Часто задаваемые вопросы по функциям и системе контроллера беспроводной LAN (WLC)

ID документа: 118833

Обновлено : 02 марта 2015

Родственные продукты

- Контроллеры беспроводных LAN серии Cisco 4400
- Контроллеры беспроводной локальной сети Cisco серии 5500
- Сервисный модуль беспроводной сети Cisco 2 (WiSM2)
- Контроллеры беспроводной сети Cisco серии 2500
- Cisco 2100 Series Wireless LAN Controllers
- Cisco Catalyst 3750 Series Integrated Wireless LAN Controllers
- Модуль беспроводных сервисов (WiSM) Cisco Catalyst серии 6500/7600
- Контроллеры беспроводных LAN серии Cisco 2000
- Cisco Wireless LAN Controller Module
- Cisco 4100 Series Wireless LAN Controllers
- + Покажите больше

Содержание

Введение

В этом документе рассмотрены наиболее часто задаваемые вопросы о технических аспектах и доступных функциях контроллера беспроводных локальных сетей (WLC).

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

Вопросы проектирования

Вопрос. . Как я настраиваю коммутатор для соединения с WLC?

О. Настройте порт коммутатора, с которым WLC связан как магистральный порт IEEE 802.1Q. Удостоверьтесь, что только необходимые VLAN позволены на коммутаторе. Обычно, управление и Интерфейс менеджера точки доступа WLC оставляют без меток. Это означает, что они принимают собственный VLAN связанного коммутатора. Это не необходимо. Можно назначить отдельную VLAN на эти интерфейсы. Для получения дополнительной информации обратитесь к *Настраиванию Коммутатора для* раздела *WLC* Примера Базовой конфигурации Контроллера беспроводной локальной сети и Облегченной точки доступа.

Вопрос. . Весь сетевой трафик от и до клиента WLAN туннелируют через Контроллер беспроводной локальной сети (WLC), как только точка доступа (AP) зарегистрирована в контроллере?

О. Когда AP присоединяется к WLC, Контролю и Инициализации протокола Точек беспроводного доступа (CAPWAP), туннель сформирован между этими двумя устройствами. Весь трафик, который включает весь трафик клиента, передается через туннель CAPWAP.

Когда AP находится в режиме ГИБРИДНОГО REAP, единственное исключение из этого. Когда их соединение с контроллером потеряно, точки доступа ГИБРИДНОГО REAP могут коммутировать трафик данных клиента локально и выполнить аутентификацию клиента локально. Когда они связаны с контроллером, они могут также передать трафик обратно в контроллер.

Вопрос. . Я могу установить Облегченные точки доступа (LAP) в удаленном офисе и установить контроллер беспроводной локальной сети Cisco (WLC) в моем главном офисе? LWAPP/CAPWAP перерабатывает глобальную сеть (WAN)?

О. Да, можно организовать работу контроллеров WLC по территориальной сети WAN через точки доступа. Когда LAP настроены в Удаленном Граничном AP (REAP) или Гибридном Удаленном Граничном AP (H-REAP) режим, LWAPP/CAPWAP перерабатывает глобальную сеть (WAN). Любой из этих режимов позволяет контроль AP удаленным контроллером, который подключен через канал WAN. Трафик перебрасывается на канал LAN локально, что позволяет избежать необязательной отправки локального трафика по каналу WAN. Это, очевидно, одно из важнейших преимуществ, которые дает размещение WLC в беспроводной сети.

Примечание: Не все Легковесные AP поддерживают эти режимы. Например, режим H-REAP поддерживается только в 1131, 1140,1242, 1250, и LAP AP801. Режим REAP поддерживается только в 1030 AP, но 1010 и 1020 AP не поддерживают REAP. Прежде чем вы запланируете внедрить эти режимы, проверьте, чтобы определить, поддерживают ли LAP его. AP Программного обеспечения Cisco IOS (Автономные AP), которые были преобразованы в LWAPP, не поддерживают REAP.

Вопрос. . Как делают REAP и режимы H-REAP работают?

O. В режиме **REAP**, всем контроле и трафике управления, который включает трафик аутентификации, туннелирован назад к WLC. Но весь трафик данных коммутирован локально в удаленной офисной LAN. Когда соединение с WLC потеряно, все WLAN завершены кроме первого WLAN (WLAN1). Все клиенты, которые в настоящее время привязываются к этому WLAN, сохранены. Чтобы позволить новым клиентам успешно аутентифицировать и получать сервис на этом WLAN в течение времени простоя, настраивать метод аутентификации для этого WLAN или как WEP или как WPA-PSK так, чтобы аутентификация была сделана локально в REAP. Для получения дополнительной информации о развертываниях REAP, обратитесь к Руководству по развертыванию REAP в Филиале компании.

В режиме **H-REAP** точка доступа туннелирует контроль и трафик управления, который включает трафик аутентификации, назад к WLC. Трафик данных от WLAN соединен локально в удаленном офисе, если WLAN настроен с локальным коммутатором H-REAP, или трафик данных передают обратно в WLC. Когда соединение с WLC потеряно, все WLAN завершены кроме первых восьми WLAN, настроенных с локальным коммутатором H-REAP. Все клиенты, которые в настоящее время привязываются к этим WLAN, сохранены. Чтобы позволить новым клиентам успешно аутентифицировать и получать сервис на этих WLAN в течение времени простоя, настраивать метод аутентификации для этого WLAN или как WEP, PSK WPA или как PSK WPA2 так, чтобы аутентификация была сделана локально в H-REAP.

Для получения дополнительной информации о H-REAP, обратитесь к Дизайну H-REAP и Руководству по развертыванию.

Вопрос. . Каково различие между AP Удаленного Края (REAP) и Гибридным REAP (H-REAP)?

O. REAP не поддерживает маркирование VLAN IEEE 802.1Q. Также, это не поддерживает несколько интерфейсов VLAN. Трафик от всех идентификаторов наборов сервисов (SSID) завершается в той же подсети, но H-REAP поддерживает маркирование VLAN IEEE 802.1Q. Трафик от каждого SSID может быть сегментирован к уникальной VLAN.

Когда подключение к WLC потеряно, т.е. в Автономном режиме, REAP служит только одному WLAN, т.е. Первому WLAN. Все другие WLAN деактивированы. В H-REAP до 8 WLAN поддерживаются в течение времени простоя.

Другое основное различие - то, что в режиме REAP трафик данных может только быть соединен локально. Это не может быть коммутировано назад к центральной ATC, но, в режиме H-REAP, у вас есть опция для коммутации трафика назад к центральной ATC. Трафик от WLAN, настроенных с локальным коммутатором H-REAP, коммутирован локально. Трафик данных от других WLAN коммутирован назад к центральной ATC.

Дополнительную информацию по REAP см. в разделе Пример конфигурации Remote-Edge AP (REAP) с облегченными точками доступа и контроллерами беспроводных ЛВС.

Дополнительную информацию по H-REAP см. в разделе Конфигурация Hybrid REAP.

Вопрос. . Сколько WLAN поддерживается на WLC?

O. Начиная с версии программного обеспечения 5.2.157.0 WLC может теперь управлять до 512 WLAN для облегченных точек доступа. Каждый WLAN имеет отдельный

ИДЕНТИФИКАТОР WLAN (1 - 512), отдельное имя профиля и SSID WLAN, и может быть назначен уникальная политика безопасности. Контроллер публикует до 16 WLAN в каждой связанной точке доступа, но можно создать до 512 WLAN на контроллере и затем выборочно публиковать эти WLAN (использующий группы точек доступа) к другим точкам доступа для лучше управления беспроводной сетью.

Примечание: Cisco 2106, 2112 и 2125 контроллеров поддерживают только до 16 WLAN.

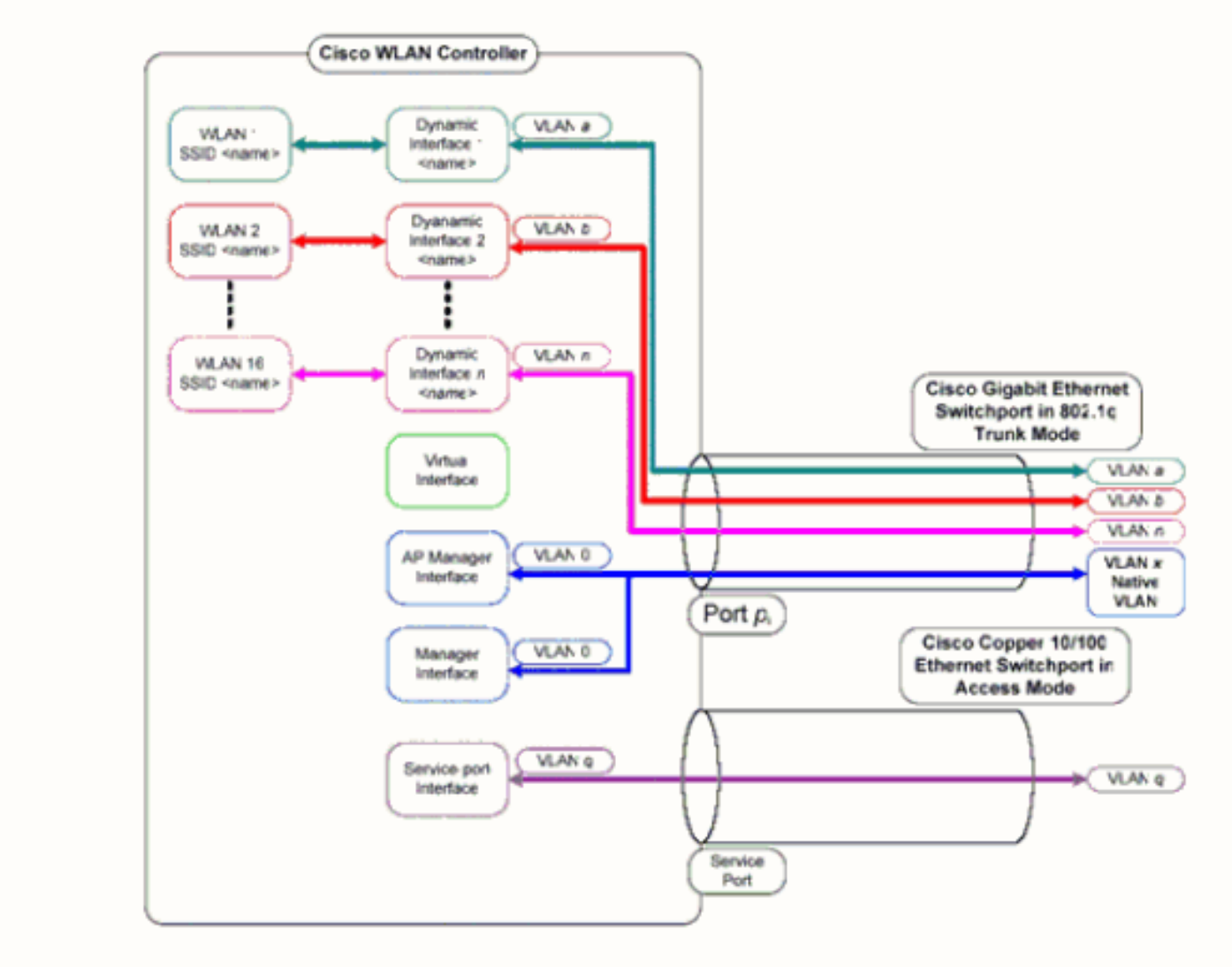
Примечание: Для получения дальнейшей информации на рекомендациях для настройки WLAN на WLC, считайте раздел WLAN Создания руководства по конфигурированию контроллера Cisco Wireless LAN, Выпуска 7.0.116.0.

Вопрос. . Как я могу настроить VLAN на своем Контроллере беспроводной локальной сети (WLC)?

O. В WLC VLAN связаны к интерфейсу, настроенному в уникальной IP - подсети. Этот интерфейс сопоставлен на WLAN. Затем клиенты, которые связываются к этому WLAN, принадлежат VLAN интерфейса и назначены IP-адрес от подсети, до которой принадлежит интерфейс. Чтобы настроить сети VLAN на контроллере беспроводной ЛВС, выполните процедуру в разделе Пример конфигурации сетей VLAN на контроллере беспроводной ЛВС.

Вопрос. . Настроены две беспроводные локальные сети с двумя разными динамическими интерфейсами. Каждый интерфейс имеет свою собственную сеть VLAN, которая отличается от сети VLAN интерфейса управления. Такая сеть работает, но не настроены магистральные порты для включения сетей VLAN, которые используют беспроводные сети. Помечает ли AP пакеты метками VLAN интерфейса управления?

O. AP не помечает пакеты с VLAN интерфейса управления. AP инкапсулирует пакеты от клиентов в Протоколе Lightweight AP Protocol (LWAPP)/CAPWAP, и затем передает пакеты на WLC. WLC тогда разделяет заголовок LWAPP/CAPWAP и передает пакеты к шлюзу с соответствующим тегом VLAN. Метка VLAN зависит от WLAN, к которой относится клиент. WLC зависит от шлюза для маршрутизации пакетов к их назначению. Чтобы передавать трафик нескольким сетям VLAN, необходимо сделать вышестоящий коммутатор магистральным портом. Данная диаграмма поясняет то, как сети VLAN работают с контроллерами:



Вопрос. . Какой IP-адрес WLC используется для аутентификации с AAA-сервером?

O. WLC использует IP-адрес интерфейса управления для любого механизма аутентификации (Уровень 2 или Уровень 3), который включает AAA-сервер. Для получения дополнительной информации о портах и интерфейсах на WLC, обратитесь к разделу *портов и Интерфейсов Настройки* руководства по конфигурированию контроллера Cisco Wireless LAN, Выпуска 7.0.116.0.

Вопрос. . В наличии имеются десять облегченных точек доступа Cisco серии 1000 (Lightweight Access Points, LAP) и два контроллера беспроводной ЛВС (Wireless LAN Controllers, WLC) в одной и той же сети VLAN. Как зарегистрировать шесть точек LAP на контроллере WLC1, а другие четыре точки LAP на контроллере WLC2?

O. LWAPP/CAPWAP обеспечивает динамическое резервирование и распределение нагрузки. Например, при определении нескольких IP-адресов для опции 43 LAP передает запросы на обнаружение LWAPP/CAPWAP к каждому из IP-адресов, которые получает AP. В WLC ответ обнаружения LWAPP/CAPWAP WLC встраивает эту информацию:

- Сведения о текущей нагрузке LAP, которая определяется как число LAP, одновременно присоединившихся к WLC

- Емкость LAP
- Число беспроводных клиентов, подключенных к WLC

Затем LAP пытается присоединиться к наименее загруженному WLC, которым является WLC с самой большой доступной емкостью LAP. Более того, после того как LAP присоединится к WLC, LAP получает от своего WLC IP-адреса других WLC в мобильной группе.

Как только LAP присоединяется к WLC, можно заставить LAP присоединиться к определенному WLC в своей следующей перезагрузке. Чтобы сделать это, назначьте основной, вторичный, и третичный WLC для LAP. Когда перезагрузки LAP, это ищет основной WLC и соединения что WLC, независимый от загрузки на том WLC. Если основной WLC не отвечает, он ищет вторичное устройство, и, если никакой ответ, третичное. Для получения дополнительной информации о том, как настроить основной WLC для LAP, обратитесь к *Назначению Основного, Вторичного, и Третичные контроллеры для Легковесного* раздела *AP* Аварийного переключения Контроллера беспроводной локальной сети для Примера конфигурации Облегченных точек доступа.

Вопрос. . Каковы функции, которые не поддерживаются на Контроллерах беспроводной локальной сети серии 2100 (WLC)?

O. Эти характеристики оборудования не поддерживаются на Контроллерах серии 2100:

- Сервисный порт (разделяют управление при нестандартном подключении 10/100-Mb/s Интерфейс Ethernet),

Эти программные характеристики не поддерживаются на Контроллерах серии 2100:

- Окончание VPN (такое как IPSec и L2TP)
- Завершение гостевых туннелей контроллера (происхождение гостевых туннелей контроллера поддерживается),
- Список веб-серверов внешней веб-аутентификации
- LWAPP уровня 2
- Связующее дерево
- Зеркалирование портов
- Cranite
- Fortress
- AppleTalk
- QoS договоры пропускной способности для каждого пользователя
- Транзит IPv6
- Агрегирование каналов (LAG)
- Одноадресный режим групповой адресации
- Гостевой доступ к проводной сети

Вопрос. . Какие функции не поддерживаются на Контроллерах серии 5500?

O. Эти программные характеристики не поддерживаются на Контроллерах серии 5500:

- Статический интерфейс менеджера точки доступа**Примечание:** Для Контроллеров серии 5500 вы не обязаны настраивать интерфейс менеджера точки доступа. Действия интерфейса управления как интерфейс менеджера точки доступа по умолчанию и точки

доступа могут присоединиться на этом интерфейсе.
- Асимметричное туннелирование мобильности
- Протокол STP (Spanning Tree Protocol)
- Зеркалирование портов
- Поддержка списка контроля доступа (ACL) уровня 2
- Окончание VPN (такое как IPSec и L2TP)
- Опция passthrough VPN
- Конфигурация 802.3 мостовых соединений, AppleTalk и Протокола PPPoE

Вопрос. . Какие функции не поддерживаются на сетях с ячеистой структурой?

O. Эти функции контроллера не поддерживаются на сетях с ячеистой структурой:

- Поддержка мультистраны
- Основанный на загрузке CAC (сети с ячеистой структурой поддерживают только основанный на пропускной способности, или статический, CAC.)
- Высокая доступность (быстрое биение и основное обнаружение присоединяются к таймеру),
- EAP-FASTv1 и аутентификация 802.1X
- Приоритет соединения точки доступа (точки доступа сетки имеют неподвижный приоритет.)
- Локально значительный сертификат
- Услуги на основе определения местоположения

Вопрос. . Что период достоверности изготовителя является установленными сертификатами (MIC) на контроллере беспроводной локальной сети и сертификатов легковесного AP?

O. Период достоверности MIC на WLC составляет 10 лет. Тот же период достоверности 10 лет применяется к сертификатам легковесного AP от создания (является ли это MIC или Подписанным сертификатом (SSC)).

Вопрос. . Имеются два контроллера беспроводной ЛВС, названные WLC1 и WLC2 и настроенные в одной мобильной группе на дублирование друг друга в случае неполадки. LAP в данный момент зарегистрирована в WLC1. Если WLC1 сбоит, будет ли зарегистрированная им AP перезагружаться во время ее передачи на запасной WLC (WLC2)? Кроме того, потеряет ли клиент WLAN соединение с LAP во время обхода отказа?

O. Да, LAP действительно вычеркивает из списка от WLC1, перезагрузки, и затем повторно регистрирует с WLC2, если отказывает WLC1. Поскольку перезагрузки LAP, связанные клиенты WLAN теряют подключение LAP перезагрузки. Для дополнительных сведений обратитесь к Распределению нагрузки AP и Нейтрализации AP в Unified Wireless Network.

Вопрос. . Действительно ли роуминг зависит от режима Протокола LWAPP, который Контроллер беспроводной локальной сети (WLC) настроен для использования? Может WLC, который работает в Режиме LWAPP уровня 2,

выполняют роуминг Уровня 3?

О. Пока мобильность, группирующаяся в контроллерах, настроена правильно, клиентский роуминг должен хорошо работать. На роуминг не влияет режим LWAPP, ни второго, ни третьего уровня. Однако рекомендуется использовать LWAPP уровня 3 там, где это возможно.

Примечание: Режим уровня 2 поддерживается только Серией Cisco 410x и 440x WLC и Точек доступа серии Cisco 1000. LWAPP уровня 2 не поддерживается другими платформами Контроллера беспроводной локальной сети и Облегченной точки доступа.

Вопрос. . Что представляет собой роуминг, который возникает при переходе клиента к другой точке доступа или контроллеру?

О. Ниже представлена последовательность событий, происходящих при роуминге к другой точке доступа:

1. Клиент отправляет запрос переассоциации к WLC через LAP.
2. WLC передает сообщение мобильности к другим WLC в группе мобильности для обнаружения, к которому WLC был ранее привязан клиент.
3. Исходный WLC отвечает информацией, такой как MAC-адрес, IP-адрес, QoS, Контекст безопасности, и т.д. о клиенте через сообщение мобильности.
4. WLC обновляет свою базу данных с предоставленной клиентской подробной информацией; клиент тогда проходит переопознавательный процесс, при необходимости. Новый LAP, к которому в настоящее время привязывается клиент, также обновлен наряду с другими подробными данными в базе данных WLC. Таким образом, IP-адрес клиента сохранен через, перемещается между WLC, который помогает предоставлять бесшовный роуминг.

Для получения дополнительной информации о роуминге в унифицированной среде обратитесь к разделу *Групп мобильности Настройки* руководства по конфигурированию контроллера Cisco Wireless LAN, Выпуска 7.0.116.0.

Примечание: Беспроводной клиент не отсылает (802.11) запрос аутентификации во время переассоциации. Беспроводной клиент просто отсылает переассоциацию сразу же. Затем это пройдет аутентификацию 802.1x.

Вопрос. . Когда существует межсетевой экран в сети, какие порты я должен разрешить для связи LWAPP/CAPWAP?

О. Необходимо разрешить следующие порты:

- Включите данные порты UDP для трафика LWAPP:Данные – 12222Управляющий трафик – 12223
- Включите эти порты UDP для трафика CAPWAP:Данные - 5247Контроль - 5246
- Включите данные порты UDP для трафика Mobility:16666 - Защищенный режим16667 - Необеспеченный режим

Мобильностью и сообщениями данных обычно обмениваются через пакеты EtherIP. **Протокол "IP" 97** должен быть позволен на межсетевом экране позволить пакеты EtherIP. При использовании **ESP** для инкапсуляции мобильных пакетов, необходимо разрешить

ISAKMP через межсетевой экран при открытии **порта 500 UDP**. Также необходимо открыть **Протокол "IP" 50**, чтобы позволить зашифрованным данным проходить через межсетевой экран.

Следующие порты открывать необязательно (зависит от ваших требований):

- TCP 161 и 162 для SNMP (для системы управления беспроводной сетью – WCS)
- UDP 69 для TFTP
- TCP 80 и/или 443 для HTTP или HTTPS для доступа GUI
- TCP 23 и/или 22 для Telnet или secure shell (SSH) для доступа CLI

Вопрос. . Контроллеры беспроводной локальной сети поддерживают и SSHv1 и SSHv2?

O. Контроллеры беспроводной локальной сети поддерживают только SSHv2.

Вопрос. . Обратный ARP (RARP) поддерживается через Контроллеры беспроводной локальной сети (WLC)?

O. Протокол RARP является протоколом канального уровня, используемым для получения IP-адреса для данного адреса канального уровня, такого как Адрес Ethernet. RARP поддерживается с WLC с версией микропрограммы 4.0.217.0 или позже. RARP не поддерживается на более ранних версиях.

Вопрос. . Я могу использовать внутренний сервер DHCP на Контроллере беспроводной локальной сети (WLC) для присвоения IP-адресов на Облегченные точки доступа (LAP)?

O. Контроллеры содержат внутренний сервер DHCP. Этот сервер, как правило, используется в филиалах компании, которые уже не имеют сервера DHCP. Для доступа к сервису DHCP нажмите **меню Controller** от GUI WLC; тогда нажмите **опцию Internal DHCP Server** на левой стороне страницы. Для получения дополнительной информации о том, как настроить область DHCP на WLC, обратитесь к разделу *DHCP Настройки* руководства по конфигурированию контроллера Cisco Wireless LAN, Выпуска 7.0.116.0.

Внутренний сервер предоставляет адреса DHCP беспроводным клиентам, LAP, AP режима устройства на интерфейсе управления и запросам DHCP, которые переданы от LAP. WLC никогда не предлагают адреса устройствам в восходящем направлении в проводной сети. Параметр DHCP 43 не поддерживается на внутреннем сервере, таким образом, AP должен использовать альтернативный метод для определения местоположения IP-адреса интерфейса управления контроллера, такого как широковещание локальной подсети, DNS, Воспламенение или Беспроводное обнаружение.

Примечание: Версии микропрограммы WLC прежде 4.0 не поддерживают сервис DHCP для LAP, пока LAP не напрямую подключаются к WLC. Функция внутреннего сервера DHCP была использована только для обеспечения IP-адресов клиентам, которые соединяются с беспроводной локальной сетью.

Вопрос. . Что делает Обязательное поле DHCP под WLAN, имеют значение?

О. Требуемый DHCP является опцией, которая может быть включена для WLAN. Это требует этого всего клиенты, которые связываются к тому определенному WLAN, получают IP-адреса через DHCP. Клиентам со статическими IP - адресами не разрешают связаться к WLAN. Эта опция найдена под Вкладкой Дополнительно WLAN. WLC разрешает к/оту трафика клиента, только если его IP-адрес присутствует в таблице MSCB WLC. WLC делает запись IP-адреса клиента во время его Запроса DHCP, или DHCP Возобновляют. Это требует, чтобы клиент возобновил его IP-адрес каждый раз, когда это повторно связывается к WLC, потому что каждый раз клиент разъединяет как часть перемещающийся процесс или превышение времени ожидания сеанса, его запись стерта из таблицы MSCB. Клиент должен снова пройти повторную проверку подлинности и повторно связаться к WLC, который снова делает запись клиента в таблице.

Вопрос. . Как централизованное управление ключами Cisco (CCKM) работает в среде LWAPP/CAPWAP?

О. Во время первоначальной регистрации клиентов точка доступа или контроллер WLC создает управляющий парный ключ (pair-wise master key, PMK) после того как беспроводной клиент проходит проверку подлинности по протоколу 802.1x. AP WLC или WDS кэширует PMK для каждого клиента. Когда беспроводной клиент повторно связывается или перемещается, это пропускает аутентификацию 802.1x и проверяет PMK сразу же.

Единственная специальная реализация WLC в CCKM состоит в том, что WLC обмениваются клиентским PMK через мобильные пакеты, такие как UDP 16666.

Вопрос. . Как задать настройки дуплекса на контроллере беспроводной ЛВС и на облегченных точках доступа?

О. Беспроводные продукты Cisco лучше всего работают, когда скорость и дуплекс автоматически согласовываются друг с другом, однако можно самостоятельно задать настройки дуплекса на контроллере WLC и облегченных точках доступа. Чтобы задать настройки скорости/дуплекса на точке доступа, нужно сначала настроить дуплекс для точек доступа на контроллере и затем, в свою очередь, передать настройки собственно точкам доступа.

настройте двусторонний Ethernet AP <автоматическая/половина/полная> скорость <auto/10/100/1000> <вся/Cisco Name> AP является командой для установки настроек дуплекса через CLI.This, команда поддерживается с версиями 4.1 и позже только.

Для установки настроек дуплекса для физических интерфейсов WLC используйте **config port physicalmode {все | порт} {100-й | 100f | 10-й | 10f}** команда.

Это наборы команд указанное или вся лицевая панель 10/100BASE-T Порты Ethernet для специализированных 10 Мбит/с или 100 Мбит/с, полудуплекс или полнодуплексный режим. Обратите внимание на то, что необходимо отключить автосогласование с **командой config port autoneg disable** перед ручной настройкой любого физического режима на порту. Кроме того, обратите внимание, что **команда config port autoneg** отвергает настройки, установленные с **командой config port physicalmode**. По умолчанию все порты установлены в автоматический, выполняют согласование.

Примечание: Нет никакого способа изменить параметры настройки скорости на волоконных портах.

Вопрос. . Можно ли узнать имя облегченной точки доступа (LAP) когда она не зарегистрирована на контроллере?

О. Если точка доступа полностью отключена и не зарегистрирована на контроллере, то отследить LAP с помощью контроллера невозможно. Единственный путь, который остается, состоит в том, что можно обратиться к коммутатору, на котором связаны эти AP, и можно найти порт коммутатора, на котором они связаны с помощью этой команды:

show mac-address-table address *<mac address>*

Это дает вам номер порта на коммутаторе, с которым связан этот AP. Затем выполните эту команду:

show cdp nei *<type/num>* **detail**

Выходные данные этой команды также дают название LAP. Когда ваш AP включен и связан с коммутатором, Однако этот метод только возможен.

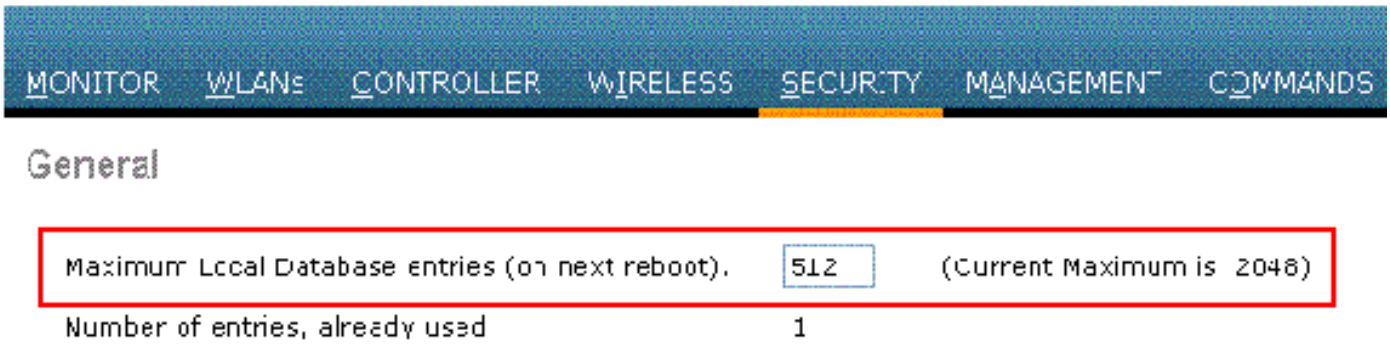
Вопрос. . На контроллере настроены 512 пользователей. Там какой-либо путь состоит в том, чтобы увеличить число пользователей на Контроллере беспроводной локальной сети (WLC)?

О. База локальных пользователей ограничена максимумом записей 2048 года в **Безопасности> страница General**. Эта база данных разделена пользователями локального управления (который включает послов лобби), сетевые пользователи (который включает гостей), записи фильтра MAC, записи списка авторизации точки доступа и записи списка Исключения. Пользователи всех этих типов вместе не могут превышать настроенный размер базы данных.

Для увеличения локальной базы данных используйте эту команду от CLI:

```
<Cisco Controller>config database size ?
<count>  Enter the maximum number of entries (512-2048)
```

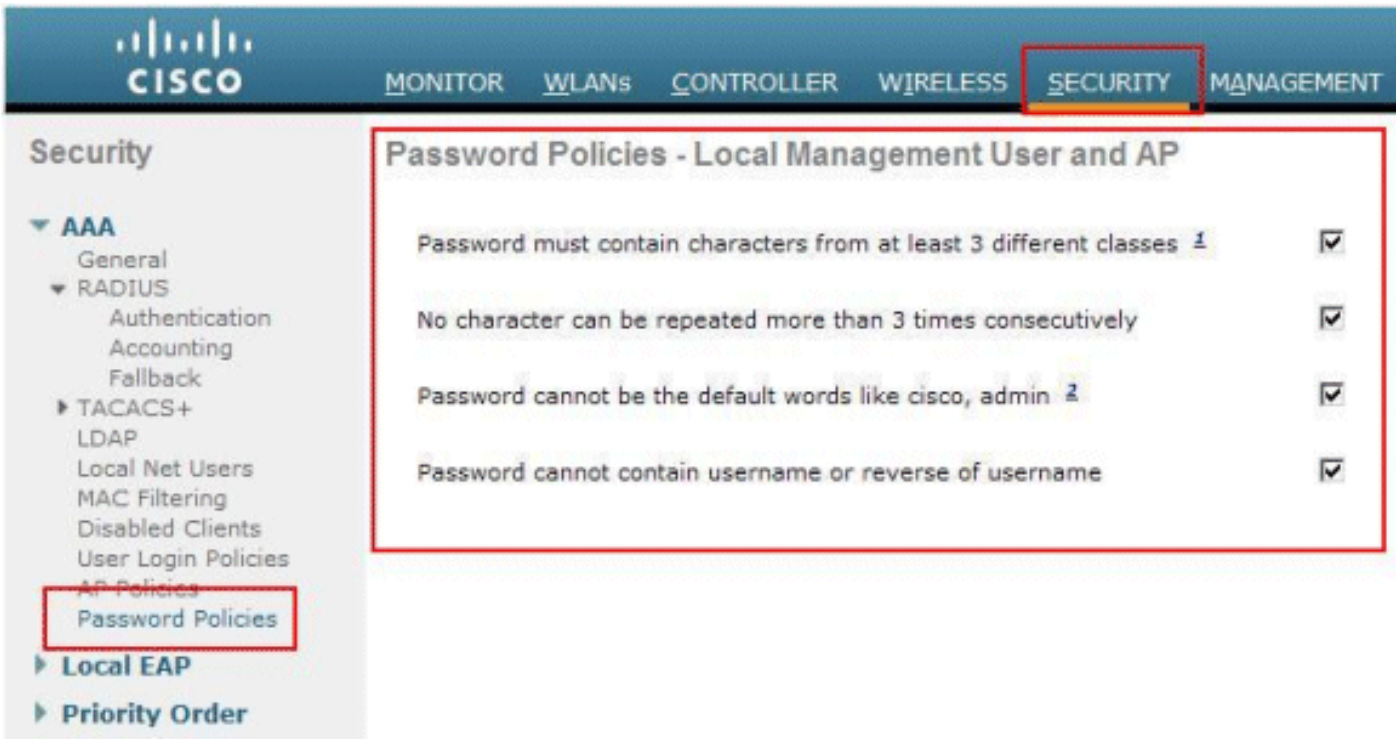
Примечание: Необходимо сохранить конфигурацию и перезагрузить систему (использующий **команду reset system**) для изменения для вступления в силу.



Вопрос. . Как я принуждаю политику по созданию стойких паролей на WLC?

О. WLC позволяют вам определять политику по созданию стойких паролей. Это может быть сделано с помощью или CLI или GUI.

В GUI перейдите **к Безопасности> AAA> Политика паролирования**. Эта страница имеет ряд параметров, который может быть выбран для осуществления стойкого пароля. Например:



Чтобы сделать это от CLI WLC, используйте **config switchconfig сильный pwd** *{проверка случая | последовательная проверка | проверка по умолчанию | проверка имени пользователя |, все-проверка} {включает |, отключают}* команда:

- **проверка случая** - Проверяет возникновение того же символа три раза последовательно.
- **последовательная проверка** - Проверяет, используются ли значения по умолчанию или ее варианты.
- **проверка по умолчанию** - Проверяет, используются ли или имя пользователя или его реверс.
- **все-проверки** - Позволяют/запрещают все проверки стойкого пароля.

Вопрос. . Как пассивная характеристика клиента используется на Контроллерах беспроводной локальной сети?

О. Пассивные клиенты являются беспроводными устройствами, такими как масштабы и принтеры, которые настроены со статическим IP - адресом. Эти клиенты не передают IP - информации, такого как IP-адрес, маска подсети и данные шлюза, когда они связываются с точкой доступа. В результате, когда пассивные клиенты используются, контроллер никогда не знает IP-адрес, пока они не используют DHCP.

WLC в настоящее время действуют как прокси для запросов ARP. После получения запроса ARP контроллер отвечает ответом ARP вместо того, чтобы передать запрос непосредственно клиенту. Этот сценарий имеет два преимущества:

- Устройство восходящего потока данных, которое отсылает запрос ARP клиенту, не будет знать, где расположен клиент.
- Питание для устройств, работающих от батареи, таких как мобильные телефоны и

принтеры сохранено, потому что они не должны отвечать на каждый запросы ARP. Так как контроллер беспроводной локальной сети не имеет никаких дополнительных сведений IP о пассивных клиентах, это не может ответить ни на какие запросы ARP. Текущее поведение не позволяет передачу запросов ARP пассивным клиентам. Любое приложение, которое пытается обратиться к пассивному клиенту, откажет.

Пассивная характеристика клиента позволяет запросам ARP и ответам быть обмененными между проводным и беспроводными клиентами. Эта функция, когда включено, позволяет контроллеру передавать запросы ARP от проводного до беспроводных клиентов, пока желаемый беспроводной клиент не добирается до состояния ВЫПОЛНЕНИЯ.

Для получения информации о том, как настроить пассивную характеристику клиента, считайте раздел по Использованию GUI для Настройки Пассивного Клиента в руководстве по конфигурированию контроллера Cisco Wireless LAN, Выпуске 7.0.116.0.

Вопрос. . Как я могу установить клиента для прохождения повторную проверку подлинности с сервером RADIUS каждые три минуты или на каком-либо указанном периоде времени?

O. Параметр превышения времени ожидания сеанса на WLC может использоваться для выполнения этого. По умолчанию параметр превышения времени ожидания сеанса настроен в течение 1800 секунд, прежде чем произойдет переаутентификация.

Измените значение, установив 180 секунд для того, чтобы клиент перерегистрировался с интервалом в три минуты.

Для доступа к параметру превышения времени ожидания сеанса нажмите меню **WLAN** в GUI. Это отображает список WLAN, настроенных в WLC. Нажмите WLAN, которому принадлежит клиент. Перейдите **к Вкладке Дополнительно**, и вы находите*, Включают* параметр *Превышения времени ожидания сеанса*. Измените значение по умолчанию на 180 и нажмите **Apply** для изменений для вступления в силу.

При использовании вместе с параметрами Access-Accept и Termination-Action в рамках запроса RADIUS-Request, атрибут Session-Timeout указывает максимальное число секунд, по истечении которых требуется повторная регистрация. В этом случае атрибут Session-Timeout используется для загрузки константы reAuthPeriod в рамках таймера повторной регистрации для 802.1X.

Вопрос. . У меня есть гостевое туннелирование, Ethernet по IP (EoIP) туннель, настроенный между моими 4400 Контроллерами беспроводной локальной сети (WLC), которые действуют как WLC привязки и несколько удаленных WLC. Действительно ли это может привязать WLC прямое широковещание в подсети через туннель EoIP от проводной сети до беспроводных клиентов, привязанных к удаленным контроллерам?

O. Нет, контроллер WLC 4400 не может направлять вещание IP-подсети от проводной сети к беспроводным клиентам по туннелю EoIP. Эта функция не поддерживается. Cisco не поддерживает туннелирование вещания подсети или мультивещания в рамках гостевой сети. Так как гостевой WLAN вызывает клиентский Point of Presence к очень определенному местоположению в сети, главным образом вне межсетевого экрана, туннелирование

широковещания в подсети может быть проблемой безопасности.

Вопрос. . Какие значения дифференцированных сервисных кодов (Differentiated Services Code Point, DSCP) используются для голосового трафика в настройках контроллера беспроводной ЛВС и облегченной точки доступа (LWAPP)? Как QoS внедрено на WLC?

О. Единая беспроводная сеть Cisco (UWN) (UWN) WLAN Решения поддерживает четыре уровня QoS:

- Платина/Голос
- Золото/Видео
- Серебряный/оптимальный выбор (по умолчанию)
- Бронза/Общие сведения

Можно настроить WLAN голосового трафика, чтобы использовать Платиновое QoS, назначить WLAN низкой пропускной способности использовать Бронзовое QoS и назначать весь другой трафик между другими уровнями QoS. См. Присвоение Профиля QoS к WLAN для получения дополнительной информации.

Вопрос. . Мосты Ethernet Linksys поддерживаются в Комплексном решении беспроводной связи Cisco?

О. Нет, WLC поддерживает только продукты WGB Cisco. WGB Linksys не поддерживаются. Несмотря на то, что унифицированное беспроводное решение Cisco не поддерживает Ethernet-мосты Linksys WET54G и WET11B, эти устройства можно использовать в среде унифицированного беспроводного решения при условии соблюдения следующих инструкций:

- Подключите только одно устройство с WET54G или WET11B.
- Активируйте опцию клонирования MAC на WET54G или WET11B для клонирования присоединенного устройства.
- Установите самые новые драйверы и микропрограммное обеспечение на устройствах, связанных с WET54G или WET11B. Эта рекомендация особенно важна для Принтеров JetDirect, потому что более ранние версии микропрограммы вызывают проблемы с DHCP.

Примечание: Другие сторонние мосты не поддерживаются. Упомянутые шаги можно также попробовать за другие сторонние мосты.

Вопрос. . Как я храню файлы конфигурации на Контроллере беспроводной локальной сети (WLC)?

О. WLC содержит два типа памяти:

- Энергозависимое ОЗУ — Держит текущую, конфигурацию активного контроллера
- Энергонезависимая память (NVRAM) — Держит конфигурацию перезагрузки

При настройке операционной системы в WLC вы модифицируете энергозависимое ОЗУ. Необходимо сохранить конфигурацию от энергозависимого ОЗУ до NVRAM, чтобы удостовериться что перезагрузки WLC в текущей конфигурации.

Важно знать, какую память вы модифицируете при выполнении этих задач:

- Используйте мастера настройки.
- Очистите конфигурацию контроллера.
- Сохраните конфигурации.
- Перезагрузите контроллер.
- Выйдите из CLI.

Вопросы по функциональным возможностям

Вопрос. . Как задать тип расширяемого протокола проверки подлинности (Extensible Authentication Protocol,EAP) на контроллере беспроводной ЛВС? При попытке зарегистрироваться на сервере контроля доступа (Access Control Server, ACS), в файле журнала появляется сообщение "unsupported EAP" (неподдерживаемая точка доступа EAP).

O. На WLC нет никакого отдельного параметра тип EAP. Для Light EAP (LEAP), гибкой аутентификации EAP по технологии Secure Tunneling (EAP-FAST) или Microsoft Protected EAP (MS-PEAP) просто настройте IEEE 802.1x или Wi-Fi Protected Access (WPA) (если используется 802.1x с WPA). Любой тип EAP, который поддерживается на сервере RADIUS и на клиенте, поддерживается через тэг 802.1x. Настройки EAP на клиенте и на сервере RADIUS должны совпадать.

Выполните эти шаги для того, чтобы включить EAP через графический интерфейс на контроллере WLC:

1. От GUI WLC нажмите **WLAN**.
2. Появляется список WLAN, настроенных в WLC. Нажмите WLAN.
3. В **WLAN> Редактируют**, нажимают **Вкладку Безопасность**.
4. Нажмите **Layer 2** и выберите Layer 2 Security в качестве 802.1x или WPA+WPA2. Можно также настроить параметры 802.1x, которые доступны в том же окне. Затем WLC переправит пакеты аутентификации EAP между беспроводным клиентом и сервером аутентификации.
5. Нажмите **AAA-серверы** и выберите сервер проверки подлинности из раскрывающегося меню для этого WLAN. Мы предполагаем, что сервер проверки подлинности уже настроен глобально. Для получения информации о том, как включить параметр EAP на WLC через интерфейс командной строки (CLI), обратитесь к *Использованию CLI Настроить* раздел *RADIUS* руководства по конфигурированию контроллера Cisco Wireless LAN, Выпуска 7.0.116.0.

Вопрос. . Что такое Быстрое Изменение SSID?

O. Быстрое Изменение SSID позволяет клиентам перемещаться между SSIDs. Когда клиент передает новую ассоциацию за другим SSID, запись клиента в таблице подключений контроллера очищена, прежде чем клиент добавлен к новому SSID. Когда Быстрое Изменение SSID отключено, контроллер принуждает задержку, прежде чем клиентам разрешат переместиться в новый SSID. Для получения информации о том, как включить Быстрое Изменение SSID, обратитесь к *Настройке Быстрый* раздел *Изменения SSID*

руководства по конфигурированию контроллера Cisco Wireless LAN, Выпуска 7.0.116.0.

Вопрос. . Я могу установить предел для количества клиентов, которые могут соединиться с Беспроводной локальной сетью?

О. Можно установить предел к количеству клиентов, которые могут соединиться с WLAN, который полезен в сценариях, где у вас есть ограниченное число клиентов, которые могут соединиться с контроллером. Количество клиентов, которых можно настроить на WLAN, зависит от платформы, которую вы используете.

Считайте Настройку раздела Максимальное число Клиентов на WLAN руководства по конфигурированию контроллера Cisco Wireless LAN, Выпуска 7.0.116.0 для получения информации о клиентских пределах на WLAN для других платформ Контроллеров беспроводной локальной сети.

Вопрос. . Что такое PKC и как он работает с Контроллером беспроводной локальной сети (WLC)?

О. PKC обозначает Упреждающее Ключевое Кэширование. Эта функция была разработана как расширение стандарта 802.11i IEEE.

PKC - это функциональная возможность, доступная в контроллерах Cisco 2006/410x/440x и позволяющая правильно настроенным беспроводным клиентам переключаться без повторной аутентификации на сервере AAA. Для понимания PKC нужно сначала понять принцип работы кэширования ключей.

Кэширование ключей - это функциональная возможность, которая была добавлена в WPA2. Это позволяет мобильной станции кэшировать главные ключи (Попарный главный ключ [PMK]), он получает посредством успешной аутентификации с точкой доступа (AP), и **снова используйте его в будущей ассоциации с тем же AP**. Это означает, что данное мобильное устройство должно аутентифицироваться однажды с определенным AP и кэшировать ключ для дальнейшего использования. Ключевое Кэширование обрабатывается с помощью механизма, известного как Идентификатор PMK (PMKID), который является хэшем PMK, строки, станции и MAC-адресов AP. PMKID уникально идентифицирует PMK.

Даже с Ключевым Кэшированием, терминал беспроводной связи должен аутентифицироваться с каждым AP, от которого это хочет получить сервис. Это представляет значительную задержку и издержки, которые задерживают процесс переключения и могут запретить способность поддержать приложения реального времени. Чтобы разрешить эту проблему, в WPA2 была внедрена технология PKC.

PKC позволяет станции повторно использовать ключ PMK, полученный ранее в результате успешной проверки подлинности. Это избавляет от необходимости станцию аутентифицироваться против новых AP при роуминге.

Поэтому в роуминге внутриконтроллера, когда мобильное устройство перемещается от одного AP до другого на том же контроллере, клиент повторно вычисляет PMKID использование ранее используемого PMK и представляет его во время процесса сопоставления. Контроллер WLC просматривает свой кэш ключей PMK и ищет совпадение. Если он находит его, то проверка подлинности 802.1X пропускается, и сразу же начинается обмен ключами WPA2. Если совпадение не найдено, происходит стандартная проверка подлинности 802.1X.

PKC включено в WPA2 по умолчанию. Поэтому при включении WPA2 как уровня безопасности Layer 2 в настройках WLAN контроллера WLC, PKC начинает работать на контроллере WLC. Следует также настроить сервер AAA и беспроводной клиент для соответствующей проверки подлинности EAP.

Запрашивающая стороны на клиенте должна также поддерживать WPA-2, чтобы PKC работало. PKC также может быть внедрено в среде роуминга между контроллерами.

Примечание: PKC не работает со служебной программой рабочего стола Aironet (ADU) как клиентский соискатель.

Вопрос. . Что является пояснениями для этих настроек времени ожидания на контроллере: Таймаут Протокола ARP, Пользовательское Время простоя и Превышение времени ожидания сеанса?

О. Тайм-аут ARP используется для удаления Записей ARP на WLC для устройств, изученных из сети.

Пользовательское Время простоя: Когда пользователь является простаивающим без любой связи с LAP для набора периода времени как Пользовательское Время простоя, клиент является deauthenticated WLC. Клиент должен повторно аутентифицироваться и повторно связаться к WLC. Это используется в ситуациях, где клиент может понизиться из его связанного LAP, не уведомляя LAP. Это может произойти, если аккумулятор идет неисправный на клиенте, или клиентские партнеры переезжают.

Примечание: Для доступа к ARP и Пользовательскому Времени простоя на GUI WLC, перейдите **к меню Controller**. Выберите **General** из левой стороны для обнаружения полей ARP и User Idle Timeout.

Превышение времени ожидания сеанса является максимальным временем для сеанса клиента с WLC. После на этот раз, WLC de-authenticates клиент и клиент проходит целую аутентификацию (повторная проверка подлинности) процесс снова. Это - часть предосторожности безопасности для вращения ключей шифрования. При использовании метода Протокола EAP с управлением ключами смена ключа происходит в каждом регулярном интервале для получения нового ключа шифрования. Без управления ключами это значение таймаута является временем, когда беспроводные клиенты должны сделать полную переаутентификацию. Таймаут сессии задается отдельно для каждой WLAN. К этому параметру можно обратиться от **WLAN> меню Edit**.

Вопрос. . Что такое система RFID? Какие метки RFID в настоящее время поддерживаются Cisco?

О. Radio Frequency Identification (RFID) является технологией, которая использует радиочастотное соединение для довольно ближней связи. Основная система RFID составлена из меток RFID, RFID-считывателей и программного обеспечения обработки.

В настоящее время Cisco поддерживает метки RFID от AeroScout и Pango. Для получения дополнительной информации о том, как настроить метки AeroScout, обратитесь к Конфигурации WLC для Меток AeroScout RFID.

Вопрос. . Я могу выполнить Аутентификацию eap локально на WLC? Есть ли

какой-либо документ, который объясняет эту Локальную функцию EAP?

О. Да, Аутентификация eap может быть выполнена локально на WLC. Локальный EAP является методом аутентификации, который позволяет пользователям и беспроводным клиентам аутентифицироваться локально на WLC. Он разработан для работы в удаленных офисах, которым необходимо поддерживать подключение к беспроводным клиентам, если нарушена связь с внутренней системой, или внешний сервер аутентификации перестал работать. При включении локального EAP WLC служит сервером проверки подлинности. Для получения дополнительной информации о том, как настраивают WLC для локальной Быстрой EAP аутентификации, обратитесь к Локальной EAP-аутентификации на Контроллере беспроводной локальной сети с Примером конфигурации Сервера LDAP и EAP-FAST.

Вопрос. . Какова функция замены WLAN? Как я настраиваю эту функцию? LAP поддержат значения замены WLAN, когда они переключатся при отказе к резервному WLC?

О. Функция замены WLAN позволяет нам выбрать WLAN из числа WLAN, настроенных на WLC, который может активно использоваться на отдельной основе LAP. Выполните эти шаги для настройки замены WLAN:

1. В GUI WLC нажмите **меню Wireless**.
2. Нажмите **опцию Radios** на левой стороне и выберите **802.11 a/n** или **802.11 b/g/n**.
3. Щелкните по ссылке **Configure** от раскрывающегося меню, найденного на правой части, которая соответствует названию AP, на котором вы хотите настроить замену WLAN.
4. Выберите **Enable** из раскрывающегося меню Замены WLAN. Это меню расположено в самой левой части окна.
5. Появится список всех WLAN, настроенных на WLC.
6. Из этого списка проверьте **WLAN**, что вы хотите появиться на LAP и нажать **Apply** для изменений для вступления в силу.
7. После внесения изменений сохраните конфигурацию.

AP сохраняют значения замены WLAN, когда они зарегистрированы к другим WLC, при условии, что профили WLAN и SSIDs, который вы хотите отвергнуть, настроены через все WLC.

Примечание: В выпуске ПО контроллера 5.2.157.0, функция замены WLAN была удалена и из графического интерфейса контроллера и из CLI. Если ваш контроллер настроен для замены WLAN, и вы обновляете к выпуску ПО контроллера 5.2.157.0, контроллер удаляет конфигурацию WLAN и передает все WLAN. Можно указать, что только определенные WLAN переданы при настройке групп точек доступа. Каждая точка доступа объявляет только включенные WLAN, которые принадлежат ее группе точек доступа.

Примечание: Группы точек доступа не позволяют WLAN быть переданными на на радиоинтерфейс AP.

Вопрос. . IPv6 поддерживается на контроллерах беспроводной локальной сети Cisco (WLC) и Облегченные точки доступа (LAP)?

О. В настоящее время 4400 и контроллеры серии 4100 только поддерживают passthrough клиента IPv6. Собственная поддержка IPv6 не поддерживается.

Для включения IPv6 на контроллере WLC отметьте пункт IPv6 Enable в настройках WLAN SSID на странице WLAN > Edit (Правка).

Также для поддержки IPv6 требуется включить режим Ethernet Multicast Mode (EMM). Если отключить EMM, связь по IPv6 с клиентскими устройствами будет разорвана. Для включения EMM перейдите к Контроллеру> страница General и из выпадающего меню режима многоадресной рассылки Ethernet, выберите **Unicast** или **Multicast**. Это включает групповую адресацию или в Одноадресном режиме или в режиме многоадресной рассылки. Когда включено широковещание в одноадресном режиме, каждая точка доступа получает по отдельной копии пакета. Это значительно нагружает процессор, так что будьте осторожны. Групповая адресация включила, как передано в многоадресном режиме, групповая адресация использует назначенный адрес групповой адресации пользователя для убирания более традиционной групповой адресации к точкам доступа (AP).

Примечание: IPv6 не поддерживается на контроллерах 2006.

Кроме того, существует идентификатор ошибки Cisco CSCsg78176, который предотвращает passthrough IPv6 использования, когда используется AAA функция Overrride.

Вопрос. . Контроллер беспроводной локальной сети Cisco серии 2000 (WLC) поддерживает Web-аутентификацию для гостей?

O. Проверка подлинности по сети поддерживается на всех контроллерах WLC Cisco. Web-аутентификация является методом аутентификации Уровня 3, используемым для аутентификации пользователей с учетными данными простой проверки подлинности. Никакое шифрование не включено. Для включения этой функции выполните следующие шаги:

1. От GUI нажмите меню **WLAN**.
2. Нажмите **WLAN**.
3. Перейдите **к Вкладке Безопасность** и выберите **Layer 3**.
4. Установите **веб-**флажок **Политики** и выберите **Authentication**.
5. Нажмите **Apply** для сохранения изменений.
6. Для создания базы данных по WLC, против которого можно аутентифицировать пользователей, перейдите **к Меню системы безопасности** на GUI, выберите **Local Net User** и завершите эти действия: Определите гостевое имя пользователя и пароль для регистрации гостя. Данные значения вводятся с учетом регистра символов.Выберите WLAN ID, который вы используете.**Примечание:** Для большего количества подробной конфигурации обратитесь к Примеру настройки веб-аутентификации в контроллере беспроводной сети LAN.

Вопрос. . WLC можно управлять в Беспроводном режиме?

O. WLC можно управлять через беспроводной режим, как только это включено. Для получения дополнительной информации о том, как включить беспроводной режим, обращаются к *Беспроводным соединениям Включения к GUI и* разделу *CLI* руководства по конфигурированию контроллера Cisco Wireless LAN, Выпуска 7.0.116.0.

Вопрос. . Что такое Агрегирование каналов (LAG)? Как включить LAG на контроллере беспроводной ЛВС?

O. LAG связывает все порты на WLC в одиночный интерфейс EtherChannel. Система динамично управляет балансировкой трафика и резервированием порта с LAG.

Обычно интерфейсу на WLC привязали множественные параметры к нему, который включает IP-адрес, default-gateway (для IP-подсети), основной физический порт, вторичный физический порт, тег VLAN и сервер DHCP. Когда LAG не используется, каждый интерфейс обычно сопоставляется с физическим портом, но Несколько интерфейсов могут также быть сопоставлены с одиночным портом WLC. Когда LAG используется, система динамично сопоставляет интерфейсы с каналом агрегированного порта. Это помогает в резервировании порта и распределении нагрузки. Когда порт отказывает, интерфейс динамично сопоставлен со следующим доступным физическим портом, и LAP сбалансированы через порты.

Когда LAG включен на WLC, WLC вперед фреймы данных на том же порте, на котором они были получены. WLC полагается на соседний коммутатор для распределения нагрузки трафика через EtherChannel. WLC не выполняет EtherChannel, распределяющего нагрузку самостоятельно.

Вопрос. . Какие модели Контроллеров беспроводной локальной сети (WLC) Агрегация канала поддержки (LAG)?

O. LAG поддержки Контроллеров серии 5500 Cisco в выпуске ПО 6.0 или позже, Cisco LAG поддержки Контроллеров серии 4400 в выпуске ПО 3.2 или позже и LAG включен автоматически на контроллерах в Cisco WiSM и Catalyst 3750G Интегрированный Коммутатор Контроллера беспроводной локальной сети. Без LAG каждого порта системы распределения на Cisco Контроллер серии 4400 поддерживает до 48 точек доступа. С включенным LAG логический порт Контроллера Cisco 4402 поддерживает до 50 точек доступа, логический порт контроллера Cisco 4404 поддерживает до 100 точек доступа и логический порт на Catalyst 3750G, Интегрированный Коммутатор Контроллера беспроводной локальной сети и на каждом контроллере Cisco WiSM поддерживает до 150 точек доступа.

WLC Cisco 2106 и 2006 не поддерживают LAG. Более ранние модели, такие как WLC Серии Cisco 4000, не поддерживают LAG.

Вопрос. . Какова функция мобильной связи автопривязки в Unified Wireless Network?

O. Мобильная функция Auto-anchor (средство автоматической мобильной привязки, также средство гостевой WLAN-мобильности) используется для улучшения распределения нагрузки при роуминге клиентов в рамках беспроводной сети. В условиях нормального роуминга клиентские устройства подключаются к WLAN и привязываются к первому контроллеру, с которым удается наладить связь. Если клиент перемещается в другую подсеть, контроллер, в который перемещается клиент, устанавливает внешний сеанс для такого клиента с якорным контроллером. С использованием функции мобильной связи автопривязки можно задать контроллер или набор контроллеров как точки привязки для клиентов на WLAN.

Примечание: Привязка к мобильности не должна быть настроена для Мобильности уровня 3. Привязка к мобильности используется только для гостевого туннелирования.

Вопрос. . Можно ли настроить контроллер Cisco 2006 для беспроводной ЛВС в качестве привязки для WLAN?

О. Беспроводной WLC-контроллер Cisco 2006 не может служить привязкой для WLAN. Однако WLAN, созданная на WLC Cisco 2000, может иметь в качестве своего якоря WLC Cisco серий 4100 и 4400.

Вопрос. . Какое туннелирование мобильности Контроллер беспроводной локальной сети использует?

О. Выпуски ПО контроллера 4.1 через 5.1 поддержки и асимметричное и симметричное туннелирование мобильности. Выпуск ПО контроллера 5.2 или более поздняя поддержка только симметричное туннелирование мобильности, которое теперь всегда включается по умолчанию.

В асимметричном туннелировании трафик клиента к проводной сети маршрутизируется непосредственно через внешний контроллер. Асимметричные туннелирующие разрывы, когда вышестоящему маршрутизатору включили фильтрацию обратного пути (RPF). В этом случае трафик клиента отброшен в маршрутизаторе, потому что Проверка переадресации по обратному пути гарантирует, что путь назад к адресу источника совпадает с путем, из которого прибывает пакет.

Когда симметричное туннелирование мобильности включено, весь трафик клиента передается якорному контроллеру и может тогда успешно передать Проверку переадресации по обратному пути. Симметричное туннелирование мобильности также полезно в этих ситуациях:

- Если установка межсетевого экрана в клиентском пакете соединяет пакеты отбрасываний каналом, потому что IP - адрес источника не совпадает с подсетью, на которой получены пакеты, это полезно.
- Если VLAN группы точек доступа на якорном контроллере является другой, чем interface VLAN WLAN на внешнем контроллере: в этом случае трафик клиента может быть передан на неправильной VLAN во время событий mobility.

Вопрос. . Когда сеть не работает, как мы обращаемся к WLC?

О. Когда сеть не работает, к WLC может обратиться сервисный порт. Этому порту назначают IP-адрес в совершенно другой подсети от других портов WLC и вызванное управление при нестандартном подключении - также. Для получения дополнительной информации обратитесь раздел *портов и Интерфейсов Настройки* руководства по конфигурированию контроллера Cisco Wireless LAN, Выпуска 7.0.116.0.

Вопрос. . Контроллеры беспроводной локальной сети Cisco (WLC) поддерживают аварийное переключение (или резервирование) функция?

О. Да, если у вас есть два или больше WLC в вашей сети WLAN, можно настроить их для резервирования. Обычно LAP соединяет с настроенным основным WLC. Как только основной WLC отказывает, перезагрузки LAP и присоединяется к другому WLC в группе мобильности. Аварийное переключение является функцией в чем опросы LAP для основного WLC и присоединяется к основному WLC, как только это функционально. См.

Аварийное переключение Контроллера беспроводной локальной сети для Примера конфигурации Облегченных точек доступа для получения дополнительной информации.

Вопрос. . Почему перед проверкой подлинности нужны списки контроля доступа (ACL) на контроллере беспроводной ЛВС?

О. С ACL процедур, предшествующих аутентификации, поскольку название подразумевает, можно позволить трафик клиента и от определенного IP-адреса даже, прежде чем аутентифицируется клиент. При использовании внешнего веб-сервера для web-аутентификации некоторым платформам WLC нужен ACL процедур, предшествующих аутентификации для внешнего веб-сервера (Контроллер серии 5500 Cisco, Cisco Контроллер серии 2100, Серия Cisco 2000 и модуль контроллерной сети). Для других платформ WLC ACL процедур, предшествующих аутентификации не является обязательным. Однако это - полезный прием для настройки ACL процедур, предшествующих аутентификации для внешнего веб-сервера при использовании внешней веб-аутентификации.

Вопрос. . У меня есть фильтруемый MAC WLAN и абсолютно открытый WLAN в моей сети. Будет ли клиент по умолчанию выбирать открытую WLAN? Либо он будет автоматически зарегистрирован на идентификаторе WLAN ID, который настроен на MAC-фильтре? И еще, зачем нужен параметр "interface" в фильтре MAC?

О. Клиент может быть зарегистрирован на любой WLAN, к которой позволяют подключаться настройки. Параметр "interface" в фильтре MAC дает возможность применить фильтр к WLAN или к интерфейсу. Если к одному интерфейсу привязаны несколько WLAN, можно применить MAC-фильтр к интерфейсу без необходимости создания фильтра для каждой отдельной WLAN.

Вопрос. . Как я могу настроить Аутентификацию TACACS для пользовательских интерфейсов управления на Контроллере беспроводной локальной сети (WLC)?

О. Запускаясь с версии 4.1 WLC, TACACS поддерживается на WLC. См. TACACS Настройки +, чтобы понять, как настроить TACACS + для аутентификации пользовательских интерфейсов управления WLC.

Вопрос. . Каково использование чрезмерного значения ошибки проверки подлинности в Контроллере беспроводной локальной сети (WLC)?

О. Эта установка является одной из клиентской политики исключения. Исключение клиентов - это функция системы безопасности контроллера. Политика используется для помещения клиентов в "черный список", нужный для предотвращения нелегального доступа к сети или атак на беспроводную сеть.

При включенной политике сильного сбоя веб-аутентификации, когда число неудачных попыток веб-аутентификации клиента превышает 5, контроллер считает, что клиент превысил максимальное число попыток веб-аутентификации и заносит его в черный список.

Выполните эти шаги, чтобы включить или отключить эту установку:

1. От GUI WLC перейдите **к Безопасности> беспроводная Политика обеспечения защиты> Клиентская Политика Исключения**.
2. **Установите или снимите флажок Excessive Web Authentication Failures.**

Вопрос. . Я преобразовал свою автономную точку доступа (AP) в облегченный режим. В Протоколе Lightweight AP Protocol (LWAPP) режим с сервером AAA RADIUS для клиентского учета обычно клиент отслежен с RADIUS, считающим на основе IP-адреса WLC. Действительно ли возможно установить RADIUS, считающий на основе MAC-адреса AP, привязанного к тому WLC а не IP-адресу WLC?

O. Да, это может быть сделано с конфигурацией стороны WLC. Выполните следующие действия:

1. От графического интерфейса контроллера, под **Безопасностью> Учет Радиуса**, существует раскрывающееся окно для Типа Идентификатора станции Вызова. **Выберите AP MAC Address.**
2. Проверьте это через журнал AP LWAPP. Там, вы видите поле ID вызываемой станции, которое отображает MAC-адрес AP, к которому привязан конкретный клиент.

Вопрос. . Как вы изменяете значение таймаута квитирования Защищенного доступа по протоколу Wi-Fi (WAP) на Контроллере беспроводной локальной сети (WLC) через CLI? Я знаю, что могу сделать это на Cisco IOS® Access Points (AP) с командой *значения* dot11 wpa handshake timeout, но как вы выполняете это на WLC?

O. Способность настроить таймаут Квитирования WPA через WLC была интегрирована в выпуске ПО 4.2 и позже. Вам не нужна эта опция в более ранних версиях программного обеспечения WLC.

Эти команды могут использоваться для изменения таймаута Квитирования WPA:

```
    config advanced eap eapol-key-timeout <value> config advanced eap eapol-key-retries <value>
```

Значения по умолчанию продолжают отражать текущее поведение WLC.

```
   - the default value for eapol-key-timeout is 1 second.
   - the default value for eapol-key-retries is 2 retries
```

Примечание: На AP IOS эта установка конфигурируема с **командой dot11 wpa handshake**.

Можно также настроить другие параметры EAP с опциями при **команде config advanced eap**.

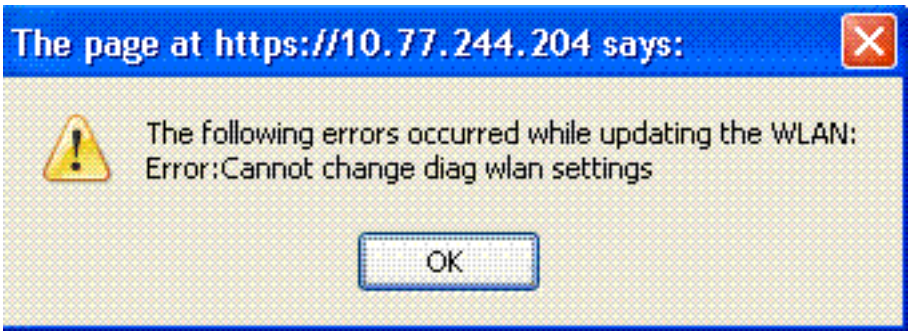
```
(Cisco Controller) >config advanced eap ?

eapol-key-timeout
   Configures EAPOL-Key Timeout in seconds.
eapol-key-retries
   Configures EAPOL-Key Max Retries.
identity-request-timeout
   Configures EAP-Identity-Request Timeout in seconds.
identity-request-retries
   Configures EAP-Identity-Request Max Retries.
key-index
```

```
   Configure the key index used for
   dynamic WEP(802.1x) unicast key (PTK).
max-login-ignore-identity-response
   Configure to ignore the same username count
   reaching max in the EAP identity response
request-timeout
   Configures EAP-Request Timeout in seconds.
request-retries
   Configures EAP-Request Max Retries.
```

Вопрос. . Какова цель диагностической функции канала на странице WLAN> Edit> Advanced?

O. Диагностическая функция канала позволяет вам устранять проблемы в отношении связи с клиентом с WLAN. Клиент и точки доступа могут быть проведены через определенный набор тестов для определения причины проблем со связью, которые испытывает клиент, и затем позвольте корректирующим показателям быть взятыми для создания клиента в рабочем состоянии в сети. Можно использовать графический интерфейс контроллера или CLI для включения диагностического канала, и можно использовать CLI контроллера или WCS для выполнения диагностических тестов.

Диагностический канал может использоваться только для тестирования. При попытке настроить аутентификацию или шифрование для WLAN с диагностическим включенным каналом, вы видите эту ошибку:



Вопрос. . Каково максимальное число групп точек доступа, которые могут быть настроены на WLC?

O. Этот список показывает максимальное число групп точек доступа, что можно настроить на WLC:

- Максимум 50 групп точек доступа для Cisco Контроллер серии 2100 и модули контроллерной сети
- Максимум 300 групп точек доступа для Cisco Контроллеры серии 4400, Cisco WiSM и Коммутатор Контроллера беспроводной локальной сети Cisco 3750G
- Максимум 500 групп точек доступа для Контроллеров серии 5500 Cisco

Дополнительные сведения

- Часто задаваемые вопросы по контроллеру беспроводной LAN (WLC)
- Часто задаваемые вопросы по системным сообщениям и сообщениям об ошибках контроллера беспроводной LAN (WLC)
- Вопросы и ответы по облегченным точкам доступа

- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 7.0.116.0
- Поддержка IPv6 на Контроллере беспроводной локальной сети
- Поддержка беспроводного продукта
- Cisco Systems – техническая поддержка и документация

Был ли этот документ полезен? Да нет

Спасибо за ваш отзыв.

Адресовать вопрос техподдержке (требует контракта сервиса Cisco.)

Соответствующие дискуссии сообщества технической поддержки Cisco

Сообщество технической поддержки Cisco является форумом, в котором можно задавать вопросы и получать ответы, обмениваться предложениями и сотрудничать со своими равноправными коллегами.

См. Условные обозначения технических советов Cisco для получения информации по условным обозначениям, которые используются в данном документе.

Обновлено : 02 марта 2015
ID документа: 118833