Пример конфигурации режимов работы H-REAP

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Общие сведения
H-REAP по REAP
Настройка
Схема сети
!--- конфигурацию
Воспламенение AP с контроллером и настраивает H-REAP
Принцип работы H-REAP
H-REAP, коммутирующий Состояния
Централизованная аутентификация, центральная коммутация
Проверьте централизованную аутентификацию, центральную коммутацию
Выключенная аутентификация, переключаясь Выключенный
Централизованная аутентификация, локальный коммутатор
Проверьте централизованную аутентификацию, локальный коммутатор
Выключенная аутентификация, локальный коммутатор
Локальная проверка подлинности, локальный коммутатор
Проверьте локальную проверку подлинности, локальный коммутатор
Устранение неполадок
Дополнительные сведения

Введение

В этом документе определяется понятие гибридной удаленной граничной точки доступа (H-REAP) и поясняются различные режимы ее работы с примером конфигурации.

Предварительные условия

Требования

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

- Знание Контроллеров беспроводной локальной сети (WLC) и как настроить основные параметры WLC
- Знание REAP

Используемые компоненты

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

- Cisco WLC серии 4400, который выполняет релиз микропрограммы 7.0.116.0
- Облегченная точка доступа (LAP) Cisco 1131AG
- Маршрутизаторы Cisco серии 2800, которые выполняют версию 12.4 (11) T.
- Cisco Aironet 802.11a/b/g Клиентский адаптер, который выполняет микропрограмму версии 4.0
- Версия 4.0 утилиты Cisco Aironet Desktop Utility
- Cisco Secure ACS, который выполняет версию 4.0

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

H-REAP является беспроводным решением для филиала компании и удаленных офисных развертываний. H-REAP позволяет клиентам настроить и управлять точками доступа (AP) в ответвлении или удаленном офисе от офиса корпорации до канала WAN, не развертывая контроллер в каждом офисе.

Когда соединение с контроллером потеряно, H-REAPs может коммутировать трафик данных клиента локально и выполнить аутентификацию клиента локально. При наличии подключения к контроллеру точки доступа H-REAP могут выполнять обратное туннелирование трафика к контроллеру. В связанном режиме гибридный AP REAP может также выполнить локальную проверку подлинности.

H-REAP поддерживается только на:

- 1130AG, 1140, 1240, 1250, 1260, AP801, AP 802, 1040, и AP AP3550
- Cisco 5500, 4400, 2100, 2500 и Flex контроллеры серии 7500
- Catalyst 3750G интегрированный коммутатор контроллера
- Модуль беспроводных сервисов серии Catalyst 6500 (WiSM)
- Модуль контроллера беспроводной локальной сети (WLCM) для маршрутизаторов ISR (ISR)

Трафик клиента на H-REAPs может или быть коммутирован локально в AP или туннелировал назад к контроллеру. Это зависит от НА КОНФИГУРАЦИЮ WLAN. Кроме того,

локально коммутированный трафик клиента на H-REAP может быть 802.1Q, помеченным для обеспечения разделения проводной стороны. Во время бездействия глобальной сети (WAN) сохраняется сервис на всех локально коммутируемых, локально аутентифицируемых WLAN.

Примечание: Если AP находятся в режиме H-REAP и локально коммутированы на удаленном узле, динамическое назначение пользователей к определенной VLAN на основе Конфигурации сервера RADIUS не поддерживается. Однако должна существовать возможность назначать пользователей на определенные VLAN на основе статической VLAN к идентификатору набора сервисов (SSID) сопоставление, сделанное локально в AP. Поэтому пользователя, который принадлежит определенному SSID, можно назначить на определенную VLAN, с которой SSID сопоставлен локально в AP.

Примечание: Если голос по WLAN важен, то AP должны быть выполнены в автономном режиме так, чтобы они получили CCKM и поддержку Контроля за установлением соединений (CAC), которые не поддерживаются в режиме H-REAP.

H-REAP по REAP

См. AP Удаленного Края (REAP) с Легковесными AP и Контроллерами беспроводной локальной сети (WLC) Пример конфигурации для получения дополнительной информации, чтобы помочь понимать REAP.

H-REAP был представлен в результате этих недостатков REAP:

- REAP не имеет разделения проводной стороны. Это происходит из-за отсутствия поддержки 802.1Q. Данные от WLAN приземляются на ту же проводную подсеть.
- Во время Сбоя WAN AP REAP прекращает услугу, предложенную на всех WLAN, кроме первого, заданного в контроллере.

Это - то, как H-REAP преодолевает эти два недостатка:

- Оказывает поддержку dot1Q и VLAN к сопоставлению SSID. Эта VLAN к сопоставлению SSID должна быть сделана в H-REAP. В то время как вы выполняете это, гарантируете, что настроенные VLAN должным образом позволены через порты в промежуточных коммутаторах и маршрутизаторах.
- Предоставляет непрерывный сервис всем WLAN, настроенным для локального коммутатора.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Схема сети

В настоящем документе используется следующая схема сети:

!--- конфигурацию

Данный пример предполагает, что контроллер уже настроен с базовыми конфигурациями.

Контроллер использует эти конфигурации:

- IP-адрес интерфейса управления — 172.16.1.10/16
- IP-адрес интерфейса менеджера точки доступа — 172.16.1.11/16
- IP-адрес Маршрутизатора основного шлюза — 172.16.1.25/16
- Действительный IP-адрес шлюза — 1.1.1.1

Примечание: Этот документ не показывает конфигурации глобальной сети (WAN) и конфигурацию маршрутизаторов и коммутаторов, доступных между H-REAP и контроллером. Это предполагает, что вы знаете об инкапсуляции WAN и протоколах маршрутизации, которые используются. Кроме того, этот документ предполагает, что вы понимаете, как настроить их для поддержания подключения между H-REAP и контроллером через канал WAN. В данном примере инкапсуляция HDLC используется на канале WAN.

Воспламенение AP с контроллером и настраивает H-REAP

Если вы хотите, чтобы AP обнаружил контроллер от удаленной сети, где механизмы обнаружения CAPWAP не доступны, можно использовать воспламенение. Этот метод позволяет вам задать контроллер, с которым должен соединиться AP.

Чтобы к началу AP H-REAP-capable, подключите AP с проводной сетью в главном офисе. Во время его начальной загрузки, AP H-REAP-capable сначала ищет IP-адрес для себя. Как только это получает IP-адрес через сервер DHCP, это загружается и ищет контроллер для выполнения процесса регистрации.

AP H-REAP может изучить IP-адрес контроллера любым из способов, объясненных в регистрации облегченных точек доступа Контроллеру беспроводной локальной сети (WLC).

Примечание: Можно также настроить LAP для обнаружения контроллера через команды CLI в AP. См. Обнаружение Контроллера H-REAP с помощью команд CLI для получения дополнительной информации.

Пример в этом документе использует параметр DHCP 43 процедуры для H-REAP для обучения IP-адреса контроллера. Затем это присоединяется к контроллеру, загружает программный образ и конфигурацию от контроллера, и инициализирует радио соединение. Это сохраняет загруженную конфигурацию в долговременной памяти для использования в автономном режиме.

Как только LAP зарегистрирован в контроллере, выполните эти шаги:

1. В Графическом интерфейсе контроллера выберите **Wireless> Access Points**.Это отображает LAP, зарегистрированный в этом контроллере.
2. Щелкните по AP, который вы хотите настроить.
3. В окне AP> Details щелкните по вкладке High Availability и определите названия контроллера, которые AP будут использовать для регистра, затем нажать **Apply**.Можно определить до трех названий контроллера (основной, вторичный, и третичный). AP ищут контроллер в том же заказе, который вы предоставляете в этом окне. Поскольку данный пример использует только один контроллер, пример определяет контроллер как главный контроллер.
4. Настройте LAP для H-REAP.Для настройки LAP, чтобы работать в режиме H-REAP, в окне AP> Details, под Вкладкой Общие, выбрать **Режим AP** в качестве H-REAP из

соответствующего выпадающего меню.Это настраивает LAP для работы в режиме H-REAP.**Примечание:** В данном примере вы видите, что IP-адрес AP изменен на статический режим, и статический IP - адрес 172.18.1.10 был назначен. Это присвоение происходит, потому что это - подсеть, которая будет использоваться в удаленном офисе. Поэтому вы используете IP-адрес от сервера DHCP, но только во время первоначально через регистрационный этап. После того, как AP зарегистрирован к контроллеру, вы изменяете адрес на статический IP - адрес.

Теперь, когда ваш LAP запущен с контроллером и настроенный для режима H-REAP, следующий шаг должен настроить H-REAP в стороне контроллера и обсудить H-REAP, коммутирующего состояния.

Принцип работы H-REAP

LAP H-REAP-capable работает в этих двух других режимах:

- **Связанный** режим:Когда его ссылка уровня управления CAPWAP на WLC подключена и в рабочем состоянии, H-REAP, как говорят, находится в связанном режиме. Это означает, что канал WAN между LAP и WLC не не работает.
- **Автономный режим**:Когда его канал WAN к WLC не работает, H-REAP, как говорят, находится в автономном режиме. Например, когда у этого H-REAP больше нет подключения к WLC, связанному через канал WAN.

Механизм аутентификации, используемый для аутентификации клиента, может быть определен как **Центральный** или **Локальный**.

- **Централизованная аутентификация** — Обращается к типу проверки подлинности, который включает процесс WLC от удаленного узла.
- **Локальная проверка подлинности** — Обращается к типам проверки подлинности, которые не включают обработки от WLC для аутентификации.

Примечание: Вся аутентификация 802.11 и обработка ассоциации происходят в H-REAP, независимо от того в каком режиме LAP находится. В то время как в связанном режиме, H-REAP тогда проксирует эти ассоциации и аутентификации к WLC. В автономном режиме LAP не может сообщить WLC таких событий.

Когда клиент соединяется с AP H-REAP, AP вперед все сообщения аутентификации к контроллеру. После успешной аутентификации ее пакеты данных тогда или коммутированы локально или туннелировали назад к контроллеру. Это находится в соответствии с конфигурацией WLAN, с которым это связано.

С H-REAP WLAN, настроенными на контроллере, можно управлять в двух других режимах:

- **Центральная коммутация:**Если трафик данных того WLAN настроен, чтобы быть туннелированным к WLC, WLAN на H-REAP, как говорят, работает в центральном режиме коммутации.
- **Локальная коммутация:**Если трафик данных того WLAN завершается локально в проводном интерфейсе самого LAP, не будучи туннелированным к WLC, WLAN на H-REAP, как говорят, работает в режиме локального коммутатора.**Примечание:** Только WLAN 1 - 8 могут быть настроены для Локального коммутатора H-REAP, потому что только эти WLAN могут быть применены к 1130, 1240 и AP серии 1250 та функциональность H-REAP поддержки.

H-REAP, коммутирующий Состояния

Объединенный с аутентификацией и режимами коммутации, упомянутыми в предыдущем разделе, H-REAP может действовать в любом из этих состояний:

- Централизованная аутентификация, центральная коммутация
- Выключенная аутентификация, переключаясь Выключенный
- Централизованная аутентификация, локальный коммутатор
- Выключенная аутентификация, локальный коммутатор
- Локальная проверка подлинности, локальный коммутатор

Централизованная аутентификация, центральная коммутация

В этом состоянии, для данного WLAN, AP передает все запросы аутентификации клиента к контроллеру и туннелирует все данные клиента к WLC. Это состояние допустимо только, когда H-REAP находится в связанном режиме. Любой WLAN, который настроен для работы в этом режиме, потерян во время бездействия глобальной сети (WAN), независимо от того каков метод аутентификации.

Данный пример использует эти параметры конфигурации:

- Название WLAN/SSID: **Центральный**
- Безопасность уровня 2: **WPA2**
- Локальный коммутатор H-REAP: **отключенный**

Выполните эти шаги для настройки WLC для централизованной аутентификации, центральной коммутации с помощью GUI:

1. Нажмите **WLAN** для создания нового WLAN под названием **Центральный**, затем нажмите **Apply**.
2. Поскольку этот WLAN использует централизованную аутентификацию, мы используем аутентификацию WPA2 в поле безопасности уровня 2. WPA2 является безопасностью уровня 2 по умолчанию для WLAN.
3. Выберите вкладку AAA Servers, и затем выберите соответствующий сервер, настроенный для аутентификации.
4. Поскольку этот WLAN использует центральную коммутацию, необходимо гарантировать, что флажок H-REAP Local Switching отключен (т.е. флажок Local Switching не установлен). **Затем нажмите Apply.**

Проверьте централизованную аутентификацию, центральную коммутацию

Выполните следующие действия:

1. Настройте беспроводного клиента с тем же SSID и конфигурациями безопасности.В данном примере SSID является *Центральным*, и метод безопасности является *WPA2*.
2. Введите имя пользователя и пароль согласно конфигурации в сервер RADIUS> Настройка пользователя для активации центрального SSID в клиенте.Данный пример использует *User1* в качестве имени пользователя и пароля.Клиент централизованно аутентифицируется сервером RADIUS и привязан к AP H-REAP. H-REAP Находится

теперь в **централизованной аутентификации, центральной коммутации**.

Выключенная аутентификация, переключаясь Выключенный

С одинаковой конфигурацией, объясненной в Централизованной аутентификации, Центральном разделе Коммутации, отключают канал WAN, который подключает контроллер. Теперь, контроллер ждет ответа биения от AP. Ответ биения подобен сообщениям поддержки активности. Контроллер пробует пять последовательных пульсов, каждый всех секунду.

Поскольку это не получено с ответом биения от H-REAP, WLC вычеркивает из списка LAP.

Выполните **команду debug capwap events enable** от CLI WLC для проверки процесса дерегистрации. Это - пример выходных данных этой **команды отладки**:

```
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Did not receive heartbeat reply from AP
00:15:c7:ab:55:90 Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90
apfSpamProcessStateChangeInSpamConte xt: Down capwap event for AP 00:15:c7:ab:55:90 slot 0 Thu
Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte xt: Deregister
capwap event for AP 00:15:c7:ab:55:90 slot 0 Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90
apfSpamProcessStateChangeInSpamConte xt: Down capwap event for AP 00:15:c7:ab:55:90 slot 1 Thu
Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte xt: Deregister
capwap event for AP 00:15:c7:ab:55:90 slot 1 Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90
Received capwap Down event for AP 00: 15:c7:ab:55:90 slot 0! Thu Jan 18 03:19:32 2007:
00:15:c7:ab:55:90 Deregister capwap event for AP 00:15: c7:ab:55:90 slot 0 Thu Jan 18 03:19:32
2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00: 15:c7:ab:55:90 slot 1! Thu Jan 18
03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15: c7:ab:55:90 slot 1
```

H-REAP входит в автономный режим.

Поскольку этот WLAN ранее централизованно аутентифицировался и централизованно коммутировался, оба контроля и трафик данных были туннелированы назад к контроллеру. Поэтому без контроллера, клиент неспособен поддержать ассоциацию с H-REAP, и это разъединено. Это состояние H-REAP и со связыванием клиента и с опознавательным не работанием упоминается как Выключенная Аутентификация, Переключаясь Выключенный.

Централизованная аутентификация, локальный коммутатор

В этом состоянии, для данного WLAN, WLC обрабатывает всю аутентификацию клиента и пакеты данных коммутаторов LAP H-REAP локально. После того, как клиент аутентифицируется успешно, контроллер передает команды контроля за capwap H-REAP и дает LAP команду коммутировать пакеты данных того данного клиента локально. Это сообщение отправляется всем клиентам после успешной аутентификации. Это состояние применимо только в связанном режиме.

Данный пример использует эти параметры конфигурации:

- Название WLAN/SSID: **центрально-локальный**
- Безопасность уровня 2: **WPA2**.
- Локальный коммутатор H-REAP: **включенный**

От Графического интерфейса контроллера выполните эти шаги:

1. Нажмите **WLAN** для создания нового WLAN под названием Центрально-локальный, затем нажмите **Apply**.

2. Поскольку этот WLAN использует централизованную аутентификацию, выберите аутентификацию **WPA2** в поле безопасности уровня 2.
3. Под разделом серверов RADIUS выберите соответствующий сервер, настроенный для аутентификации.
4. Проверьте флажок **H-REAP Local Switching** для коммутации трафика клиента, который принадлежит этому WLAN локально в H-REAP.

Проверьте централизованную аутентификацию, локальный коммутатор

Выполните следующие действия:

1. Настройте беспроводного клиента с тем же SSID и конфигурациями безопасности.В данном примере SSID *Централизованно-локален*, и метод безопасности является *WPA2*.
2. Введите имя пользователя и пароль согласно конфигурации в сервер RADIUS> Настройка пользователя для активации централизованно-локального SSID в клиенте.Данный пример использует *User1* в качестве имени пользователя и пароля.
3. **Нажмите кнопку ОК.**Клиент централизованно аутентифицируется сервером RADIUS и привязан к AP H-REAP. H-REAP Находится теперь в **централизованной аутентификации, локальном коммутаторе**.

Выключенная аутентификация, локальный коммутатор

Если локально коммутируемый WLAN настроен для какого-либо типа проверки подлинности, который требуется, чтобы, обработаны на WLC (таком как Аутентификация eap [динамический WEP/WPA/WPA2/802.11i], WebAuth или NAC), после Сбоя WAN, это вводит **аутентификацию вниз,** состояние **локального коммутатора**. В этом состоянии, для данного WLAN, H-REAP отклоняет любых новых клиентов та попытка аутентифицироваться. Однако это продолжает передавать сигналы-маяки и тестовые ответы для хранения существующих клиентов должным образом связанными. Это состояние действует только в автономном режиме.

Для проверки этого состояния используйте одинаковую конфигурацию, объясненную в Централизованной аутентификации, разделе Локального коммутатора.

Если канал WAN, который подключает WLC, не работает, WLC проходит процесс вычеркивания из списка H-REAP.

После того, как вычеркнутый из списка, H-REAP входит в автономный режим.

Клиент связался через этот WLAN, все еще поддерживает его подключение. Однако, потому что контроллер, средство проверки подлинности не доступно, H-REAP не позволяет новых соединений от этого WLAN.

Это может быть проверено активацией другого беспроводного клиента в том же WLAN. Можно найти, что аутентификация для этого клиента отказывает и что клиенту не разрешают связаться.

Примечание: Когда количество клиента WLAN равняется нулю, H-REAP прекращает все связанные функции 802.11 и больше сигналы-маяки для данного SSID. Это перемещает WLAN в следующее состояние H-REAP, **аутентификация вниз, переключаясь вниз**.

Локальная проверка подлинности, локальный коммутатор

В этом состоянии LAP H-REAP обрабатывает аутентификации клиента и пакеты данных клиента коммутаторов локально. Это состояние допустимо только в автономном режиме и только для типов проверки подлинности, которые могут быть обработаны локально в AP и не включают обработку контроллера

H-REAP, который был ранее в **централизованной аутентификации,** состоянии **локального коммутатора**, шагах в это состояние, если настроенный тип проверки подлинности может быть обработан локально в AP. Если настроенная аутентификация не может быть обработана локально, такие как аутентификация 802.1x, то в автономном режиме, H-REAP переходит **к аутентификации вниз,** режиму **локального коммутатора**.

Это некоторые популярные механизмы аутентификации, которые могут быть обработаны локально в AP в автономном режиме:

- Открытый
- Совместно используемый
- WPA-PSK
- PSK WPA2

Примечание: Когда AP находится в связанном режиме, все процессы проверки подлинности обрабатываются WLC. В то время как H-REAP находится в автономном режиме, открытом, разделенном, и WPA/WPA2-PSK аутентификации переданы LAP, где происходит вся аутентификация клиента.

Примечание: Внешняя веб-аутентификация не поддерживается при использовании ГИБРИДНОГО REAP с локальным коммутатором, включенным на WLAN.

Данный пример использует эти параметры конфигурации:

- Название WLAN/SSID: **ЛОКАЛЬНЫЙ**
- Безопасность уровня 2: **WPA-PSK**
- Локальный коммутатор H-REAP: **включенный**

От Графического интерфейса контроллера выполните эти шаги:

1. Нажмите **WLAN** для создания нового WLAN под названием Локальный, затем нажмите **Apply**.
2. Поскольку этот WLAN использует локальную проверку подлинности, выберите **WPA-PSK** или любой из упомянутых механизмов обеспечения безопасности, которые могут быть обработаны локально в поле безопасности уровня 2.Данный пример использует **WPA-PSK**.
3. После того, как выбранный, необходимо настроить Предварительный общий ключ / Фраза - пропуск, которая будет использоваться.Это должно быть тем же в клиентской стороне для аутентификации, чтобы быть успешным.
4. Проверьте флажок **H-REAP Local Switching** для коммутации трафика клиента, который принадлежит этому WLAN локально в H-REAP.

Проверьте локальную проверку подлинности, локальный коммутатор

Выполните следующие действия:

1. Настройте клиента с тем же SSID и конфигурациями безопасности.Здесь, SSID *Локален*, и методом безопасности является *WPA-PSK*.
2. Активируйте Локальный SSID в клиенте.Клиент аутентифицируется централизованно в контроллере и партнерах с H-REAP. Трафик клиента настроен для коммутации локально. Теперь, H-REAP находится в Централизованной аутентификации, состоянии Локального коммутатора.
3. Отключите канал WAN, который соединяется с контроллером.Контроллер, как обычно, проходит процесс дерегистрации. H-REAP вычеркнут из списка от контроллера.После того, как вычеркнутый из списка, H-REAP входит в автономный режим.Однако клиент, который принадлежит этому WLAN все еще, поддерживает ассоциацию с H-REAP.Кроме того, потому что тип проверки подлинности здесь может быть обработан локально в AP без контроллера, H-REAP действительно разрешает ассоциации от любого нового беспроводного клиента через этот WLAN.
4. Для проверки этого активируйте любого другого беспроводного клиента на том же WLAN.Вы видите, что клиент аутентифицируется и привязывается успешно.

Устранение неполадок

- Чтобы продолжить устранение неполадок клиентских подключений, введите следующую команду через порт консоли H-REAP:`AP_CLI#show capwap reap association`
- Чтобы продолжить устранение неполадок клиентских подключений и ограничить выходные данные отладки, используйте следующую команду:`AP_CLI#debug mac addr <client's MAC address>`
- Для отладки подключений клиента, основанных на протоколе 802.11, используйте следующую команду:`AP_CLI#debug dot11 state enable`
- Отладка процесса аутентификации 802.1X и его ошибок выполняется с помощью следующей команды:`AP_CLI#debug dot1x events enable`
- Для отладки сообщений внутреннего контроллера и RADIUS используется следующая команда:`AP_CLI#debug aaa events enable`
- **Или, чтобы запустить полный набор команд отладки клиентов, введите следующую команду:**`AP_CLI#debug client <client's MAC address>`

Дополнительные сведения

- Пример базовой конфигурации контроллера беспроводной локальной сети и "облегченной" точки доступа
- Пример конфигурации сетей VLAN на контроллерах беспроводной LAN
- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 7.0
- Гибридный дизайн REAP и руководство по развертыванию
- Поиск и устранение простых неисправностей Hybrid Remote Edge Access Point (H-REAP)
- Пример конфигурации при отказе контроллера WLAN для "облегченных" точек доступа
- Поддержка беспроводного продукта
- Cisco Systems – техническая поддержка и документация