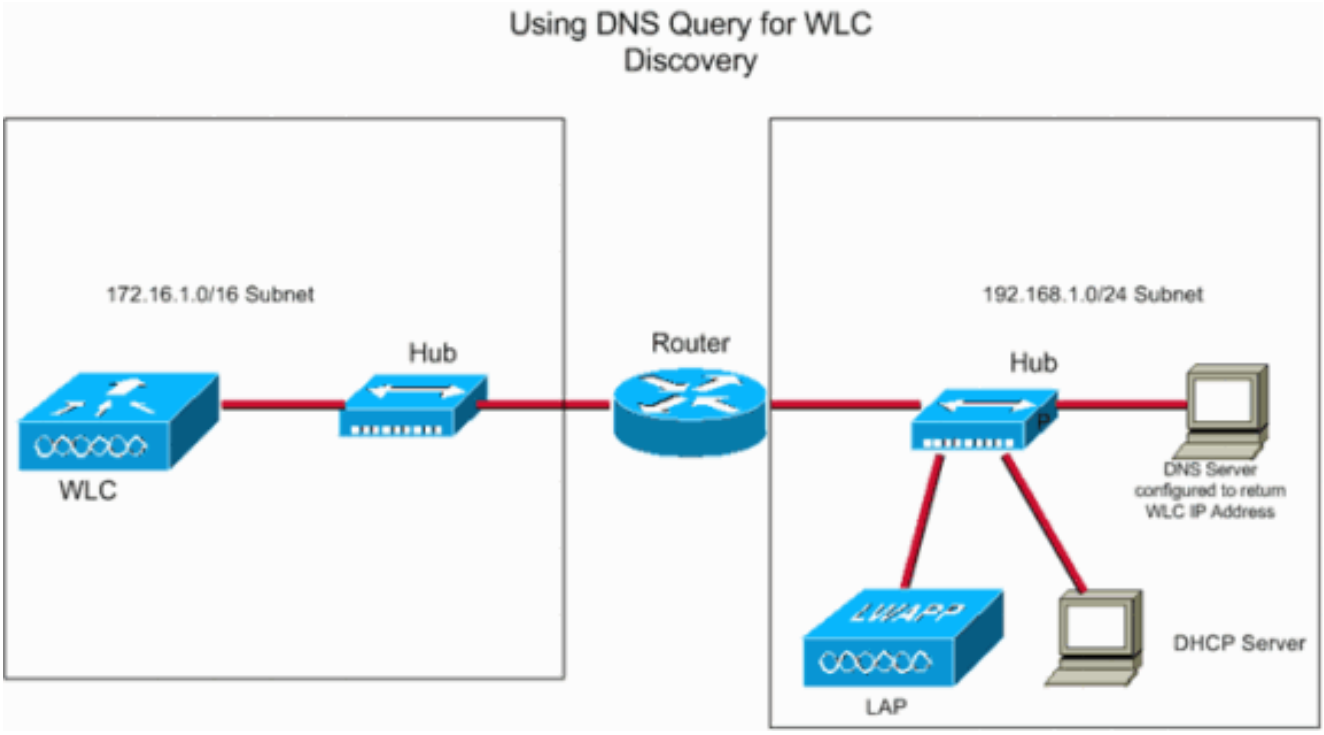
4. Можно также программировать серверы DHCP для возврата IP-адресов WLC в определяемой поставщиком "опции 43" в предложении DHCP к LAP. Это - процесс обнаружения:Когда LAP получает IP-адрес от сервера DHCP, LAP ищет IP-адреса WLC в поле опции 43 предложения DHCP.LAP отправляет запрос обнаружения LWAPP Уровня 3 к каждому из WLC, которые перечислены в параметре DHCP 43.WLC, которые получают ответ на сообщение обнаружения LWAPP с сообщением одноадресного ответа обнаружения LWAPP к LAP.**Примечание:** Когда LAP и WLC находятся в других подсетях, можно использовать параметр DHCP 43.



Вот пример сценария. Предположите, что у вас есть WLC в одной подсети (как пример, 172.16.1.0/16) и LAP и сервер DHCP в другой подсети (например, 192.168.1.0/24). Маршрутизация включена между этими двумя подсетями. Можно настроить сервер DHCP для возврата IP-адресов WLC к LAP в сообщении предложения DHCP. Можно использовать любой сервер DHCP, который поддерживает опцию 43.**Примечание:** См. ПАРАМЕТР DHCP 43 для Легковесного Примера конфигурации точек доступа Cisco Aironet для получения информации о том, как настроить Сервер DHCP Windows 2000 для опции 43.Так, когда LAP включается, он ищет сервер DHCP для получения IP-адреса. Сервер DHCP выделяет IP-адрес LAP и также предоставляет списку IP-адресов WLC с использованием параметра DHCP 43. LAP отсылает запрос на обнаружение индивидуальной рассылки в каждый из WLC. WLC, которые слышат эти сообщения ответ с ответом обнаружения, который инициирует процесс регистрации. Эти выходные данные **команды debug lwapp events enable** показывают последовательность сообщений 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** Вот выходные данные **команды debug lwapp packet enable**, которые указывают, что параметр DHCP 43 использовался в качестве метода обнаружения для обнаружения IP-адресов WLC: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. Наконец, можно также использовать сервер DNS для возврата IP-адресов WLC к LAP. Это - процесс обнаружения:LAP пытается решить имя DNS "CISCO-CAPWAP-CONTROLLER.local-domain" или "CISCO-LWAPP-CONTROLLER.local-domain". **Примечание:** В этом синтаксисе имени DNS localdomain обращается к доменному имени, которое должно быть решено. Например, если домен является

cisco.com, то это имя DNS является CISCO-LWAPP-CONTROLLER.cisco.com. AP нужно сообщить о доменном имени, которое должно быть решено так, чтобы AP мог отправить запрос к серверу DNS, который выполнил запрос для решения этого названия отдельного домена. AP сообщают об этом доменном имени через параметр DHCP 15. Параметр DHCP 15 задает доменное имя, которое AP должен использовать для Разрешения DNS. Поэтому необходимо что параметр DHCP 15 быть настроенным с данными имен домена. Это позволяет сервер DHCP, который передает IP-адрес сервера DNS, чтобы также передать этому параметру DHCP 15 информации (доменное имя, которое будет решено) к AP.Когда LAP в состоянии решить это название к одному или более IP-адресам WLC, LAP отправляет запрос обнаружения LWAPP Уровня 3 индивидуальной рассылки к каждому из WLC.WLC, которые получают ответ на сообщение обнаружения LWAPP с сообщением одноадресного ответа обнаружения LWAPP к AP.Данный пример использует ту же настройку, которая использовалась для параметра DHCP 43 (шаг 3). Однако в данном примере, сервер DHCP не использует опцию 43. Вместо этого сервер DHCP предоставляет LAP IP-адрес и также дает IP-адрес сервера DNS в предложении DHCP. После того, как LAP получает IP-адрес сервера DNS, LAP отсылает запрос DNS для имени DNS "CISCO-CAPWAP-CONTROLLER.local-domain" или "CISCO-LWAPP-CONTROLLER.local-domain". Сервер DNS должен быть настроен таким образом, что он возвращает IP-адрес WLC для этого запроса. Когда LAP получает IP-адрес WLC, LAP запускает процесс регистрации с
WLC.



Эти выходные данные **команды debug lwapp packet enable** показывают тип обнаружения как 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: **Примечание:** Если после завершения шагов 1 - 5 LAP не получает ответ обнаружения LWAPP, LAP перезагружает и перезапускает алгоритм поиска.

6. **Используйте вспомогательный IP - адрес на маршрутизаторе**Несмотря на то, что это не часть алгоритма обнаружения Уровня 3, это - более простой метод, который может использоваться, когда WLC и LAP находятся в других подсетях. После того, как LAP получает IP-адрес от сервера DHCP, LAP передает сообщение обнаружения LWAPP Уровня 3 на своей локальной подсети. IP-адрес WLC настроен как адрес *IP-помощника* на маршрутизаторе. Маршрутизатор вперед эти широковещательные сообщения к IP-адресам настроили с *командой ip-helper* на *интерфейсе*, на котором слышат широковещание. При использовании *команды ip helper-address*, АДРЕСНЫХ ТРАНСЛЯЦИЙ, а также индивидуальных рассылок, восемь других портов UDP переданы автоматически. Те порты являются Передачей Простейшего файла (TFTP) (порт 69), Система доменных имен (порт 53), Сервис времени (порт 37), Сервер имен NETBIOS (порт 137), Сервер Датаграммы NetBIOS (порт 138), Протокол загрузки (BOOTP) Клиент и сервер (порт 67 и порт 68), сервис TACACS (порт 49). Начиная с широковещательного *порта 12223* UDP использования LWAPP это должно быть явно переданный на маршрутизаторе. Вот пример сценария. Предположите, что у вас есть WLC в одной подсети, такой как 172.16.0.0/16, и LAP и сервер DHCP в другой подсети, такие как 192.168.1.0/24. Маршрутизация включена между этими двумя подсетями. Данный пример показывает конфигурацию на маршрутизаторе:`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` **Примечание:** При выполнении версии 5.2 WLC или позже используйте Номер порта UDP 5246, потому что CAPWAP передавал порт 5246 UDP использования.`Router(config)ip forward-protocol udp 5246`

Процесс выбора WLC

После того, как LAP завершает шаги 1 - 5 Алгоритма Обнаружения WLC LWAPP Уровня 3, LAP выбирает WLC из списка WLC кандидата и передает тому WLC Запрос на присоединение LWAPP.

WLC встраивают эту важную информацию в ответ обнаружения LWAPP:

- Контроллер sysName
- Тип контроллера
- Емкость AP контроллера и ее текущая загрузка AP
- Флаг Master Controller
- IP-адрес AP - диспетчера

LAP использует эту информацию, чтобы сделать выбор контроллера с использованием этих правил приоритетов:

1. Если LAP был ранее настроен с основным, вторичным, и/или третичный контроллер, LAP исследует контроллер sysName поле (от ответов обнаружения LWAPP) в попытке найти WLC, который настроен как "основной" . Если LAP находит соответствие sysName для главного контроллера, LAP передает Запрос на присоединение LWAPP к тому WLC. Если LAP не может найти свой главный контроллер или если соединение LWAPP отказывает, LAP пытается совпасть со вспомогательным контроллером sysName к ответам обнаружения LWAPP. Если LAP находит соответствие, он тогда

передает LWAPP, соединяют со вспомогательным контроллером. Если вторичный WLC не может быть найден или сбои соединения LWAPP, LAP повторяет процесс для своего третичного контроллера.

2. Если один из этих элементов истинен, LAP посмотрел на поле флага Главного контроллера в ответах обнаружения LWAPP от WLC кандидата:Никакой основной, вторичный, и/или третичные контроллеры, не был настроен для AP.Эти контроллеры не могут быть найдены в списке кандидатов.LWAPP соединяет с теми контроллерами, отказали.Если WLC настроен как Главный контроллер, LAP выбирает тот WLC и передает ему Запрос на присоединение LWAPP.
3. Если LAP не может успешно присоединиться к WLC на основе критериев в шаге 1 и шаге 2, LAP пытается присоединиться к WLC, который имеет самую большую избыточную мощность.

После того, как LAP выбирает WLC, LAP передает Запрос на присоединение LWAPP к WLC. В Запросе на присоединение LWAPP LAP встраивает снабженный цифровой подписью сертификат X.509. Когда сертификат проверен, WLC передает ответ соединения LWAPP, чтобы указать к LAP, что это успешно соединено с контроллером. WLC встраивает свой собственный снабженный цифровой подписью сертификат X.509 в ответ соединения LWAPP, который должен проверить LAP. После того, как LAP проверяет сертификат WLC, процесс соединения LWAPP завершен.

LAP и Контроллер беспроводной локальной сети обрабатывают фрагментацию и повторную сборку для туннеля LWAPP. Они работают под 1500-байтовым предположением MTU. Это не параметр с изменяемой конфигурацией. В AP или WLC, если MTU больше, чем 1500 байтов, он фрагментирует пакет и передает пакет через. Система обрабатывает до четырех фрагментов с Версии 3.2. Более ранние версии поддерживают только до двух фрагментов.

Вот ссылка на видео на Сообществе Cisco Support, которое объясняет процесс регистрации LAP:

Регистрация облегченной точки доступа с контроллерами беспроводной локальной сети (WLC)

Устранение неполадок

Контроллер имеет версию микропрограммы 3.2.78.0. При выполнении **команды debug lwapp events** эти выходные данные появляются:

```
Sun Sep 3 21:49:51 2006 [ERROR] spam_lrad.c 2544:
 Security processing of Image Data failed from AP 00:17:59:67:76:80
```

Это сообщение об ошибках означает, что образ 3.2.78.0 не поддерживает LAP. По существу контроллер не может найти образ для LAP в его списке образов. Поэтому LAP не в состоянии загрузить образ от WLC. Для решения этого вопроса обновите контроллер к 3.2.116.0 или позже. Это решает проблему, и LAP присоединяется к контроллеру и загружает образ от контроллера.

Иногда, можно встретиться с этим сообщением об ошибках в контроллере:

```
Received a Discovery Request with subnet broadcast with wrong AP IP address (source address).
```

Это сообщение об ошибках означает, что контроллер получил запрос на обнаружение через адрес широковещательного IP, которому (дали) IP - адрес источника, который не находится ни в каких настроенных подсетях на контроллере. Это также означает, что контроллер отбросил пакет. Это, как правило, происходит, когда клиент соединяет весь позволенный vlans магистралью вместо ограниченного их к беспроводным сетям VLAN.

Можно также встретиться с этим сообщением об ошибках:

```
Received a Discovery-Request from <source MAC address>
 for someone else (IP address).
```

Это означает, что контроллер получил запрос на обнаружение, где (данный) IP - адрес назначения не является своим управлением IP-адресами. Это также означает, что контроллер отбросил пакет.

Существует много причин, Облегченная точка доступа (LAP) может быть не в состоянии присоединяться к WLC. См. Устранение неполадок Облегченная точка доступа, Не Присоединяющаяся к Контроллеру беспроводной локальной сети для получения информации о некоторых причинах, LAP не в состоянии присоединяться к WLC и как решить проблемы.

AP переключается между другими группами мобильности

Рассмотрим следующий сценарий. Группа мобильности **MG1** содержит два контроллера, C1 и C2. Эти контроллеры развернуты в одном здании с LAP, распределенными нагрузку между двумя. Филиал компании компании развертывает третий контроллер C3 и настраивает его для группы мобильности **MG2**. LAP от того контроллера (C3) не переключаются при отказе к одному из других двух контроллеров, но однажды, когда Контроллер перезагрузки C3, LAP, которые были первоначально зарегистрированы в C3 теперь, регистрирует к C1 в группе мобильности **MG1**.

Теперь, даже при том, что основной LAP является C3, и нет никакого вторичного устройства или третичное, LAP присоединились к C1; перезагрузка LAP не возвращает его C3. В чем проблема?

Причина позади этого состоит в том, что в рамках первоначального развертывания, компания создала один из двух сценариев:

- Запись DNS для "CISCO-CAPWAP-CONTROLLER.local-domain" или "CISCO-LWAPP-CONTROLLER.local-domain" для обращения к C1 или C2.
- Добавление параметра DHCP 43 для обращения к C1 или C2 для упрощения начальной установки. Как только установка первого здания была сделана, эти записи никогда не удалялись.

Примечание: AP может также учиться о C1 или контроллерах C2 любым другим методом обнаружения, таких как широковещание L3 и OTAP, поэтому удостоверьтесь, что надлежащие меры предосторожности приняты, что AP может только учиться о контроллерах от одной группы мобильности до любого из методов.

Когда контроллер, C3 выключается, LAP, которые были связаны с ним перезагрузка. Они подвергаются своему процессу обнаружения, как выделено. Они не только передают запросы на обнаружение к тем контроллерам в конфигурации NVRAM (энергонезависимой памяти), но также и к IP-адресам, изученным через DNS и DHCP, который, в результате включайте C1 или C2.

Так как C3 не работает во время обнаружения, LAP не получают ОТВЕТ ОБНАРУЖЕНИЯ, таким образом, они не могут продолжить присоединяться к его настроенному главному контроллеру и должны присоединиться к контроллеру, они учились через DHCP или DNS.

Как только эти LAP присоединяются к C1 или C2, они загружают новый список группы мобильности, который включает IP-адреса для только C1 и C2, таким образом, если они перезагружены, у них нет способа изучить IP-адрес C3, к которому можно передать запросы на обнаружение; они не могут присоединиться к тому контроллеру. Единственный способ возвратить LAP C3 состоит в том, чтобы добавить C3 к списку группы мобильности C1 и C2 или изменить опцию 43 или Запись DNS.

Существует несколько способов предотвратить такие проблемы:

- Предложено, чтобы DNS и параметры DHCP использовались только в рамках первоначального развертывания и были удалены, как только настроена сеть. Таким образом, AP в сети не имеют никакого способа учиться о других группах мобильности.
- Разделите области DHCP или Домены DNS. Имейте одну область для построения 1 и другую область для построения 2 в корпоративном сервере DHCP; администратор может настроить другие IP-адреса Опции 43 для каждой области. То же самое касается Доменов DNS; с building1. company Name (Название компании). имя хоста com для одного здания и building2. company Name (Название компании). com для другого, у вас могут быть различные варианты для КОНТРОЛЛЕРА LWAPP CISCO для каждого субдомена.
- Можно также использовать функции в WLC для управления некоторыми способами поведения:В случае AP с Подписанными сертификатами (SSC) только добавьте SSCs к контроллерам, к которым вы хотите, чтобы AP присоединились.В случае AP с Установленными изготовителями сертификатами (MIC) используйте **Авторизовать AP против функции AAA** на WLC (с **командой config auth-list ap-policy authorize-ap enable**), чтобы сказать контроллеру проверять, должно ли это принять AP.Чтобы позволить AP присоединяться, используйте одну из этих опций:Добавьте их к списку авторизации WLC: используйте **команду config auth-list add mic <MAC-Address>**.Добавьте их как клиентов к серверу RADIUS. Вызванный Station-ID является MAC-адресом контроллера. Если вы разделяете AP на группы, можно создать политику для определения, какие AP могут аутентифицироваться против который Вызванные Station-ID.

Чтобы заставить LAP присоединяться к контроллеру, который не является частью группы мобильности контроллера, к которому в настоящее время присоединяются, необходимо удостовериться, что название главного контроллера является названием контроллера, к которому вы хотите передать LAP.

Как только это сделано, все, что необходимо сделать, дают LAP способ обнаружить тот контроллер. Это может быть сделано через любой из методов, описанных в алгоритме обнаружения WLC, как объяснено в этом документе.

Дополнительные сведения

- Управление облегченными точками доступа
- Пример базовой конфигурации контроллера беспроводной локальной сети и "облегченной" точки доступа
- LWAPP (облегченный режим) к автономному преобразованию и наоборот
- Исследование трафика LWAPP
- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 6.0
- Cisco Systems – техническая поддержка и документация