Наружное руководство по дизайну мобильности

Содержание

Введение

Этот документ содержит руководство по проектированию развертывания инфраструктуру мобильности в уличной среде. Этот документ касается кратко только соответствующих продуктов, которые подходят и рекомендованы для развертываний Мобильности в улице. Для полного понимания этих линеек продуктов обратитесь к обновлениям соответствующего продукта на Web - сайте Cisco или пройдите соответствующие руководства по развертыванию.

Примечание: Вам нужен специальный автономный образ на автономных точках доступа (AP), используемые в качестве Моста подключения для рабочих групп (WGB) или Мобильного маршрутизатора доступа (MAR) для совместимости с Унифицированной инфраструктурой CAPWAP.

Важные, полезные ссылки предоставлены в Annexure, подключенном в конце.

Сегодняшние путешественники требуют более безопасный, безопасный, и надежные методы транспортировки для персонального и потребностей организации. С повышенным спросом людьми, которые будут связаны где угодно в любое время, мобильность в уличной направляющей использования или любой другой инфраструктуре является подготовкой для удовлетворения их растущий спрос от их пассажиров. В то время как мобильные телефоны могут предоставить решение для голосовой связи, они не оказались полезными в отправке бизнес-данных и связи персональных данных, которую общественность привыкла использовать.

Для отправки более надежного, безопасного, и безопасного решения для транспортировки операции направляющей должны улучшиться с помощью мобильных технологий. Путем обеспечения высокой скорости надежная мобильная связь, не только к серии, но и к любой другой инфраструктуре, путешественникам и сотрудникам может оставаться связанной с их бизнес-информацией и личными данными.

С миллионами путешественников в год, отрасль транспортировки перемещалась быстро, чтобы развернуть и улучшить операции направляющей через мобильные технологии (решения).

Основные бизнес-факторы мотивации для мобильности являются доступом в режиме реального времени к данным по сравнению с пакетными обновлениями, улучшенными операциями наблюдения в движущихся сериях, который помогает в отслеживании местоположения в случае аварийной ситуации, уменьшенных затрат, и увеличенная пропускная способность связи путем замены использования спутниковых и/или сотовых ссылок с землей базировала беспроводные соединения.

Архитектура унифицированной беспроводной связи Cisco предоставляет надежное подключение высокой пропускной способности при перемещении серий. Это руководство по дизайну помогает вам понимать, как создать такую систему эффективно.

Беспроводные технологии разработаны с помощью систем радиосвязи, которые подвергаются интерференции радиоволны. Причины этой интерференции могут быть случайными или преднамеренными. Независимо от источника интерференция может прервать беспроводное соединение, отключив любое решение, которое зависит от Wi-Fi. Учитывая такие риски, решения, которые влияют на общественную безопасность, не должны зависеть SOLELY от беспроводных технологий. Избыточный, наложение и независимые системы (например, оба соединенные проводом и радио) предпочтены. В контексте систем центра управления движением поездов, примерах наложения, избыточные системы включают, но не ограничены: соединяя беспроводные технологии с двумя или больше независимыми системами, механические системы (например, “мертвец переключается”), центр управления движением поездов, сигнализирующий по металлическим направляющим и встроенному и центральному человеческому упущению (машинист) или супервизоры центрального управления. Если один системный сбой, другая независимая система все еще была бы доступна, порция снижают риск для общественной безопасности.

Развертывания мобильности могут быть разделены на два основных раздела. Сначала стационарная инфраструктура, в которой будет взаимодействовать быстрый беспроводной клиент роуминга, и второй является мобильная инфраструктура, состоящая из клиента роуминга радио сама. Существуют некоторые определенные Беспроводные продукты Cisco, которые имеют специфический набор функций, делающий их подходящий для Мобильности.

Стационарная инфраструктура может быть создана с помощью Cisco Наружные точки доступа Сетки (MAP) (серии AP1520). Не пытайтесь создать сеть с ячеистой структурой в уличных использующих внутренних MAP (AP1130 и AP1240), поскольку эти AP не усилены для наружного использования и ограничили питание. Используйте внутренний MAP в закрытом помещении только.

Точно так же для роуминга по инфраструктуре, можно или использовать беспроводную связь Cisco Автономные AP в режиме WGP или Cisco Мобильный Маршрутизатор доступа MAR3200.

Набор функций соответствующих продуктов, которые делают их подходящими для Мобильности, будет выделен в этом документе.

Стационарная инфраструктура Использование MAP

Наружные развертывания также требуют специализированных навыков радиочастот (RF), могут иметь более низкую пользовательскую плотность, чем внутренние развертывания и могут быть развернуты в среде, которая менее отрегулирована, чем в здании. Эти функции оказывают давление на общую стоимость владения (TCO) наружных решений и требуют решения, которое легко развернуть и поддержать.

Сетевое решение сетки беспроводной связи Cisco включает экономически эффективные и безопасные развертывания предприятия, кампуса и столичных наружных сетей Wi-Fi.

MAP Серии AP1520 основываются на CAPWAP, работающем с программным обеспечением Cisco Wireless LAN Controllers (WLCs) и Cisco Wireless Control System (WCS) для обеспечения централизованного и масштабируемого управления, высокого уровня безопасности и мобильности, которая является бесшовной между внутренними и наружными развертываниями.

Множественные WLC могут группироваться в группу мобильности, так, чтобы все AP, которыми они управляют, сформировали одиночный, бесшовный домен беспроводной связи. Максимальное число WLC в одиночной группе равняется 24. Это обсуждено более подробно позже в этом документе.

Подробные сведения о различных контроллерах и их возможностях могут быть найдены при этой ссылке: http://www. cisco . com/en/US/products/ps6302/Products_Sub_Category_Home.html.

Разработанный для поддержки простоты развертываний Cisco MAP серии 1520 на основе CAPWAP, легко и надежно присоединяется к сети с ячеистой структурой и доступен, чтобы управлять и контролировать сеть через контроллер и графический WCS или интерфейс командной строки (CLI). Совместимый с Защищенным доступом по протоколу Wi-Fi 2 (WPA2) и использование аппаратного шифрования Расширенного стандарта шифрования (AES) между беспроводными узлами, Cisco MAP серии 1520 предоставляет сквозную безопасность.

AP1520 сертифицировался к IP67, спецификациям NEMA4X, избавляя от необходимости иметь дополнительную НЕМУ или другие защищенные от атмосферных воздействий корпуса и может работать в температурах в пределах от-40°C полностью к +55°C без любых внешних устройств влияния температуры. Весь модуль разработан, чтобы противостоять и все еще работать в серьезных условиях включая очень сильный ветер и осадки всех типов.

Платформа AP1520 (AP1524 и AP1522) в целом является модульной конструкцией и может быть настроена с этими интерфейсами дополнительного модуля восходящего интерфейса:

- DOCSIS 2.0 кабельного модема с источником питания кабеля
- Оптический интерфейс с 100BaseBX SFP
- 1000BaseT гигабитный Ethernet

Эта платформа также дает выходным данным 802.3af PoE готовый порт для соединения любых периферийных устройств (как камеры).

AP серии 1520 поддерживает четыре Интерфейса Gigabit Ethernet:

- Порт 0 (g0) - Питание над PoE входного порта Ethernet (в)
- Порт 1 (g1) - Питание над PoE порта вывода Ethernet
- Порт 2 (g2) - кабельное соединение
- Порт 3 (g3) - оптоволоконное соединение

Интерфейсы на MAP

Платформа AP1520 родила много MAP как AP1522, AP1524PS (Общественная безопасность) и AP1524SB (Последовательный Обратный рейс).

С 7.0 кодами можно упорядочить AP1523 CV, который имеет в основном те же аппаратные средства как AP1524SB, за исключением того, что это имеет встроенный кабельный модем, подобный модели AP1522PC-X-K9. В то время как AP1524SB и модели AP1524PS не доступны с кабельным модемом, в более простых сроках AP1522 и AP1523CV могут быть настроены с кабельным модемом при заказе.

Примечание: AP1523CV только доступен в –A домене с 7.0 кодами. В этом документе вся функциональность, объясненная для AP1524SB, также применима к AP1523CV.

Становится важно понять ключевые характеристики AP1524SB, которые делают его лучше всего подходящим для линейного типа развертываний. Главным образом развертывания мобильности требуют этого типа инфраструктуры:

Инфраструктура для развертываний мобильности

AP1524 последовательный обратный рейс (AIR-LAP1524SB-X-K9) функциональность

Радио и каналы

AP1524 имеет три радио: одно радио на 2.4 ГГц и два радио на 5 ГГц. Его радио на 2.4 ГГц используется прежде всего для доступа клиента. Два радио на 5 ГГц прежде всего используются для обратного рейса. Эти два обратных рейса предоставляют соединительный и нисходящий доступ. Путем хранения их на исключительных каналах или полосах частот, потребность использовать ту же совместно используемую беспроводную среду между северным и движущимся на юг трафиком в сетке избегают основанной на дереве сети. В более простых сроках мы можем сказать, что каждый переход использует другую частоту. Это улучшает производительность и избегает проблем, привязанных к среде совместного доступа.

Важно понять, какое радио находится в который Слот. AP1524SB имеет в основном 4 слота, но только 3 слота заняты этими 3 радио: AP1524SB: (Слот 0) Доступ клиента 2.4 ГГц; (Слот 1 и 2) радио 5 ГГц: Канал от абонента к оператору и нисходящий обратный рейс.

AP1524SB был запущен в-A,-N и, C домен с выпуском 6.0.

Примечание: В выпуске 6.0 радио на 5 ГГц только работают в полосе на 5.8 ГГц с 5 каналами (149 - 165).

С выпуском 7.0, AP1524SB доступно в-E,-K,-M,-S, и домене T. Кроме того, с выпуском 7.0, UNII2 и UNII2 Плюс полосы были представлены в домене по существующим радио на 5 ГГц. В результате оба 802.11a радиоустройства поддерживают всю полосу на 5 ГГц. Другими словами, с выпуском 7.0 радио могут работать в UNII 2 (5.25 – 5.35 ГГц), UNII 2 плюс (5.47 – 5.725 ГГц), и верхний ISM (5.725 – 5.850 ГГц) полосы.

Доступность канала зависит от управляющего домен. В целом, с последними 7.0 выпусками вы получаете 5 каналов в верхней полосе ISM, 4 канала в полосе UNII 2 и 11 каналов в UNII 2 плюс полоса. См. Таблицу 1 для полного обзора каналов, поддерживаемых в каждом домене.

Для последней информации об инструкциях обратитесь к правилам и нормам вашего соответствующего домена регулятора.

Таблица 1: Каналы, поддерживаемые согласно управляющему домен

Формирование сетки

Расположения антенны для каждого радио исправлены и маркированы. Это - конфигурация радио с антеннами:

- !--- слот0: (11b) (Доступ)
- Гнездо 1: (11a, 5 ГГц) (Универсальный доступ) – Omni / Направленная антенна

- Слот 2: (11a, 5 ГГц) (обратный рейс) – направленная антенна

Типичная сеть с ячеистой структурой

Как показано на этом рисунке, Слоте 2 - радио на 5 ГГц в Точке доступа к корневому каталогу (RAP) используется для расширения обратного рейса в нисходящем направлении, тогда как Слот 2 - радио на 5 ГГц в MAP используется для обратного рейса в канале связи. MAP расширяет Разъем 1 в нисходящем направлении. Сигналы-маяки AWPP только передаются на нисходящей линии, чтобы позволить дочерним AP присоединяться.

Cisco рекомендует использовать направленную антенну с Разъемом 2 в минимуме. Обоснование для этого объяснено позже в этом документе.

Слот 2 радио (на 5 ГГц) внутренне связан с Портом для антенны 6.

Порты для антенны маркированы как (Подвешенная сторона, сталкивающаяся вперед):

Порты для антенны на AP серии 1520

Порты для антенны маркированы на аппаратных средствах и связаны внутренне с радио в каждом слоте на AP1524SB/AP1523CV SKU как:

- Порт для антенны 1: 5 ГГц (разъем 1)
- Порт для антенны 2: 2.4 ГГц (радио слота 0)
- Порт для антенны 3: 2.4 ГГц (радио слота 0)
- Порт для антенны 4: 2.4 ГГц (радио слота 0)
- Порт для антенны 5: Не связанный
- Порт для антенны 6: 5 ГГц (разъем 2)

Необходимо настроить канал только на RAP для нисходящей линии, и затем MAP сделают выбор канала автоматизированной формой. Каналы выбраны автоматически от подмножества канала, дав каждый переход на другом канале. Например, набор канала для 5.8 полос {149, 153, 157, 161, 165}. Если нисходящая линия RAP выбрана, чтобы быть каналом 153, выбор канала берет альтернативные соседние каналы для MAP вниз дерево сетки.

Выбор канала в сети с ячеистой структурой

Каждый переход не является только другим каналом, но также и использует другую пару радио. Так, с точки зрения слотов это - то, как это похоже на переход:

Слоты на переход на Сети с ячеистой структурой

Это расположение не только предоставляет высокую пропускную способность вниз дерево сетки, поскольку пропускная способность не уменьшена экспоненциально вниз переходы по сравнению с AP1522 и моделями AP1524PS, но также и предоставляет высокую пропускную способность и устойчивую сеть против интерференции.

Примечание: Полоса Общественной безопасности (4.94 к 4.99 ГГц) не поддерживается или для Обратного рейса или для доступа клиента. Причина состоит в том, что у нас есть только 2 канала в списке общественной безопасности: 20 и 26. Интерференция между каналом связи и нисходящей линией не может избегаться использования эти каналы. Кроме того, сеть не может иметь соединения общественной безопасности и каналов общественной безопасности non. Далее, вы не можете программировать каналы радио доступа от контроллера для модели AP1524SB. Это присвоение является автоматическим в зависимости от выбора канала для других радио слота на AP.

Несмотря на то, что прежде всего радио на 2.4 ГГц используется клиентами для доступа к инфраструктуре сетки, но доступ клиента также доступен по двум радио на 5 ГГц. Доступ клиента на обоих радио обратного рейса на 5 ГГц называют свойством доступа Универсального клиента. Поскольку бродящий беспроводной клиент может приблизиться к линейным развертываниям AP1524SB с севера, и юг связал направления, свойство доступа Универсального клиента по обоим радио на 5 ГГц упрощает это.

Режим нейтрализации

Режим нейтрализации для MAP

Радио слота 1 5 ГГц в MAP также выполняет еще одну важную функцию. Это может действовать как соединительное радио для обратного рейса в случае этих сценариев:

- Сбои разъема 2
- Антенна для Разъема 2 разлагается
- Разъем 2 не в состоянии найти канал связи из-за плохого дизайна RF
- Интерференция умирает, и долгосрочный исчезает, нарушают канал связи к расширению того разъема 2, высвобождает соединительное соединение чаще

Когда Разъем 1 вступает во владение для Разъема 2, это называют Режимом нейтрализации. Разъем 2 помещен для сна на невмешивающемся канале. Другими словами, аппаратные средства уменьшены до AP1522 (два радио). Радио Slot1 расширено на канал связи. 15-минутный таймер собирается делать попытку перепросмотра для обнаружения Родителя на Слоте 2 снова.

Поведение на родительском выборе

После того, как родитель выбран, соседние узлы поддерживаются и только ищутся на том же канале как канал связи. Нисходящее радио **НЕ** будет искать лучшие соседние узлы; это будет только использоваться для расширения дерева для входящих потомков для присоединения к дереву. Нисходящее Радио не обработает сигналов-маяков, которые услышали.

Когда RAP переключается как MAP (соединение RAP с контроллером выключается), это будет использовать только одно из своих радио обратного рейса, чтобы попытаться соединиться как MAP (Лучший Родитель). Второе радио на 5.8 ГГц не привяжет клиентов и не сформирует отношения сетки.

Функциональная маршрутизация трех радио-карт

Для надлежащего линейного выравнивания и фокусирующейся радиочастоты в одном направлении, важно подключить направленную антенну к Разъемам 2 в минимуме. Необходимо выровнять и точно настроить каждую ссылку для уменьшения скрытого эффекта узла. Например, на вышеупомянутом рисунке, MAP в местоположении “C” должен быть выровненный к MAP в местоположении, MAP “B.” в местоположении “C” не должен быть в состоянии видеть AP в местоположении “A”. Это может быть достигнуто первым выравниванием антенн и затем оптимизацией каждой ссылки путем настройки питания RF.

Для получения дальнейшей информации о AP1524SB и функциях обращаются к Выпуску 7.0 Дизайна и Руководства по развертыванию Сетки.

Важные моменты, связанные, чтобы поймать в сети линейку продуктов

- AP1524SB/AP1523CV может полностью взаимодействовать с AP1522, AP1524PS, AP1240 и AP1130 как RAP или MAP.
- С этими 5.2 кодами поймайте в сети мир, объединенный назад с выпуском ПО основного контроллера, или, другими словами, мы представили сетку как комплексное решение с 5.2 кодами, которые находятся на Cisco.com.
- Много новых характеристик для увеличения пропускной способности и производительности были добавлены и в 6.0 и в 7.0 версиях.
- Cisco объявила об окончании срока службы (EOL) и для AP1505 и для MAP AP1510. Последняя дата продажи была 30 ноября 2008. Клиенты поощрены переместить свои сети на AP1520s.
- Выпуск 5.2 или больше не поддерживает AP1510 и 1505.

Конфигурация сетки

Выберите контроллер беспроводной локальной сети

Решение для беспроводной полносвязной сети поддерживается Cisco, серии 2100, Cisco WLC серии 4400, WLC серии 5500 и Беспроводной модуль интегрированного сервиса (WiSM). Cisco 5500, WiSM и 4400 контроллерам рекомендуют для развертываний беспроводной полносвязной сети, потому что они могут масштабироваться к большим числам AP, и может уровень поддержки 3 CAPWAP.

Примечание: Для всех платформ контроллера кроме 5500, MAP (AP СЕТКИ) посчитаны как “половина aps”. Другими словами, Сетка Aps (MAP) / (RAP) посчитана как “полный aps” на 5508 контроллерах.

В результате высокопроизводительный WiSM модели может управлять больше чем 300 AP Сетки. WiSM находится в форм-факторе линейной карты, и это вписывается и в 6500 и 7600 шасси.

5508 Базовых лицензий (LIC-CT5508-X) контроллера достаточны для наружных и внутренних AP (AP152X). Лицензия WPlus (LIC-WPLUS-X) была недавно объединена с Базовой лицензией и больше не требуется для внутренних MAP (1242/1130-x).

Подробные сведения о различных контроллерах и их возможностях могут быть найдены в http://www. cisco . com/en/US/products/ps6302/Products_Sub_Category_Home.html.

CAPWAP несет контроль и трафик данных между AP и WLC. Контрольным трафиком является CCM AES, но Transport Layer Security Плоскости Данных (DTLS) не поддерживается на сетке.

После выбора контроллера настройте контроллер в режиме Уровня 3.

WLC в режиме уровня 3

Обновите контроллер к этим 7.0 кодам

Cisco рекомендует обновить контроллер к 7.0 кодам в минимуме, поскольку этот код вводит много полезных возможностей для Мобильности.

Примечание: Сохраните рабочую конфигурацию контроллера с существующим кодом в некотором месте для ссылки перед обновлением. Если необходимо понизить сеть назад до старого кода по какой-либо причине, у вас будет конфигурация удобной. Несмотря на то, что конфигурация будет сохранена во время обновления к бете - коду.

Примечание: Официально, Cisco не поддерживает Переходы на более ранние версии для контроллеров.

От интерфейса графического интерфейса контроллера перейдите **к Командам> файл Загрузки**. Выберите **Code** в качестве **Типа файла** и дайте IP-адрес своего сервера TFTP. Определите путь и название файла.

Примечание: Используйте Сервер TFTP, который поддерживает передачи Размера файла на больше чем 32 МБ. Например, **tftpd32**. Под **Путем к файлу** введите**./**.

Загрузка образа на WLC с помощью TFTP

Закончено устанавливая новую микропрограмму, проверьте через CLI с помощью **команды show sysinfo**, которая новая микропрограмма действительно на месте:

```
(Cisco Controller) >show sysinfo Manufacturer's Name..............................  Cisco Systems
Inc. Product Name.....................................  Cisco Controller Product
Version.................................  6.0.61.0 RTOS
Version.....................................  6.0.61.0 Bootloader
Version.............................  4.1.171.0 Emergency Image
Version.........................  Error Build Type.....................................  DATA +
WPS System Name.....................................  SEVT-CONTROLLER System
Location.................................  System Contact.................................
System ObjectID.................................  1.3.6.1.4.1.14179.1.1.4.3 IP
Address.....................................  10.51.1.10 System Up
Time.................................  0 days 2 hrs 17 mins 13 secs System Timezone
Location.........................  Current Boot License Level.......................  Next Boot
License Level.........................  Configured Country.............................  US -
United States Operating Environment...........................  Commercial (0 to 40 C) Internal
Temp Alarm Limits.....................  0 to 65 C --More-- or (q)uit Internal
Temperature............................  +53 C State of 802.11b Network.....................
Enabled State of 802.11a Network.......................  Enabled Number of
WLANs.................................  1 3rd Party Access Point Support..................
Disabled Number of Active Clients.......................  0 Burned-in MAC
Address..........................  00:0B:85:40:4A:E0 Crypto Accelerator
1............................  Absent Crypto Accelerator 2............................  Absent
Power Supply 1.................................  Absent Power Supply
2.................................  Present, OK Maximum number of APs
supported..................  100
```

[Добавьте AP]

Если MAC-адрес BVI AP существует в контроллере, MAP могут только присоединиться к контроллеру. Фильтрация по MAC-адресам включена по умолчанию. Контроллер Cisco ведет список MAC-адреса авторизации MAP. Контроллер только отвечает на запросы на обнаружение от наружных радио, которые появляются на списке авторизации. На контроллере введите MAC-адреса всех радио, которые вы будете использовать в своей сети путем выполнения инструкций ниже.

Примечание: Для AP152X (AP IOS), MAC-адрес BVI используется на контроллере в качестве фильтра MAC. Введите MAC-адрес BVI AP на контроллере. В течение многих 1240-х и 1130-х, MAC - адрес в сети Ethernet является MAC BVI и должен использоваться в контроллере.

Если MAC-адрес AP не маркирован на AP, выполните эту команду на консоли AP:

```
At AP console: sh int | i Hardware
```

```
AP0017.94fe.d43f#sh int | i Hardware Hardware is BVI, address is 0017.94fe.d43f (bia
0017.94fe.d43f) Hardware is 802.11G Radio, address is 0017.94fe.d430 (bia 0017.94fe.d430)
Hardware is 802.11A Radio, address is 0017.94fe.d430 (bia 0017.94fe.d430) Hardware is 88E6131
Ethernet Switch Port, address is 0009.b7ff.dba4 (bia 0009.b7ff.dba4) Hardware is 88E6131
Ethernet Switch Port, address is 0009.b7ff.dba5 (bia 0009.b7ff.dba5) Hardware is 88E6131
Ethernet Switch Port, address is 0009.b7ff.dba6 (bia 0009.b7ff.dba6) Hardware is 88E6131
Ethernet Switch Port, address is 0009.b7ff.dba7 (bia 0009.b7ff.dba7)
```

На интерфейсе графического интерфейса контроллера перейдите к Безопасности и выберите MAC Filtering на левой части окна. Щелкните New... вводить MAC-адреса:

Также введите имена радио для удобства в соответствии с Описанием. Например, как названия перекрестных улиц, где радио были установлены для легкой ссылки в любое время.

Безопасность

Другая безопасность, которая может быть переключена, является EAP (по умолчанию) или PSK. Можно также сделать выбор Режима безопасности как EAP, PSK или Внешняя проверка подлинности на той же странице. От графического интерфейса пользователя (GUI) контроллера используйте этот путь:

Путь Графического интерфейса пользователя (GUI): Беспроводные сети> Сетка.

Включите безопасность на MAP

Безопасность может также быть настроена от контроллера с помощью этого CLI:

```
(Cisco Controller) >config mesh security ? eap Enable mesh security EAP for Mesh AP. psk Enable
mesh security PSK for Mesh AP. rad-mac-filter Configure Mesh security radius mac-filter for Mesh
AP. force-ext-auth Configure Mesh security to force external authentication.
```

Режим безопасности может быть проверен на контроллере этими командами:

```
(Cisco Controller) >show mesh config Mesh Range..................................... 12000
Backhaul with client access status.............. disabled Background Scanning
State..................... enabled Mesh Security Security
Mode................................ EAP External-Auth.............................
disabled Use MAC Filter in External AAA server......... disabled Force External
Authentication................. disabled Mesh Alarm Criteria Max Hop
Count.............................. 4 Recommended Max Children for MAP.............. 10
Recommended Max Children for RAP.............. 20 Low Link SNR.............................
12 High Link SNR............................... 60 Max Association
Number..................... 10 Association Interval.......................... 60 minutes
Parent Change Numbers....................... 3 Parent Change Interval.....................
60 minutes --More-- or (q)uit Mesh Multicast Mode............................ In-Out Mesh Full
Sector DFS............................ enabled Mesh Ethernet Bridging VLAN Transparent
Mode..... disabled
(Cisco Controller) >show network summary RF-Network Name............................ SEVT Web
Mode................................ Disable Secure Web Mode.........................
Enable Secure Web Mode Cipher-Option High..... Disable Secure Web Mode Cipher-Option
SSLv2..... Enable Secure Shell (ssh)..................... Enable
Telnet.................................. Enable Ethernet Multicast Mode.................
Disable Ethernet Broadcast Mode.................. Disable AP Multicast
```

```
Mode..... Unicast IGMP snooping..... Disabled
IGMP timeout..... 60 seconds User Idle
Timeout..... 300 seconds ARP Idle Timeout..... 300
seconds Cisco AP Default Master..... Disable AP Join
Priority..... Disable Mgmt Via Wireless Interface..... Enable
Mgmt Via Dynamic Interface..... Disable Bridge MAC filter
Config..... Enable Bridge Security Mode..... EAP Mesh Full
Sector DFS..... Enable --More-- or (q)uit Over The Air Provisioning of
AP's..... Disable Apple Talk ..... Disable AP Fallback
..... Enable Web Auth Redirect Ports ..... 80 Fast
SSID Change ..... Disabled 802.3 Bridging .....
Disable
```

Внешняя проверка подлинности поддерживается с помощью одного или более серверов Cisco Secure Access Control Server (ACS). ACS должен быть рабочей версией 4.1 или 4.2.

Примечание: ACS Express (5.0) не была протестирована явно, и начальные тесты указывают, что это несовместимо с существующими сертификатами VxWorks.

Конфигурация требуется на контроллере и ACS. Поддержка внешнего AAA выполнена путем проверки сертификата AP с сертификатом, установленным на ACS.

Для сети с ячеистой структурой L3, если вы используете сервер DHCP, помещает контроллер в режим L3. Сохраните конфигурацию и перезагрузите контроллер. Удостоверьтесь вы Опция configure 43 на сервере DHCP. После того, как контроллер перезапустил, недавно соединился, AP получат свой IP-адрес от сервера DHCP.

Опция 43 может использоваться для начальной загрузки таблицы адреса контроллера RAP с адресом контроллера. Это очень важно, если вы добавляете RAP к разделу сети, где это должно пересечь переход Уровня 3 для достижения контроллера. Если RAP никогда не связывался с подсетью, где контроллер подключен, это никогда не было в состоянии обнаружить эту информацию.

MAP Cisco 152X Series принимают формат Строки ASCII для Опции 43 от сервера DHCP. Cisco Aironet AP серии 152X использует разделенный от запятой формат строки для Параметра DHCP 43. Другие AP Cisco Aironet используют формат Type Length Value (TLV) для Параметра DHCP 43.

Серии AP152X является платформа IOS, таким образом, она принимает Шестнадцатеричный формат для Опции 43.

Серверы DHCP должны быть запрограммированы для возврата опции на основе строки Идентификатора класса поставщика (VCI) DHCP AP (Параметр DHCP 60).

Для конфигурации сервера DHCP в Cisco IOS Опции 43 используйте эти команды:

ip dhcp pool *<pool name>* **network** *<IP Network>* *<Netmask>* **default-router** *<Default router>* **dns-server** *<DNS Server>* **option 43 hex** *<0xf1>* *<1 byte len>* *<Controller IP addresses>*

Например, если вы хотите настроить 2 IP-адреса контроллеров для Бедра, вы имеете к Опции configure 43 как шестнадцатеричная строка в этом формате:

option 43 hex f10801041d0301041d21 | ^ ^ ^ | ^ ^ ^1.4.29.33 | ^ ^ | ^ ^1.4.29.3 | ^ | ^ length = 4 * number of ip addresses (4 * 2 = 8) | | f1 is hardcoded value that needs to be added here

Вот пример от сервера DHCP (который является CAT6K, который работает для Бедра):

```
ip dhcp pool vlan192 network 1.4.29.0 255.255.255.0 default-router 1.4.29.1 option 60 ascii
"Cisco AP c1520" option 43 hex f108.0104.1d03.0104.1d21
```

Опция Add 60 для AP152X с помощью этой команды:

```
option 60 ascii "Cisco AP c1520"
```

Определите менеджера AP

Для развертываний L3 необходимо определить **менеджера AP**. Менеджер AP действует как IP - адрес источника для связи от Контроллера до AP.

Путь: **Контроллер> Интерфейсы> менеджер AP> редактирует**.

Менеджер AP на WLC

Интерфейсу диспетчера точки доступа нужно назначить IP-адрес в той же подсети и VLAN как ваш интерфейс управления.

Примечание: “AP - диспетчер” не требуется для WLC 5508. Сам Интерфейс управления может действовать как интерфейс диспетчера точки доступа dynamic.

Группа мобильности

Группа мобильности позволяет контроллерам взаимодействовать друг с другом для поддержки бесшовного роуминга через границы контроллера. AP изучают IPs других участников группы мобильности после процесса Соединения CAPWAP. Контроллер может быть участником, одиночной группы мобильности которого до 24 контроллеров возможны. Мобильность поддерживается через 72 контроллера. Может быть до 72 участников (WLC) в списке мобильности максимум с 24 участниками (WLC) в той же группе мобильности (или домен) участвующий в клиентской руке-offs. Основное преимущество этой функции - то, что IP-адрес клиента не должен быть возобновлен в том же домене мобильности. Другими словами, возобновление IP-адреса не важно в основанной на контроллере архитектуре при помощи этой функции.

Клиенты могут переместиться эффективно (обновление no IP address, и т.д.) между группами мобильности в домене мобильности. Домен мобильности состоит из всех настроенных групп мобильности. Большое число групп мобильности может быть создано, составив домен мобильности. Предел является 72 общими количествами контроллеров в домене мобильности.

Примечание: Наличные деньги PMK только происходят в группе мобильности. В результате быстрый роуминг возможен в группе мобильности, но бесшовный роуминг возможен в целом домене мобильности (между группами мобильности).

Участники контроллера этой группы мобильности должны быть представлены вручную, нет никакого протокола для автообнаруживания других контроллеров, которые являются участниками нашей группы мобильности:

Группа мобильности на WLC

Когда беспроводной клиент связывается и аутентифицируется на AP, контроллер AP размещает запись для того клиента в ее клиентской базе данных. Эта запись включает MAC и IP-адреса клиента, контекст безопасности и ассоциации, контексты качества

обслуживания (QoS), WLAN и связанный AP. Контроллер использует эту информацию, чтобы передать кадры и управлять трафиком к и от беспроводного клиента.

Когда беспроводной клиент перемещает его ассоциацию от одного AP до другого, контроллер просто обновляет клиентскую базу данных с недавно связанным AP. Если необходимо, новый контекст безопасности и ассоциации установлены также.

Когда клиент связывается к AP, соединенному с новым контроллером, новый контроллер обменивается сообщениями мобильности с исходным контроллером, и клиентская запись базы данных перемещена в новый контроллер. Данные туннелированы между контроллерами с помощью Ether в Туннеле IP (RFC3378). Новый контекст безопасности и ассоциации установлены при необходимости, и клиентская запись базы данных обновлена для нового AP. Этот процесс остается очевидным для пользователя.

Мобильность обменивается сообщениями на WLC

После начальной настройки каждый WLC будет только знать о локальном контроллере. Информация относительно другого WLC должна быть представлена. **Щелкните New**. Вы должны для каждого WLC настроить другой WLC.

От веб-интерфейса выберите **Controller> группа мобильности** и добавьте другой WLC с его MAC-адресом менеджмента (MAC-адрес может быть найден под **Контроллером> Интерфейс> менеджмент**), и IP-адрес.

Радио-роли

По умолчанию новый AP из коробки имеет радио-роль MAP. MAP имеют беспроводное соединение и никакое прямое проводное соединение с WLC. MAP всегда сходятся через RAP.

RAP должен быть явно настроен как RAP. Это решительно уменьшает усилие по настройке как теперь, необходимо просто предварительно сконфигурировать RAP – и RAP - меньше в номере по сравнению с MAP.

Можно использовать CLI контроллера, чтобы предварительно сконфигурировать радио-роли на AP, если AP физически связан с коммутатором, или вы видите AP на коммутаторе как RAP или MAP:

```
(CiscoController) >config ap role ? rootAP RootAP role for the Cisco Bridge. meshAP MeshAP role for the Cisco Bridge. (CiscoController) >config ap role meshAP ? <Cisco AP> Enter the name of the Cisco AP. (CiscoController) >config ap role meshAP Map3 Changing the AP's role will cause the AP to reboot. Are you sure you want to continue? (y/n) y
```

Роль MAP

Установка и проверка соединения

Разверните радио (MAP) в желаемых местоположениях.

См. руководство по развертыванию для сетки.

См. руководство по установке оборудования.

Подключите AP, который вы хотите как RAP к сетевому помещению, состоящему из WLC и других сетевых компонентов и т.д.

Должна существовать возможность видеть все радио на контроллере:

Радио на WLC

```
(Cisco Controller) >show mesh ap summary AP Name AP Model BVI MAC CERT MAC Hop Bridge Group Name
------ ----------------- ---------------- ---------------- --- ----------- HPRAP1 AIR-
LAP1524PS-A-K9 00:1e:14:48:43:00 00:1e:14:48:43:00 0 test HJRAP1 AIR-LAP1522AG-A-K9
00:1d:71:0d:e1:00 00:1d:71:0d:e1:00 0 huckmesh HPMAP1 AIR-LAP1524PS-A-K9 00:1b:d4:a7:78:00
00:1b:d4:a7:78:00 1 test HJMAP1 AIR-LAP1522AG-A-K9 00:1d:71:0c:f4:00 00:1d:71:0c:f4:00 1
huckmesh HJMAP2 AIR-LAP1522AG-A-K9 00:1d:71:0c:f0:00 00:1d:71:0c:f0:00 1 huckmesh HJMAP1 AIR-
LAP1522AG-A-K9 00:1d:71:0d:d5:00 00:1d:71:0d:d5:00 1 huckmesh Number of Mesh
APs.............................. 6 Number of RAPs.................................. 2 Number
of MAPs.................................. 4
```

На интерфейсе графического интерфейса контроллера, **clickWireless** для наблюдения RAP и MAP.

RAP и MAP на WLC

Если у вас есть несколько контроллеров, подключенных к той же сети с ячеистой структурой, то необходимо задать имя главного контроллера, использующего глобальную конфигурацию для каждого AP, или задавать главный контроллер на каждом узле; иначе, наименее загруженный контроллер будет предпочтен. Если AP были ранее связаны с контроллером, они уже изучили название контроллера.

После настройки названия контроллера AP перезагрузят. Перейдите к Подробному экрану AP для наблюдения **Названия Главного контроллера** AP:

Путь: **Беспроводные сети> AP Cisco> Подробность**.

Главный контроллер на WLC

Используйте преимущества Функции обеспечения высокой доступности путем настройки IP-адресов контроллеров на каждом AP:

Настройте Функцию обеспечения высокой доступности на WLC

Ввод IP-адреса для резервного контроллера является дополнительным. Если резервный контроллер вне группы мобильности, с которой связан MAP (главный контроллер), то необходимо предоставить IP-адрес основного, вторичного, или третичный контроллер, соответственно. Название контроллера и IP-адрес должны принадлежать тому же основному, вторичному, или третичный контроллер. В противном случае MAP не может присоединиться к резервному контроллеру. Приоритет аварийного переключения AP для MAP всегда “важен”.

Примечание: Перезагрузка AP после Высокой доступности настроена.

Постороннее обнаружение

Удостоверьтесь, что обнаружение помады выключено для наружных MAP. Это было отключено по умолчанию для сохранения пропускной способности обратного рейса. Однако это - конфигурируемое использование этой команды:

```
(controller) config mesh ids-state ?
```

enable - Включает IDS (Обнаружение Жулика/Подписи) сообщающий для наружных MAP.

отключите - Отключает IDS (Обнаружение Жулика/Подписи) сообщающий для наружных MAP.

Имя группы моста

Имена группы моста (BGN) управляют ассоциацией AP. BGN могут логически сгруппировать радио для предотвращения двух сетей на том же канале от связи друг с другом. Если у вас есть несколько RAP в вашей сети в том же секторе (область), эта установка также полезна. BGN является строкой 10 максимальных чисел символов.

Установленное на заводе имя группы моста назначено в стадии производства (ПУСТОЕ ЗНАЧЕНИЕ). Это не видимо вам. В результате даже без определенного BGN, радио могут все еще присоединиться к сети. Перезагрузки точки доступа после конфигурации BGN.

Примечание: BGN должен быть настроен очень тщательно на действующей сети. Необходимо всегда запускать с самого дальнего узла (последний узел) и двигать RAP. Обоснование состоит в том, что, если вы начинаете настраивать BGN где-нибудь посреди мультиперехода, тогда узлы вне этой точки будут отброшены, поскольку эти узлы будут иметь другой BGN (старый BGN).

BGN пуст по умолчанию.

Можно настроить или проверить BGN с помощью графического интерфейса контроллера:

Путь: **Беспроводные сети> Все AP> Подробные данные**.

BGN на WLC

Если вы имеете рабочую сеть, берете предварительно сконфигурированный AP с другим BGN и заставляете его присоединиться к сети. Вы будете видеть этот AP в контроллере с помощью BGN “по умолчанию” после добавления его MAC-адреса в контроллере:

```
(CiscoController) >show mesh path Map3:5f:ff:60 00:0B:85:5F:FA:60 state UPDATED NEIGH PARENT
DEFAULT (106b), snrUp 48, snrDown 48, linkSnr 49 00:0B:85:5F:FA:10 state UPDATED NEIGH PARENT
BEACON (86B), snrUp 72, snrDown 63, linkSnr 57 00:0B:85:5F:FA:10 is RAP
```

Соседние узлы на RAP

AP152X с помощью BGN по умолчанию в качестве MAP, привяжет беспроводных клиентов и сформирует отношения сетки, но не передаст трафика Клиента Ethernet.

Удостоверьтесь, что у вас есть соответствующие BGN для каждой шпоры развертываний. Кроме того, удостоверьтесь, что у вас нет AP как “родитель по умолчанию или потомок”, поскольку эти AP войдут в режим сканирования после 15 минут, и клиентское подключение будет потеряно.

Развертывания мобильности очень чувствительны к “BGN по умолчанию”, поскольку подключение к родительскому узлу и клиентам теряется каждые 15 минут.

Интерфейс обратного рейса

“Обратный рейс” используется только для создания беспроводного соединения между AP. Интерфейс Обратного рейса по умолчанию 802.11a. Вы не можете изменить интерфейс обратного рейса на 11b/g.

В AP1524 SB Слоте 2 - радио на 5 ГГц в RAP используется для расширения обратного рейса в нисходящем направлении, где как Слот 2 - радио на 5 ГГц в MAP используется для обратного рейса в канале связи. Cisco рекомендует использовать направленную антенну с Разъемом 2. MAP расширяют Разъем 1 в нисходящем направлении с Omni или направленной антенной, также предоставляющей доступ клиента. Доступ клиента может быть предоставлен на Разъеме 2 от 7.0 кодов и позже.

Скорость передачи данных обратного рейса играет важную роль в развертываниях мобильности, поскольку скорость передачи данных решает минимальный Signal to Noise Ratio (SNR) требование для каждого перехода.

Скорости передачи данных также влияют на покрытие RF и производительность сети. Меньшие скорости передачи данных (такие как 1 Мбит/с) могут расшириться дальше от AP, чем может более высокие скорости передачи данных (такие как 54 Мбит/с). В результате скорость передачи данных влияет на покрытие ячейки и следовательно количество требуемых AP. Другие скорости передачи данных достигнуты, передав больший сигнал с избыточностью на беспроводном соединении, позволив данным быть более легко восстановленными с шума. Количество символов, отосланных для пакета в скорости передачи данных на 1 Мбит/с, больше, чем количество символов, используемых для того же пакета в 11 Мбит/с. Это означает, что передача данных в более низких битовых скоростях занимает больше времени, чем передача эквивалентных данных в более высокой битовой скорости, приводящей к пониженной пропускной способности.

Как правило, 24 мбит/с выбраны в качестве оптимальной скорости обратного рейса, потому что это выравнивается с максимальным покрытием части WLAN клиентского WLAN MAP; т.е. расстояние между MAP с помощью 24 обратных рейсов мбит/с должно обеспечить бесшовное покрытие клиента WLAN между MAP. Более низкая битовая скорость могла бы позволить большее расстояние между MAP, но в покрытии клиента WLAN, вероятно, будут разрывы, и емкость сети Backhaul уменьшена. Увеличенная битовая скорость для сети Backhaul или требует большего количества MAP или результатов в уменьшенном SNR между MAP, ограничивая надежность сетки и соединение.

Команда CLI контроллера для скорости Обратного рейса:

(Контроллер Cisco)> config ap bhrate *<скорость обратного рейса> <ap-name>*

Динамическая адаптация скорости передачи

Динамическая адаптация скорости передачи (DRA) была представлена для всех платформ сетки в выпуске 6.0. Выбор скорости является ключевой вещью для надлежащего использования доступного диапазона радиочастот. Безусловно, скорость может также влиять на пропускную способность устройств клиента, и пропускная способность является ключевой метрикой, используемой отраслевыми изданиями для оценки устройств поставщиков.

DRA представляет процесс оценки оптимального коэффициента передачи для передач пакетов. Важно должным образом выбрать скорости. Если скорость будет слишком высока, то передачи пакетов откажут получающийся в сбое связи. Если скорость будет слишком низка, то доступная пропускная способность канала не будет использоваться, приводя к нижним продуктам и потенциалу для катастрофического коллапса перегрузки сети.

Скорость передачи данных по умолчанию для обратного рейса сетки 5 ГГц остается 24 МГц.

Для использования преимуществ DRA настройте скорость передачи данных обратного рейса к “автоматическому”. С “автоматической” установкой обратный рейс сетки выбирает самую высокую скорость, где следующая более высокая скорость не может использоваться из-за условий, не являющихся подходящим для той скорости и не из-за условий, которые влияют на все скорости. Например, если Обратный рейс сетки выбрал 48 Мбит/с, то это решение было принято после проверки, что мы не можем использовать 54 Мбит/с, поскольку существует недостаточно SNR для 54 и не потому что кто-то просто включил микроволновую печь, которая будет влиять на все скорости.

Для развертываний Мобильности Cisco рекомендует использовать преимущества DRA. AP1524SB предоставляет вам лучшую пропускную способность, и пропускная способность едва ухудшается после первого перехода. Его производительность намного лучше, чем AP1522 и AP1524PS, потому что эти AP имеют только одиночное радио для канала связи обратного рейса и нисходящей линии.

С DRA каждый переход будет использовать самую лучшую скорость передачи данных для обратного рейса. Скорость передачи данных может быть изменена на основе на AP.

Скорость передачи данных может быть установлена на обратном рейсе на основе на AP. Это не команда global. После обновления к 6.0 или более поздние версии, будет сохранено предварительно сконфигурированное значение скорости передачи данных обратного рейса.

Пример: Если =24 Мбит/с RAPon, Мбит/с MAP1=18 и т.д., то конфигурации будут сохранены.

Скорость передачи данных на обратном рейсе

Используйте этот CLI для обнаружения, в какой скорости обратный рейс:

```
(Cisco Controller) >show ap bhate ? <Cisco AP> Enter the name of the Cisco AP. (Cisco Controller) >show ap bhrate HPRAP1 Backhaul Rate is auto.
```

Используйте этот CLI для настройки скорости на обратном рейсе:

```
(Cisco Controller) >config ap bhrate ? <rate in kbps> | "auto" Configures Cisco Bridge Backhaul Tx Rate. (Cisco Controller) >config ap bhrate 36000 HPRAP1 (Cisco Controller) >show ap bhrate HPRAP1 Backhaul Rate is 36000.
```

Теперь, если скорость установлена в “автоматический”, и вы хотите знать о текущей скорости, используемой на обратном рейсе, затем использовать этот CLI:

```
(Cisco Controller) >show mesh neigh summary HPRAP1 AP Name/Radio Channel Rate Link-Snr Flags State ----------------- ------- ---- -------- ------- ----- 00:0B:85:5C:B9:20 0 auto 4 0x10e8fcb8 BEACON 00:0B:85:5F:FF:60 0 auto 4 0x10e8fcb8 BEACON DEFAULT 00:0B:85:62:1E:00 165 auto 4 0x10e8fcb8 BEACON OO:0B:85:70:8C:A0 0 auto 1 0x10e8fcb8 BEACON HPMAP1 165 54 40 0x36 CHILD BEACON HJMAP2 0 auto 4 0x10e8fcb8 BEACON
```

На вышеупомянутом экране RAP использует "автоматическую" скорость передачи данных обратного рейса, и это в настоящее время использует 54 Мбит/с со своим дочерним MAP.

Последовательное питание MAP обратного рейса и конфигурация канала

Настройте канал только на RAP для нисходящей линии, и затем MAP делают выбор канала автоматизированной формой. Каналы выбраны автоматически от подмножества канала, дающего каждый переход на другом канале.

Важно иметь в виду структуру слота для радио также. Эта команда может быть дана для быстрой проверки статуса слота радиоблока:

```
(Cisco Controller 1) >show ap slots Number of APs..................................... 9 AP Name
Slots AP Model Slot0 Slot1 Slot2 Slot3 ------------------ ----- ------------------- ------- ----
---- ------- ------- HPRAP1 3 AIR-LAP1524PS-A-K9 b/g a-5.8 a-4.9 RAPSB 3 AIR-LAP1524SB-A-K9 b/g
a-all a-all HJRAP1 2 AIR-LAP1522AG-A-K9 b/g a-all HPMAP1 3 AIR-LAP1524PS-A-K9 b/g a-5.8 a-4.9
MAP1SB 3 AIR-LAP1524SB-A-K9 b/g a-all a-all HJMAP1 2 AIR-LAP1522AG-A-K9 b/g a-all HJMAP2 2 AIR-
LAP1522AG-A-K9 b/g a-all HJMAP3 2 AIR-LAP1522AG-A-K9 b/g a-all MAP2SB 3 AIR-LAP1524SB-A-K9 b/g
a-all a-all
```

От графического интерфейса контроллера используйте этот путь: **Беспроводные сети> 802.11a/n** под **Радио**.

Статус слота радиоблока

Наряду с AP соответствующие слоты радиоблока заняли и Радио-Роли, отображены для Последовательных Развертываний Обратного рейса.

Как показано в вышеупомянутом снимке экрана, Слоте 2 - радио на 5 ГГц в RAPSB (последовательный обратный рейс) используется для расширения обратного рейса в НИСХОДЯЩЕМ направлении, тогда как Слот 1 – радио на 5 ГГц в RAPSB используется для доступа клиента. Слот 2 - радио на 5 ГГц в MAPSB используется для КАНАЛА ОТ АБОНЕНТА К ОПЕРАТОРУ, и Разъем 1 в MAPSB используется для НИСХОДЯЩЕГО Omni ДОСТУПА или направленной антенны, также предоставляющей доступ клиента и так далее. С выпуском 7.0 у вас может также быть доступ клиента на Разъеме 2. Вышеупомянутый снимок экрана был взят с 6.0 кодами и был изменен с 7.0 кодами. Для получения дополнительной информации обратитесь к “Двойному Свойству доступа Универсального клиента на 5 ГГц.

Двойной доступ универсального клиента

Поскольку бродящий клиент может приблизиться к инфраструктуре сетки от любого направления, таким образом, становится важно включить доступ клиента на обоих радио обратного рейса 5 ГГц (Slot1 и 2). От 7.0 релизов кода и позже, доступ клиента возможен и по радио обратного рейса в AP1524SB и по AP1523CV. Доступ клиента отключен по обоим Радио Обратного рейса по умолчанию.

Вот рекомендации, которые будут придерживаться для включения или отключения доступа клиента на слотах радиоблока, составляющих радио на 5 ГГц, независимо от радио, используемых в качестве нисходящей линии или канала связи:

- Даже если доступ клиента на слоте 2 отключен, можно включить доступ клиента на slot1.
- Даже если доступ клиента на слоте 2 отключен, можно включить доступ клиента на slot1.
- При отключении доступа клиента на slot1, доступ клиента на слоте 2 автоматически отключен на CLI.
- Для того, чтобы только запретить расширенный доступ клиента (на разъеме 2) нужно использовать GUI.
- Вся перезагрузка MAP каждый раз, когда доступ клиента включен или отключен.

Два 802.11a радио обратного рейса используют тот же MAC-адрес. В результате могут быть экземпляры, где те же WLAN сопоставляют с тем же BSSID на нескольких слотах.

В целях документации мы вызовем доступ клиента на Разъеме 2 как Расширенный универсальный доступ (EUA).

!--- конфигурацию

Доступ клиента по обоим радио обратного рейса может быть настроен или от CLI Контроллера или от Графического интерфейса контроллера или WCS. Эти конфигурации объяснены здесь:

Настройте ЭУА от CLI контроллера

Эта команда используется для включения доступа клиента по обоим радио обратного рейса. При выполнении этой команды предупреждающее сообщение генерируется, указывая, что “тот же BSSID будет использоваться и на слотах обратного рейса и на всех Последовательных AP Сетки Обратного рейса, перезагрузит”.

config mesh client-access enable extended

Это сообщение отображено:

```
Enabling client access on both backhaul slots
Same BSSIDs will be used on both slots
All Mesh Serial Backhaul APs will be rebooted
Are you sure you want to start? (y/N)
```

И "Обратный рейс со статусом доступа клиента" и "Обратный рейс с доступом клиента расширились, статус" может быть определен с помощью **команды show mesh client-access**.

show mesh client-access

Статус появляется:

```
Backhaul with client access status: enabled
Backhaul with client access extended status(3 radio AP): enabled
```

Нет никакой явной команды для отключения доступа клиента только на Slot2 (ЭУА). Необходимо отключить доступ клиента на обоих слоты обратного рейса с помощью этой команды:

config mesh client-access disable

Это сообщение отображено:

```
All Mesh APs will be rebooted
Are you sure you want to start? (y/N)
```

От GUI можно отключить ЭУА, не нарушая доступ клиента на Разъеме 1. Но, снова, радио перезагрузят.

Возможно включить доступ клиента только на Слоте 1 а не на Слоте 2 с помощью этой команды:

config mesh client-access enable

Это сообщение отображено:

```
All Mesh APs will be rebooted
Are you sure you want to start? (y/N)
```

Настройте ЭУА от графического интерфейса контроллера

От графического интерфейса контроллера используйте этот путь: **Беспроводные сети> Сетка**.

Когда доступ клиента Обратного рейса отключен, вот снимок экрана графического интерфейса контроллера:

ЭУА на WLC

Выберите флажок **Backhaul Client Access** для отображения флажка **Extended Backhaul Client Access**. Предупреждающее сообщение будет генерироваться после нажатия **Apply** с проверенной опцией **Extended Backhaul Client Access**:

Настройте расширенный доступ клиента обратного рейса

Как только ЭУА включен, 802.11a, радио отображены как показано ниже. Слот 2 - радио на 5 ГГц в RAPSB (последовательный обратный рейс) используется для расширения обратного рейса в **НИСХОДЯЩЕМ** направлении и отображено как **НИСХОДЯЩИЙ ДОСТУП**, тогда как Слот 1 – радио на 5 ГГц в RAPSB используется для доступа клиента, отображен как **ДОСТУП**. Слот 2 - радио на 5 ГГц в MAPSB используется для **КАНАЛА ОТ АБОНЕНТА К ОПЕРАТОРУ**, отображен как **ДОСТУП КАНАЛА ОТ АБОНЕНТА К ОПЕРАТОРУ**, и Разъем 1 в MAPSB используется для **НИСХОДЯЩЕГО ДОСТУПА** со Всенаправленной антенной, также предоставляющей доступ клиента и так далее.

802.11a Радио

Создайте WLAN на WLC с надлежащим SSID, сопоставленным с корректным interface (VLAN). При создании WLAN ему применяются ко все радио по умолчанию. Если вы намереваетесь включить доступ клиента только на 802.11a радио, затем выбрать радио-политику соответственно:

Настройте ЭУА от WCS

На WCS используйте этот путь: **настройте> контроллеры> 'ip контроллера'> Сетка> Параметры настройки Сетки**.

Когда Доступ клиента Обратного рейса отключен, вот страница сетки WCS:

Выберите **Доступ клиента на** коробке **Проверки канала связи Обратного рейса** для отображения флажка **Extended Backhaul Client Access**. Предупреждающее сообщение будет генерироваться после нажатия **Save** с проверенной опцией **Extended Backhaul Client Access**:

Предупреждающее сообщение

Отмена выбора канала обратного рейса

Основная цель этой функции состоит в том, чтобы предоставить средство, при помощи которого конечный пользователь может ограничить набор каналов, доступных, чтобы быть назначенным для Последовательных RAP/MAP Обратного рейса. Обычно, для мира сетки, каналы выбраны пользователем для RAP и MAP автоматическая мелодия к каналам RAP (для AP1522 и AP1522PS) или выбирают каналы автоматически (AP1524SB и AP1523CV). Присвоение динамического канала (DCA) не было связано с миром сетки до выпуска 6.0. Однако с выпуском 7.0, существует подключение между списком DCA и последовательными MAP обратного рейса, только если кто-то использует (активирует) эту опцию.

Путем это, которым работы состоят в том, что при удалении определенных каналов из списка DCA и включения **dca-команды-канала обратного рейса сетки**, те каналы никогда не будут назначаться ни на какие последовательные AP обратного рейса согласно никакому сценарию. Даже если радар будет обнаружен на всех каналах в каналах списка DCA, то радио будет закрыто, а не перемещение к каналам снаружи. Сообщение прерывания будет передаваться WCS, и сообщение будет отображено, показывая, что радио было закрыто из-за DFS. Пользователь не будет в состоянии назначить канал на последовательный RAP обратного рейса за пределами списка DCA с **обратным рейсом сетки config dca-channels, включают**. Однако это не сценарий в случае 1522/1524PS AP. Для этих AP пользователь может назначить любой канал, даже вне списка DCA в случае RAP, и контроллер/AP может также выбрать канал вне списка DCA в случае, если никакой радарный свободный канал не доступен из списка.

Так как последовательные каналы MAP обратного рейса автоматически назначены, эта функция помогает в регулировании набора каналов, которые назначены на MAP. Например, если вы не хотите, чтобы канал 165 был назначен на какой-либо MAP 1524 года, удаляете канал 165 из DCA, перечисляют и активируют эту опцию.

Эта функция подходит лучше всего для наружных сценариев совместимости сетки с внутренними MAP или WGB, которые поддерживают набор канала, отличающийся от наружных AP. Например, канал 165 поддерживается наружными AP, но не внутренними AP в-A домене.

Полоса выбирает функцию, упрощает мобильность WGB или MAR3200 с инфраструктурой сетки, поскольку это позволяет пользователю настраивать единый набор каналов, доступных на MAP и бродящем WGB или MAR3200. Путем включения функции отмены выбора канала транзитного соединения можно ограничить назначение канала только теми каналами, которые доступны автономным AP и наружным AP.

Примечание: Отмена выбора канала только возможна в 7.0 кодах и позже.

В некоторых сценариях у вас могло бы быть две линейных дорожки или дороги для мобильности бок о бок. Поскольку выбор канала MAP происходит автоматически, таким образом, может быть переход в канале, который не доступен на автономной стороне, или канал должен быть пропущен из-за того же или соседнего канала, выбираемого в AP окружения, который принадлежит другой линейной цепочке. Можно сделать лучшее планирование частоты двух смежных шпор путем использования этой функции.

Мобильность бок о бок

[Конфигурация от CLI]

1. Используйте **команду show advanced 802.11a channel** для рассмотрения списка канала, уже настроенного в списке DCA:

```
(Controller) >show advanced 802.11a channel Automatic Channel Assignment Channel Assignment
Mode..................... AUTO Channel Update Interval..................... 600
seconds Anchor time (Hour of the day)................. 0 Channel Update
Contribution.................. SNI.. CleanAir Event-driven RRM option.............
Enabled CleanAir Event-driven RRM sensitivity.......... Medium Channel Assignment
Leader..................... 09:2b:16:28:00:03 Last
Run..................................... 286 seconds ago DCA Sensitivity
Level........................ MEDIUM (15 dB) DCA 802.11n Channel
Width..................... 20 MHz DCA Minimum Energy Limit..................... -95 dBm
Channel Energy Levels Minimum..................................... unknown
Average..................................... unknown
```

```
Maximum..................................... unknown Channel Dwell Times
Minimum..................................... 0 days, 17 h 02 m 05 s
Average..................................... 0 days, 17 h 46 m 07 s
Maximum..................................... 0 days, 18 h 28 m 58 s 802.11a 5 GHz Auto-RF
Channel List Allowed Channel List.....36,40,44,48,52,56,60,64,116,140 Unused
Channel List.................100,104,108,112,120,124,128,132,136 DCA Outdoor AP
option..................... Disabled
```

2. Для добавления канала к списку DCA используйте **config, усовершенствованный 802.11a, канал добавляет** команду *<channel number>*. Можно также удалить номер канала из списка DCA с помощью **config, усовершенствованного 802.11a, канал удаляет** команду *<channel number>*.**Примечание:** Прежде чем вы добавите или удалите номер канала из списка DCA, 802.11a, сеть должна быть отключена. Используйте **сеть config 802.11a disable** и **команды config 802.11a enable network**, чтобы отключить и включить 802.11a сеть соответственно.Кроме того, вы не можете непосредственно удалить канал из списка DCA, если он назначен на какой-либо последовательный RAP обратного рейса. Для удаления канала, назначенного на RAP, необходимо сначала переключить канал, назначенный на RAP, и затем выполнить **config, усовершенствованный 802.11a, канал удаляет** команду *<channel number>* из контроллера.

```
(Controller) >config 802.11a disable network Disabling the 802.11a network may strand mesh
APs. Are you sure you want to continue? (y/n)y (Controller) >config advanced 802.11a
channel add 132 802.11a network needs to be disabled (Controller) >config advanced 802.11a
channel delete 116 802.11a 5 GHz Auto-RF: Allowed Channel List.....
36,40,44,48,52,56,60,64,116, 132,140 DCA channels for Serial Backhaul Mesh APs is enabled.
DCA list should have at least 3 non public safety channels supported by Serial Backhaul
Mesh APs. Otherwise, the Serial Backhaul Mesh APs can get stranded. Are you sure you want
to continue? (y/N)y Failed to delete channel. Reason: Channel 116 is configured for one of
the Serial Backhaul RAPs. Disable mesh backhaul dca-channels or configure a different
channel for Serial Backhaul RAPs. (Controller) >config advanced 802.11a channel delete 132
802.11a 5 GHz Auto-RF: Allowed Channel List.....
36,40,44,48,52,56,60,64,116, 132,140 DCA channels for Serial Backhaul Mesh APs is enabled.
DCA list should have at least 3 non public safety channels supported by Serial Backhaul
Mesh APs. Otherwise, the Serial Backhaul Mesh APs can get stranded. Are you sure you want
to continue? (y/N)y (Controller) >config 802.11a enable network
```

3. Как только подходящий список DCA был создан, используйте **команду config mesh backhaul dca-channels enable** для включения функции отмены выбора канала транзитного соединения для последовательной точки доступа сетки обратного рейса. Можно выполнить **команду config mesh backhaul dca-channels disable** в случае, если должна быть отключена опция.**Примечание:** Это не требуется, чтобы отключать 802.11a сеть к позволить/запретить эта функция.

```
(Controller) >config mesh backhaul dca-channels enable 802.11a 5 GHz Auto-RF: Allowed
Channel List..... 36,40,44,48,52,56,60,64,116, 140 Enabling DCA
channels for Serial Backhaul mesh APs will limit the channel set to the DCA channel list.
DCA list should have at least 3 non public safety channels supported by Serial Backhaul
Mesh APs. Otherwise, the Serial Backhaul Mesh APs can get stranded. Are you sure you want
to continue? (y/N)y (Controller) >config mesh backhaul dca-channels disable
```

4. Можно проверить текущий статус функции отмены выбора канала транзитного соединения с помощью **команды show mesh config**.

```
(Cisco Controller) >show mesh config Mesh Range.....
12000 Mesh Statistics update period..... 3 minutes Backhaul with client
access status..... enabled Background Scanning State.....
enabled Backhaul Amsdu State..... disabled Mesh Security Security
Mode..... PSK External-Auth.....
enabled Radius Server 1..... 9.43.0.101 Use MAC Filter in External
AAA server..... disabled Force External Authentication..... disabled Mesh
Alarm Criteria Max Hop Count..... 4 Recommended Max Children
for MAP..... 10 Recommended Max Children for RAP..... 20 Low Link
```

```
SNR.............................. 12 High Link SNR.............................. 60
Max Association Number.................... 10 Association
Interval.......................... 60 minutes Parent Change
Numbers........................ 3 Parent Change Interval..................... 60
minutes Mesh Multicast Mode............................ In-Out Mesh Full Sector
DFS............................ enabled Mesh Ethernet Bridging VLAN Transparent Mode.....
enabled Mesh DCA channels for Serial Backhaul Mesh APs................ disabled
```

5. Для присвоения определенного канала на радио нисходящей линии RAP 1524 года используйте **слот config** *<номер слота>* **канал AP** *<ap-name>* команда *<channel number>*.**Примечание:** Слот 2 действует как нисходящее радио в случае 1524SB RAP. Кроме того, если отмена выбора канала обратного рейса включена, то можно назначить только те каналы, которые доступны в списке DCA.
```
(Cisco Controller) >config slot 2 channel ap RAP2-1524 136 Mesh backhaul dca-channels is
enabled. Choose a channel from the DCA list. (Cisco Controller) >config slot 2 channel ap
RAP2-1524 140
```

Конфигурация от GUI

Выполните эти шаги для настройки списка DCA и функции отмены выбора канала транзитного соединения:

Выберите **Controller> Wireless> 802.11a/n> RRM> DCA** и выберите один или несколько каналов, которые будут включены в список DCA:

Выберите **Wireless> Mesh** и выберите опцию **Mesh DCA Channels** для включения отмены выбора канала обратного рейса с помощью списка DCA. Эта опция применима для 1524SB AP.

Выполните эти шаги для установки канала для радио нисходящей линии RAP:

Выберите **Wireless>> Radio Access Points> 802.11a/n**, для настройки каналов по радио нисходящей линии RAP. Из списка AP выберите выпадающий список Антенны для RAP и выберите **Configure**:

От раздела **Назначения канала Обратного рейса RF** выберите **Custom**, и затем выберите канал для радио нисходящей линии RAP:

Полезные сведения / Вещи Иметь в виду

- Канал для последовательного RAP обратного рейса 11a радио доступа и оба 11a радио последовательных MAP обратного рейса назначен автоматически. Они не могут быть настроены пользователем.
- Часы для trap-сообщения входят в систему контроллера. В случае радарного обнаружения и изменения следующего канала, вы будете видеть сообщения, подобные этому:
```
Channel changed for Base Radio MAC: 00:1e:bd:19:7b:00 on 802.11a
radio. Old Channel: 132. New Channel: 116. Why: Radar. Energy before/after change: 0/0.
Noise before/after change: 0/0. Interference before/after change: 0/0. Radar signals have
been detected on channel 132 by 802.11a radio with MAC: 00:1e:bd:19:7b:00 and slot 2
```
- Для каждого последовательного AP обратного рейса должен всегда невмешиваться канал по его нисходящему и соединительному радио (например, если канал связи является каналом 104, какой-либо из 100, 104 и 108 каналов не могут быть назначены для нисходящего радио на том AP). В результате альтернативный соседний канал также

выбран для 11a радио доступа на RAP.

- В случае, если радарные сигналы обнаружены на всех каналах кроме соединительного радио-канала, нисходящее радио будет закрыто, и само соединительное радио будет действовать и как канал связи и как нисходящая линия (т.е. поведение подобно 1522 AP в этом случае).
- Радарное обнаружение очищено после 30 минут, таким образом, любое радио завершило работу из-за радарного обнаружения, должно быть резервное копирование и в рабочем состоянии после этой продолжительности.
- Существует 60-секундный период тишины сразу после перемещения во включенный канал DFS (независимо от того, было ли изменение канала из-за радарного обнаружения или настройки пользователя в случае RAP), во время которого AP, как предполагается, просматривает для радарных сигналов, ничего не передавая. Следовательно, если новый назначенный канал является также включенным DFS, маленький период (60 секунд) времени простоя может наблюдаться в случае радарного обнаружения. Если радарное обнаружение будет наблюдаться снова на новом канале в течение периода тишины, то родитель переключит его канал, не сообщая дочернему AP, поскольку не позволено передать в течение периода тишины. В этом случае дочерний AP разъединит и вернется к режиму сканирования, откроет вновь родителя на новом канале, и затем присоединится назад, приводя немного дольше (приблизительно трехминутный) ко времени простоя.
- В случае RAP канал для нисходящего радио всегда выбирается из списка DCA, независимо от того, включена ли функция отмены выбора канала транзитного соединения или нет. Поведение является другим для MAP, которые могут выбрать любой канал, обеспечил тот домен, пока функция отмены выбора канала транзитного соединения не включена, который ограничит набор допустимого канала. Даже если функция отмены выбора канала транзитного соединения не используется, в результате рекомендуется иметь много каналов, добавленных к 802.11a список канала DCA для предотвращения любого радио, закрываемого из-за отсутствия каналов.
- Так как тот же список DCA, который до сих пор использовался для функции RRM, также используется для MAP через функцию отмены выбора канала транзитного соединения, имейте в виду, что любое добавление/удаление каналов из списка DCA будет влиять на ввод списка канала к функции RRM MAP non также. RRM выключен для сетки.
- **Примечание:** В случае –M доменных AP немного более длинный временной интервал может требоваться для сети с ячеистой структурой подойти, так как у вас теперь есть более длинный список включенных каналов DFS в –M домене, который каждый AP будет просматривать прежде, чем присоединиться к родителю, и поэтому может взять 25 времени на %-50% больше, чем обычный для присоединения.

Подготовка к узлу и планирование

Cisco рекомендует выполнить радио-обзор узла прежде, чем установить оборудование. Обзор узла показывает проблемы, такие как интерференция, Зона Френеля или проблемы логистики. Надлежащий обзор узла включает временно устанавливающие каналы ячеистой сети и проводящие измерения, чтобы определить, точны ли ваши вычисления антенны. Обязательно определите корректное местоположение и антенну прежде, чем развернуть дыры, прокладки кабелей или установить оборудование. Посещение каждого узла, где каждый AP должен быть развернут, помогает много. Каждый видит, существует ли clear line вида (LOS), доступный и в северных и в южных направлениях.

Рекомендации по развертыванию

Это рекомендации по проектированию для каналов ячеистой сети:

- Развертывания MAP не могут превысить 35 футов в высоте выше улицы.
- MAP развернуты с антеннами, указанными и в северных и в южных направлениях с небольшим downtilt к основе для лучшего энергетического потенциала линии связи и LOS.
- Типичные расстояния RAP К MAP на 5 ГГц составляют 1000 - 4000 футов.
- Местоположения RAP, как правило, являются башнями, высокими зданиями или скрутками кабеля.
- Типичные расстояния ОТ MAP К MAP на 5 ГГц составляют 500 - 1000 футов.
- Местоположения MAP являются, как правило, короткими вершинами здания или уличными фонарями. MAP не должны быть развернуты на скрутках кабеля, поскольку нет никакого кабельного модема, требуемого в MAP.
- Типичные 2.4 / расстояния MAP КЛИЕНТУ на 5 ГГц составляют 300 - 500 футов.
- Клиентские местоположения, как правило, являются портативными ПК, CPE или профессионально установленными антеннами поверх движущегося механизма.

Будьте творческими в выборе антенн. Всегда рассматривайте усиление, направленность и поляризацию вместе при выборе антенны.

См. Антенну Cisco Aironet и Справочное руководство Accessories на антеннах Cisco и accessories.

Желательно пойти с направленными антеннами, а не всенаправленными антеннами, поскольку покрытие фокусируется вдоль дорожек или линейных контуров. С надлежащим расположением направленных антенн можно фокусировать большую часть доступной энергии RF на дорожках. Наряду с использованием большей части энергии RF, направленные антенны также увеличивают диапазон.

Антенны с шириной луча в горизонтальной плоскости и шириной луча в вертикально плоскости 30-50 ° подходят лучше всего для большинства развертываний.

Лучи

AP1524SB/1523CV имеет 5 N-разъёмов для присоединения 3 2.4 Антенны ghz (для Максимального Объединения Соотношения) и 2 N-разъёма для 5 Антенн ghz. Каждое радио имеет по крайней мере один порт TX/RX. Каждому радио нужно было подключить антенну с по крайней мере одним из ее доступных портов TX/RX.

Можно также выбрать Антенны не-Cisco. При выборе антенн из за пределами Cisco помните эти вещи:

- Cisco не отслеживает или поддерживает информацию о качестве, производительности или надежности несертифицированных антенн и кабелей.
- Подключение RF и соответствие являются ответственностью клиента.
- Соответствие только гарантируется с антеннами Cisco или антеннами, которые имеют тот же дизайн и усиление как антенны Cisco.
- Центр технической поддержки Cisco (TAC) не имеет никакого обучения или истории клиента относительно антенн не-Cisco и кабелей.

Удостоверьтесь, что у вас есть надлежащие расположения установить эти удаленные

антенны рядом с AP:

В типичном успешном развертывании клиент развернул AP1523CVs на скрутках кабеля, идущих параллельно железнодорожным путям. Две направленных антенны на обоих, радио обратного рейса использовались как серии, несущие беспроводных клиентов, приближались от обеих сторон.

Специальные монтажные кронштейны были запущены для присоединения этих 14 направленных антенн dBi к самому AP.

Если доступ клиента требуется на 2.4 ГГц в улице, то используйте преимущества Максимального Соотношения, Объединяющегося при помощи по крайней мере 2 антенн на AP1520s для полосы на 2.4 ГГц. Существуют компактные антенны, доступные для 2.4 ГГц, которые удобны для использования.

Радио (802.11a) на 5 ГГц в AP Серии AP1520 является архитектурой Одиночного в выбирают (SISO), и радио на 2.4 ГГц (802.11 b/g) 1x3 архитектура Одиночного во множественном (SIMO).

Радио на 2.4 ГГц имеет один передатчик и три приемника. С его 3 приемниками, разрешающими объединение максимального соотношения (MRC), это радио имеет лучшую чувствительность и диапазон, чем типичный SISO 802.11b/g радио для скоростей OFDM. При работе со скоростями передачи данных выше, чем 12 мбит/с, можно увеличить усиление по радио на 2.4 ГГц к 2.7 дБ путем добавления двух антенн и к 4.5 дБ путем добавления трех антенн.

Существуют короткие прямоугольные 5 Антенны ghz, доступные, который может быть подключен непосредственно к AP:

Этот перехват показывает MAP, развернутые на вершине полюса использование 17 антенн сектора dBi:

Низкая потеря кабели LMR600, выполненные от этих антенн до MAP. Здесь, направленные антенны указаны в противоположном направлении, и они используют альтернативные соседние каналы согласно дизайну последовательной сети Backhaul, таким образом, разделение антенны прекрасно. Идеально, необходимо разделить антенны вертикально на 10 футов для альтернативного плана соседнего канала. Это также минимизирует интерференцию от “Передней стороны до назад” излучений лепестка.

Можно ли задаться вопросом, где MAP?

MAP установлен на основе. Это связано с антеннами на полюсе с помощью кабелей с малыми потерями.

AP, установленный на уровне земли

Удостоверьтесь, что нет никаких других AP от наших конкурентов, развернутых рядом с нашими AP, поскольку это может создать большую интерференцию.

Близко развернутый AP конкурента

Если существует много деревьев с отключениями, они могут поглотить энергию RF, и это может создать большую вмятину в соединительном бюджете от клиента к AP, который уже борется за хорошее радиочастотное соединение к инфраструктуре сетки.

Это становится чрезвычайно важным, чтобы гарантировать, что существуют “ясные” или “близкие” условия LOS, не только между AP, но также и между серией и AP.

При зависании AP на скрутках кабеля не предоставляет ясные условия LOS, специальные приготовления установки могут быть сделаны на деревянных полюсах как показано здесь:

Кроме того, относительно “линейных развертываний”, что произойдет, если дорожка, на которой мобильность внедряется повороты? Превращение дорожки сломает соединения перехода сетки. Существуют способы обработать эту ситуацию. Одним путем является запуск новая шпора переходов путем развертывания RAP в повороте. Это очень требуется, чтобы устанавливать родительский AP в этих местоположениях, поскольку линейная ссылка перехода сломается, если вы не сделаете аналогично.

RAP, установленный в повороте

От угла логистики ищите электропитание для AP. Существует множественное электропитание, которое может принять платформа AP1520.

Электропитание включает:

- Питание уличного фонаря на 90 - 480 В переменного тока
- 12-ВОЛЬТОВЫЙ DC
- Питание кабеля
- PoE с помощью отдельной системы впрыска питанияДля получения дополнительной информации на инжекции питания, ее спецификации и установка обращаются к Cisco Aironet серии 1520 Наружные Инструкции по установке Инжектора питания точки доступа Сетки.
- Резервное питание внутренней батареи
- 802.3af-совместимый PoE для соединения IP - устройств (такой как видеокамеры)

Дополнительный модуль запасной батареи (часть № AIR-1520-BATT-6AH) доступен для AP1520s. Интегрированный аккумулятор может использоваться для временного резервного питания во время прерываний внешнего питания. Время выполнения аккумулятора для AP1520s:

- 3-часовой APoperation использование 2 радио в 77°F (25°C) с портом вывода PoE Выключено.
- 2-часовая операция AP с помощью двух радио в 77°F (25°C) с портом вывода PoE На.

Примечание: Батарейный блок не поддерживается на конфигурации кабеля AP.

- Для быстрой проверки, если AP несут аккумулятор, и заряжены ли батареи или нет, используйте эту команду, которая также показывает статус этих четырех каналов связи, нагревателя и температуры каждого AP. На этой команде можно также работать на основание AP:

```
(Cisco Controller) >show mesh env summary AP Name Temperature(C/F) Heater Ethernet Battery -
---------------- ---------------- ------ -------- ------- HPRAP1 38/100 OFF UpDnNANA N/A
HPRAP1 33/91 OFF DnDnNANA N/A HJRAP1 39/102 OFF UpDnNANA 94 % HJMAP3 33/91 OFF DnDnNANA 95 %
HJMAP2 35/95 OFF DnDnNANA 99 % HJMAP1 35/95 OFF DnDnNANA 94 % AP1510Map 33/91 OFF DOWN N/A
```

Сигнал к отношениям сигнал/шум (SINR)

При выполнении разделения территории на соты и решении расстояний между AP, важно решить вещи как типичный интервал между AP, счетчиком переходов, минимальным SNR

между AP (узлы) и т.д.

Cisco рекомендует, чтобы максимальное расстояние между этими двумя соседними узлами не превышало 2000 футов. Типичное расстояние составляет 1000 футов. Максимальные числа транзитных участков в одном направлении от RAP должны быть сведены к четырем переходам для лучшего контроля вещей.

Эта таблица показывает минимальный SNR ссылки для каждой скорости передачи данных обратного рейса:

Таблица 2: Скорости передачи данных обратного рейса и минимум требования LinkSNR

Скорость передачи данных	Минимальный требуемый SNR ссылки
54 Мбит/с	31 дБ
48 Мбит/с	29 дБ
36 Мбит/с	26 дБ
24 Мбит/с	22 дБ
18 Мбит/с	18 дБ
12 Мбит/с	16 дБ
9 Мбит/с	15 дБ
6 Мбит/с	14 dB

Требуемое минимальное значение LinkSNR делают по условию скоростью и этой формулой:

Минимальный SNR + границы замирания сигнала

- Минимальный SNR обращается к идеальному состоянию невмешательства, нешума и частоты ошибок системных пакетов (PER) не больше, чем 10%.
- Типичные границы замирания сигнала составляют приблизительно 9 - 10 дБ.
- Мы не рекомендуем использовать скорости передачи данных, больше, чем 24 мбит/с в муниципальных развертываниях ячеистой сети, поскольку требования SNR не делают расстояния практичными. Лучше использовать Динамическую функцию Присвоения Скорости для скорости обратного рейса для регулировки как доступные требования SNR.

Для надлежащего линейного выравнивания и фокусирующейся радиочастоты в одном направлении, важно подключить направленную антенну к Разъемам 2 в минимуме. Необходимо выровнять и точно настроить каждую ссылку для уменьшения скрытого эффекта узла. Дочерние узлы должны только видеть и выбрать непосредственного родителя, вместо того, чтобы перепрыгнуть к следующему переходу и выбрать соответствующий AP как родителя. Это может быть достигнуто первым выравниванием антенн и затем оптимизацией каждой ссылки путем настройки питания RF.

Существуют некоторые полезные команды, которые должны использоваться для проверки состояния ссылок между узлами.

покажите, что сетка и **сетка config** являются мощными командами, используемыми для проверки взаимосвязанности в сети:

(Cisco Controller 1) >show mesh ? env Show mesh environment. backhaul Show mesh AP backhaul info. neigh Show AP neigh list. path Show AP path. astools show mesh astools list stats Show AP stats. secbh-stats Show Mesh AP secondary backhaul stats. per-stats Show AP Neighbor Packet Error Rate stats. queue-stats Show AP local queue stats. security-stats Show AP security stats. ap Show mesh ap summary config Show mesh configurations. secondary-backhaul Show mesh secondary-backhaul ids-state Show mesh ids-state client-access Show mesh backhaul with client access. public-safety Show mesh public safety. cac Show mesh cac.
(Cisco Controller 1) >config mesh ? linktest Run linktest on the backhaul between two neighboring APs. linkdata Retrieves sampled link test data from a AP. range range from RAP to MAP Cisco Bridge (150..132000) astools Configures mesh anti-stranding. public-safety Enable/Disable 4.9GHz Public Safety Bands for Mesh AP. battery-state Disables the Battery-State for an AP client-access Enable/Disable backhaul with client access CiscoAP. multicast Configure Mesh Multicast Mode. security Set Bridge Security Mode. radius-server Configure Mesh Radius Server full-sector-dfs Configure Mesh full sector DFS status. ids-state Configures enabling/disabling of IDS)Rogue/Signature Detection) Reporting for Outdoor Mesh APs alarm Configure mesh alarm parameters. backhaul Config Mesh Backhaul. ethernet-bridging Mesh

Команда show mesh path покажет MAC-адреса, радио-роли узлов, канала и SNR Ссылки в дБ для отдельного пути:

(Cisco Controller) >show mesh path HPRAP1 AP Name/Radio Channel Rate Link-Snr Flags State ------ ----------- ------- ---- -------- ------- ----- HPRAP1 is a Root HP. (Cisco Controller) >show mesh path HPMAP1 AP Name/Radio Channel Rate Link-Snr Flags State ----------------- ------- ---- -------- ------- ----- HPRAP1 165 auto 37 0x10e8fcb8 UPDATED NEIGH PARENT BEACON HPRAP1 is a Root AP.

Канал, показанный в вышеупомянутой команде, соответствует каналу Разъема 2 в случае последовательных развертываний обратного рейса с помощью AP24SB/1523CV.

Команда show mesh neigh показывает MAC-адреса, родительско - дочерние отношения, Ссылка SNRs в дБ:

(Cisco Controller) >show mesh neigh ? detail Show Link rate neigh detail. summary Show Link rate neigh summary. (Cisco Controller) >show mesh neigh summary HJRAP1 AP Name/Radio Channel Rate Link-Snr Flags State ----------------- ------- ---- -------- ------- ----- 00:0B:85:5C:B9:20 0 auto 4 0x10e8fcb8 BEACON 00:0B:85:5F:FF:60 0 auto 3 0x10e8fcb8 BEACON 00:0B:85:62:1E:00 165 auto 2 0x10e8fcb8 BEACON 00:19:30:76:32:72 0 auto 4 0x10e8fcb8 BEACON 00:1B:0C:DE:13:34 0 auto 4 0x10e8fcb8 BEACON HJMAP2 161 54 45 0x36 CHILD BEACON HJMAP1 161 54 65 0x36 CHILD BEACON HJMAP3 161 54 44 0x36 CHILD BEACON **(Cisco Controller) >show mesh neigh summary HJMAP1** AP Name/Radio Channel Rate Link-Snr Flags State ----------------- ------- ---- -------- ------- ----- 00:0B:85:5C:B9:20 0 auto 4 0x10e8fcb8 BEACON 00:0B:85:5F:FF:60 0 auto 4 0x10e8fcb8 BEACON 00:0B:85:62:1E:00 165 auto 17 0x10e8fcb8 NEEDUPDATE BEACON DEFAULT 00:19:30:76:32:72 0 auto 19 0x10e8fcb8 BEACON 00:1B:0C:DE:13:34 0 auto 5 0x10e8fcb8 BEACON 00:1B:54:D1:FA:CE 0 auto 0 0x10e8fcb8 BEACON HJMAP2 161 auto 37 0x10e8fcb8 UPDATED NEIGH BEACON HJMAP3 161 auto 38 0x10e8fcb8 NEIGH BEACON HJMAP1 161 36 59 0x24 UPDATED NEIGH PARENT BEACON

Команда show mesh ap tree отображает счетчик переходов, SNR Ссылки и BGN:

(Cisco Controller) >show mesh ap tree ========== || AP Name [Hop Counter, Link SNR, Bridge Group Name] ||
========== [Sector 1] ---------- RAP[0, 0, shobhit] |-MAP1[1, 26, shobhit] |-MAP2[2, 14, shobhit] ---------- -- Number of Mesh APs..... 3 Number of RAPs..... 1 Number of MAPs..... 2 ----------

Роуминг по клиентской инфраструктуре Использование режима WGB

WGB является маленьким автономным устройством, которое может предоставить беспроводное подключение к инфраструктуре для Устройств с возможностью подключения к Ethernet. Устройства, не имеющие беспроводных клиентских адаптеров, для соединения с беспроводной сетью могут быть подключены к WGB через Ethernet-порт.

WGB является устройством, которое связывается к AP и предоставляет прозрачный режим моста его проводным клиентам. О каждом проводном клиенте, которого WGB изучает на его Интерфейсе Fast Ethernet, сообщают root WGB при помощи межточки доступа (IAPP) обмен сообщениями. IAPP является составляющая собственность Cisco; это работает только с AP Cisco.

WGB также предоставляет сильный канал связи к инфраструктуре AP с помощью ее высокой мощности и коэффициента усиления антенны. Обычный клиент, встроенный в портативный ПК, не может предоставить этот тип сильного канала связи, поскольку это ограничило питание и почти 0 коэффициентов усиления антенны dBi.

Роуминг в режиме WGB

Для роуминга по инфраструктуре можно или использовать беспроводную связь Cisco, автономные AP в режиме WGB или карте WMIC на MAR3200 могут быть настроены как WGB для соединения Wi-Fi с AP инфраструктуры, установленными вдоль железнодорожных путей, дороги или туннеля.

Это настроено с **мостом рабочей группы роли станции**.

Существует другой подобный беспроводной режим под названием Универсальный WGB (uWGB). Эта конфигурация позволяет WGB связываться к сети инфраструктуры Wi-Fi как клиент, это называют “универсальным”, потому что это просматривается от AP как обычный клиент с одиночным MAC-адресом (MAC-адрес от MARC). Универсальный WGB был сделан иметь совместимое WGB/WMIC с AP не-Cisco. Это не связано к IAPP или CCX.

Это настроено с **мостом рабочей группы роли станции универсальный mac-address**, mac-address, являющийся один замеченный от Инфра AP.

uWGB не так гибок как WGB в том смысле, что только одиночный клиент/интерфейс может поддерживаться позади него. Существует немного преимуществ uWGB, как он, не может быть немного быстрее как никакой IAPP, это - не-CCX и может говорить с любым AP (включая non Cisco) инфраструктура. Однако WGB может поддержать множественный MAC/клиентов позади него, не имея необходимость к NAT или маршруту.

Примечание: Наружные MAP поддерживают uWGB совместимость режима. Кроме того, uWGB только поддерживается на MAR3200 802.11bg WMIC 3201. Это не поддерживается на WMICs 3202 (4.9 ГГц) и 3205 (5 ГГц).

Существует два режима в WGB автономные AP: Режим инфраструктуры и клиентский режим BSS. Режим инфраструктуры поддерживает несколько интерфейсов VLAN позади WGB, и клиентский режим BSS только поддерживает одиночный VLAN позади WGB.

С 6.0 кодами в текущей унифицированной архитектуре Cisco поддерживает ассоциацию WGB к AP LWAPP/CAPWAP только в клиенте (или BSS) режим. Нет никакой поддержки режима инфраструктуры как в случае автономного решения. В результате WGB рассматривается как обычный беспроводной клиент контроллером. Другими словами, Cisco не поддерживает несколько интерфейсов VLAN позади WGB.

С 7.0 кодами несколько интерфейсов VLAN позади WGB поддерживаются для проводных клиентов только. Это предоставляет сегрегацию трафика на основе VLAN для других приложений, работающих на других устройствах, связанных с коммутатором позади WGB в сети с ячеистой структурой. Если у клиента будет сеть с ячеистой структурой, как правило, состоящая из 1524 AP с двойным обратным рейсом, то трафик от клиентов WGB будет передаваться в правильной очереди с приоритетами в обратном рейсе сетки на основе значений DSCP/dot1p.

Примечание: Вам нужен специальный автономный образ на автономных AP, используемых в качестве WGB или MAR для совместимости с Унифицированной инфраструктурой CAPWAP.

Мы рекомендуем выбрать любой из этих AP, которые будут использоваться в качестве WGB: AP1240, AP1250, AP1130, AP1310 или MAR3200.

AP с внешними антеннами, как AP1240, нужно дать предпочтение, как они дают сравнительно лучший энергетический потенциал линии связи.

WGB полностью совместим с наружной и внутренней инфраструктурой сетки.

Совместимость WGB

- BH — Обратный рейс
- RAP/MAP — Показывает определенные AP, используемые в качестве RAP/MAP комбинации.

Примечание: Свойство доступа универсального клиента не доступно на AP1524PS (Общественная безопасность) модель.

Примечание: Несмотря на то, что мы говорим здесь, что можно использовать AP1250 AP в качестве WGB, должно быть ясно, что вы не можете вытащить преимущества на 802.11 H из него, как использование множественных потоков, более высоких скоростей передачи данных и связывания канала, и т.д. Это - ограничение, потому что эти функции еще не доступны на стороне инфраструктуры сетки, невзирая на то, что MAP используют SISO и способы SIMO. Радио (802.11a) на 5 ГГц в AP серии AP1520 является архитектурой SISO, и радио на 2.4 ГГц (802.11 b/g) 1x3 архитектура SIMO.

A #2. Радио на 4 ГГц имеет 1 передатчик и 3 приемника. С его 3 приемниками, разрешающими объединение максимального соотношения (MRC), это радио имеет лучшую чувствительность и диапазон, чем типичный SISO 802.11b/g радио для скоростей OFDM.

Например, вы не настраиваете канал на WGB, поскольку это - клиент. Вы настраиваете канал на AP. В результате, если AP настроен с каналом 40 МГц шириной, то WGB должен быть способен к использованию верхних скоростей MCS. Однако настройка более широких каналов, чем 20 МГц еще не возможна на стороне сетки. Кроме того, Cisco имеет только 1 схему (1x3) передатчика, столь устаревший 802.11a/b/g только возможен.

Кроме того, Cisco не видит преимуществ использования AP1252 по сравнению с 1242 как WGB в 11g/11a сети из-за этих причин:

- Это стоит больше.
- Это намного больше и более тяжело.
- Это использует большее питание.
- Это не поддерживает значение "расстояния" (не релевантный для сцеплений, было бы

важно для клиента WGB моста IOS).

Преимущества 1252 (более быстрый ЦП, больше DRAM и флэш-памяти, концерта по сравнению с 100baseT) - ни один из них не предоставил бы практического преимущества в 11g/a приложении.

Роуминг по масштабируемости

Унифицированная архитектура Cisco предоставляет много масштабируемости. Как описано ранее, WLC могут принять большое число AP. Можно легко добавить контроллеры для резервирования. До 72 контроллеров могут быть частью кластера N+1. Домен мобильности (состоящий из многих групп мобильности) является зоной уверенного приема, состоящей из количества AP, группировавшихся, в котором клиент может иметь бесшовный, перемещаются, не проигрывая ее сеанс. Бродящее определение масштабируемости должно запуститься с идеи того, сколькими AP могут быть в одиночном домене мобильности.

Если вы рассматриваете пример WiSM, одиночный контроллер WiSM может управлять до 300 AP. Возможно иметь три группы мобильности. Каждая группа мобильности может иметь до 24 контроллеров. Поэтому возможно иметь 7200 AP в одиночной группе мобильности. Таким образом, решение может масштабировать больше чем 100 миль. Поскольку клиент может также свободно быстро переместиться в группах мобильности, и дизайн может быть увеличен до 72 контроллеров с клиентом, бродящим эффективно (не быстро бродящий, поскольку PMK не обменен на деньги между группами мобильности). Так, у вас может быть до 21600 AP, доказывающих бесшовный роуминг для многих миль.

Точно так же, если вы рассматриваете WLC 5508, он может управлять до 500 AP. Так, для 72 контроллеров для клиента для роуминга эффективно с помощью 3 групп мобильности у вас может быть 36000 AP, снова provding бесшовный роуминг для миль.

На стороне управления 1 WCS может управлять до 3000 AP или до 750 Контроллеров в высокой производительности. На нижнем уровне, 500 AP и 50 контроллерах. Навигатор WCS может управлять 20 WCS и 20,000 AP.

Поддержка беспроводного клиента в WGB

AP с двумя радио как WGB, конечно, предоставляют лучшее преимущество, поскольку одно из радио может использоваться для доступа клиента, и второе радио может использоваться для доступа к AP. Наличие 2 независимых радио, делающих 2 независимых функции, предоставляет лучший контроль и понижает задержку. Кроме того, беспроводные клиенты по второму радио для WGB не становятся разъединенными WGB после потери его канала связи или в бродящем сценарии. В более простых сроках одно радио должно быть настроено как Root (радио-роль), и второе радио должно быть настроено как WGB (радио-роль).

Примечание: Если одно радио настроено как WGB, то второе радио не может быть WGB или Повторителем.

Эти функции не поддерживаются для использования с WGB:

- Гибридный REAP

- Время простоя
- Web-аутентификация: Если WGB связывается к WLAN web-аутентификации, WGB добавлен к списку исключения, и все соединенные проводом клиенты WGB удалены. (WLAN web-аутентификации является другим названием для Гостевого WLAN.)
- Для проводных клиентов позади WGB, фильтрации по MAC-адресам, тестирования канала и времени простоя.

Точки для Запоминания перед Настройкой

- Cisco рекомендует использовать радио на 5 ГГц для канала связи к инфраструктуре MAP. Путем выполнения этого можно использовать преимущества сильного доступа клиента по двум радио на 5 ГГц, доступным на MAP. Кроме того, полоса на 5 ГГц главным образом позволяет больше Effective Isotropic Radiated Power (EIRP) и менее загрязнена. В двух радио-WGB настройте радио на 5 ГГц (радио 1) режим как WGB. Это радио будет использоваться для доступа к инфраструктуре сетки. Настройте второе радио 2.4 ГГц (радио 0) режим, как Поддерживают доступ клиента.
- На автономных AP только один SSID может быть назначен на собственный VLAN. Несколько интерфейсов VLAN в одном SSID не возможны на автономной стороне. Другими словами, сопоставление SSID К VLAN должно быть уникальным, поскольку это - способ, которым мы выделяем трафик на других VLAN. С другой стороны, в унифицированной архитектуре, несколько интерфейсов VLAN могут быть назначены на один WLAN (SSID).
- Только один WLAN (SSID) для связи с беспроводным устройством WGB к инфраструктуре AP поддерживается. Этот SSID должен быть настроен как SSID инфраструктуры и должен быть сопоставлен с собственным VLAN. WGB отбросит все, что не находится в собственном VLAN к инфраструктуре сетки.
- Динамический интерфейс должен быть создан в контроллере для каждой VLAN, настроенной в WGB.
- Второе радио (2.4 ГГц) на AP должно быть настроено для доступа клиента. Необходимо использовать тот же SSID по обоим радио и сопоставить с собственным VLAN. Если вы создадите отдельный SSID, то вы не будете в состоянии сопоставить его с собственным VLAN, из-за уникальных требований сопоставления VLAN/SSID. И, при попытке сопоставить SSID с другой VLAN, тогда у вас нет поддержки несколько интерфейсов VLAN беспроводных клиентов согласно сегодня.
- Все типы безопасности L2 поддерживаются для WLAN (SSIDs) для ассоциации беспроводного клиента в WGB.
- Эта функция не имеет никакой надежности от платформы AP. На стороне контроллера поддерживаются обе сетки и AP несетки.
- Если WGB говорит с инфраструктурой AP на основе унифицированной архитектуры, существует ограничение 20 клиентов в WGB. Те 20 клиентов включают и соединенный проводом и беспроводные клиенты. Если WGB говорит с автономными AP, то клиентский предел очень высок.
- Контроллер рассматривает радио и соединенных проводом клиентов позади WGB как то же, таким образом, функции как macfiltering и тестирование канала не поддерживаются для беспроводных клиентов WGB от контроллера.
- При необходимости пользователь может выполнить тестирование канала для беспроводного клиента WGB от автономного AP.

- Несколько интерфейсов VLAN для беспроводных клиентов, привязанных к WGB, не поддерживаются.
- Несколько интерфейсов VLAN до 16 поддерживаются для проводных клиентов позади WGB от выпуска 7.0 и позже.
- Роуминг поддерживается для радио и соединенных проводом клиентов позади WGB. Беспроводные клиенты по другому радио не будут отделены WGB после потери его канала связи или в бродящем сценарии.

Cisco рекомендует настроить Радио 0 (2.4 ГГц) как Root (один из режима операций для Автономного AP) и Радио 1 (5 ГГц) как WGB.

Пример конфигурации

Когда вы настраиваете от CLI, они являются обязательными:

1. dot11 SSID (безопасность для WLAN может быть решена на основе требования).
2. Сопоставьте интерфейсы sub в обоих радио к одной группе мостов.**Примечание:** Собственный VLAN всегда сопоставляется с Группой мостов 1 по умолчанию. Для другого номера виртуальной локальной сети (VLAN) соответствий Номера группы моста VLAN, как для VLAN 46, Группа мостов равняется 46.
3. Сопоставьте SSID с радиоинтерфейсами и определите роль радиоинтерфейсов.

В данном примере один SSID (WGBTEST) используется и по радио и по SSID, SSID инфраструктуры, сопоставленный с СОБСТВЕННЫМ VLAN 51. Все радиоинтерфейсы сопоставлены с группой мостов-1.

```
WGB1#config t WGB1(config)#interface Dot11Radio1.51 WGB1(config-subif)#encapsulation dot1q 51
native WGB1(config-subif)#bridge-group 1 WGB1(config-subif)#exit WGB1(config)#interface
Dot11Radio0.51 WGB1(config-subif)#encapsulation dot1q 51 native WGB1(config-subif)#bridge-group
1 WGB1(config-subif)#exit WGB1(config)#dot11 ssid WGBTEST WGB1(config-ssid)#vlan 51 WGB1(config-
ssid)#authentication open WGB1(config-ssid)#infrastructiure-ssid WGB1(config-ssid)#exit
WGB1(config)#interface Dot11Radio1 WGB1(config-if)#ssid WGBTEST WGB1(config-if)#station-role
workgroup-bridge WGB1(config-if)#exit WGB1(config)#interface Dot11Radio0 WGB1(config-if)#ssid
WGBTEST WGB1(config-if)#station-role root WGB1(config-if)#exit
```

Можно также использовать GUI автономного AP для настройки этих вещей. От GUI автоматически созданы подинтерфейсы, как только определена VLAN.

Проверка ассоциации WGB

И ассоциация WGB к контроллеру и ассоциация беспроводного клиента к WGB могут быть проверены с помощью **команды show dot11 associations client** в автономном AP:

```
WGB#show dot11 associatoions client 802.11 Client Stations on Dot11Radio1: SSID [WGBTEST] : MAC
Address IP address Device Name Parent State 0024.130f.920e 10.51.1.10 LWAPP-Parent RAPSB - Assoc
```

От контроллера выберите **Monitor> Clients**. WGB и беспроводной/проводной клиент позади WGB будут обновлены, и беспроводного/проводного клиента показывают как клиент WGB:

Результат тестирования канала

Тестирование канала может также быть выполнено от CLI контроллера с помощью этой команды:

```
(Cisco Controller) > linktest <client mac address>
```

Тестирование канала от контроллера только ограничено WGB, и это не может быть выполнено вне WGB от контроллера до проводного или беспроводного клиента, связанного с WGB. Можно выполнить тестирование канала для беспроводного клиента, связанного с WGB от самого WGB с помощью этой команды:

ap#dot11 dot11Radio 0 linktest target <client mac> Start linktest to 0040.96b8.d462, 100 512 byte packets ap# POOR (4 % lost) Time Strength(dBm) SNR Quality Retries msec In Out In Out In Out Sent : 100,Avg 22 - 37 - 83 48 3 Tot: 34 35 Lost to Tgt: 4, Max 112 - 34 - 78 61 10 Max: 10 5 Lost to Src: 4, Min 0 - 40 - 87 15 3 Rates (Src/Tgt) 24Mb 0/5 36Mb 25/0 48Mb 73/0 54Mb 2/91 Linktest Done in 24.464 msec

Проводной WGB / Беспроводной клиент

Команды TheseCLI также удобны для использования:

(Cisco Controller) >show wgb summary Number of WGBs..... 2 MAC Address IP Address AP Name Status WLAN Auth Protocol Clients ---------- ---------- ---------- ------ ---- ---- --- 00:1d:70:97:bd:e8 9.47.184.54 c1240 Assoc 2 Yes 802.11a 2 00:1e:be:27:5f:e2 9.47.184.55 c1240 Assoc 2 Yes 802.11a 5 **(Cisco Controller) >show client summary** Number of Clients..... 7 MAC Address AP Name Status WLAN/Guest-Lan Auth Protocol Port Wired 00:00:24:ca:a9:b4 R14 Associated 1 Yes N/A 29 No 00:24:c4:a0:61:3a R14 Associated 1 Yes 802.11a 29 No 00:24:c4:a0:61:f4 R14 Associated 1 Yes 802.11a 29 No 00:24:c4:a0:61:f8 R14 Associated 1 Yes 802.11a 29 No 00:24:c4:a0:62:0a R14 Associated 1 Yes 802.11a 29 No 00:24:c4:a0:62:42 R14 Associated 1 Yes 802.11a 29 No 00:24:c4:a0:71:d2 R14 Associated 1 Yes 802.11a 29 No **(Cisco Controller) >show wgb detail 00:1e:be:27:5f:e2** Number of wired client(s): 5 MAC Address IP Address AP Name Mobility WLAN Auth ---------- ---------- ---------- ---------- ---- ---- 00:16:c7:5d:b4:8f Unknown c1240 Local 2 No 00:21:91:f8:e9:ae 9.47.184.83 c1240 Local 2 Yes 00:21:55:04:07:b5 9.47.184.66 c1240 Local 2 Yes 00:1e:58:31:c7:4a 9.47.185.75 c1240 Local 2 Yes 00:23:04:9a:0b:12 Unknown c1240 Local 2 No

Роуминг WGB

Роуминг по времени является временем, потраченным ролью радио WGB, чтобы разъединить с одним AP и повторно связаться к другому AP. Во время этого интервала нет никакой передачи данных, и, поэтому, бродящее время является значительным для поддержания сеансов.

Обратите внимание на то, что роль WGB может быть установлена или на любом автономном AP или на любой из беспроводных карт микрометра (WMIC) MAR (MAR3200).

Роуминг включает два основных процесса:

- Сканирование
- Переассоциация

Сканирование

WGB поддерживает два основных режима бродящей операции:

- “Статический” режим по умолчанию - Роуминг основывается на двух основных переменных: пакетные повторные передачи или потеря восьми последовательных сигналов-маяков.
- Режим мобильной станции - Поверх предыдущих переменных, AP может сделать периодический анализ отбрасываний уровня сигнала и сдвигов скорости передачи

данных.

В основном существует четыре условия, которые инициируют WGB, чтобы начать просматривать для лучшего AP:

- Потеря восьми последовательных сигналов-маяков.
- Сдвиг в скорости передачи данных.
- Максимальное число повторов данных превышено (значение по умолчанию равняется 64).
- Измеренный период времени понижения порога уровня сигнала.

Только последние два элемента в этом списке конфигурируемы и объяснены здесь. Остаток трудно закодирован. Когда любому из вышеупомянутых критериев будут соответствовать, WGB инициирует процесс роуминга, просматривая приблизительно 10 к 20ms/channel. Можно также ограничить каналы, которые будут просмотрены через конфигурацию. Рекомендуемое использование каналов в развертываниях 3 для 802.11b/g в случае высокопроизводительного приложения, невзирая на то, что для низких сценариев пропускной способности канала передачи данных, возможно использовать уменьшенный набор, минимизировать время сканирования.

Сканирование придерживавшейся методологии является “Активным Сканированием”. Вместо того, чтобы слушать сигналы-маяки от AP, WGB активно отошлет "тестовый запрос": пакеты и ждут 20 мс для получения ответа в каждом канале. AP прекратит просматривать после того, как он получит первый ответ с удовлетворяющим сигналом. Так, период сканирования может продлиться приблизительно 40 мс. На этот раз может быть короче в зависимости от радио-типа оборудования.

Настройте мост рабочей группы для роуминга

Существует две основных формы для настройки параметров роуминга WGB:

- Используйте packet retries.
- Используйте **команду mobile station**.

Packet retries позволяет больше консервативного подхода, где WGB не запустит процесс роуминга, пока потеря данных не будет обнаружена, или пропущены восемь последовательных сигналов-маяков.

Мобильная станция запустит обычный процесс на WGB, чтобы сделать “вытесняющий” роуминг, который контролирует уровни сигнала и изменения скорости скорости, и вызовите новый роуминг, прежде чем текущий сигнал AP будет слишком низок. Когда радио выполнит просмотр канала, этот процесс просмотра инициирует маленькие разрывы в передаче радиосигналов.

Обе команды принимают эту форму под интерфейсом dot11Radio:

```
ap(config-if)#packet retries <data retry count> {drop} ap(config-if)#mobile station period X threshold Y (in dBm)
```

Если WGB начинает просматривать из-за потери восьми последовательных сигналов-маяков, сообщение "Слишком много пропущенных сигналов-маяков" отображено на консоли. В этом случае WGB действует как Универсальный Клиент Моста, во многом как любой другой беспроводной клиент в его поведении.

В некоторых ситуациях содержательно использовать дополнительную опцию

"отбрасывания" в packet retries, сохранить ассоциацию, даже на сбое для передачи пакета данных. Это полезно для стимулирующих сред RF, где роуминг может быть также инициирован мобильной командой просмотра.

Алгоритм мобильной станции оценивает две переменные: сдвиг скорости передачи данных и уровень сигнала и отвечают как:

- Если драйвер делает долгосрочное, вниз переключают скорость передачи на нижний регистр для пакетов родителю, WGB инициирует просмотр для нового родителя (не больше, чем один раз в настроенный период).
- Если драйвер делает долгосрочное, вниз переключают скорость передачи на нижний регистр для пакетов родителю, WGB инициирует просмотр для нового родителя (не больше, чем один раз в настроенный период).

Сдвиг скорости передачи данных может быть отображен с помощью этой команды:

```
debug dot11 dot11Radio 0 trace print rates
```

Однако это не покажет алгоритм сдвига скорости реальных данных в действии, но только изменения в скорости передачи данных. Это определяет период времени для сканирования, в зависимости от того, насколько была уменьшена скорость передачи данных.

Период мобильной станции должен быть установлен в зависимости от приложения. Значение по умолчанию — 20 секунд. Если, например, порог ниже установленного значения, этот период задержки предотвращает WGB от постоянного сканирования для лучшего родителя.

Некоторые ситуации могут потребовать более быстрого таймера; например, на скоростных поездах. Период не должен быть ниже, чем время, которое требуется AP завершить процесс проверки подлинности. Например, для 802.1x + сети CCKM, это не должно быть установлено ниже 2 секунд. Сети PSK могут использовать одну секунду. Фактическому периоду будут всегда добавлять одну секунду к таймеру, продукту разрешения планировщика AP для этой задачи.

Пороговые наборы уровень, на котором алгоритм инициирован для сканирования для лучшего родителя. Этот порог должен быть установлен к noise+20dBm, но не больше, чем-70dBm (+70, потому что ввод для порога положителен). По умолчанию составляет-70 дБм. Корректный порог будет зависеть от намеченной скорости передачи данных, по сравнению с уровнем покрытия, предлагаемым в среде, где будет работать WGB. Принимая надлежащее покрытие, мы должны установить этот порог, чтобы быть немного меньше, чем тогда "точка останова" для необходимой скорости передачи данных для приложений в использовании.

При включении этих параметров настройки просмотров WGB для новой родительской ассоциации, когда она встречается с плохим индикатором мощности принимаемого сигнала (RSSI), чрезмерными радиопомехами или высоким процентом потери кадра. Использование этого критерии, WGB, настроенный как мобильная станция, ищут новую родительскую ассоциацию и перемещаются новому родителю, прежде чем оно потеряет свою текущую ассоциацию. Когда значение мобильной станции отключено (настройка по умолчанию), WGB не ищет новую ассоциацию, пока это не теряет свою текущую ассоциацию.

Пороговые значения должны быть установлены согласно используемой полосе частот, поскольку она непосредственно отнесена к интерференции. Например, порог для 2.4 ГГц

должен быть установлен немного выше (на 5 дБ) по сравнению с полосой на 4.9 ГГц или на 5 ГГц, поскольку полоса на 2.4 ГГц имеет сравнительно большую интерференцию. Обратите внимание на то, что порог имеет отрицательные значения.

Пример:

- Для 2.4 ГГц`ap(config-if)#`**`mobile station period 3 threshold 70`**
- Для 5 ГГц`ap(config-if)#`**`mobile station period 3 threshold 75`**

Настройте мост рабочей группы для ограниченного сканирования канала

В мобильных средах, таких как железные дороги, WGB вместо того, чтобы просмотреть все каналы будет ограничен для сканирования только ряда ограниченных каналов для сокращения задержки переключения, когда WGB перемещается от одного AP до другого. Путем ограничения количества каналов просмотры WGB к только требуемые, мобильный WGB достигают и поддерживают непрерывное подключение WLAN с быстрым и беспрепятственный роуминг. Этот ограниченный набор канала настроен с помощью этой команды CLI:

`ap(config-if)#`**`mobile station scan`** *`<set of channels>`*
Команда CLI вызывает сканирование ко всем или указанным каналам. Нет никакого ограничения на максимальное число каналов, которые могут быть настроены. Максимальное число каналов, которые могут быть настроены, ограничено только количеством каналов, которые может поддержать радио. Когда выполняется, WGB только просматривает этот ограниченный набор канала. Эта ограниченная функция канала также влияет на известный список канала, который WGB получает от AP, до которого это в настоящее время привязывается. Каналы добавлены к известному списку канала, только если они - также часть ограниченного набора канала.

Вот пример конфигурации для вышеупомянутых конфигураций роуминга:

`ap(config)#`**`interface dot11radio 1`** `ap(config-if)#`**`ssid outside`** `ap(config-if)#`**`packet retries 16`** `ap(config-if)#`**`station role workgroup-bridge`** `ap(config-if)#`**`mobile station`** `ap(config-if)#`**`mobile station period 3 threshold 50`** `ap(config-if)#`**`mobile station scan 5745 5765`**
Используйте **команду no mobile station scan** для восстановления сканирования ко всем каналам.

MAP усилили усовершенствования 802.11 WNBU для быстрого роуминга, такие как IE QBSS, Соседняя информация о AP, централизованное управление ключами Cisco (CCKM), и т.д. MAP внедряют усовершенствования CCXV4 как AP, которому помогают, перемещаются, Расширенный соседний Список, и Перемещаются отчёт о причине. Роуминг по времени также зависит от безопасности беспроводной связи (аутентификация и шифрование) параметры настройки на WGB и используемом WLAN.

Будучи знающими о длинном времени просмотра, которое выдвигает задержку передачи выше, существует три типа просмотров, внедренных для WGB:

- Обычный просмотр
- Быстрый просмотр
- Очень быстрый просмотр

Обычный просмотр начинается на связанном канале и продолжает циклически повторяться через остаток каналов. Например, если WGB с 13 каналами был привязан к AP на канале 6,

WGB запустит свой просмотр на канале 6 тогда 7, 8, 9, 10, 11, 12, 13, 1, 2, 3, 4 и 5. После сканирования всех 11 каналов и получения нескольких тестовых ответов, WGB выполнит сравнить функцию, которая сравнивает все отвечающие AP с тем, что это было ранее привязано к в средствах уровня сигнала, загрузки и переходов. Если было только одиночный отвечающий AP, WGB не выполнит сравнить функцию и пытается сразу аутентифицироваться и связаться к новому AP.

Когда трафик между 10 и 20 пакетами в секунду, WGB выполняет **быстрый просмотр**. Просмотры WGB и партнеры к первому отвечающему AP во время быстрого просмотра.

Во время **очень быстрого просмотра** WGB не просматривает вообще и пытается связаться к лучшему AP в смежном списке, который создан с IAPP и CCX.

После того, как любая процедура сканирования завершена, WGB сравнивает отвечающие AP и пытается аутентифицироваться и связаться к лучшему AP.

WGB сравнивает отвечающие AP

Настройте соседний список поддержки

Как упомянуто ранее, WGB получит соседний список других потенциальных родительских AP, которые находятся в области. В некоторых сценариях содержательно удалить это, поскольку родительский список может иметь “направленность”. Например, в туннеле, поскольку серия переходит данное направление, полученный список только частично допустим, поскольку некоторые соседние узлы к текущему родительскому AP не будут достижимы на направлении, которое серия перемещает (серия переезжает от некоторых из них).

```
ap(config-if)# mobile station ignore neighbor-list
```

Переассоциация

Как только соседний AP найден, который удовлетворяет сигнальные характеристики, WGB будет инициировать переключение к следующему AP. WGB выполнит эти шаги:

1. Прекратите передавать данные в состоянии ожидания.
2. Передайте запрос аутентификации.
3. Получите ответ на аутентификацию.
4. Отправьте запрос переассоциации.
5. Получите ответ переассоциации.
6. Сделайте аутентификацию 802.1x.
7. Сделайте обмен EAPoL.
8. Начните передавать данные на новом AP.

802.11 Стандартные примеры процесса сопоставления

Для всех таймеров, упомянутых здесь, мы не рассматриваем повторные передачи или таймауты, которые могут варьироваться от системы до системы из-за конфигурации, или реализация (автономная и унифицированная инфраструктура имеют другие значения таймаута, например). Повторные передачи Протокола EAP могут колебаться от 100 мс до нескольких секунд длиной, и повторные передачи радиуса обычно находятся в области 2 - 5 секунд. Мы показываем здесь "лучший случай" сценарий с минимальным случаем повторных передач. В реальной жизни возможно, что некоторые повторные передачи наблюдаются, в зависимости от качества RF и/или использования сети.

Обновление IAPP является рядом обмена пакетами между WGB и WLC/WDS. Этот обмен может взять приблизительно 10 - 200 мс. Это только необходимо на режиме WGB. При использовании Универсального режима WGB не имеет место этот шаг. Это позволяет WGB сообщать об устройствах позади него и запускает их трафик.

Шаг 1 состоит на AP, исчерпывающем его текущую радио-очередь TX. Может потребоваться немного миллисекунд в зависимости от того, насколько занятый среда RF, и сколько пакетов помещено в очередь по радио в данный момент, что инициирован роуминг. Поскольку это не предсказуемо, не добавляйте его к вычислению. Это может взять максимум 4 секунд в худшем сценарии.

Обмены пакетами шагов 2-3 обрабатываются непосредственно корневой точкой доступа и могут, как правило, происходить в 1-2ms.

Шаги 4 и 5 передаются WLC в унифицированной инфраструктуре и должны быть обработаны еще в 2 мс плюс любая задержка распространения, добавленная сетью между AP и WLC. В случае автономного (IOS) инфраструктура они обрабатываются непосредственно AP.

Setp 6: 802.1X предоставляет WLAN сильным, обоюдной проверкой подлинности между клиентом и сервером проверки подлинности. Кроме того, 802.1X предоставляет динамичный для каждого пользователя, для каждого сеанса ключи шифрования, удаляя административные накладные расходы и проблемы безопасности, окружающие статические ключи шифрования. 802.1X поддерживается и Расширенным режимом WPA и Расширенным режимом WPA2.

С 802.1x учетные данные, используемые для аутентификации, такие как пароли входа, никогда не передаются в ясном, или без шифрования по беспроводной среде. В то время как аутентификация 802.1X предоставляет строгую проверку подлинности для беспроводных локальных сетей через метод EAP. TKIP или AES также необходимы для шифрования в дополнение к 802.1X, так как стандартное Шифрование WEP 802.11 уязвимо для сетевых атак.

После того, как обоюдная проверка подлинности была успешно завершена, клиент и сервер RADIUS, каждый получает тот же ключ шифрования, который используется для шифрования всех переданных данных. Использование безопасного канала на проводной LAN, сервер RADIUS передает ключ к контроллеру беспроводной локальной сети, который хранит его для клиента. Результат для каждого пользователя, для каждого сеанса ключи шифрования, с длиной сеанса, определенного политикой, определенной на сервере RADIUS. Когда сеанс истекает, или клиент перемещается от одного AP до другого, переаутентификация происходит и генерирует новый ключ сеанса.

Некоторые типы EAP более безопасны, чем у других – т.е. LEAP EAP есть имя пользователя/пароль, как mschap имеет, но вскрываем, EAP-MD5 и NULL EAP очень неуверенны.

Они более безопасны, как имя пользователя/пароль с безопасными туннелями типа:

- EAP-FAST (ГИБКАЯ АУТЕНТИФИКАЦИЯ EAP через Безопасное Туннелирование)
- EAP-TLS (Transport Layer Security)
- PEAP (защищенный расширяемый протокол аутентификации)
- EAP-TTLS (туннелировавший EAP TLS)

Cisco не рекомендует использование LEAP из-за известной уязвимости с подборами пароля по словарю. Быстрый EAP или EAP-TLS рекомендуемые более безопасные методы проверки подлинности.

Из списка выше, только EAP-FAST и EAP-TLS поддерживаются на WGB. EAP-TLS требует сервера сертификатов.

EAP-TLS более безопасен в факте, что с EAP-FAST пользователь/пароль может быть скопирован с EAP-TLS, мы используем сертификат, который будет работать только на определенные аппаратные средства.

EAP-TLS был разработан Microsoft Corporation, чтобы позволить использованию EAP как расширение PPP предоставить аутентификацию в PPP и TLS для обеспечения защищенного от целостности согласования набора шифров и обмена ключами.

EAP-TLS, который определен в RFC 2716, использует инфраструктуру открытых ключей (PKI) X.509 аутентифицируемый на сертификате IEEE 802.1X управление доступом на основе порта и в частности предназначен для адресации ко многим слабым местам в других протоколах EAP, таких как EAP-MD5. Однако в адресации к этим слабым местам, сложность развертываний увеличивается вследствие того, что не только серверы, но также и клиенты требуют сертификатов для обоюдной проверки подлинности.

EAP-FAST был разработан Cisco и подвергся IETF как интернет-проект в феврале 2004. Интернет-проект был пересмотрен и подвергся в апреле 2005. Протокол EAP-FAST является архитектурой безопасности клиент-сервер, которая шифрует транзакции EAP в туннеле TLS. В то время как подобный PEAP в этом отношении, это отличается значительно по этому, установка туннеля EAP-FAST основана на сильных общих секретных ключах, которые уникальны для пользователей. Эти тайны называют Учетными данными Защищенного доступа (PAC) и можно распределить автоматически (автоматическая или внутриполосная инициализация) или вручную (ручная или внеполосная инициализация) к устройствам клиента. Поскольку квитирования, основанные на общих секретных ключах, внутренне быстрее, чем квитирования, основанные на инфраструктуре PKI, EAP-FAST значительно быстрее, чем EAP-TLS, которые предоставляют зашифрованные транзакции EAP. EAP-FAST может использовать сертификаты для аутентификации его фазы 2 при помощи EAP-TLS во внутреннем туннеле.

Аутентификация 802.1x может варьироваться от 20 мс до нескольких секунд. Причина является дополнительными обменами кадра между клиентским и конечным сервером аутентификации плюс это любые таймеры повторной передачи на EAP, который может занять одну или более секунд. Это может включить говорящий с сервером RADIUS и/или базой данных внешнего пользователя, которая может добавить некоторую задержку на процессе.

802.1x использует метод EAP для аутентификации, каждому типу, возможно, понадобится другое количество обменов для завершения. Например, LEAP может закончиться во всего 2 кадрах, но это небезопасно. EAP-TLS, возможно, понадобятся 10 или больше обменов в зависимости от размера сертификата.

Шаг 7: После того, как 802.1x завершен потребности устройства завершить обмен EAPoL для завершения генерации ключевого материала для начала шифрования пользовательских данных. Это - 4 кадра, и может потребоваться приблизительно 20 мс для завершения

Шаг 8: После того, как аутентификация завершена, и о ключевом материале выполняют согласование, шифрование может запуститься, и WGB теперь теперь передает данные на новом AP.

Централизованное управление ключами Cisco (CCKM)

Для уменьшения времени аутентификации 802.1x Cisco поддерживает “быстрый безопасный роуминг” (CCKM) функция. С функцией CCKM 802.1x может произойти в приблизительно 50-100ms.

Каждый раз, когда WGB повторно связывается с новым AP, он должен пройти повторную проверку подлинности. Когда AAA-сервер включен, В зависимости от типа аутентификации это может увеличить бродящее время особенно.

Как показано здесь с LEAP, шесть обменов необходимы с сервером RADIUS для завершения аутентификации. (EAP подобен):

Пример LEAP

CCKM использует быстрый способ смены ключа, который позволяет клиентам переместиться от одного AP до другого. Полный 802.1X/АУТЕНТИФИКАЦИЯ EAP не требуется. CCKM уменьшает время, требуемое клиентом взаимно аутентифицироваться с новым AP и получить новый ключ сеанса во время переассоциации. CCKM быстро защищает роуминг, гарантирует, что нет никакой заметной задержки критичных по времени приложений. CCKM является CCXv4-совместимой функцией.

Пример CCKM

С CCKM первая ассоциация WMIC к инфраструктуре сделает полную аутентификацию 802.1x + согласование ключевого материала, предпринимая шаги, как ранее описано.

Затем на следующих событиях роуминга, CCKM сделает аутентификацию в то же время, это делает переассоциацию (Шаги 4 и 5), и затем повторное использование ранее согласованного ключевого материала, на первой ассоциации.

В целом CCKM удалит 802.1x и времена EAPoL от полного процесса роуминга.

Высокоскоростной роуминг совместимого с Cisco расширение (CX), клиенты версии 4 (v4) поддерживаются на скоростях до 70 миль в час в наружных развертываниях ячеистой сети AP1522s и AP1524s. Роуминг по времени зависит от различных вещей, и это было объяснено позже в этом разделе.

3 клиента уровня 2 Cisco CX v4 бродящие усовершенствования поддерживаются:

- **Точка доступа помогла роумингу** — Эта функция помогает клиентам экономить время сканирования. Когда клиент Cisco CXv4 связывается к AP, он передает информационный пакет к новой точке доступа, перечисляющей характеристики ее предыдущего AP. Роуминг по уменьшениям времени, когда клиент распознает и использует список точки доступа, созданный путем компиляции всех предыдущих AP, к который каждый клиент был привязан и передан (индивидуальная рассылка) клиенту сразу после ассоциации. Список точек доступа содержит каналы, BSSIDs соседних AP, которые поддерживают текущий SSID клиента, и время истекло начиная с разъединения.

- **Расширенный соседний список** — Эта функция внимание на улучшение клиента Cisco CX v4 перемещается опыт и производительность границы сети, особенно при обслуживании голосовых приложений. AP предоставляет свои связанные сведения о клиенте о его соседних узлах, использующих одноадресное сообщение обновления соседнего списка.
- **Переместитесь отчёт о причине** — Эта функция позволяет клиентам Cisco CX v4 сообщить о причине, почему они переместились к новому AP. Это также позволяет администраторам сети создавать и контролировать перемещаться историю.

Шифрование

Единая беспроводная сеть Cisco (UWN) включает поддержку WPA сертификаций Wi-Fi Alliance и WPA2. WPA был представлен Wi-Fi Alliance в 2003. WPA2 был представлен Wi-Fi Alliance в 2004. Весь Wi-Fi продуктов, Сертифицированный для WPA2, требуется, чтобы быть совместимым с продуктами, которые являются Wi-Fi, Сертифицированным для WPA.

WPA и WPA2 предлагают высокий уровень обеспечения для конечных пользователей и администраторов сети, что их данные останутся частными, и тот доступ к их сетям будет ограничен авторизованными пользователями. Оба имеют персональный и расширенные режимы операции, которые удовлетворяют отдельные потребности этих двух сегментов рынка. Расширенный режим каждого IEEE 802.1X использования и EAP для аутентификации. Персональный режим каждого PSK использования для аутентификации. Cisco не рекомендует персональный режим для бизнеса или правительственных развертываний, потому что это использует PSK для проверки подлинности пользователя. PSK не является масштабируемым и безопасным для Сред предприятия. WPA обращается ко всем известным уязвимостям WEP в исходной реализации безопасности IEEE 802.11, приносящей непосредственное решение по обеспечению безопасности WLAN и на предприятии и на средах small office office (SOHO). WPA использует TKIP для шифрования. WPA 2 – это следующее поколение систем безопасности Wi-Fi. Это - совместимая реализация Wi-Fi Alliance ратифицированного стандарта IEEE 802.11i. Это внедряет Национальный институт стандартов и технологий (NIST), рекомендуемый использование алгоритма шифрования AES, Отвечают на Режим Протоколом Кода аутентификации сообщения Cipher Block Chaining (CCMP). WPA2 упрощает правительство FIPS соответствие 140-2.

Для WLAN на WLC используйте или WPA1 или WPA2. Для WPA2 **AES** проверен по умолчанию, и для WPA1, **TKIP** проверен по умолчанию:

Примечание: WGB не могут связаться к MAP, если обобщенный WLAN настроен с WPA1 (TKIP), +WPA2 (AES), и интерфейс соответствующего WGB настроен с ONLY одно из этого шифрования (или WPA1 или WPA2).

WPA (2) - PSK

На этом механизме PSK используется для создания непосредственно парного главного ключа (PMK), обходящего процесс 802.1x. Это все еще должно сделать обмен EAPoL.

Фактическое время Роуминга (Просматривающий + Переассоциация + Издержки):

Приложение, Бродящее по времени = Сканирование времени + время Переассоциации + издержки WLC/WDS (Обновление IAPP).

Для WPA (2) - PSK сроки 20-40ms (бродящий по просмотру) + 2 мс (запрос на аутентификацию) + 2 мс (req помощника) + 20 мс (EAPOL) + 3-100ms (IAPP). **Мог бы варьироваться от 47-164 мс.**

Аутентификация 802.1x (без CCKM)

Для сроков Аутентификации 802.1x are20-40ms (бродящий по просмотру) + 2 мс (запрос на аутентификацию) + 2 мс (req помощника) + 20-2500ms или больше (dot1x) + 20 мс (EAPOL) + 3-100ms (IAPP). **Мог бы варьироваться от 67-2664 мс.**

Аутентификация 802.1x плюс CCKM

20-40ms (бродящий по просмотру) + 2 мс (запрос на аутентификацию) + 2 мс (req помощника) + 3-100ms (IAPP). **Мог бы варьироваться от 27-144 мс.**

Заключение

CCKM менее восприимчив к проблемам, поскольку он имеет только два кадра, которые должны быть правильно переданы для завершения бродящего изменения состояния. Общее время для успешного перемещается, является в среднем очень маленьким, который полезен для голоса и/или видеоприложений.

PSK является одной альтернативой, но в среднем каждый раз роуминга медленнее, чем CCKM и более вероятен для сбоя из-за проблем RF (больше необходимых обменов пакетами). Кроме того, это, может быть менее безопасным в зависимости от используемого ключа проверки подлинности. Преимущество является более быстрым временем восстановления, при сравнении с полным 802.1x, необходимым на сценарии отказов CCKM.

Основное различие в PSK по сравнению с CCKM, то, что для PSK, любая повторная передача процесса EAPoL умножит общее время. В PSK необходимо завершить шесть обменов кадров (ассоциация + EAPoL M1 к M4), которые являются большей частью критической точки, поскольку любой сбой здесь будет влиять на общее время роуминга.

CCKM, бродящий по сбою, означает, что следующий роуминг является основанным 802.1x (замедляются), тогда последующий роуминг является CCKM снова.

Ситуация проста: или они используют ключевое кэширование, которое мы поддерживаем и рекомендуем быть CCKM или работать на 802.1x, основанный, бродя, с временами между 1 и 20 секундами на каждом роуминге, который не предсказуем.

Таблица 3: Роуминг и другие числа производительности

Тип защиты	Роуминг по задержке	Вероятность
802.1x WPA2 с CCKM	<200 мс	95% времени
802.1x WPA2 с CCKM	200 мс – 800 мс	4% времени

802.1x WPA2 с CCKM	> 800 мс	1% времени

Примечание: Беспроводные технологии разработаны с помощью систем радиосвязи, которые подвергаются интерференции радиоволны. Причины этой интерференции могут быть случайными или преднамеренными. Независимо от источника интерференция может прервать беспроводное соединение, отключив любое решение, которое зависит от Wi-Fi. Учитывая такие риски, решения, которые влияют на общественную безопасность, не должны зависеть SOLELY от беспроводных технологий. Избыточный, наложение и независимые системы (например, оба соединенные проводом и радио) предпочтены. В контексте систем центра управления движением поездов, примерах наложения, избыточные системы включают, но не ограничены: соединяя беспроводные технологии с двумя или больше независимыми системами, механические системы (например, “мертвец переключается”), центр управления движением поездов, сигнализирующий по металлическим направляющим и встроенному и центральному человеческому упущению (машинист) или супервизоры центрального управления. Если один системный сбой, другая независимая система все еще была бы доступна, порция снижают риск для общественной безопасности.

Советы по поиску и устранению неполадок

Если беспроводной клиент не связывается к WGB, выполните эти шаги в устранение неполадок:

1. Проверьте конфигурацию клиента и удостоверьтесь, что конфигурация клиента является надлежащей.
2. Проверьте **выходные данные show bridge** в автономном AP и соответствуйте, AP читает MAC - адрес клиента в правильном интерфейсе.
3. Подтвердите, что интерфейсы sub, соответствующие конкретным VLAN в других интерфейсах, сопоставлены с той же группой мостов.
4. При необходимости очиститесь, запись моста с помощью **команды clear bridge** (помните, что эта команда удалит все соединенные проводом и беспроводные клиенты, привязанные в WGB, и заставит их связаться снова).
5. Проверьте **показывают** выходные данные **ассоциации dot11** и соответствуют, WGB привязан к контроллеру успешно.
6. WGB имеет ограничение с 20 клиентами, поэтому удостоверьтесь, что вы не превысили предел.

В обычном сценарии, если **show bridge** и **показывают**, выходные данные **ассоциации dot11** как ожидалось, ассоциация беспроводного клиента должна быть успешной.

Если существуют какие-либо проблемы канала связи WGB, эти команды могут использоваться:

```
debug dot11 d0/1 tr pr uplink debug dot11 wpa-cckm-km-dot1x debug dot11 mgmt msg debug dot11 mgmt int
```

Важные сценарии

- Беспроводные клиенты должны рассматриваться как обычный клиент для автономного

AP и функций как ACL, фильтрация по MAC-адресам и аутентификация от LRS, который может быть применимым для этих клиентов, если настроено от WGB (все автономные функции поддерживаются).
- Беспроводные клиенты по другому радио не должны быть отделены WGB после потери его канала связи или в бродящем сценарии.
- Групповая адресация должна поддерживаться для беспроводных клиентов позади WGB.
- Беспроводные клиенты позади WGB должны получить то же право проводного клиента позади WGB в контроллере.

Несколько интерфейсов VLAN и поддержка QoS WGB проводные клиенты

Обзор функций

WGB является маленьким автономным устройством, которое может предоставить беспроводное подключение к инфраструктуре для Устройств с возможностью подключения к Ethernet. Устройства, не имеющие беспроводных клиентских адаптеров, для соединения с беспроводной сетью могут быть подключены к WGB через Ethernet-порт. Мост WGB связывается с корневой точкой доступа через беспроводной интерфейс. Таким образом проводные клиенты получают доступ к беспроводной сети.

Эта функция предоставляет сегрегацию трафика на основе VLAN для других приложений, работающих на других устройствах, связанных с коммутатором позади WGB. Трафик от клиентов WGB будет передаваться в правильной очереди с приоритетами в обратном рейсе сетки на основе значений DSCP/dot1p.

До 16 VLAN поддерживаются для проводных клиентов позади WGB.

Примечание: Вам нужен специальный автономный образ на автономных AP, используемых в качестве WGB для совместимости с Унифицированной инфраструктурой CAPWAP. Этот образ будет объединен со следующим официальным автономным выпуском. Эта функция не доступна для MAR.

WGB и несколько интерфейсов VLAN

WGB сообщает WLC о проводной клиентской информации VLAN в сообщении ассоциации IAPP. WGB удаляет 802.1q заголовок от пакета при передаче к WLC. WLC передаст пакет к WGB без 802.1q, метка и WGB добавляют 802.1q заголовок к проводному коммутатору, на основе MAC - адреса назначения.

WLC будет рассматривать клиента WGB как клиента VLAN и передавать пакет в правильном интерфейсе виртуальной локальной сети (VLAN) на основе источника с MAC-адресом

Объединенному клиенту WGB нужно включить для поддержки несколько интерфейсов VLAN на WGB. Это отключено по умолчанию.

```
WGB(config)#workgroup-bridge unified-vlan-client
```

Необходимо настроить подинтерфейсы на WGB, соответствующем VLAN на портах коммутатора, с которыми связаны соединенные проводом клиенты.

Точки для Запоминания перед Настройкой

- Динамический интерфейс должен быть создан в контроллере для каждой VLAN, настроенной в WGB.
- Только один WLAN (SSID) для связи с беспроводным устройством WGB к инфраструктуре AP поддерживается. Этот SSID должен быть настроен как SSID инфраструктуры и должен быть сопоставлен с собственным VLAN. WGB отбросит все, что не находится в собственном VLAN к инфраструктуре сетки.
- WGB считает порт коммутатора позади как клиента в его таблице MAC-адресов.
- Рекомендуется настроить тот же собственный VLAN в соединительном WLC порта коммутатора, WGB, и в коммутаторе позади WGB.Все клиенты собственного VLAN на Стороне Ethernet WGB будут частью той же VLAN, в которой WGB является asscoicated. WGB будет частью VLAN, к которой WLAN (в который WGB связался), сопоставлен.Например, если радио WGB 5 ГГц (dot11radio 1) сопоставлено с собственным VLAN 184, и коммутатор позади WGB соединил клиентов проводом только в VLAN 185 и 186, то вы не можете потребовать, чтобы собственный VLAN на порте коммутатора был идентичен собственному VLAN на WGB (VLAN 184). Однако Cisco всегда рекомендует настроить тот же собственный VLAN на порте коммутатора как собственный VLAN WGB.**Неидентичные собственные VLAN** С другой стороны, если вы добавляете 1 проводного клиента в VLAN 184, и этот клиент VLAN в WGB принадлежит собственному VLAN, необходимо определить тот же собственный VLAN на коммутаторе.**Тот же собственный VLAN**
- Мобильность межподсети поддерживается с этой функцией клиентов VLAN позади WGB с ограничением, что, динамический интерфейс для всех VLAN WGB должен быть настроен во всех контроллерах.
- Совместимость с объединяющей VLAN функцией не поддерживается. Когда объединяющая VLAN опция будет активирована, WGB и его клиенты собственного VLAN будут частью той же VLAN.
- Замена AAA для клиентов WGB не поддерживается. Однако замена AAA для WGB поддерживается.
- Только групповая адресация Уровня 3 предоставлена для клиентов VLAN WGB и нет никакой поддержки групповой адресации уровня 2.
- Существует ограничение 20 клиентов в WGB, и беспроводные клиенты включены в этот номер.
- Тестирование канала для соединенного проводом клиента WGB не поддерживается.
- Роуминг поддерживается для радио и соединенных проводом клиентов позади WGB.
- Групповая адресация поддерживается для проводных клиентов позади WGB
- Широковещание поддерживается.

Схема сети

Настройте через CLI в WGB (Пример)

В данном примере VLAN 184 и 185 существуют на проводном коммутаторе позади WGB. Собственный VLAN WGB равняется 184. SSID является **auto-wgb**, сопоставленным с собственным VLAN 184. Радио 1 радио (на 5 ГГц) используется для соединения с инфраструктурой CAPWAP с помощью этого SSID.

```
ap#config t ap(config)#workgroup-bridge unified-vlan-client ap(config)#int FastEthernet0.184
ap(config-subif)#encapsulation dot1q 184 native ap(config-subif)#bridge-group 1 ap(config-
subif)#exit ap(config)#int FastEthernet0.185 ap(config-subif)#encapsulation dot1q 185 ap(config-
subif)#bridge-group 185 ap(config-subif)#exit ap(config)#int Dot11Radio 1.185 ap(config-
subif)#encapsulation dot1q 185 ap(config-subif)#bridge-group 185 ap(config-subif)#exit
ap(config)#int Dot11Radio 1.184 ap(config-subif)#encapsulation dot1q 184 native ap(config-
subif)#bridge-group 1 ap(config-subif)#exit ap(config)#dot11 ssid auto-wgb ap(config-
ssid)#authentication open ap(config-ssid)#infrastructure-ssid ap(config-ssid)#vlan 184
ap(config-ssid)#exit ap(config)#int Dot11Radio 1 ap(config-if)#station-role workgroup-bridge
ap(config-if)#ssid auto-wgb ap(config-if)#exit ap(config)#bridge irb ap(config)#hostname WGB
```

bridge irb используется для включения Интегрированной маршрутизации и соединение при помощи мостов; что-то, что Автоматический код AP сохранил от других более высокопроизводительных платформ.

Нужно создать динамические интерфейсы 184 и 185 на WLC для вышеупомянутой конфигурации для работы. WGB обновит WLC о проводных клиентских сведениях о виртуальной локальной сети (VLAN) в сообщении ассоциации IAPP. WLC будет рассматривать клиента WGB как клиента VLAN и передавать пакет в правильном интерфейсе виртуальной локальной сети (VLAN) на основе источника с MAC-адресом. В восходящем направлении WGB удалит 802.1q заголовок от пакета при передаче к WLC. В нижележащем направлении WLC передаст пакет к WGB без 802.1q, метка и WGB добавят 802.1q заголовок на основе MAC - адреса назначения при передаче пакета к коммутатору, подключающему проводного клиента.

Выходные данные моста WGB

```
WGB#sh bridge Total of 300 station blocks, 292 free Codes: P - permanent, S – self Bridge Group
1: Address Action Interface Age RX count TX count 0023.049a.0b12 forward Fa0.184 0 2 0
0016.c75d.b48f forward Fa0.184 0 21 0 0021.91f8.e9ae forward Fa0.184 0 110 16 0017.59ff.47c2
forward Vi0.184 0 23 22 0021.5504.07b5 forward Fa0.184 0 18 6 0021.1c7b.38e0 forward Vi0.184 0 6
0 Bridge Group 185: 0016.c75d.b48f forward Fa0.185 0 10 0 001e.5831.c74a forward Fa0.185 0 9 0
```

Подробность WGB о контроллере

```
(Cisco Controller) >show wgb summary Number of WGBs................................... 2 MAC
Address IP Address AP Name Status WLAN Auth Protocol Clients ----------------- --------------- -
---------------- --------- ---- ---- --- 00:1d:70:97:bd:e8 9.47.184.54 c1240 Assoc 2 Yes 802.11a
2 00:1e:be:27:5f:e2 9.47.184.55 c1240 Assoc 2 Yes 802.11a 5 (Cisco Controller) >show client
summary Number of Clients.............................. 7 MAC Address AP Name Status
WLAN/Guest-Lan Auth Protocol Port Wired 00:00:24:ca:a9:b4 R14 Associated 1 Yes N/A 29 No
00:24:c4:a0:61:3a R14 Associated 1 Yes 802.11a 29 No 00:24:c4:a0:61:f4 R14 Associated 1 Yes
802.11a 29 No 00:24:c4:a0:61:f8 R14 Associated 1 Yes 802.11a 29 No 00:24:c4:a0:62:0a R14
Associated 1 Yes 802.11a 29 No 00:24:c4:a0:62:42 R14 Associated 1 Yes 802.11a 29 No
00:24:c4:a0:71:d2 R14 Associated 1 Yes 802.11a 29 No (Cisco Controller) >show wgb detail
00:1e:be:27:5f:e2 Number of wired client(s): 5 MAC Address IP Address AP Name Mobility WLAN Auth
----------------- --------------- ----------------- ---------- ---- ---- 00:16:c7:5d:b4:8f
Unknown c1240 Local 2 No 00:21:91:f8:e9:ae 9.47.184.83 c1240 Local 2 Yes 00:21:55:04:07:b5
9.47.184.66 c1240 Local 2 Yes 00:1e:58:31:c7:4a 9.47.185.75 c1240 Local 2 Yes 00:23:04:9a:0b:12
Unknown c1240 Local 2 No WGB_1#sh ip int brief Interface IP-Address OK? Method Status Protocol
BVI1 9.47.184.55 YES DHCP up up Dot11Radio0 unassigned YES unset admindown down Dot11Radio1
unassigned YES TFTP up up Dot11Radio1.184 unassigned YES unset up up Dot11Radio1.185 unassigned
YES unset up up FastEthernet0 unassigned YES other up up FastEthernet0.184 unassigned YES unset
up up FastEthernet0.185 unassigned YES unset up up Virtual-Dot11Radio0 unassigned YES TFTP up up
Virtual-Dot11Radio0.184 unassigned YES unset up up Virtual-Dot11Radio0.185 unassigned YES unset
up up
```

Советы по поиску и устранению неполадок

Если клиент WGB не связывается к WGB, эти шаги могут использоваться для устранения проблем:

1. Собственный VLAN, настроенный на WGB, должен быть тем же на порте коммутатора, с которым связан WGB. Порт коммутатора, связанный с WGB, должен быть Транком.
2. Проверьте конфигурацию клиента и удостоверьтесь, что конфигурация клиента является надлежащей.
3. Проверьте **выходные данные show bridge** в автономном AP и подтвердите, что AP читает MAC - адрес клиента в правильном интерфейсе.
4. Подтвердите интерфейсы sub, соответствующие конкретным VLAN, и sub другие интерфейсы сопоставлены с группой мостов.
5. При необходимости очиститесь, запись моста с помощью **команды clear bridge** (помните, что эта команда удалит все соединенные проводом и беспроводные клиенты, привязанные в WGB, и заставит их связаться снова).
6. WGB имеет ограничение с 20 клиентами, поэтому удостоверьтесь, что вы не превысили предел.
7. До 16 VLAN поддерживаются для Проводных Клиентов позади WGB.

QoS на инфраструктуре сетки

Cisco поддерживает 802.11e на локальном доступе и на обратном рейсе. MAP располагают по приоритетам трафик пользователя на основе классификации, и поэтому весь трафик пользователя рассматривается на наилучшим образом основание.

Ресурсы, доступные пользователям сетки, варьируются, согласно местоположению в сетке и конфигурации, которая предоставляет ограничение пропускной способности в одной точке сети, может привести к превышению подписки в других частях сети.

Точно так же ограничение клиентов на их проценте от RF не подходит для клиентов сетки. Ограничивающий ресурс не является клиентским WLAN, но ресурсами, доступными на обратном рейсе сетки. Подобный проводным Сетям Ethernet, WLAN 802.11 используют Множественный доступ с контролем несущей (CSMA), но вместо того, чтобы использовать обнаружение коллизий (CD), WLAN используют предотвращение коллизий (CA). Это означает, что вместо каждой станции, пытающейся передать, как только среда свободна, устройства WLAN будут использовать механизм предотвращения коллизий, чтобы препятствовать тому, чтобы множественные станции передали в то же время.

Механизм предотвращения коллизий использует два значения, названные aCWmin и aCWmax. CW обозначает окно конфликта. CW определяет, какое дополнительное количество времени оконечная точка должна ждать, после межкадрового пространства (IFS), чтобы попытаться передать пакет. Улучшенная распределенная функция координации (EDCF) является моделью, которая позволяет конечные устройства, которые имеют чувствительный к задержке мультимедийный трафик для изменения их aCWmin и значений aCWmax для учета статически больше (и более частый) доступ к среде.

AP Cisco поддерживают подобное EDCF QoS. Это предоставляет до восьми очередей для QoS. Эти очереди могут быть выделены несколькими другими способами:

- На основе TOS / параметры пакетов DiffServ.
- На основе списков доступа Уровня 2 или Уровня 3.
- На основе VLAN.
- На основе динамической регистрации устройств (IP-телефоны).

1520 Cisco Aironet, в сочетании с контроллерами Cisco, предоставляет минимальную

возможность интегрированных сервисов в контроллере, в котором клиентские потоки имеют колпачки максимальной пропускной способности, и более устойчивые дифференцированные сервисы (diffServ) возможность на основе значений IP DSCP и замен WLAN QOS.

Когда емкость очереди была достигнута, дополнительные кадры отброшены (отбрасывание остатка).

Encapsulation

Существует несколько инкапсуляций, используемых системой сетки. Они включают контроль за CAPWAP и данные между контроллером и RAP по обратному рейсу сетки, и между MAP клиенту. Инкапсуляция мостового соединения трафика (трафик неконтроллера от LAN) по обратному рейсу совпадает с инкапсуляцией данных CAPWAP.

Существует две инкапсуляции между контроллером и RAP. Первое для контроля за CAPWAP и второго для данных CAPWAP. В экземпляре контроля CAPWAP используется в качестве контейнера для контрольной информации и директив. В экземпляре данных CAPWAP целый пакет, включая Ethernet и IP - заголовки, передан в контейнере CAPWAP (см. Инкапсуляции).

Инкапсуляции

Для обратного рейса существует только один тип инкапсуляции, инкапсулируя трафик сетки. Однако два типа трафика инкапсулируются: мостовое соединение трафика и контроля за CAPWAP и трафика данных. Оба типа трафика инкапсулируются в составляющем собственность заголовке сетки.

В случае мостового соединения трафика Фрейм Ethernet целого пакета инкапсулируется в заголовке сетки (см. Трафик Сетки Инкапсуляции).

Все кадры обратного рейса рассматриваются тождественно, независимо от того, являются ли они MAP к MAP, RAP к MAP или MAP к RAP.

Инкапсуляция трафика сетки

В случае мостового соединения переданы кадры, поскольку они получены во входе к Порту Ethernet AP.

Организация очереди на AP

AP использует высокоскоростной ЦП для обработки входных кадров, Ethernet и радио на сначала прибывшей основе первой подачи. Они помещены в очередь для передачи к соответствующему устройству вывода, или Ethernet или радио. Выходные кадры могут быть предназначены или для клиентской сети 802.11, сети Backhaul 802.11 или для Ethernet.

AP Cisco Aironet серии 1520 поддерживает четыре FIFOs для передач беспроводного клиента. Эти FIFOs соответствуют 802.11e платина, золото, серебро и бронзовые очереди, и повинуются 802.11e правила передачи для тех очередей. FIFOs имеют конфигурируемую пользователем глубину очереди.

Аналогично, обратный рейс (кадры, предназначенные для другой внешней точки доступа), использует четыре FIFOs, хотя трафик пользователя ограничен золотом, серебром и бронзой. Платиновая очередь используется исключительно для контрольного трафика

CAPWAP и Голоса, и была переделана из стандарта 802.11e параметры для CWMIN, CWMAX, и так далее, для обеспечения большей устойчивой передачи, но более длительные задержки.

Точно так же 802.11e параметры для CWMIN, CWMAX, и так далее, для золотой очереди были переделаны для обеспечения более низкой задержки за счет немного более высокой частоты ошибок и агрессивности. Цель этих изменений состоит в том, чтобы предоставить канал, более способствующий видеоприложениям.

Кадры, предназначенные для Ethernet, помещены в очередь как FIFO до максимального доступного пула буфера передачи (256 кадров). Существует поддержка Кодовой точки дифференцированных сервисов (DSCP) IP Уровня 3, таким образом отмечание пакетов там также.

(В контроллере к пути RAP для трафика данных внешнее DSCP-значение установлено в DSCP-значение кадра входящего IP. Если интерфейс находится в тэговом режиме, контроллер устанавливает ИДЕНТИФИКАТОР VLAN 802.1Q и происходит 802.1p UP (внешний) от 802.1p поступление UP и потолок приоритета по умолчанию WLAN. Кадры с ИДЕНТИФИКАТОРОМ VLAN 0 не будут помечены (см. Контроллер к Пути RAP).

Контроллер к пути RAP

Для CAPWAP контрольный трафик к значению IP DSCP установлен в *46*, и 802.1p, приоритет пользователя установлен в *7*. До передачи беспроводного кадра по обратному рейсу, независимо от соединения узла (RAP/MAP) или направление, DSCP-значение во внешнем заголовке используется для определения приоритета обратного рейса. Следующие разделы описывают сопоставление между четырьмя очередями обратного рейса использование AP и DSCP-значения, показанные в QoS Пути Обратного рейса.

Таблица 4: QoS пути обратного рейса

DSCP-значение	Очередь обратного рейса
2, 4, 6, 8-23	Бронза
26, 32-63	Золото
46-56	Платина
Все другие, включая 0	Серебро

Примечание: Платиновая очередь обратного рейса зарезервирована для контрольного трафика CAPWAP, контрольного трафика IP и Голосовых пакетов. DHCP, DNS и запросы ARP также переданы на платиновом уровне QoS. Программное обеспечение сетки осматривает каждый кадр, чтобы определить, является ли это контролем за CAPWAP или управляющим фрейм IP для защиты платиновой очереди от использования non-CAPWAP приложениями.

Для MAP к тракту клиента существует две других процедуры, в зависимости от того, является ли клиент клиентом WMM или обычным клиентом. Если клиент является клиентом WMM, DSCP-значение во внешнем кадре исследовано, и 802.11e, очередь с приоритетами используется (см. MAP к QoS Тракта клиента).

Таблица 5: MAP к QoS тракта клиента

DSCP-значение	Очередь обратного рейса
2, 4, 6, 8-23	Бронза
26, 32-45, 47	Золото
46, 48-63	Платина
Все другие, включая 0	Серебро

Организация очереди на AP

Если клиент не является клиентом WMM, замена WLAN (согласно конфигурации в контроллере) определяет 802.11e очередь (бронза, золото, платина или серебро), на котором передан пакет.

Для клиента к AP существуют модификации, сделанные к кадрам входящего клиента при подготовке к передаче на обратном рейсе сетки или Ethernet. Для клиентов WMM MAP иллюстрирует путь, которым внешнее DSCP-значение установлено от входящего кадра клиента WMM.

MAP к пути RAP

Минимум поступления 802.11e приоритет пользователя и приоритет замены WLAN преобразован с помощью информации, перечисленной в определить DSCP-значение кадра IP. Например, если входящий фрейм имеет как его значение приоритет, указывающий на золотой приоритет, но WLAN настроен для серебряного приоритета, минимальный приоритет серебра используется для определения DSCP-значения.

Таблица 6: DSCP к сопоставлению очередности обратного рейса

DSCP-значение	802.11e UP	Очередь обратного рейса	Типы пакета
2, 4, 6, 8 - 23	1, 2	Бронза	Пакеты самый низкого приоритета, если любой
26, 32-34	4, 5	Золото	Видеопакеты
46 - 56	6, 7	Платина	Контроль CAPWAPP, AWPP, DHCP/DNS, пакеты ARP, Голосовые пакеты
Все другие, включая 0	0, 3	Серебро	Наилучшим образом, Пакеты данных CAPWAPP

Если нет никакого входящего приоритета WMM, приоритет WLAN по умолчанию используется для генерации DSCP-значения во внешнем заголовке. Если кадр является инициируемым управляющим фрейм CAPWAP, DSCP-значение 46 размещено во внешний заголовок.

С 5.2 усовершенствованиями кода информация о DSCP сохранена в заголовке AWPP.

Весь проводной трафик клиента ограничен максимальным 802.1p значение UP 5, кроме DHCP/DNS и пакетов ARP, они пройдут платиновую очередь.

Трафик беспроводного клиента не-WMM получает приоритет QoS по умолчанию своего WLAN. В то время как, трафик беспроводного клиента WMM может иметь максимум 802.11e значение 6, но они должны быть ниже профиля QoS, настроенного для его WLAN. Если контроль доступа настроен, клиенты WMM должны использовать сигнализацию TSPEC и допускаться CAC.

Трафик данных CAPWAPP несет трафик беспроводного клиента и следовательно имеет тот же приоритет и обработку как трафик беспроводного клиента.

Теперь, когда DSCP-значение определено, правила, описанные ранее для пути обратного рейса от RAP до MAP, используются для дальнейшего определения очереди обратного рейса, на которой передан кадр. Кадры, переданные с RAP на контроллер, не помечены. Внешние DSCP-значения оставляют неповрежденными, поскольку они были сначала созданы.

Мостовое соединение пакетов обратного рейса

Соединяющие сервисы рассматриваются немного по-другому от обычных основанных на контроллере сервисов. Нет никакого внешнего DSCP-значения в мостовом соединении пакетов, потому что они не инкапсулировавший CAPWAP. Поэтому DSCP-значение в IP - заголовке, поскольку это было получено AP, используется для индексации в таблицу, как описано в пути от AP до AP (обратный рейс).

Мостовое соединение Пакетов от и до LAN

Пакеты, полученные от станции на LAN, не модифицируются ни в каком случае. Нет никакого значения замены для приоритета LAN. Поэтому в режиме моста LAN должна быть должным образом защищена. Единственная защита, предлагаемая обратному рейсу сетки, состоит в том, что non-CAPWAP управляющие фрейм, которые сопоставляют с платиновой очередью, понижены в должности золотой очереди.

Пакеты переданы к LAN точно, поскольку они получены на входе в Ethernet записи к сетке.

Единственный способ интегрировать QoS между Портами Ethernet на AP1520 и 802.11a путем маркировки Пакетов Ethernet с DSCP. AP1520 возьмет Пакет Ethernet с DSCP и разместит его в соответствующее 802.11e очередь.

1520 не помечает сам DSCP:

- На входном порте 1520 видит метку DSCP и будет инкапсулировать Фрейм Ethernet и применять соответствие 802.11e приоритет.
- On выходной порт, 1520 декапсулирует Фрейма Ethernet и размещает его в провод с нетронутым полем DSCP.

Устройства ethernet, как видеокамеры, должны иметь возможность отметить биты DSCP-значением для использования преимуществ QoS.

Установка WGB

AP в режиме WGB установлен в движущейся серии или механизме. Этот AP соединится с сетью беспроводной инфраструктуры вдоль железнодорожных путей или дороги линейной формой. Если все необходимые конфигурации будут сделаны на инфраструктуре AP и WGB, WGB сделает быстро роуминг и поддержит подключение.

Перемещение примера серии

Здесь также, желательно пойти с направленной антенной для лучшего использования энергии RF. Антенны исправления предпочтительны в этом случае, поскольку на это не будет влиять ветровое сопротивление на быстро двигающихся сериях.

Серии регулярно подвергаются промывке со струями воды и химикатами и если AP WGB установлены снаружи, они могут быть повреждены. Серии также работают в высоких скоростях, таким образом, важно выбрать антенну, которая предназначается для улицы и может противостоять сильному ветру скорости. Сильные ветры могут разорвать антенну, если установлено снаружи.

Роуминг клиента WiFi, как правило, инициируется низким уровнем сигнала, повышением коэффициента пакетных ошибок или факторами загрузки AP. В вышеупомянутом случае, когда AP работает в головке серии, сигнал WiFi на WGB получит в уровне сигнала, поскольку серия придвигается поближе к AP, тогда сигнальные изменения от самого сильного состояния до самого слабого состояния в AP точки перемещаются. Это задержит AP времени, чтобы сделать роуминг.

Когда WGB будет установлен на хвосте железнодорожного вагона, сигнал WiFi на WGB получит в силе, поскольку серия переезжает от AP, это привязано к. Сигнальные изменения от самого слабого состояния до самого сильного состояния в AP точки перемещаются, и это позволяет AP принять бродящее решение быстрее.

AP серии

Поэтому желательно установить AP Серии на хвосте серии.

Разнообразие является важным аспектом получения большего количества усиления. Нужно попытаться получить Max. преимущество его — как, чем больше энергетический потенциал линии связи в канале связи, тем лучше производительность. Выбрал антенну, которая имеет два входных порта и может соблюдать порты разнообразия, прибывающие из AP. Удостоверьтесь, что использовали кабели с малыми потерями, подключающие антенну и точку доступа. При использовании антенны одного порта то удостоверьтесь, что вы выключили разнообразие, поскольку разнообразие с одиночной антенной может создать худшие условия.

Следующие данные показывают 13 внешних антенн dBi 5 ГГц с двумя портами от Huber+Suhner с 30 градусов по вертикали и Горизонтальными Пропускными способностями. Антенна установлена в задней части тренера. Конечно, если то же тип перемещается в северное и южное направление, чем два WGB могут быть установлены в каждом тренере/car серии в двух оконечностях. Это не только увеличит резервирование, но также и увеличит емкость неконфликтных клиентов, поскольку одиночный WGB может только привязать 20 клиентов в то время как говорящий с унифицированной инфраструктурой AP.

13 Внешних антенн dBi 5 ГГц 13 Внешних антенн dBi 5 ГГц, Установленных в тренере

Если установка антенны вне движущегося механизма не возможна, тогда антенны могут, как правило, фиксироваться или исправляться к направлению стекла снаружи перед серией. Стеклянный экран на серии может вызвать потерю 2-4 db в зависимости от толщины.

Антенна должна иметь достаточно усиления для компенсации ту потерю.

Антенны, установленные к стеклу

Иногда, железнодорожные пути могут иметь мощные служебные данные линии (до 4,000 ватт). Эти серии убегают электроэнергия вместо угля или дизеля. Несмотря на то, что эти линии питания не создают радиочастотную помеху, они действительно создают специальные требования заземления для антенн, которые идут на крыши серии. Много поставщиков как Huber+Suhner специализируются на обеспечении антенн серии, которые удовлетворяют эти требования.

Для установки WGB всегда продолжайте “из узла - из ума” подход для предотвращения вандализма. WGB в серии должен предоставить страховую защиту доступу на 2.4 ГГц. В результате надлежащие меры должны быть приняты для установки этих антенн свободным способом. Следующее изображение показывает тому такую установку в одном из угла в тренере серии в крыше. Это полностью скрыто и не видимо. Два низких кабеля RF потери были взяты снаружи от двух портов для антенны AP1242 и подключены к внешней сторонней антенне. Это изображение показывает поперечное сечение тренера серии, где был установлен AP1242 WGB:

Поперечное сечение тренера серии

Это сечение фактически покрыто металлическим покрытием, совпадающим с внутренней конструкцией кузова тренера точно.

Обратите внимание на то, что доступ клиента может также быть сделан доступным для пассажиров или клиентов, стоящих на платформе, станция ожидания и т.д., как инфраструктура MAP уже там. В результате доступ клиента может быть предоставлен и на 5 ГГц и на 2.4 ГГц непосредственно от MAP. Теперь клиенты переместятся от автономных AP (WGB) к унифицированным AP CAPWAP (сетка). Лучшая часть этого доступа клиента - то, что он не требует быстро роуминга! Другая лучшая часть - то, что бюджет прочной связи доступен не только в нисходящем направлении из-за высокой мощности, но также и в соединительном направлении из-за множественных антенн. Для доступа клиента на 2.4 ГГц непосредственно от MAP, максимальное объединение соотношения (MRC) может использоваться для использования преимуществ более высоких усилений получателя. При работе со скоростями передачи данных выше, что 12 мбит/с, можно увеличить усиление по радио на 2.4 ГГц к 2.7 дБ путем добавления 2 антенн и к 4.5 дБ путем добавления 3 антенн.

Также необходимо проверить относительно того, сколько напряжения доступно на серии или движущемся механизме. Иногда приготовления третьей части должны быть сделаны, чтобы преобразовать или вниз преобразовать доступное напряжение для включения WGB. Обычно в USA, 72 В доступны на серии, таким образом, преобразователи Напряжения постоянного тока с 72 48V должны быть установлены, и кабели были выполнены внутренне для каждого тренера для обеспечения 72-вольтового элекропитания постоянного тока от механизма серии до каждого тренера.

Мобильный маршрутизатор доступа

MAR Cisco серии 3200 состоит из 1 или более модулей PC104/Plus, которые складывают вместе для формирования конфигурации беспроводного маршрутизатора. Эти комбинации модульной карты или доступны как связки (bundle) карты или как полные системы, собранные в жестком окружении Cisco 3200.

Cisco MAR серии 3200

Опция Жесткого окружения Cisco для серии 3200 разработана для использования в механизме, обратившись к определенным потребностям мобильности общественной безопасности, транспортировки, защиты и рынков государственной безопасности. Опция Жесткого окружения полностью изолирована и разработана для противостояния резким средам, включая большие изменения в температуре и высоте, интенсивном шоке/вибрации и воздействии сырости, влажности или пыли.

См. таблицу данных Корпусов маршрутизаторов Cisco ISR серии 3200 с конструкцией повышенной прочности для получения дополнительной информации и более подробную информацию жесткого окружения.

Cisco связки (bundle) маршрутизатора серии 3200 состоит из Cisco 3230 и моделей Cisco 3270. Связка (bundle) состоит из Мобильной карты маршрутизатора доступа (MARC), Последовательной мобильной интерфейсной карты (SMIC), Fast Ethernet, коммутирующего мобильную интерфейсную карту (FESMIC), беспроводные мобильные интерфейсные карты (WMICs) и Плата питания мобильного маршрутизатора (MRPC).

Для вашей ссылки связку (bundle) MAR3230 показывают здесь:

Для получения дополнительной информации о Cisco 3200 связки (bundle) карты ссылаются на таблицу данных Маршрутизаторов с конструкцией повышенной прочности Cisco 3230.

MARC

MARC является маршрутизатором IOS 3250:

Это включает процессор главного хоста, память и заголовки для Fast Ethernet, консоли и вспомогательных сигналов для маршрутизатора.

1: ШИНА PCI, 2: ШИНА ISA, 3: Fast Ethernet, 4: многофункциональный заголовок

Разъём шины PCI поддерживает связь между SMIC, FESMIC и MARC. WMIC связывается с маршрутизатором через внутренний Порт Fast Ethernet и настроен через независимый консольный порт; WMIC только тянет питание из шины.

FESMIC

FESMIC является Коммутатор Fast Ethernet с 4 портами:

1: ШИНА PCI, 2:LED разъём, 3: ШИНА ISA, 4: Поворотный переключатель, 5-8:Fast Заголовки ethernet.

Позиция поворотного переключателя определяет назначения порта. Ротационная позиция для MAR, установленного на шинах, будет 2, который соответствует Fast Ethernet 2/0-2/3. Карта связывается с MARC через шину PCI.

WMIC

Существует три типа WMICs, в зависимости от полосы частот:

- “802.11a” интерфейсная карта 5 ГГц (C3205WMIC-TPEK9)

- “802.11bg” интерфейсная карта 2.4 ГГц (C3201WMIC-TPEK9)
- “802.11a” интерфейсная карта 4.9 ГГц (C3202WMIC-TPEK9)

Существует 2 из них на MAR 3230.

Они могут быть настроены как WGB. WGB подобен клиенту AP:

Это позволит MAR соединяться с AP инфраструктуры вдоль дорожки/железной дороги или в туннеле и т.д.

1: ШИНА PCI, 2: Оставленная Антенна, 3: Правильная Антенна, 4: ШИНА ISA, 5: Fast Ethernet, 6: светодиодный и разъем пульта.

WMIC не использует PCI и шину ISA. Это связывается с маршрутизатором через внутренний Порт Fast Ethernet.

SMIC

SMIC предоставляет маршрутизатор максимум четырьмя высокоскоростными наборами последовательных сигналов и в терминальном оборудовании пользователя (DTE) и в режимах оборудования линии передачи данных (DCE):

1: ШИНА PCI, 2: 60-контактный многофункциональный заголовок для Serial 0 и Последовательного 1 сигнала, 3: ШИНА ISA, 4: Поворотный переключатель

Разъём шины PCI поддерживает связь между SMIC и MARC. Позиция поворотного переключателя определяет назначения порта. Несмотря на то, что поворотный переключатель имеет 8 позиций, только позиция 0, 1, и 2 поддерживается на SMIC с 4 портами.

MRPC

MRPC:

Карта DC/ЭЛЕКРОПИТАНИЯ ПОСТОЯННОГО ТОКА является износоустойчивым, специализированным, тройными выходными данными, ПК/104 — Плюс-совместимый преобразователь. Это принимает 12 В постоянного тока или вводы 24VDC от системы аккумулятора транспортного средства и предоставляет, полностью защитил 3.3 В, 5V и выходные данные 12V. Адаптер питания AC/DC предоставляет совместимый Вход постоянного тока, если не используясь в приложение 24VDC или 12 В постоянного тока.

Эти 3200 имеют несколько интерфейсов:

- Интерфейсы Ethernet используются для подключения любых проводных клиентов в механизме, таких как портативный ПК, камера или устройства телематики к сети.
- Последовательные интерфейсы предоставляют подключение беспроводным модемам глобальной сети (WAN), которые соединяются с сотовыми сетями, такими как CDMA или GPRS.
- WMIC настроен как WGB для подключения к беспроводным сетям.

Преимущество использования MAR3200 состоит в том, что это может дать резервное подключение по сотовым сетям, таким как GPRS или CDMA. Беспроводные соединения 802.11 рассматриваются как предпочтительные сервисы, потому что они предлагают

большую часть пропускной способности. Однако, когда подключение WLAN не доступно, сотовая технология предоставляет резервное соединение. Приоритет соединения может быть установлен приоритетом маршрутизации или приоритетом для Мобильного IP.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация