Содержание

[Введение](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Условные обозначения](#)
[Общие сведения](#)
[H-REAP, устраняющий неполадки](#)
[H-REAP не присоединяется к WLC](#)
[Проверка режима работы H-REAP](#)
[Команды консоли H-REAP не В рабочем состоянии и Возвращают Ошибку](#)
[Клиенты не могут соединиться с H-REAP](#)
[Wireless Control System (WCS) сообщает о неправильных клиентских количествах AP в режиме H-REAP](#)
[Дополнительные сведения](#)

Введение

Гибридная удаленная граничная точка доступа (H-REAP) представляет собой решение для развертывания в филиалах и удаленных офисах компаний. Это позволяет клиентам настроить и управлять двумя или тремя точками доступа (AP) в ответвлении или удаленном офисе от офиса корпорации до ссылки глобальной сети (WAN) без потребности развернуть контроллер в каждом офисе. Этот документ обсуждает некоторые общие проблемы, которые могут произойти в среде H-REAP. Этот документ также предоставляет сведения о том, как решить эти проблемы. См. Дизайн H-REAP и Руководство по развертыванию для вопросов проектирования H-REAP, когда вы развертываете H-REAP и Гибрид Настройки REAP для действий настройки.

Предварительные условия

Требования

- Функциональное знание H-REAP и его рабочих режимов
- Знание процесса регистрации Облегченной точки доступа (LAP) к контроллеру
- Знание протокола LWAPP

Используемые компоненты

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

- Cisco 4400 и Контроллеры беспроводной локальной сети серии 2100 (WLC), которые выполняют Версию 5.1

- AP Cisco 1130AG, 1240 AP AG и 1250 AP
- Cisco 2800 и маршрутизаторы серии 3800, которые выполняют Версию 12.4

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

Это ограничения для запоминания при использовании H-REAP.

- Гибридный REAP поддерживается только на 1130AG, 1140, 1240, 1250, 1260, AP801, AP 802, 1040, и AP AP3550 и на Cisco WiSM, Cisco 5500, 4400, 2100, 2500, Flex Контроллеры серии 7500, Catalyst 3750G Интегрированный Коммутатор Контроллера беспроводной локальной сети и Модуль Контроллерной сети для Маршрутизаторов ISR.
- Все типы безопасности, которые требуют, управления путями данных (например VPN), не работают с трафиком в сетях WLAN с локальной коммутацией, так как контроллер не может управлять данными, которые не туннелируются к нему. Любой другой тип безопасности работает или на централизованно или на локально коммутированные WLAN, при условии, что путь между H-REAP и контроллером подключен. Когда этот conduit не работает, только подмножество этих параметров безопасности позволяет новым клиентам соединяться с локально коммутируемыми WLAN.
- Когда точка доступа H-REAP переходит в автономный режим, WLAN, которые настроены для открытого, совместно использовали, WPA-PSK, или аутентификация PSK WPA2 вводит "локальную проверку подлинности, локальный коммутатор" сообщают и продолжают новые аутентификации клиента.В выпуске ПО контроллера 4.2 или позже, это также истинно для WLAN, которые настроены для 802.1X, 802.1X WPA, 802.1X WPA2 или централизованного управления ключами Cisco (CCKM). Однако эти типы проверки подлинности требуют, чтобы был настроен внешний сервер RADIUS. Другие WLAN вводят любого "аутентификация вниз, коммутируя вниз" состояние (если WLAN был настроен для центральной коммутации), или "аутентификация вниз, локальный коммутатор" состояние (если WLAN был настроен для локального коммутатора).
- С H-REAP в Связанном режиме контроллер свободен наложить клиентское исключение/помещение в черный список, чтобы препятствовать тому, чтобы некоторые клиенты связались с его AP. Эта функция может произойти или автоматизированной или ручной формой. В отношении глобального и НА КОНФИГУРАЦИИ WLAN, клиенты могут быть исключены для хоста причин, которые колеблются от повторных неудачных попыток аутентификации до кражи IP, а также для любого данного промежутка времени. Кроме того, клиенты можно добавить в список исключения вручную. В то время как AP находится в Связанном режиме, использование этой функции только возможно. Клиенты, которые были размещены в этот список исключения, остаются неспособными

соединиться с AP, даже в то время как это находится в Автономном режиме
- WLAN, которые не используют Проверку подлинности MAC (локальный или восходящий) больше, позволяют дополнительные аутентификации клиента, когда AP находится в Автономном режиме, который идентичен способу, которым столь же настроенный WLAN с 802.1X или WebAuth работает в том же режиме.
- Версии WLC 4.2.61.0 и более поздняя поддержка быстро защищают роуминг с помощью CCKM. Режим H-REAP поддерживает Уровень 2, быстро защищают роуминг с помощью CCKM. Эта функция предотвращает потребность в полной Аутентификации eap RADIUS, поскольку клиент перемещается от одного AP до другого. Для использования CCKM, быстро бродящего с точками доступа H-REAP, необходимо настроить группы H-REAP.

H-REAP, устраняющий неполадки

Существует несколько общих сценариев и ситуаций, в которых процессы настройки H-REAP и подключения клиентов могут быть нарушены. Это всего несколько таких ситуаций с их предложенными действиями по устранению проблем.

H-REAP не присоединяется к WLC

Это основные причины для H-REAP для не присоединения к WLC:

- H-REAP неспособен получить IP-адрес к себе, или он был назначен с неправильным IP-адресом.
- Нет никакого подключения уровня 3 между H-REAP и WLC.
- Нет подключения Протокола LWAPP между H-REAP и WLC.
- Другие причины являются H-REAP, соединяющим с другим контроллером, несоответствием сертификата, проблемой с WLC или H-REAP самим, и т.д.

Выполните эти шаги для устренения этих проблем:

1. Проверьте, что AP H-REAP назначают IP-адрес.Если DHCP используется через консоль AP, проверьте, что AP получает адрес с этой командой:.`AP_CLI#show dhcp lease`Если выходные данные этой команды не ни один, это подразумевает, что Адресация DHCP не используется для этого AP.Теперь, гарантируйте, что статический IP - адрес назначен на AP в правильном пути. Это может быть проверено с этой командой:`AP_CLI#show lwapp ip config`LWAPP Static IP Configuration**IP Address 10.77.244.222**IP netmask 255.255.0.0Default Gateway 10.77.244.220Выходные данные отображают статический IP - адрес 10.77.244.222 назначенных к AP. Если это не намеченный IP-адрес, который будет назначен, исправьте IP-адрес.
2. Проверьте возможность подключения с помощью IP-адреса между AP и интерфейсом управления контроллера.Как только IP-адрес был проверен, пропингуйте управление IP-адресами контроллера, чтобы удостовериться, что AP может связаться с контроллером. Используйте команду ping через консоль AP с этим синтаксисом:`AP_CLI#ping 10.77.244.210`*`!--- 10.77.244.210/27 is the example management interface IP address of the controller.`*Если эхо-запрос не успешен, он указывает, что существует проблема в возможности подключения с помощью IP-адреса между AP и контроллером. Гарантируйте, что восходящая сеть должным образом настроена и что

Доступ через WAN назад к корпоративной сети подключен. Проверьте, что контроллер в рабочем состоянии и **не** находится позади никаких границ **NAT/PAT**. Эхо-запрос от контроллера до AP с тем же синтаксисом. Удостоверьтесь**, что MTU** для пути между контроллером и H-REAP в минимуме **1500**. Это может быть проверено с **эхо-запросом-l** команда *<WLC Management IP>* **1500 года** от компьютера на стороне H-REAP глобальной сети (WAN).Вот пример выходных данных команды **успешного завершения команды ping**:**ping -l 1500 10.77.244.210**Pinging 10.77.244.204 with 1500 bytes of data:Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252Ping statistics for 10.77.244.204: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),Approximate round trip times in milli-seconds: Minimum = 6ms, Maximum = 6ms, Average = 6ms

3. Проверьте подключение LWAPP между AP и контроллером.Однажды возможность подключения с помощью IP-адреса между H-REAP и контроллером был проверен, выполните отладки LWAPP на контроллере, чтобы подтвердить, что сообщения LWAPP переданы через глобальную сеть (WAN) и определить связанные проблемы. На контроллере создайте MAC-фильтр, чтобы уменьшить объем выходных данных отладки. Используйте эту команду для ограничения выходных данных последующей команды к одиночному AP:AP_CLI#**debug mac addr** <AP?s wired MAC address>.Как только это собирается ограничить выходные данные отладки, включить отладку LWAPP с этой командой:Controller_CLI#**debug lwapp events enable**Вы видите сообщения отладки, подобные им:---------- ---------- ---------- ---------- Thu Mar 15 15:07:56 2007: 00:12:44:b2:ae:d0 **Received LWAPP DISCOVERY REQUEST from AP 00:12:44:b2:ae:d0** to ff:ff:ff:ff:ff:ff on port '1' Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0 **Received LWAPP JOIN REQUEST from AP 00:12:44:b2:ae:d0** to 00:0b:85:33:84:a0 on port '1' Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0 AP AP0012.d92b.3a5e: txNonce 00:0B:85:33:84:A0 rxNonce 00:12:44:B2:AE:D0 Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0 **LWAPP Join-Request MTU path from AP 00:12:44:b2:ae:d0** is 1500, remote debug mode is 0 Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0 Successfully added NPU Entry for AP 00:12:44:b2:ae:d0 (index 50)Switch IP: 10.77.244.211, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 172.16.1.10, AP Port: 45989, next hop MAC: 0 0:12:d9:2b:3a:5e Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0 **Successfully transmission of LWAPP Join-Reply to AP 00:12:44:b2:ae:d0** Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0 **Register LWAPP event for AP 00:12:44:b2:ae:d0 slot 0** Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0 Register LWAPP event for AP 00:12:44:b2:ae:d0 slot 1 Thu Mar 15 15:08:08 2007: 00:12:44:b2:ae:d0 Received LWAPP CONFIGURE REQUEST from AP 00:12:44:b2:ae:d0 to 00:0b:85:33:84:a0 ---------- -------- ---------- ---------- ----------Эти выходные данные отладки указывают на успешную передачу сообщений LWAPP между контроллером и AP, придерживавшимся успешным запросом Соединения от AP и параллельным ответом Соединения от контроллера. Позже AP зарегистрирован в контроллере.Если никакие такие сообщения отладки LWAPP не замечены, гарантируют, что у H-REAP есть по крайней мере один метод, которым может быть обнаружен контроллер. Если такие методы существуют (как широковещание Локальной подсети, параметр DHCP 43, или DNS), проверяют, что должным образом настроены. Если никакой другой метод обнаружения не существует, гарантируйте, что IP-адрес контроллера вручную введен в AP через консольный CLI.AP_CLI#**lwapp ap controller ip address** <management interface Ip address of controller>
4. При ручной настройке H-REAP удостоверьтесь, что вы очищаете ранее привязанные сведения о контроллере при перемещении AP в другое местоположение в сети. Это позволяет вашему AP связываться с контроллером в новом местоположении. Для очистки предыдущей конфигурации выполните AP **команда private-config lwapp**

CLI#clear. Затем проверьте, присоединяется ли AP к корректному контроллеру.Для проверки, с которыми контроллерами AP связывается, выполните **команду debug ip udp** к CLI AP. От выходных данных этой команды просмотрите адреса источника и назначения каждого пакета, который пересекает стек IP AP.Ниже представлен пример:**IP UDP AP_CLI#debug**`*Mar 15 16:41:47.999: UDP: sent src=10.77.244.222(45989), dst=10.77.244.211(12223), length=60`**`*Mar 15 16:41:47.999: UDP: sent src=10.77.244.222(45989), dst=10.77.244.210(12223), length=75*Mar 15 16:41:48.000: UDP: rcvd src=10.77.244.211(12223), dst=10.77.244.222(45989), length=22 *Mar 15 16:41:48.000: UDP: rcvd src=10.77.244.210(12223), dst=10.77.244.222(45989), length=49 *Mar 15 16:41:57.778: UDP: sent src=10.77.244.222(45989), dst=10.77.244.211(12223), length=76`**`*Mar 15 16:41:57.779: UDP: rcvd src=10.77.244.211(12223), dst=10.77.244.222(45989), length=22`**От** этих выходных данных вы видите, что пакеты UDP получены от AP и что они достигают интерфейса управления (10.77.244.210) и интерфейса диспетчера точки доступа (10.77.244.211) из контроллера.

5. Решите проблемы сертификата, если AP пытается присоединиться к контроллеру, но сбоям.Если сообщения LWAPP замечены на контроллере, но AP не в состоянии присоединяться, это вероятно проблема сертификата. Для большего количества советов по устранению проблем LWAPP, которые включают решающие проблемы сертификата, обращаются к Советам Устранения неполадок Инструмента обновления LWAPP.
6. Еще одна причина, что AP H-REAP не присоединяются к WLC, состоит в том, если Прокси - протокол преобразования адресов отключен на шлюзе для AP H-REAP. От консоли AP зарегистрировано это сообщение:`*Mar 15 16:41:47.999: UDP: sent src=10.77.244.222(45989), dst=10.77.244.211(12223), length=60`**`*Mar 15 16:41:47.999: UDP: sent src=10.77.244.222(45989), dst=10.77.244.210(12223), length=75*Mar 15 16:41:48.000: UDP: rcvd src=10.77.244.211(12223), dst=10.77.244.222(45989), length=22 *Mar 15 16:41:48.000: UDP: rcvd src=10.77.244.210(12223), dst=10.77.244.222(45989), length=49 *Mar 15 16:41:57.778: UDP: sent src=10.77.244.222(45989), dst=10.77.244.211(12223), length=76`**`*Mar 15 16:41:57.779: UDP: rcvd src=10.77.244.211(12223), dst=10.77.244.222(45989), length=22`**Это может быть вызвано идентификатором ошибки Cisco CSCse92856. Эта проблема применяется только к AP1130 и AP1240. Эта проблема не применяется к AP1000s, AP1100 или AP1200.Когда эти условия соблюдают, эта проблема происходит:Режим HREAP используется в WLAN. На автономный режим не влияет эта проблема. Сопоставление Собственного VLAN требуется.AP должны быть на другой IP-подсети, чем Менеджер AP WLC.Прокси - протокол преобразования адресов отключен на шлюзе по умолчанию для AP.AP H-REAP получает шлюз по умолчанию от сервера DHCP.Для решения этого вопроса включите Прокси - протокол преобразования адресов на маршрутизаторе основного шлюза AP.

Проверка режима работы H-REAP

Как только H-REAP присоединился к корректному контроллеру, можно проверить, связан ли AP H-REAP с контроллером когда-либо. Другими словами, можно проверить, в котором режиме функционирует AP H-REAP. Это может быть проверено с **командой show lwapp reap status** от CLI AP.

Lwapp AP_CLI#show пожинает статус

```
AP Mode:        REAP, Connected                 Radar detected on:
```

Эти выходные данные говорят, что AP H-REAP находится в режиме H-REAP и Связанном

режиме. Другими словами, канал WAN между AP и контроллером подключен UP (связанный), и Рабочий режим является H-REAP.

Lwapp AP_CLI#show пожинает статус

```
AP Mode:        REAP, Standalone                Radar detected on:
```

Эти выходные данные говорят, что AP находится в Автономном режиме, что означает, что канал WAN между AP и контроллером не работает. Рабочим режимом AP является REAP. Это означает, что WLAN, которые настроены для локального коммутатора с локальной проверкой подлинности, функциональны и позволяют новым клиентам этому WLAN. См. Пример конфигурации Режимов работы H-REAP для понимания других рабочих режимов H-REAP.

Команды консоли H-REAP не В рабочем состоянии и Возвращают Ошибку

Любые команды настройки (или установка или очистка конфигурации) выполненный через CLI H-REAP возвращают **ОШИБКУ!!! Command is disabled**. Это может произойти по одной из двух причин:

- AP H-REAP, которые находятся в Связанном режиме (зарегистрированный к контроллеру) не позволяют никаким конфигурациям быть установленными или очищенными через консоль. Когда AP находится в этом состоянии, конфигурации должны быть реализованы через интерфейс контроллера. Если доступ к командам настройки в AP требуется, гарантируйте, что AP находится в Автономном режиме, прежде чем вы попытаетесь ввести любые команды настройки.
- Как только AP соединился или зарегистрировался к контроллеру в любой точке, гарантируйте, что изменен enable password по умолчанию H-REAP, **Cisco**. Если этот пароль по умолчанию не изменен, вы не можете обратиться, Консольный CLI H-REAP перемещен в Автономный режим. Enable password может только быть установлен через CLI контроллера, с которым связан AP. Этот синтаксис команды может использоваться в контроллере для установки или пароля консоли отдельного AP или пароля ко всем AP контроллера: (WLC_CLI)**> config ap username** *<user-id>* **пароль** *<passwd>* **{все | <name> AP}**.Например:`WLC-1>config ap username hreap password hreap all`**Примечание:** При выполнении версии 5.0 WLC и позже используйте эту команду: **config ap mgmtuser добавляет** *тайну* **тайны** *password password username username* **{все | название AP}Примечание:** Для AP, которому не установили его пароли консоли, знать, что эта конфигурация только передается AP, когда команда введена в контроллер. Любые AP, которые впоследствии присоединяются к WLC, требуют, чтобы команда была введена снова.**Примечание:** Эти команды продолжают работать **Из** - H-REAPs **Коробки**, даже когда не изменен пароль по умолчанию:**lwapp** *<name>* **имени хоста APlwapp IP-адрес AP** *<IP-адрес AP> <маска подсети>***lwapp IP-шлюз по умолчанию AP** *<IP-адрес шлюза>***lwapp ap controller ip address** *<IP-адрес WLC>***clear lwapp private-config**
- **Примечание:** Для завершенного возврата AP к заводским настройкам, на начальную загрузку AP, нажмите **кнопку Mode**, пока световой сигнал Ethernet не становится желтым. На 1131 этот свет около кнопки Mode и ясно отмечен Ethernet. На 1242 это находится под белым пластмассовым фасадом и записанный нотами с E. Освободите кнопку Mode и позвольте AP загрузиться. AP возвращен к интерфейсу, который доступен через Образ для восстановления IOS AP. Знайте, что, если новые команды настройки желаемы, AP должен выполнить релиз 12.3 программного обеспечения Cisco

IOS (11) JX1 или позже. Это может быть проверено через консоль AP путем ввода **команды Show version.Примечание:** Все **показывают**, и **команды отладки** продолжают работать без устанавливаемого пароля по умолчанию и в то время как AP находится в Связанном режиме.Только на этом этапе могут любые конфигурации LWAPP быть сделанными.

Клиенты не могут соединиться с H-REAP

Если беспроводные клиенты не могут соединиться с H-REAP, выполнить эти шаги:

1. Гарантируйте, что канал WAN между Контроллером и H-REAP подключен.
2. Проверьте, что AP должным образом присоединился к контроллеру и что контроллер имеет по крайней мере один должным образом настроенный (и включил), WLAN. Гарантируйте, что **H-REAP** находится во Включенном состоянии для локально коммутируемых WLAN
3. В контроллере настройте WLAN для широковещательной передачи его SSID, чтобы помочь устранять неполадки этого процесса. На клиентской стороне проверьте, в состоянии ли клиент найти AP с SSID. Отразите название SSID и конфигурацию безопасности WLAN на клиенте. Конфигурация безопасности на стороне клиента — основная причина большинства проблем с подключением.
4. Гарантируйте, что клиенты на локально коммутируемых WLAN являются должным образом обращенным IP. Если DHCP используется, удостоверьтесь, что восходящий сервер DHCP должным образом настроен и что это предоставляет адреса клиентам. Если статическая адресация используется, гарантируйте, что клиенты должным образом настроены для правильной подсети.
5. **Убедитесь, что UDP-порты 12222 и 12223 открыты на всех промежуточных брандмауэрах.**
6. Для дальнейшего решения проблем клиентского подключения в консольном порту H-REAP выполните эту команду:`AP_CLI#show lwapp reap association`
7. Для отладки проблем с подключением 802.11 клиента выполните эту команду:`AP_CLI#debug dot11 state enable`
8. Для отладки процесса проверки подлинности 802.1X и сбоев клиента, выполните эту команду:`AP_CLI#debug dot1x events enable`

Wireless Control System (WCS) сообщает о неправильных клиентских количествах AP в режиме H-REAP

Если вашей Беспроводной средой управляет Wireless Control System (WCS), иногда этот WCS может сообщить о неправильных клиентах AP H-REAP, в противоположность корректному клиентскому количеству, заданному контроллером.

Эта проблема происходит из-за идентификатора ошибки Cisco CSCsg48059 (только зарегистрированные клиенты). WCS сообщает о клиентском количестве, которое слишком высоко, когда H-REAP включают на контроллере. Чтобы избежать ошибок согласования, жестко задайте использование дуплексного режима на обеих сторонах соединения.

1. Для обнаружения, сколько клиентов привязано к AP или данному контроллеру, используйте **Монитор WCS>** функция **Клиентов**.

2. Поиск AP или контроллером, который ограничен радио-типом, для предотвращения копий.
3. Используйте общее число элементов, найденных как ваша истинная численность населения.Можно также использовать WLC для обнаружения корректного клиентского количества.

Этот вопрос решен в выпуске 4.0.206.0 Контроллера беспроводной локальной сети.

Дополнительные сведения

- Устранение неполадки: облегченная точка доступа не соединяется с контроллером беспроводной LAN
- Руководство по разработке и развертыванию H-Reap
- Гибрид Настройки REAP
- Пример конфигурации режимов работы H-REAP
- Гибрид Настройки REAP на WCS
- Вопросы и ответы по облегченным точкам доступа
- Cisco Systems – техническая поддержка и документация