Руководство по разработке и развертыванию H-Reap

Содержание

Введение

Технология H-REAP — это беспроводное решение для развертывания в филиалах и удаленных офисах. Она позволяет заказчикам настраивать точки доступа в филиале или удаленном офисе и управлять ими из офиса корпорации через канал глобальной сети

(WAN), без развертывания контроллера в каждом офисе. Точки доступа H-REAP выполняют локальную коммутацию клиентских данных, а также локальную аутентификацию клиентов, когда подключение к контроллеру обрывается. При наличии подключения к контроллеру точки доступа H-REAP могут выполнять обратное туннелирование трафика к контроллеру.

Предварительные условия

Требования

Гибридный REAP поддерживается только на этих 1040, 1130, 1140, 1240, 1250, 3500, 1260, AP801, точки доступа AP802 и на Cisco WiSM, Cisco 5500, 4400, 2100, 2500 и Flex Контроллеры серии 7500, Catalyst 3750G Интегрированный Коммутатор Контроллера беспроводной локальной сети, Модуль Контроллерной сети для Маршрутизаторов ISR.

Используемые компоненты

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

- Cisco Унифицированная версия 7.0 Контроллеров
- Контроль и Инициализация точек доступа (CAPWAP) протокол базировались 1040, 1130, 1140, 1240,1250, 1260, AP801, AP802 и LAP серии 3500

Условные обозначения

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

Общие сведения операций CAPWAP

CAPWAP, на котором базируется архитектура единой беспроводной сети Cisco, задает два других основных режима операции точки беспроводного доступа:

- **Split-MAC. В режиме Split-MAC система делит основные функции 802.11между точками доступа и контроллером.** В таких конфигурациях контроллер выполняет не только обработку процессов, таких как аутентификация и сопоставление 802.11. Он также служит единой точкой входа и выхода для всего пользовательского трафика. Точки доступа раздельного MAC туннелируют весь трафик клиента к контроллеру через туннель данных CAPWAP (контроль CAPWAP также придерживается того же пути.).
- **Local MAC. При внедрении всех функциональных возможностей 802.11 в точке доступа режим Local MAC обеспечивает разделение плоскости данных и пути управляющих сигналов, завершая весь клиентский трафик в проводном порте точки доступа.** Это позволяет не только для прямого беспроводного доступа к ресурсам, локальным для точки доступа, но это предоставляет упругость ссылки, позволяя контрольному пути CAPWAP (ссылка между AP и контроллером) не работать, в то время как сохраняется беспроводной сервис. Эта функция будет особенно полезна для малых удаленных офисов и филиалов, которые используют каналы WAN и нуждаются в небольшом количестве точек доступа, которое не позволяет обосновать приобретение локального

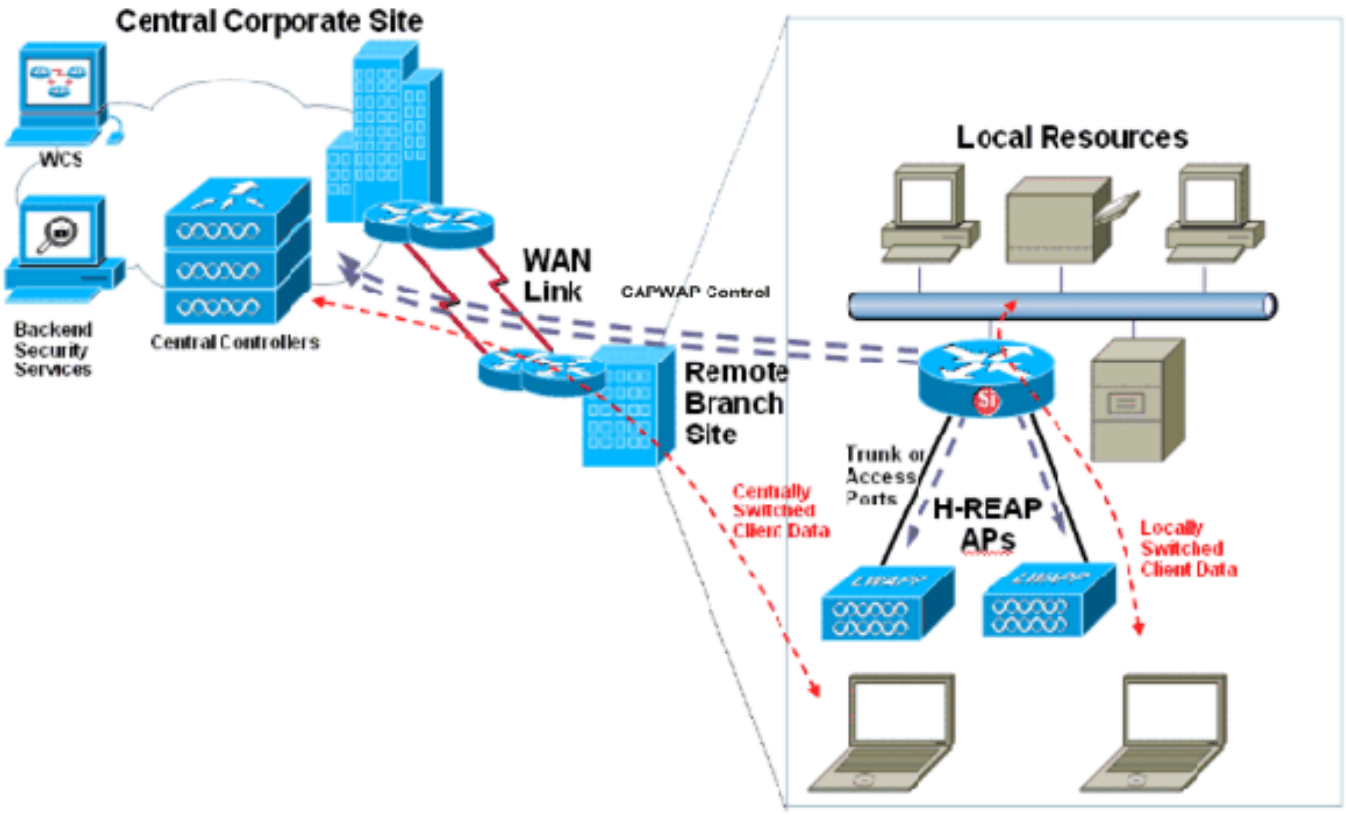
контроллера.

Примечание: Перед выпуском 5.2 контроллера Унифицированная беспроводная архитектура Cisco основывалась на протоколе LWAPP.

Технология Hybrid Remote-Edge Access Point

Гибридная Удаленная Граничная точка доступа или REAP H, является функцией, поддерживавшей 1040, 1130, 1140, 1240, 1250, 3500, 1260, AP801, точки доступа AP802 и на Cisco WiSM, Cisco 5500, 4400, 2100, 2500 и Flex Контроллеры серии 7500, Catalyst 3750G Интегрированный Коммутатор Контроллера беспроводной локальной сети, Модуль Контроллерной сети для Маршрутизаторов ISR. Функция REAP H поддерживается только в окончательном релизе контроллера единой беспроводной сети Cisco (UWN) 4.0 или позже, выбираемая функция этого программного обеспечения обеспечивает слияние и Разделения и Локального MAC - адреса операции CAPWAP для максимальной гибкости развертывания. Трафик клиента на REAPs H может или быть коммутирован локально в точке доступа или туннелировал назад к контроллеру, который зависит от каждой конфигурации WLAN. Далее, локально коммутированный трафик клиента на REAP H может быть 802.1Q, помеченным для обеспечения проводного разделения стороны. Во время простоя канала WAN обслуживание сетей WLAN с локальной аутентификацией и коммутацией сохраняется.

Стандартная схема внедрения H-REAP:



Как показано на схеме, технология H-REAP была разработана специально для развертывания в средах малых офисов и филиалов.

В этом документе описывается принцип работы H-REAP, конфигурация контроллеров и точек доступа, а также приводятся соображения по проектированию сетей.

Принцип работы H-REAP

Основные концепции H-REAP

Существует несколько других режимов, которыми функциональность REAP H работает для обеспечения и локальной и центральной коммутации, а также жизнеспособности канала WAN. Комбинирование этих двух групп режимов предоставляет богатый набор функциональных возможностей, но при этом становится причиной различных ограничений, которые зависят от комбинации режимов.

Существует две группы режимов:

- **Центральный по сравнению с Локальная коммутация**WLAN (комплекты безопасности, QoS и других параметров конфигурации, связанных к SSIDs) на REAPs H, могут или собираться потребовать всего трафика данных, который будет туннелирован назад к контроллеру (названный центральной коммутацией), или WLAN могут быть настроены для отбрасывания всех данных клиента локально в проводном интерфейсе REAP H (известный как локальный коммутатор). Сети WLAN с локальной коммутацией могут поддерживать маркировку 802.1Q (необязательно), что обеспечивает их сегментацию с использованием проводной сети (порта Ethernet точки доступа).
- **Связанный по сравнению с автономным**Гибридный REAP, как говорят, находится в Связанном режиме, когда его уровень управления CAPWAP назад к контроллеру подключен и в рабочем состоянии, означая, что канал WAN не не работает. Режим Standalone определяется как операционное состояние, в которое переходит точка доступа H-REAP, когда теряет обратное подключение к контроллеру.

Примечание: В то время как точка доступа находится в связанном состоянии, вся обработка аутентификации безопасности REAP H (такая как Проверка подлинности RADIUS бэкэнда и деривация попарного главного ключа [PMK]) происходит в контроллере. Вся обработка сопоставления и аутентификации 802.11 выполняется в точке доступа H-REAP, независимо от того, в каком режиме она работает. Находясь в подключенном режиме точка доступа H-REAP транслирует данные сопоставления и проверки подлинности в контроллер. В автономном режиме точка доступа не может сообщить контроллеру о подобных событиях.

Функциональность H-REAP меняется в зависимости от режима работы (от того, в каком режиме находится точка доступа H-REAP — подключенном или автономном), настройки коммутации WLAN (центральная или локальная) и также параметров безопасности беспроводной связи.

Когда клиент подключается к точке доступа H-REAP, она пересылает все сообщения аутентификации контроллеру и, если аутентификация успешна, пакеты данных коммутируются локально или туннелируются в контроллер, в зависимости от параметров сети WLAN, к которой подключена точка доступа. В зависимости от механизма аутентификации клиента и режима коммутации пакетов, сети WLAN в среде H-REAP могут находиться в одном из следующих состояний, которые определяются конфигурацией WLAN и состоянием соединения между точкой доступа и контроллером:

- **центральная аутентификация, центральная коммутация. В этом состоянии сети WLAN точка доступа пересылает все запросы на аутентификацию клиента в контроллер, а также туннелирует в него все клиентские данные.** Это состояние допустимо только, когда контрольный путь точки доступа CAPWAP подключен. Т. е. точка доступа H-REAP

находится в подключенном режиме. Любой WLAN, который туннелирован назад к контроллеру, потерян во время бездействия глобальной сети (WAN), независимо от того метод аутентификации.

- **централизованная аутентификация, локальный коммутатор** — В этом состоянии, для данного WLAN, контроллер обрабатывает всю аутентификацию клиента и пакеты данных коммутаторов точки доступа REAP H локально. После того, как клиент аутентифицируется успешно, контроллер передает команду контроля за CAPWAP к REAP H, дающему точке доступа команду коммутировать пакеты данных того данного клиента локально. Это сообщение отправляется всем клиентам после успешной аутентификации. Это состояние применимо только в Связанном режиме.
- **локальная проверка подлинности, локальный коммутатор** — В этом состоянии, точка доступа REAP H обрабатывает аутентификации клиента и пакеты данных клиента коммутаторов локально. Это состояние действует только в автономном режиме и только для типов аутентификации, которые могут быть локально обработаны в точке доступа. Когда точка доступа ГИБРИДНОГО REAP переходит в автономный режим, WLAN, которые настроены для открытого, совместно использовали, WPA-PSK, или аутентификация PSK WPA2 входит, `local authentication, local switching` сообщают и продолжают новые аутентификации клиента.**Примечание:** Все шифрование беспроводных данных Уровня 2 всегда обрабатывается в точке доступа. Все процессы аутентификации клиентов выполняются в контроллере (или передаются из контроллера, в зависимости от конфигурации WLAN и контроллера), когда точка доступа находится в подключенном состоянии.
- **аутентификация вниз, локальный коммутатор** — В этом состоянии, для данного WLAN, REAP H отклоняет любых новых клиентов, которые пытаются аутентифицироваться, но это продолжает передавать сигналы-маяки и тестовые ответы для хранения существующих клиентов должным образом связанными. Это состояние действует только в автономном режиме.Если в сети WLAN с локальной коммутацией используется любой тип коммутации, который должен обрабатываться в контроллере (или к северу от него, например аутентификация EAP [динамическая аутентификация WEP/WPA/WPA2/802.11i], WebAuth или NAC), при отказе канала WAN сеть переходит в состояние "аутентификация отключена, локальная коммутация". Предыдущее состояние такой сети — "центральная аутентификация, локальная коммутация". Существующие беспроводные подключения клиентов и доступ к локальным ресурсам сохраняются, но новые сопоставления не допускаются. Если время ожидания пользовательского веб-сеанса истекает при использовании WebAuth или истекает срок действия пользовательского ключа EAP и требуется его повторное создание при использовании 802.1X, существующие клиенты теряют подключение и не получают возможности его восстановить (это период определяется сервером RADIUS, стандартные значения отсутствуют). Кроме того, операции роуминга 802.11 (между точками доступа H-REAP) вызывают полную повторную аутентификацию 802.1X и, следовательно, вызывают обрыв подключения для существующих клиентов.Когда число клиентских подключений WLAN достигает нуля, точка доступа H-REAP закрывает соответствующие функции 802.11 и прекращает рассылку сигналов-маяков для заданных SSID. Сеть WLAN переходит в следующее состояние H-REAP: аутентификация вниз, переключаясь вниз.**Примечание:** В выпуске ПО контроллера 4.2 или позже, WLAN, которые настроены для 802.1X, 802.1X WPA, 802.1X WPA2 или CCKM, могут также работать в Автономном режиме. Но эти типы проверки подлинности требуют, чтобы был настроен внешний сервер RADIUS. Больше подробной информации об этом предоставлено в разделах

для прибытия. Но, от выпуска ПО контроллера 5.1, REAP H самого может быть настроен как сервер RADIUS.

- **аутентификация вниз, переключаясь вниз** — В этом состоянии, WLAN на данном REAP H разъединяет существующих клиентов и прекращает передавать сигналы-маяки и тестовые ответы. Это состояние действует только в автономном режиме.Когда точка доступа REAP H переходит в автономный режим, она разъединяет всех клиентов, которые находятся на централизованно коммутируемых WLAN. Для WLAN web-аутентификации не разъединены существующие клиенты, но точка доступа REAP H больше не передает сигналы-маяки, когда количество связанных клиентов достигает нуля (0). Это также передает сообщения разъединения новым клиентам, которые связываются к WLAN web-аутентификации. Отключены зависимые от контроллера действия, такие как управление доступом к сети (NAC) и web-аутентификация (гостевой доступ), и точка доступа не передает отчётов о системе обнаружения проникновения (IDS) контроллеру.**Примечание:** Если ваш контроллер настроен для NAC, клиенты могут связаться только, когда точка доступа находится в связанном режиме. Когда NAC включен, необходимо создать нездоровое (или изолированный) VLAN так, чтобы трафик данных любого клиента, который назначен на эту VLAN, прошел через контроллер, даже если WLAN настроен для локального коммутатора. После того, как клиента назначают на изолированную VLAN, все ее пакеты данных централизованно коммутированы.Точка доступа ГИБРИДНОГО REAP поддерживает клиентское подключение даже после того, как это перейдет в автономный режим. Однако, как только точка доступа восстанавливает соединение с контроллером, она разъединяет всех клиентов, применяет новые сведения о конфигурации от контроллера и повторно позволяет клиентское подключение.

Функциональные и архитектурные ограничения H-REAP

Соображения по использованию каналов WAN в H-REAP

Поскольку REAP H был специально разработан для работы через каналы WAN, это было оптимизировано для таких установок. Несмотря на то что H-REAP предлагает достаточную гибкость в работе с подобными сценариями проектирования удаленных сетей, при разработке архитектуры сети с функциональными возможностями H-REAP необходимо следовать нескольким указаниям.

- Точка доступа REAP H может быть развернута или со статическим IP - адресом или с адресом DHCP. В случае DHCP сервер DHCP должен быть доступным локально и должен быть в состоянии предоставить IP-адрес для точки доступа в загрузке.
- H REAP поддерживает до четырех фрагментированных пакетов или минимальный блок передачи с 500 максимальными размерами в байтах (MTU) канал WAN.
- Задержка туда и обратно не должна превышать 300 миллисекунд (мс) для данных и 100 мс для речи и данных между точкой доступа и контроллером, и управляющие пакеты CAPWAP должны быть расположены по приоритетам по всему другому трафику.
- Контроллер может передать пакеты групповой адресации в форме индивидуальной рассылки или пакеты групповой адресации к точке доступа. В режиме REAP H точка доступа может получить пакеты групповой адресации только в форме индивидуальной рассылки.

- Для использования CCKM, быстро бродящего с точками доступа REAP H, необходимо настроить группы REAP H.
- H точки доступа REAP поддерживают множественный SSIDs.
- NAC внеполосная интеграция поддерживается только на WLAN, настроенных для REAP H центральная коммутация. Это не поддерживается для использования на WLAN, настроенных для локального коммутатора REAP H.

Примечание: Во время обновления каждый AP должен получить обновление кода на 4 МБ через канал WAN. Обновления плана и Windows изменения соответственно.

Чтобы гарантировать, что поддержка этого установленного ограничения задержки существует, строго рекомендуется, чтобы между точкой доступа и контроллером, приоритет был настроен в посреднической инфраструктуре для подъема CAPWAP (порт 5246 UDP) доступной очереди наивысшего приоритета. Без приоритета, размещенного в контроль за CAPWAP, скачки в другом сетевом трафике могут вероятная причина H точки доступа REAP для частого смещения от связанного до Автономных режимов, поскольку перегрузка канала WAN предотвращает точку доступа / сообщения контроллера (и пакеты Keepalive) от того, чтобы быть отправленным. Это настоятельно рекомендовано Проектировщикам сети, которые планируют развернуть AP REAP H по каналам WAN, протестировать все их приложения.

Частая смена режима в точках доступа H-REAP становится причиной серьезных проблем подключения. Без приоритизации исправной сети на месте, благоразумно разместить контроллеры на удаленных узлах для обеспечения последовательного и стабильного беспроводного доступа.

Примечание: Настроен ли REAP H для туннелирования трафика клиента назад к контроллеру или нет, путь данных CAPWAP используется для передачи всех зондов клиента 802.11 и запросов аутентификации/ассоциации, сообщений соседнего узла RRM, и EAP и запросов web-аутентификации назад к контроллеру. Также, гарантируйте, что данные CAPWAP (порт 5247 UDP) не заблокированы нигде между точкой доступа и контроллером.

Гибридные группы REAP

Чтобы лучше организовать и управлять вашими точками доступа REAP H, можно создать группы REAP H и назначить определенные точки доступа на них. Все точки доступа REAP H в группе совместно используют тот же CCKM, WLAN, и резервируют информацию о Конфигурации сервера RADIUS. Эта функция полезна, если у вас есть множественные точки доступа REAP H в удаленном офисе или на этаже здания, и вы хотите настроить их внезапно. Например, можно настроить резервный сервер RADIUS для группы REAP H вместо того, чтобы иметь необходимость настроить тот же сервер на каждой точке доступа.

Scalability	Flex 7500	WLC 5500/Wism-2/Wism-1
Total Access Points	2,000	500
Total Clients	20,000	7,000
Max HREAP Groups	500	100
Max APs per HREAP Group	50	25
Max AP Groups	500	500

Выпуски ПО контроллера 5.0.148.0 и позже содержат две новых функции группы REAP H:

- **Резервный сервер RADIUS** — можно настроить контроллер, чтобы позволить точке доступа REAP H в автономном режиме выполнять полную аутентификацию 802.1X к резервному серверу RADIUS. Можно настроить основной сервер RADIUS или обоих основной и дополнительный сервер RADIUS.
- **Локальная проверка подлинности** — можно настроить контроллер, чтобы позволить точке доступа REAP H в автономном режиме выполнять LEAP или аутентификацию FAST EAP до 20 статически настроенных пользователей. С Выпуском ПО контроллера 5.0 и далее, это было увеличено до 100 статически настроенных пользователей. Контроллер передает статический список имен пользователя и паролей к каждой точке доступа REAP H, когда это присоединяется к контроллеру. Каждая точка доступа в группе аутентифицирует только своих собственных связанных клиентов. Этой функцией является идеально подходит для клиентов, кто перемещает от сети автономной точки доступа до CAPWAP H сеть точки доступа REAP и не должен поддержать большую базу данных пользователей, ни добавить другое аппаратное устройство для замены функциональности сервера RADIUS, доступной в автономной точке доступа.

Выпуски ПО контроллера 7.0.116.0 и позже содержат эти новые функции группы REAP H:

- **Локальная проверка подлинности** — Эта функция теперь поддерживается, даже когда точки доступа REAP H находятся в Связанном Режиме.
- **OKC, Быстро Бродящие** — H REAP Groups, требуются для CCKM/OKC, быстро бродящего для работы с точками доступа REAP H. Быстрый роуминг достигнут путем кэширования производной главного ключа от полной Аутентификации eap так, чтобы простой и безопасный обмен ключами мог произойти, когда беспроводной клиент перемещается к другой точке доступа. Эта функция предотвращает потребность выполнить полную Аутентификацию eap RADIUS, поскольку клиент перемещается от одной точки доступа до другого. Точки доступа REAP H должны получить данные кэша CCKM/OKC для всех клиентов, которые могли бы связаться так, они могут обработать их быстро вместо того, чтобы передать их обратно в контроллер. Если, например, у вас есть контроллер с 300 точками доступа и 100 клиентами, которые могли бы связаться, передавание кэша CCKM/OKC для всех 100 клиентов не практично. При создании H REAP Group, включающей ограниченное число точек доступа (например, вы создаете

группу для четырех точек доступа в удаленном офисе), клиенты перемещаются только среди тех четырех точек доступа, и кэш CCKM/OKC распределен среди тех четырех точек доступа только, когда клиенты связываются одному из них. Эта функция, наряду с Резервным Радиусом и Локальной проверкой подлинности (Локальный EAP), не гарантирует в рабочем состоянии времени простоя для ваших узлов филиала.

Примечание: CCKM, быстро бродящий среди REAP H и non-H точек доступа REAP, не поддерживается.

См. раздел Configuring Hybrid-REAP Groups руководства по конфигурированию контроллера Cisco Wireless LAN, Выпуска 7.0 для получения дополнительной информации о том, как настроить группы REAP H.

Следует ли использовать магистраль

H точки доступа REAP может быть связан со ссылками магистрали "802.1q" или без меток соединениями доступа. Когда связано с магистральной линией, H точки доступа REAP передают обратно их контроль за CAPWAP и трафик данных к контроллеру через собственный VLAN. Сети WLAN с локальной коммутацией могут сбросить свой трафик в любую доступную сеть VLAN (стандартную или любую другую). Когда установлено для работы на соединение доступа (без видимости 802.1Q), H REAPs передают все сообщения CAPWAP и локально выключил пользовательские данные к синглу, без меток подсеть, с которой это связано.

Общие указания для выбора switchport mode для REAPs H следующие:

- Используйте магистральный канал, если на локальную коммутацию трафика настроено более одной сети WLAN и если трафик для этих SSID должен сбрасываться в разные подсети. Точку доступа и входной порт коммутатора необходимо настроить на транкинг 802.1Q. Конфигурация REAPs H для транкинга 802.1Q является наиболее распространенной конфигурацией и предоставляет наибольшую гибкость. Собственный VLAN также должен быть настроен на порте коммутатора, что REAP H связан с как вся связь CAPWAP между AP, и WLC находится на собственном VLAN.
- Используйте канал доступа, если точки доступа H-REAP используют только одну сеть WLAN с локальной коммутацией или несколько сетей WLAN с локальной коммутацией, которые не требуют разделения в проводном порте. Знайте, что магистральная линия может все еще быть выбираемой при этих условиях, если желаемо разделение между обменом сообщениями CAPWAP и пользовательскими данными. Но, это ни конфигурационное требование, ни угроза безопасности.

Примечание: H по умолчанию точек доступа REAP для работы на без меток, интерфейсы соединения доступа.

Обнаружение контроллера H-REAP

H REAP поддерживает каждую характеристику механизма обнаружения контроллера точек доступа в архитектуре единой беспроводной сети Cisco. Как только точка доступа получает IP-адрес (который может выделяться динамически с через DHCP или с помощью статической адресации), она пытается обнаружить контроллеры в системе с помощью широковещательной рассылки IP-пакетов, параметра DHCP 43, DNS и OTAP. На завершающей стадии точки доступа H-REAP вызывают из памяти IP-адреса контроллеров, к которым они были подключены ранее. См. дополнительные сведения о других методах

регистрации точек доступа LAP на контроллере WLC в документе Регистрация точек доступа LAP на контроллерах WLC.

Существует несколько предупреждений иметь в виду в отношении обнаружения контроллера. Они относятся ко всем точкам доступа Aironet, не только к точкам доступа H-REAP.

- Если точка доступа получает свою IP-адресацию через DHCP, параметр DHCP 43 является только жизнеспособным механизмом обнаружения для REAP H.
- OTAP работает только в точках доступа Aironet, которые уже подключались к контроллеру и загружали код. Они поставляются без микропрограммы радиомодуля, поэтому OTAP не будет работать на новом устройстве. Кроме того, OTAP требует, чтобы все ближайшие точки доступа обнаружили контроллер с включенной функцией OTAP и подключились к нему. Эта функция является устаревшей от выпуска WLC 6.0 и далее.
- Точка доступа, на которой поддерживается функциональность REAP H, не поддерживает LWAPP режим Уровня 2 CAPWAP. Контроллеры должны собираться управлять с LWAPP Уровня 3 CAPWAP.
- См. Развертывание Контроллеров беспроводной локальной сети Cisco 440X Series для получения дополнительной информации о точке доступа / обнаружение контроллера. операции

Вне этих традиционных механизмов обнаружения контроллера, выпуск ПО 4.0 и позже позволяет Точки доступа Aironet с консольными портами к теперь инициализации руководства по получению поддержки через консольный CLI. Теперь в точках доступа можно вручную настраивать статическую IP-адресацию, а также назначать имена хостов и IP-адреса контроллеров, к которым должны подключаться точки доступа. Это означает, что на узлах, где другие механизмы обнаружения не доступны, точки доступа могут быть настроены со всей конфигурацией нужного соединения вручную через консольный порт.

Эта функция поддерживается на всех точках доступа Aironet с портом консоли (не только на точках доступа с поддержкой H-REAP), но она будет особенно полезна для точек доступа H-REAP, так как вероятность, что они будут установлены на узлах без DHCP-серверов и механизмов обнаружения контроллеров (например в филиале), достаточно высока. Таким образом, этот новый консольный доступ исключает необходимость в двукратной транспортировке точек доступа H-REAP: в первый раз на узел контроллера для инициализации и во второй раз на удаленный узел для установки.

H поддерживаемые характеристики REAP

Поскольку точки доступа REAP H разработаны, чтобы быть размещенными через каналы WAN от контроллеров, мало того, что существуют вопросы проектирования, которые должны быть учтены при проектировании беспроводной сети с REAPs H, но существуют также некоторые функции, которые являются полностью или частично неподдерживаемые.

Нет никакого ограничения развертываний на количество точек доступа REAP H для каждого местоположения.

H матрица функций REAP

См. Матрицу функций REAP H для получения дополнительной информации о функциях,

поддерживавших с REAP H.

Поддерживаемые характеристики безопасности

Поддержка безопасности на REAP H варьируется, который зависит от режимов и состояний, ранее упомянутых. 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. Все остальные типы безопасности работают в сетях WLAN с локальной или центральной коммутацией при условии, что путь между точкой доступа H-REAP и контроллером доступен. Когда этот путь отключен, подключение новых клиентов к сети WLAN с локальной коммутацией поддерживают только некоторые параметры безопасности.

Как ранее упомянуто, для поддержки Аутентификации eap 802.1X, H точки доступа REAP в автономном режиме должен иметь их собственные серверы RADIUS для аутентификации клиентов. Этот резервный сервер RADIUS может быть тем, используемым контроллером. Можно настроить резервный сервер RADIUS для отдельных точек доступа REAP H через CLI контроллера или для групп REAP H или через GUI или через CLI. Сервер резервного копирования, настроенный для индивидуальной точки доступа, отвергает Конфигурацию сервера RADIUS для группы REAP H.

Версия 4.2.61.0 WLC и более поздняя поддержка быстро защищают роуминг с централизованным управлением ключами Cisco (CCKM). H режим REAP поддерживает Уровень 2, быстро защищают роуминг с CCKM. Эта функция предотвращает потребность в полной Аутентификации eap RADIUS, поскольку клиент перемещается от одной точки доступа до другого. Для использования CCKM, быстро бродящего с точками доступа REAP H, необходимо настроить группы REAP H. CCKM работает в автономном режиме для уже подключенных клиентов, но не для новых клиентов.

См. раздел Configuring Hybrid-REAP Groups руководства по конфигурированию контроллера Cisco Wireless LAN, Выпуска 7.0 для получения дополнительной информации о том, как настроить группы REAP H.

С REAP H в Связанном режиме контроллер свободен наложить клиентское исключение/помещение в черный список, чтобы препятствовать тому, чтобы некоторые клиенты связались к его точкам доступа. Эта функция может реализовываться с использованием как ручных, так и автоматических методов. Согласно глобальному и НА КОНФИГУРАЦИИ WLAN, клиенты могут быть исключены для хоста причин, который колеблется от повторных неудачных попыток аутентификации до кражи IP, и для любого данного промежутка времени. Кроме того, клиенты можно добавить в список исключения вручную. Применение этой функции возможно только когда точка доступа находится в подключенном режиме. Но клиенты, добавленные в список исключения, не смогут подключаться к точке доступа, даже когда она находится в автономном режиме.

Примечание: WLAN, которые используют Проверку подлинности MAC (локальный или восходящий), больше не не позволяют дополнительные аутентификации клиента, когда точка доступа находится в Автономном режиме, идентичном способу, которым столь же настроенный WLAN с 802.1X или WebAuth работал бы в том же режиме.

Поддержка web-аутентификации

Внутренняя веб-аутентификация, размещенная на Контроллере беспроводной локальной

сети, поддерживается для WLAN, которые или централизованно или локально коммутированы. Однако Внешняя веб-аутентификация только поддерживается на централизованно коммутируемом WLAN.

Примечание: В то время как REAP H находится в Автономном режиме, никакой метод Web-аутентификации не поддерживается.

Поддерживаемые функции инфраструктуры

RRM

Из-за факта, что много удаленных развертываний имеют только маленькое небольшое количество REAPs H, полная функциональность Управления радиоресурсами (RRM) не могла бы поддерживаться на каждом узле REAP H. Полный код RRM присутствует в REAP H, но алгоритмы Контроля за мощностью передачи (TPC) в RRM не инициированы, пока четыре или больше точки доступа не в диапазоне друг друга. Так, некоторые установки REAP H никогда не могли бы выключать свои радио. Следовательно, не имея возможности уменьшить мощность радиомодулей, точки доступа H-REAP не могут повышать мощность передачи для компенсации пропусков в зоне охвата.

В автономном режиме функции RRM, которые требуют обработки на контроллере, не поддерживаются для точек доступа H-REAP.

См. Управление радиоресурсами под Unified Wireless Network для получения дополнительной информации и в рабочем состоянии подробными данными RRM.

DFS

Динамический выбор частоты (DFS) поддерживается как в подключенном и в автономном режимах.

Отслеживание местоположения

Способность обеспечить точное определение размещения устройства варьируется значительно от местоположения до местоположения, основанного значительно на номере, плотности и размещении REAPs H. Точность определения местоположения устройства сильно зависит от полноты сбора сигнальной информации устройства, а это напрямую связано с количеством точек доступа, которые могут "слышать" данное устройство. Поскольку развертывания REAP H варьируются по области, эти сведения о размещении могут быть значительно уменьшены, и таким образом точность размещения могла бы пострадать соответственно. Среды H-REAP пытаются определить положение устройства с максимальной возможной точностью, но заявленная Cisco точность определения местоположения не относится к таким средам.

Примечание: H REAP не был разработан для обеспечения служб определения местоположения. Поэтому Cisco не может распространять заявленную точность на среды H-REAP.

L2 и мобильность L3

Обычный слой 2 роуминга поддерживается для локально коммутируемых WLAN. Чтобы обеспечить работу такого роуминга, убедитесь, что сети VLAN назначенные сетям WLAN,

согласованы для всех точек доступа H-REAP, для которых требуется роуминг. Это значит, что клиенты не должны повторно получать IP-адрес от сервера DHCP во время событий роуминга. Это позволяет снизить время задержки для этих событий.

Роуминг по событиям между REAPs H на локально коммутируемых WLAN может взять между 50 мс и 1500 мс, которые зависят от задержки глобальной сети (WAN), дизайнов RF и характеристик среды, а также типов безопасности и клиентско-специфичных реализаций роуминга.

Роуминг уровня 3 не поддерживается для локально коммутируемых WLAN, но поддерживается для централизованно коммутируемых WLAN.

NAT/PAT

NAT и PAT не поддерживаются для точек доступа REAP H.

Другие ограничения REAP H

- H REAPs не поддерживают WGB.
- Если вы настроили локально коммутируемый WLAN, то Списки контроля доступа (ACL) не работают и не поддерживаются. На централизованно коммутируемом WLAN поддерживаются ACL.
- Любые изменения к локально коммутируемой конфигурации WLAN на Контроллере вызывают временные потери в подключении, поскольку новая конфигурация применена к REAP H. Также, любые клиенты на них локально коммутированный WLAN временно разъединены. WLAN включен сразу же, и клиенты повторно связываются назад.
- Контроллер может передать пакеты групповой адресации в форме индивидуальной рассылки или пакеты групповой адресации к точке доступа. В режиме ГИБРИДНОГО REAP точка доступа может получить пакеты групповой адресации только в форме индивидуальной рассылки.

Примечание: Если REAP H связан со ссылкой магистрали "802.1q" и существуют локально коммутированные WLAN, настроенные для VLAN, то заказ конфигурации WLAN становится важным из-за ограничения в дизайне. При изменении заказа WLAN, например, WLAN 1 настроен для ssid `wlan-a`, и WLAN 2 настроен для ssid `wlan-b`, и их заказ изменен через конфигурацию WLAN 1, становится ssid `wlan-b`, и WLAN 2 становится ssid `wlan-a`, то оба, WLAN теряют свою VLAN, сопоставляющую, который настроен от WLC.

Примечание: Та же проблема применяется REAP H, который присоединяется к другому контроллеру, который имеет другой заказ тех же WLAN. У основного и вспомогательных контроллеров для гибридной точки доступа REAP должна быть одинаковая конфигурация. В противном случае точка доступа может потерять свою конфигурацию и определенные функции, такие как замена WLAN, VLAN группы точек доступа, статический номер канала, и т.д, не может потенциально работать правильно. Кроме того, удостоверьтесь, что копировали SSID точки доступа REAP H и ее номера индекса на обоих контроллерах.

Отказоустойчивость

H Отказоустойчивость REAP позволяет беспроводному доступу и сервисам переходить клиенты когда:

- H AP Ответвления REAP теряют подключение с главным контроллером.

- H AP Ответвления REAP переключаются вспомогательному контроллеру.
- H AP Ответвления REAP восстанавливают соединение с главным контроллером.

H Отказоустойчивость REAP, наряду с Локальным EAP, как выделено выше, вместе предоставляют нулевое время простоя ответвления во время выхода сети из строя. Эта опция активирована по умолчанию и не может быть отключена. Это не требует никакой конфигурации на контроллере или AP. Однако для обеспечения Отказоустойчивости работает беспрепятственно и применимо, это, критерии должны быть поддержаны:

- Заказ WLAN и конфигурации должны быть идентичными через основного и резервные контроллеры.
- Сопоставление VLAN должно быть идентичным через основного и резервные контроллеры.
- Доменное имя мобильности должно быть идентичным через основного и резервные контроллеры.
- Рекомендуется использовать платформу контроллера и в качестве основного и в качестве резервных контроллеров.

Сводка

- H REAP не разъединит клиентов, когда AP соединяется назад с тем же контроллером, если нет никакого изменения в конфигурации на контроллере.
- H REAP не разъединит клиентов при соединении с резервным контроллером, если нет никакого изменения в конфигурации, и резервный контроллер идентичен главному контроллеру.
- H REAP не перезагрузит его радио при соединении назад с главным контроллером, если нет никакого изменения в конфигурации на контроллере.

Ограничения

- Поддерживаемый только для REAP H с Центральным / Локальной проверки подлинности с Локальным коммутатором.
- Если таймер сеанса клиента истекает перед коммутаторами AP REAP H от Автономного до Связанного режима, централизованно аутентифицированные клиенты требуют полной повторной проверки подлинности.
- Основной и резервные контроллеры должен быть в том же домене мобильности.

Конфигурация H-REAP

Подготовка проводной сети

Первый шаг к развертыванию сети H REAP должен настроить коммутатор, с которым соединится REAP H. Конфигурация коммутатора данного примера включает конфигурацию исходной виртуальной локальной сети (VLAN) (подсеть, на которой REAPs H свяжется с контроллером с CAPWAP), и две подсети, на которых локально переключились данные от клиентов двух лет, WLAN завершатся. Если IP-адресация не предоставляется точкам доступа и клиентам сети WLAN с локальной коммутацией при помощи коммутатора более высокого уровня (как показано ниже), необходимо обеспечить службы DHCP другими способами или настроить статическую адресацию. Cisco рекомендует адресацию DHCP, но некоторые заказчики выбирают статическую адресацию для точек доступа и используют DHC для предоставления адресов беспроводным пользователям. Избыточные конфигурации коммутаторов были удалены из этого примера для простоты.

```
ip dhcp excluded-address 10.10.10.2 10.10.10.99

ip dhcp pool NATIVE
network 10.10.10.0 255.255.255.0
default-router 10.10.10.1
!
ip dhcp pool VLAN11
network 10.10.11.0 255.255.255.0
default-router 10.10.11.1
!
ip dhcp pool VLAN12
network 10.10.12.0 255.255.255.0
default-router 10.10.12.1
!
interface FastEthernet1/0/1
description H REAP Example Config
switchport trunk encapsulation dot1q
switchport trunk native vlan 10
switchport trunk allowed vlan 10,11,12
switchport mode trunk
!
interface Vlan10
ip address 10.10.10.1 255.255.255.0
!
interface Vlan11
ip address 10.10.11.1 255.255.255.0
!
interface Vlan12
ip address 10.10.12.1 255.255.255.0
end
```

Примечание: Фактическая IP-адресация в данном примере и всех последующих конфигурациях просто для пояснительных целей. Поэтому IP-адресацию НЕОБХОДИМО планировать для каждой отдельной сети с учетом ее потребностей.

В этом примере конфигурации точка доступа H-REAP подключена к первому интерфейсу FastEthernet и получает IP-адрес с помощью DHCP на коммутаторе стандартной сети VLAN (VLAN 10). Ненужные сети VLAN удаляются из магистрального канала, подключенного к H-REAP, чтобы уменьшить объем обработки внешних пакетов. Сети VLAN 11 и 12 подготовлены для предоставления IP-адресации клиентам двух сетей WLAN, которые с ними связаны.

Примечание: Коммутатор, к которому REAPs H подключает потребности восходящее подключение с инфраструктурой маршрутизации. H оптимальные методы REAP диктуют, что remote-site/WAN инфраструктура маршрутизации располагает по приоритетам контроль за CAPWAP (порт 5246 UDP).

Вот пример конфигурации вышестоящего маршрутизатора, где AP REAP H был связан для расположения по приоритетам трафика CAPWAP.

```
ip cef
!
frame-relay switching
!
class-map match-all 1
  match access-group 199
!
policy-map mypolicy
  class 1
   bandwidth 256
!
```

```
interface Serial0/0
ip address 10.1.0.2 255.255.255.0
encapsulation frame-relay
frame-relay interface-dlci 101
frame-relay intf-type dce
service-policy output mypolicy
!
access list 199 permit udp any any eq 5246
```

Обнаружение контроллера H-REAP с помощью команд CLI

H REAPs обычно обнаружит восходящие контроллеры через параметр DHCP 43 или Разрешение DNS. Если ни один из этих методов недоступен, желательно предоставить администраторам удаленных узлов подробные инструкции по настройке всех точек доступа H-REAP на использование IP-адреса контроллера, к которому они будут подключаться. Кроме того, можно настроить IP-адресацию H-REAP вручную (необязательно), если использование DHCP недоступно или нежелательно.

В этом примере приводятся сведения о том, как настроить IP-адрес H-REAP, имя хоста и IP-адрес контроллера с помощью порта консоли точки доступа.

```
AP_CLI#capwap ap hostname ap1130 ap1130#capwap ap ip address 10.10.10.51 255.255.255.0
ap1130#capwap ap ip default-gateway 10.10.10.1 ap1130#capwap ap controller ip address
172.17.2.172
```

Примечание: Точки доступа должны выполнить поддерживающий LWAPP IOS® Recovery Image Cisco IOS Software Release 12.3 (11) JX1 или позже для поддержки этих команд CLI из коробки. В точках доступа с префиксом SKU, равным LAP, например, AIR-LAP-1131AG-A-K9, поставленные начиная с 13 июня 2006 года, работает ПО Cisco IOS начиная с версии 12.3(11)JX1. Эти команды доступны любой точке доступа, которая отправляет от изготовителя, выполняющего этот уровень кода, обновила код вручную к этому уровню или обновлена автоматически путем соединения с рабочей версией 6.0 контроллера или позже.

Эти команды конфигурации принимаются только когда точка доступа находится в автономном режиме.

Точки доступа, которые раньше не подключались к контроллеру, будут иметь стандартный пароль CLI компании Cisco. После того, как точки доступа подключаются к контроллеру, изменение конфигурации CLI будет недоступно, пока пароль консоли не будет изменен. Эта команда поддерживается только интерфейсом CLI и имеет следующий синтаксис:

```
(WLC_CLI)>config ap username <user-id> password <passwd> {all | <AP name>}
```

Для точки доступа, описанной выше, можно использовать следующую команду:

```
(WLC_CLI)>config ap username admin password pass ap1130
```

Примечание: Несмотря на то, что эта команда требует создания имени пользователя, это поле в настоящее время не внедрено и зарезервировано для дальнейшего использования.

Примечание: Все **показывают**, и **команды отладки** будут работать прекрасный без изменяемых паролей по умолчанию точки доступа.

Конфигурация контроллера H-REAP

Как только REAP H обнаружил и присоединился к контроллеру, все конфигурации REAP H реализованы через сеть или интерфейсы командной строки контроллера (альтернативно, конфигурация может быть реализована централизованно через Беспроводную систему

управления [WCS]). Действия по настройке H-REAP, описанные в этом разделе, выполняются с помощью графического интерфейса контроллера.

Начните с создания и настройки необходимых сетей WLAN. *В этом примере сети WLAN имеют следующую конфигурацию (при необходимости конфигурация может быть изменена в соответствии с потребностями среды):*

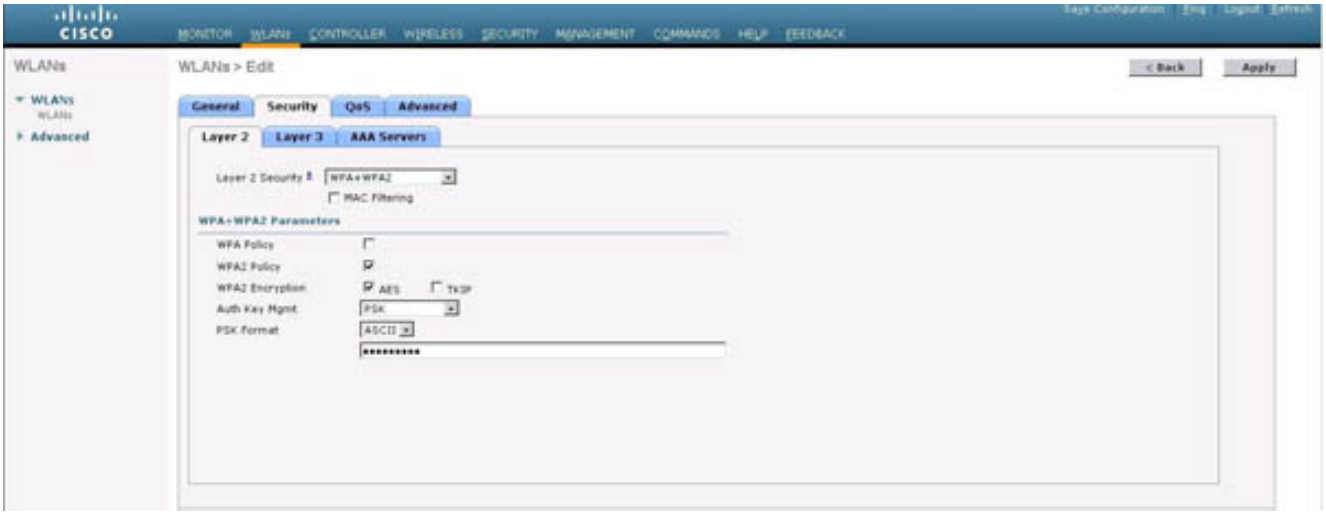
SSID WLAN	Безопасность	Коммутация
Корпоративный	WPA2 (802.1X)	ЛОКАЛЬНЫЙ
Удаленный сайт	WPA2 - PSK	ЛОКАЛЬНЫЙ
Гость	WebAuth	Центральный

Для точки доступа REAP H для работы в качестве REAP H контроллер, с которым это связано, должен иметь по крайней мере один локально коммутируемый WLAN (без этого, H функциональность высокой доступности REAP не будет понят).

Для настройки сети WLAN с локальной коммутацией выполните следующие действия:

1. Перейдите к главной странице контроллера, выберите **WLAN** и нажмите **New**.
2. Назначьте WLAN название, которое также используется в качестве SSID, и нажмите **Apply**.

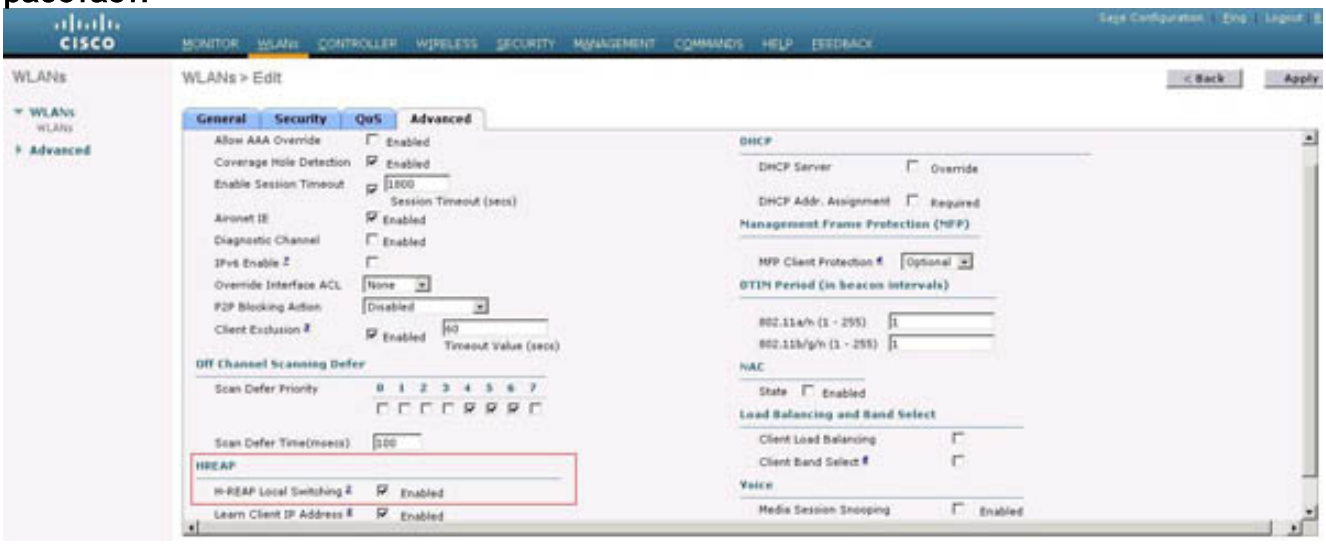
3. В WLAN> страница Edit, нажмите **Вкладку Безопасность**. Под безопасностью уровня 2 выберите тип безопасности.В этом примере предпочтительным вариантом будет WPA2-PSK. Выберите **WPA+WPA2**.



4. Проверьте **Политику WPA2** для определения использования WPA WLAN.
5. **Установите флажок AES, чтобы задать метод шифрования.**
6. **В окне "Auth Key Mgmt", выберите PSK в раскрывающемся меню.**В зависимости от желаемого формата ключа выбор здесь зависит от простоты использования и поддержки клиентов, выберите или **ASCII** или **hex**. Ascii, как правило, проще, так как поддерживает буквенно-цифровые символы. Выберите **ASCII** и введите желаемый

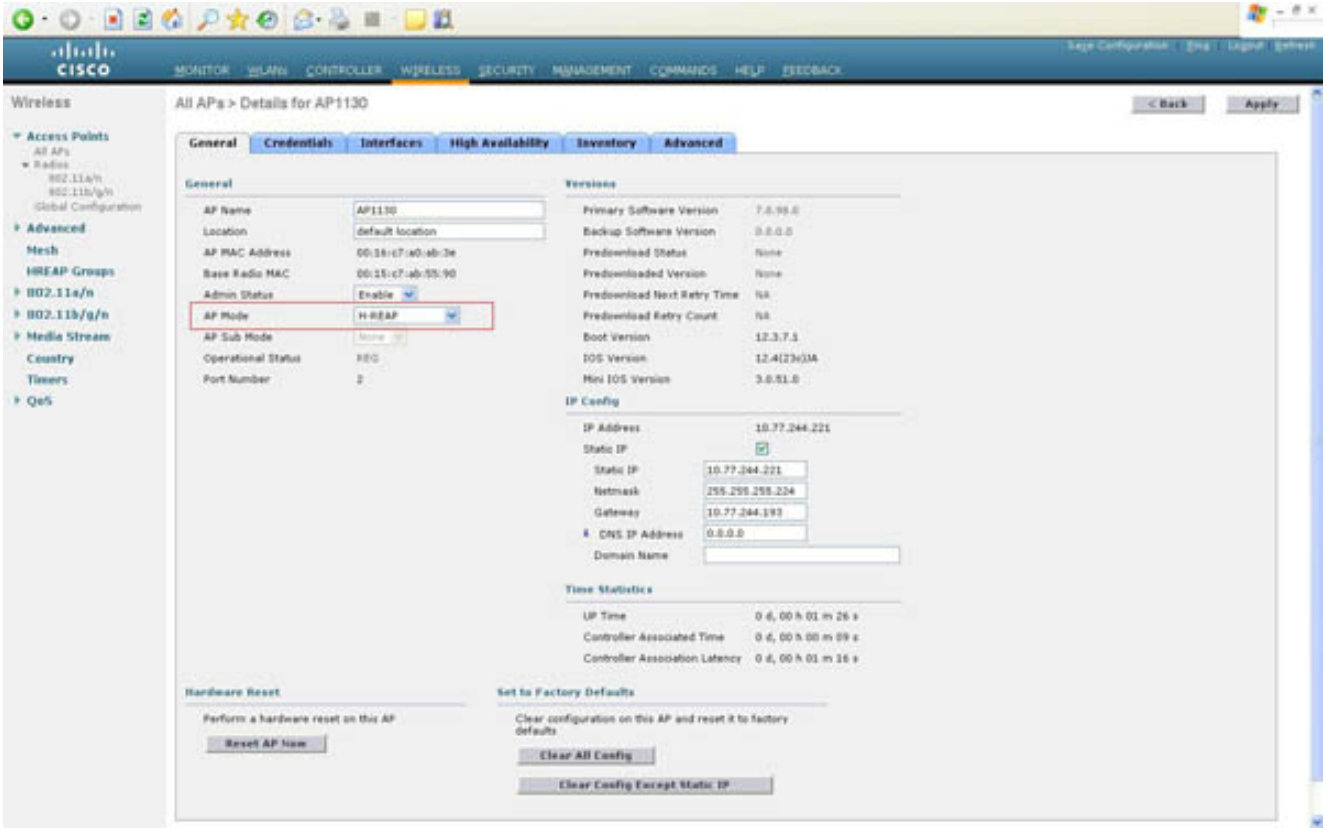
предварительный общий ключ.

7. **Щелкните вкладку Advanced ("Дополнительно"). Установите флажок H-REAP Local Switching и убедитесь, что сеть WLAN работает.**

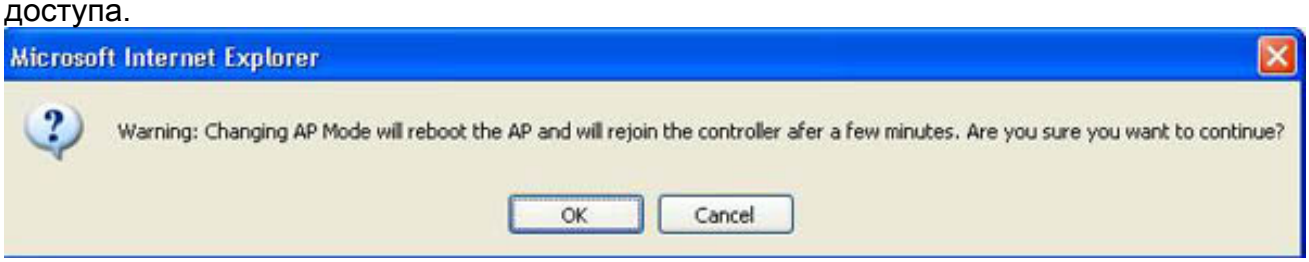


Без этого действия WLAN не позволит выполнять локальное завершение данных в точках доступа H-REAP или даже не предложит этой возможности (если точка доступа находится в автономном режиме).**Примечание:** Точки доступа, не настроенные для работы в режиме REAP H, игнорируют значение Локального коммутатора REAP H, и весь трафик клиента туннелирован назад к контроллеру.По окончании установки сети H-REAP WLAN, можно настроить точки доступа на работу в режиме H-REAP.

8. **После того, как точки доступа обнаружат контроллер и подключатся к нему, откройте раздел "Wireless" веб-интерфейса контроллера и нажмите Detail рядом с выбранной точкой доступа.**
9. **В раскрывающемся меню "AP Mode" выберите H-REAP, чтобы перевести точку доступа из режима по умолчанию (local) в режим H-REAP.**

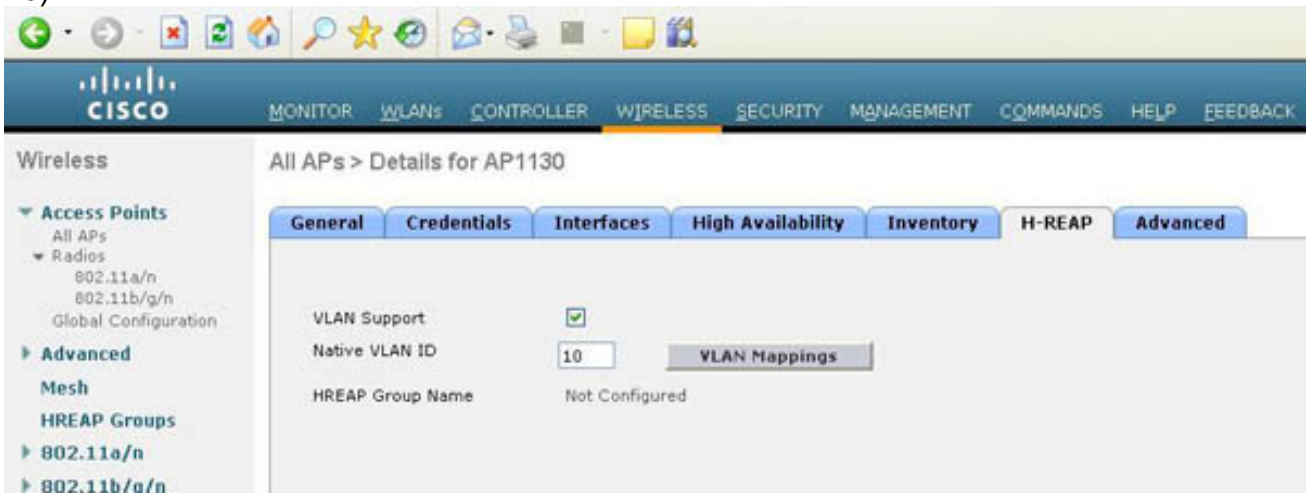


10. **Щелкните "Применить".** Для применения изменений конфигурации необходимо перезагрузить точку
доступа.

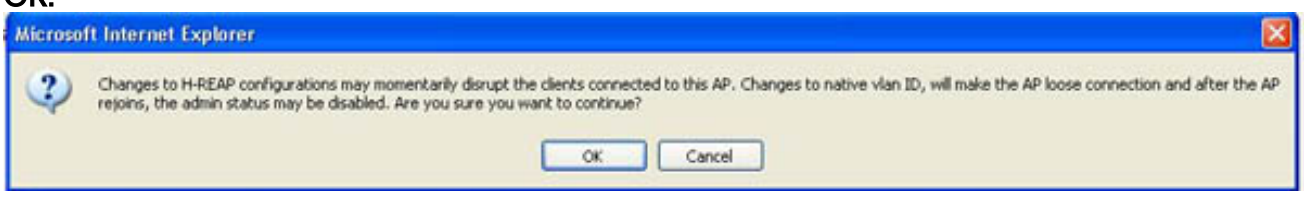


Точка доступа перезагрузится, а затем повторно обнаружит контроллер и подключится к нему.

11. Возвратитесь к **беспроводному** заголовку графического интерфейса контроллера и выберите ту же **Подробную** ссылку точки доступа, как сделано прежде.По умолчанию точка доступа H-REAP не настроена на использование магистрального канала. Хотя порт коммутатора, с которым это связано, может быть установлен в магистральную линию, точка доступа все еще связывается с контроллером по собственному VLAN. Если порт коммутатора работает в режиме магистрального канала и необходимо, чтобы точка доступа H-REAP работала в том же режиме, необходимо включить поддержку VLAN.
12. Нажмите вкладку **H REAP**. **Установите флажок VLAN Support.**
13. На основе конфигурации порта коммутатора, с которым связан REAP H, введите Номер ID Собственного VLAN точки доступа рядом с заголовком с тем же названием (в данном примере, VLAN
10).



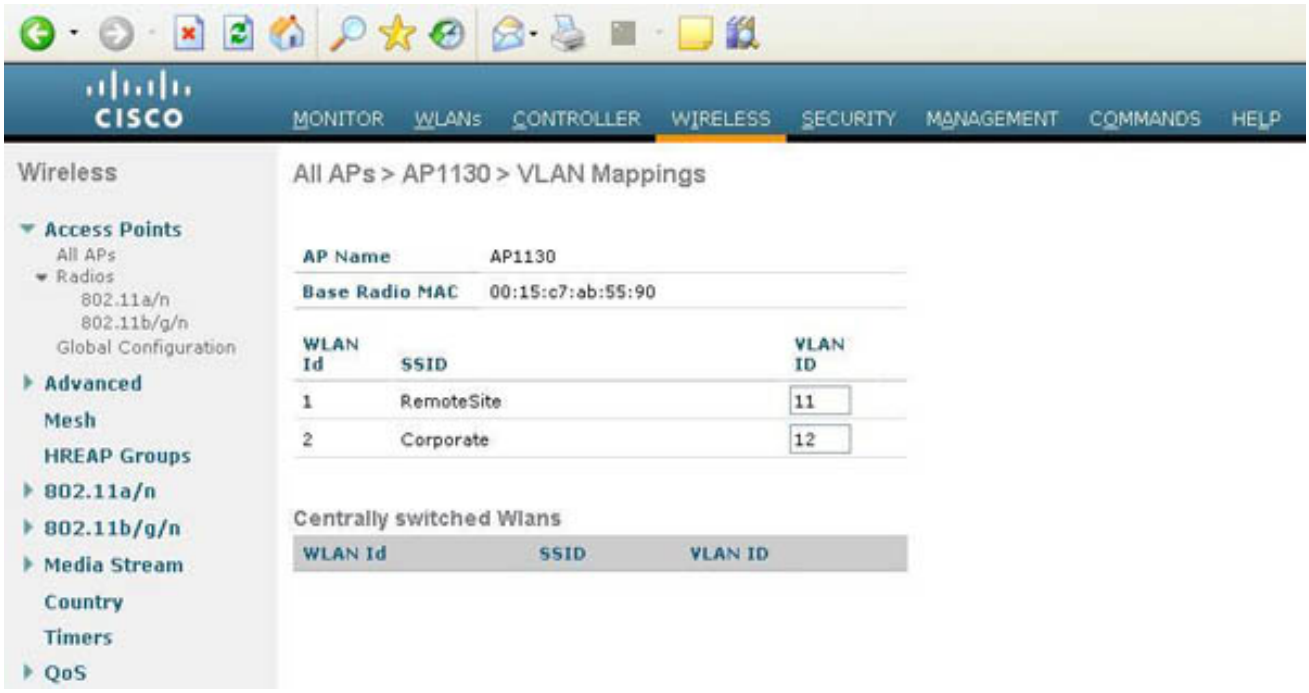
14. Нажмите **Apply** для предписания изменений.Поскольку REAP H перезагружает конфигурацию его Порта Ethernet на основе данных параметров конфигурации, точка доступа может кратко потерять подключение с контроллером. Всплывающее окно предупредит о такой возможности. **Нажмите кнопку**
OK.



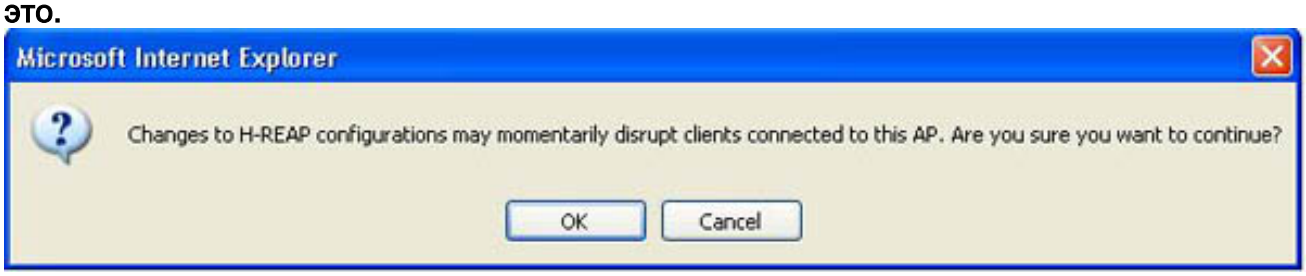
Примечание: Как всплывающее окно, предупреждающее, указывает, существует невысокая вероятность, точка доступа воссоединится с контроллером в Отключенном состоянии. Повторный выбор, что **Подробные данные** точки доступа связываются от

беспроводного заголовка контроллера. **Затем выберите значение Enable для параметра "Admin Status".** Примените параметры и продолжите настройку.

15. Введите страницу Detail желаемой точки доступа, выберите метку REAP H снова и нажмите **VLAN Mapping** для настройки маркировки 802.1Q на локально коммутируемый
WLAN.



16. Установите VLAN на локально коммутируемый WLAN, на котором должен быть завершен трафик клиента.**Примечание:** WLAN, не настроенные для поддержки Локального коммутатора REAP H, не позволяют метке 802.1Q быть настроенной здесь. Конфигурация VLAN для этих WLAN установлена в глобальных параметрах контроллера, потому что данные клиента туннелированы назад к контроллеру для завершения.**Примечание:** Локально коммутированные WLAN могут все совместно использовать тот же ИДЕНТИФИКАТОР VLAN или могут иметь дискретные присвоения. Здесь нет никаких ограничений, если назначенный VLAN присутствует в порте коммутатора REAP H.
17. Нажмите **Apply** для сохранения изменений.В то время как сопоставление VLAN/WLAN изменено, услуга беспроводной локальной сети разрушена на мгновение. **Нажмите OK, чтобы подтвердить
это.**



Необходимые WLAN созданы и настроены, набор точек доступа для работы в режиме REAP H, поддержка VLAN включила, и VLAN, настроенные на локально коммутируемый WLAN. Предоставленные сервисы DHCP доступны на каждой VLAN, клиенты должны быть в состоянии соединиться с каждым WLAN, получить адреса на их соответствующих виртуальных локальных сетях (VLAN) и трафик прохода. Настройка H-REAP завершена.

Устранение неполадок H-REAP

Существует несколько общих сценариев и ситуаций, в которых процессы настройки H-REAP и подключения клиентов могут быть нарушены. Этот раздел предоставляет нескольким таким ситуациям с их предложенными средствами.

Точка доступа H-REAP не подключается к контроллеру

Это может произойти по нескольким причинам. Первым делом проверьте следующее:

- **Для каждой точки доступа H-REAP необходимо обеспечить корректную IP-адресацию.**Если DHCP используется через консоль точки доступа, проверьте, что точка доступа получает адрес.`AP_CLI#show dhcp lease` Если статическая адресация используется через консоль точки доступа, проверьте, чтобы удостовериться, что применена корректная IP-адресация.`AP_CLI#show capwap ip config`
- **Убедитесь, что точка доступа имеет соединение с IP-сетью и получает ответ на эхо-запрос, отправленный в управляющий интерфейс контроллера.**Как только IP-адресация проверена, проверьте, чтобы удостовериться, что точка доступа может связаться с контроллером путем прозванивания управления IP-адресами контроллера. Используйте **команду ping** через консоль точки доступа с этим синтаксисом:`AP_CLI#ping <WLC management IP address>` Если это не успешно, гарантируйте, что восходящая сеть должным образом настроена, и тот Доступ через WAN назад к корпоративной сети доступен. Убедитесь, что контроллер работает и не находится внутри границ NAT/PAT. Гарантируйте, что порты 5246 и 5247 UDP открыты на любых посреднических межсетевых экранах. Отправьте эхо-запрос с контроллера в точку доступа, используя тот же синтаксис.
- **Проверьте, что существует подключение CAPWAP между точкой доступа и контроллером.**Однажды возможность подключения с помощью IP-адреса между REAP H и контроллером проверен, выполните отладки CAPWAP на контроллере, чтобы подтвердить, что сообщения CAPWAP 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 единой точке доступа.`AP_CLI#debug mac addr <AP's wired MAC address>` После того, как набор для ограничения выходных данных отладки включите отладку CAPWAP.`AP_CLI#debug capwap events enable` Если никакие сообщения отладки CAPWAP не замечены, гарантируют, что REAP H имеет по крайней мере один метод, которым может быть обнаружен контроллер. Если такие методы доступны (например, параметр DHCP 43 или DNS), убедитесь, что они настроены должным образом. Если никакой другой метод обнаружения не существует, гарантируйте, что IP-адрес контроллера введен в точку доступа через консольный CLI.`AP_CLI#capwap ap controller ip address <WLC management IP address>`
- **Проверьте операции CAPWAP и на контроллере и на REAP H.**Если, по крайней мере, одиночный метод обнаружения контроллера доступен REAP H, проверьте, что сообщения CAPWAP передаются с точки доступа на контроллер. Эта команда уже выполнена по умолчанию.`AP_CLI#debug capwap client errors` Дополнительная информация, о котором контроллерах точка доступа связывается с, может быть замечена IP-адресами сообщения UDP, которое это передает. Просмотрите адреса источника и назначения каждого пакета, который пересекает стек IP точки доступа.`AP_CLI#debug ip udp` Если кажется от консоли точки доступа, что это связывается с контроллером, возможно, что это присоединилось к другому контроллеру в кластере. Чтобы убедиться, что точка доступа H-REAP подключена к контроллеру, используйте

следующую команду.`AP_CLI#show capwap reap status`

- **Убедитесь, что точка доступа подключилась к верному контроллеру.**Если другие IP-адреса контроллера вручены точке доступа во время фазы обнаружения, REAP H мог присоединиться к другому контроллеру. Убедитесь, что IP-адрес, предоставленный механизмами обнаружения, верен. Определите, к какому контроллеру подключена точка доступа.`AP_CLI#show capwap reap status` Войдите в тот веб-GUI контроллера. Гарантируйте всего IP, и MAC-адреса контроллеров введены в Список Мобильности контроллера и что они все совместно используют то же Название Группы мобильности. Затем заставьте основного точки доступа, вторичного, и третичные контроллеры диктовать, к какому контроллеру точка доступа присоединяется. Это сделано посредством Подробной ссылки точки доступа. Если проблема не исчезает при подключении точки доступа H-REAP к другому контроллеру, ее можно решить с помощью управления точками доступа в масштабах системы, которые предлагает WCS.
- **Устраните проблемы сертификата, если точка доступа пытается подключится к контроллеру, но ей это не удается.**Если сообщения CAPWAP замечены на контроллере, но точка доступа не в состоянии присоединяться, это, вероятно - проблема сертификата..

Команды консоли H-REAP не работают или возвращают ошибки

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

- Точки доступа H-REAP, которые находятся в подключенном режиме, не позволяют изменять или сбрасывать конфигурации с консоли. Когда точка доступа находится в этом состоянии, конфигурирование необходимо выполнять из интерфейса контроллера. Если необходим доступ к командам конфигурации из точки доступа, убедитесь, что точка доступа находится в автономном режиме перед тем, как вводить команды конфигурации.
- Как только точка доступа подключается к контроллеру (даже если H-REAP переходит обратно в автономный режим), консоль точки доступа не позволяет вводить команды конфигурации, пока не будет задан новый пароль. Необходимо изменить все пароли H-REAP. Это можно сделать только с помощью интерфейса командной строки контроллера, к которому подключена точка доступа. Синтаксис этой команды можно использовать на контроллере для установки паролей консоли на отдельных точках доступа или для задания одного пароля для всех точек доступа:`(WLC_CLI)>config ap username <user-id> password <passwd> {all | <AP name>}` **Примечание:** Для точки доступа, которой не установили ее пароли консоли, знать, что эта конфигурация только передается точке доступа в точке, команда введена в контроллер. Все точки доступа, которые будут подключаться к контроллеру в дальнейшем, потребуют повторного ввода команды.Даже после того, как на точке доступа будет задан пользовательский пароль и она будет переведена в автономный режим, она не будет разрешать доступ к этим командам. Чтобы внести изменения в конфигурацию точки доступа H-REAP, необходимо удалить существующие конфигурации статических IP-адресов и IP-адрес контроллера. Эту конфигурацию называют Частной Конфигурацией CAPWAP и должны будут удалить, прежде чем любые новые команды CLI точки доступа могут быть вводом. Для этого введите следующую команду:`AP_CLI#clear capwap private-config`

Примечание: Также AP может быть возвращен к заводским настройкам, в то время как он соединен с контроллером. Нажмите **кнопку Clear Config** на подробной странице AP под заголовком беспроводных сетей в GUI WLC. Конфигурация AP вытерта, и она перезагружена.**Примечание:** Все **показывают**, и **команды отладки** продолжат работать даже без устанавливаемого пароля ня по умолчанию и с AP в Связанном режиме.Только на этом этапе могут любые конфигурации CAPWAP быть сделанными.

Клиенты не могут подключиться к точке доступа H-REAP

Выполните следующие действия:

1. Убедитесь, что точка доступа правильно подключена к контроллеру, у контроллера есть хотя бы одна настроенная и включенная сеть WLAN, и что точка доступа H-REAP находится в состоянии "Enabled".
2. На стороне клиента, убедитесь, что идентификатор SSID сети WLAN доступен (настройка сети WLAN на контроллере на широковещательную рассылку SSID может помочь в процессе устранения неполадок). Выполните зеркальное копирование конфигурации безопасности WLAN на клиент. Конфигурация безопасности на стороне клиента — основная причина большинства проблем с подключением.
3. Убедитесь, что для клиентов в сетях WLAN с локальной коммутацией обеспечена корректная IP-адресация. Если используются службы DHCP, убедитесь, что DHCP-сервер более высокого уровня корректно настроен для предоставления адресов клиентам. Если используется статическая IP-адресация, убедитесь что клиенты правильно настроены и находятся в нужной подсети.
4. Чтобы продолжить устранение неполадок клиентских подключений, введите следующую команду через порт консоли H-REAP.AP_CLI#**show capwap reap association**
5. Чтобы продолжить устранение неполадок клиентских подключений и ограничить выходные данные отладки, используйте следующую команду.AP_CLI#**debug mac addr <client's MAC address>**
6. Для отладки подключений клиента, основанных на протоколе 802.11, используйте следующую команду.AP_CLI#**debug dot11 state enable**
7. Отладка процесса аутентификации 802.1X и его ошибок выполняется с помощью следующей команды.AP_CLI#**debug dot1x events enable**
8. КОНТРОЛЛЕР/СООБЩЕНИЯ RADIUS бэкэнда может быть отлажен с помощью этой команды.AP_CLI#**debug aaa events enable**
9. Или, чтобы запустить полный набор команд отладки клиентов, введите следующую команду.AP_CLI#**debug client <client's MAC address>**

H-REAP КАС

Вопрос. . Если я настраиваю LAP в удаленном местоположении как H REAPs, я могу дать тем LAP основной и дополнительный контроллер?

Пример: Существует главный контроллер на узле A и вспомогательный контроллер на узле B.

Если контроллер на узле сбои, LAP делает аварийное переключение к контроллеру на узле B. Если оба контроллера недоступны, LAP попадает в автономный режим REAP H?

О. Да. Сначала LAP переключается при отказе к своему вторичному устройству. Все WLAN, которые локально коммутированы, не имеют никаких изменений и всего, что централизованно коммутировано, просто имеют трафик, переходят к новому контроллеру. И, если вторичное устройство отказывает, все WLAN, которые отмечены для локального коммутатора (и открытый опознавательные/вы / опознавательные/вы предварительный общий ключ делают средство проверки подлинности AP) остаются.

Вопрос. . Как делают точки доступа, настроенные в **Автономном режиме**, имеют дело с WLAN, настроенными с Локальным коммутатором REAP H?

О. Точки доступа автономного режима рассматривают эти WLAN как обычные WLAN. Аутентификация и трафик данных туннелированы назад к WLC. Во время сбоя соединений WAN этот WLAN полностью не работает, и никакие клиенты не активны на этом WLAN, пока не восстановлено соединение с WLC.

Вопрос. . Я могу сделать web-аутентификацию с Локальным коммутатором?

Да, вы можете иметь SSID с включенной web-аутентификацией и отбросить трафик локально после web-аутентификации. Web-аутентификация с Локальным коммутатором хорошо работает.

Вопрос. . Я могу использовать свой Гостевой Портал на Контроллере для SSID, который обрабатывается локально REAP H? Если да, что происходит, если я теряю подключение контроллеру? Текущие клиенты сразу понижаются?

Да. Так как этот WLAN локально коммутирован, WLAN доступен, но никакие новые клиенты не в состоянии аутентифицироваться, поскольку веб-страница не доступна. Однако существующие клиенты не понижены.

Дополнительные сведения

- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 4.0
- Обновление программного обеспечения контроллера беспроводной локальной сети
- Wireless LAN Controller (WLC) Troubleshoot FAQ
- Поддержка технологии WLAN
- Пример конфигурации режимов работы H-REAP
- Поиск и устранение простых неисправностей Hybrid Remote Edge Access Point (H-REAP)
- Примеры конфигурации и технические примечания контроллера беспроводной локальной сети
- Часто задаваемые вопросы по системным сообщениям и сообщениям об ошибках контроллера беспроводной LAN (WLC)
- Системные сообщения и сообщения об ошибках Wireless Control System (WCS)
- Cisco Systems – техническая поддержка и документация