

Cisco CleanAir - Руководство по дизайну единой беспроводной сети Cisco (UWN)

Содержание

- [Введение](#)
- [Предварительные условия](#)
- [Требования](#)
- [Используемые компоненты](#)
- [Условные обозначения](#)
- [Теория CleanAir операций](#)
- [CleanAir AP](#)
- [Компоненты системы Cisco CleanAir](#)
- [Интерференционная классификация и SAgE](#)
- [Информационные элементы CleanAir AP](#)
- [Отчет об устройствах, создающих помехи](#)
- [Air Quality](#)
- [Понятия CleanAir](#)
- [Режимы AP CleanAir операции](#)
- [Индекс степеней серьезности ошибки и Air Quality](#)
- [PMAC](#)
- [Слияние](#)
- [Точность размещения Wi-Fi non](#)
- [Модели развертывания CleanAir и Рекомендации](#)
- [Чувствительность обнаружения CleanAir](#)
- [Развертывание с нуля](#)
- [Развертывания наложения MMAP](#)
- [Функции CleanAir](#)
- [Требования к лицензии](#)
- [Матрица функций CleanAir](#)
- [Сводка](#)
- [Установка и проверка](#)
- [CleanAir включен на AP](#)
- [CleanAir включен на WCS](#)
- [CleanAir включил установку MSE и проверку](#)
- [Глоссарий](#)
- [Дополнительные сведения](#)

Введение

Анализ спектра (SI) – одна из базовых технологий, разработанных для предупреждения

проблем при совместном использовании радиочастотного спектра. По существу SI приносит усовершенствованные интерференционные идентификационные алгоритмы, подобные используемым в вооруженных силах к коммерческому миру беспроводной сети. SI предоставляет видимость всем пользователям совместно используемого спектра, и устройства Wi-Fi и внешние источники помех. Для каждого устройства, которое работает в нелицензированный диапазоне, SI говорит вам: Что это? Где это? Как это влияет на сеть Wi-Fi? Cisco сделала полужирный шаг для интеграции SI непосредственно в кремний Wi-Fi и инфраструктурное решение.

Интегрированное решение, называемое Cisco CleanAir, означает, что впервые менеджер по ИТ WLAN в состоянии определить и определить местоположение источников помех не802.11, который повышает панель на простоте управления и безопасности беспроводных сетей. Самое главное интегрированный SI готовит почву для новой породы Управления радиоресурсами (RRM). В отличие от предыдущих решений для RRM, которые могли только понять и адаптироваться к другим устройствам Wi-Fi, SI открывает путь для решения для RRM второго поколения, которое полностью осведомлено обо всех пользователях беспроводного спектра и в состоянии оптимизировать производительность перед лицом этих различных устройств.

Первый важный момент, который должен быть сделан, то, что с точки зрения дизайна. Включенные точки доступа CleanAir (AP) являются просто этим; AP и производительность фактически идентичны AP 1140 года. Разработка для покрытия Wi-Fi является тем же с обоими. CleanAir или интерференционные идентификационные процессы являются пассивным процессом. CleanAir основывается на получателе, и для классификации для функционирования, источник должен быть достаточно громким, чтобы быть полученным в на 10 дБ выше минимального уровня шума. Если ваша сеть развернута таким способом, которым ваши клиенты и AP могут услышать друг друга, то CleanAir может услышать достаточно хорошо для предупреждения вас к беспокойству интерференции в вашей сети. Требования покрытия для CleanAir подробно изложены в этом документе. Существуют некоторые особые случаи в зависимости от реализации CleanAir, направляют вас, в конечном счете выбирают. Технология была разработана для похвалы текущим оптимальным методам в развертываниях Wi-Fi. Это включает модели развертывания других широко используемых технологий, такие как Адаптивный WIPS, Голос и развертывания местоположения.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с CAPWAP и единой беспроводной сетью Cisco (UWN) (CUWN).

Используемые компоненты

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

- CleanAir способные AP является Aironet 3502e, 3501e, 3502i, и 3501i
- Контроллер беспроводной локальной сети Cisco (WLC) рабочая версия 7.0.98.0
- Cisco Wireless Control System (WCS) рабочая версия 7.0.164.0
- Рабочая версия 7.0 ядра сервисов мобильности (MSE) Cisco

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

Теория CleanAir операций

CleanAir является системой, не функцией. Компоненты программного и аппаратного обеспечения CleanAir предоставляют способность точно измерить качество Канала Wi-Fi и определить источники не-Wi-Fi интерференции канала. Это не может быть сделано со Стандартными комплектами микросхем Wi-Fi. Для понимания целей проекта и требований для успешного внедрения, необходимо понять, как CleanAir работает над высоким уровнем.

Для уже знакомых с технологией Эксперта по Спектру Cisco, CleanAir является естественным эволюционным шагом. Но, это - абсолютно новая технология, в которой это - основанная на предприятии распределенная технология спектрального анализа. Также, это подобно Cisco Spectrum Expert в некотором отношении, но очень отличается в других. Компоненты, функции и функции обсуждены в этом документе.

CleanAir AP

Новыми CleanAir способные AP является Aironet 3502e, 3501e, 3502i, и 3501i. E определяет Внешнюю антенну, я определяет Внутреннюю антенну. Оба - полностью функциональное следующее поколение 802.11n AP и работают на стандартном питании на 802.3 акрофута.

Рисунок 1: C3502E и C3502I CleanAir способные AP

Аппаратные средства Спектрального анализа непосредственно интегрированы в комплекты микросхем радио. Это добавление добавило более чем 500 логических элементов К к радио-кремнию и предоставило исключительно сильную связь функций. Существует много других традиционных опций, которые были добавлены или улучшены с этими радио. Но, это выходит за рамки этого документа, и они не покрыты здесь. Удовлетворите, что это должно сказать, что самостоятельно без CleanAir AP серии 3500 упаковывают много функций и производительности в привлекательный и устойчивый AP предприятия.

Компоненты системы Cisco CleanAir

Базовая архитектура Cisco CleanAir состоит из включенных AP Cisco CleanAir и контроллера беспроводной локальной сети Cisco (WLC). Cisco Wireless Control System (WCS) и ядро сервисов мобильности (MSE) является дополнительными компонентами системы. Для получения полного значения от информации, что предоставления системой CleanAir, WCS и MSE вместе являются ключевыми для усиления более широкой эффективности CleanAir. Это предоставляет интерфейсы пользователя для усовершенствованных возможностей спектра, таких как исторические диаграммы, отслеживая интерференционные устройства, службы определения местоположения и анализ влияния.

AP, оборудованный технологией Cisco CleanAir, собирает информацию об источниках помех не-Wi-Fi, обработайте его и передайте WLC. WLC является интегральной базовой частью системы CleanAir. WLC управляет и настраивает CleanAir способные AP, собирает и обрабатывает данные спектра и предоставляет его WCS и/или MSE. WLC предоставляет интерфейсы локального пользователя (GUI и CLI), чтобы настроить основные функции

CleanAir и сервисы и отобразить текущую информацию о спектре.

Cisco WCS предоставляет расширенные интерфейсы пользователя для CleanAir, которые включают включение функции и конфигурацию, консолидированный отображают информацию, исторические записи Air Quality и создание отчетов о механизмах.

Рис. 2: Логический системный поток

Cisco MSE требуется для местоположения и исторического отслеживания интерференционных устройств, и предоставляет координацию и консолидацию интерференционных отчетов через множественные WLC.

Примечание: Одиночный WLC может только консолидировать интерференционные предупреждения для AP, непосредственно связанных с ним. Координация отчетов, которые прибывают из AP, подключенных к другим контроллерам, требует MSE, который имеет представление в масштабе всей системы всех AP CleanAir и WLC.

Интерференционная классификация и SAgE

Основа системы CleanAir является Механизмом Спектрального анализа (SAGE) ASIC, анализатор спектра на микросхеме. Однако это намного больше, чем просто анализатор спектра. В ядре мощные 256 точек механизм FFT, который предоставляет удивительный RBW на 78 кГц (Ширина полосы разрешения, минимальное разрешение, которое может быть отображено), цель созданный импульс и сборочные механизмы статистики, а также DSP Ускоренный Векторный Механизм (DAvE). Аппаратные средства SAgE выполняются параллельно с комплектами микросхем Wi-Fi и процессами около информации о скорости линии. Все это позволяет экстремальную точность и масштабы для больших чисел подобных источников помех без штрафа в пропускной способности трафика пользователя.

Комплекты микросхем Wi-Fi всегда находятся на линии. Просмотры SAgE выполнены один раз во второй. Если преамбула Wi-Fi обнаружена, через нее проходят к комплектам микросхем непосредственно и не влияют параллельные аппаратные средства SAgE. Никакие пакеты не потеряны во время сканирования SAgE, SAgE отключен, в то время как пакет Wi-Fi обработан через получатель. SAgE очень быстр и точен. Даже в занятой среде, существует более чем достаточно времени просмотра для точной оценки среды.

Почему делает вопрос RBW? Если необходимо посчитать и измерить различие между несколькими радио Bluetooth, скачкообразно двигающимися с узкими сигналами в 1600 переходах в секунду, необходимо разделить другие переходы передатчиков в выборке, если вы хотите знать, сколько существует. Это берет разрешение. В противном случае это было бы все похоже на один импульс. SAgE делает это, и он делает это хорошо. Из-за DAvE и привязываемый на борту памяти, способность обработать множественные выборки/источники помех параллельно там. Это увеличивает скорость, которая позволяет вам обработать поток данных в псевдореальное время. Псевдореальное время означает, что существует некоторая задержка, но это таким образом минимально, это берет компьютер для измерения его.

Информационные элементы CleanAir AP

AP Cisco CleanAir производят два базовых типа информации для системы CleanAir. IDR (Отчет об устройствах, создающих помехи) генерируется для каждого классифицированного источника помех. AQI's (Индекс Air Quality) отчеты генерируют каждые 15 секунд и передают

к Cisco IOS® для усреднения и возможной передачи к контроллеру на основе заданного интервала. Обмен сообщениями CleanAir все обрабатывается на уровне управления в двух новых типах сообщения CAPWAP: Конфигурация Спектра и Данные Спектра. Форматы для этих сообщений перечислены здесь:

Конфигурация спектра:

WLC - AP CAPWAP msg: CAPWAP_CONFIGURATION_UPDATE_REQUEST = 7 payload type: Vendor specific payload type (104 -?) vendor type: SPECTRUM_MGMT_CFG_REQ_PAYLOAD = 65
 AP-WLC Payload type: Vendor specific payload type (104 -?) vendor types:
 SPECTRUM_MGMT_CAP_PAYLOAD = 66 SPECTRUM_MGMT_CFG_RSP_PAYLOAD = 79 SPECTRUM_SE_STATUS_PAYLOAD = 88

AP данных спектра – WLC

CAPWAP: IAPP message
 IAPP subtype: 0x16
 data type: AQ data - 1
 main report 1
 worst interference report 2
 IDR data - 2

Отчет об устройствах, создающих помехи

Отчет об устройствах, создающих помехи (IDR) является подробным отчетом, который содержит информацию о классифицированном интерференционном устройстве. Этот отчет подобен информации, которая замечена в Активных устройствах Cisco Spectrum Expert или Представлении Устройств. Активный IDRs может быть просмотрен на CLI GUI/и WLC для всех радио CleanAir на том WLC. IDRs переданы MSE только.

Это - формат для отчёта IDR:

Таблица 1 - отчет об устройствах, создающих помехи

Имя параметра	Модули	Примечания
Идентификатор устройства		Номер однозначно определяет интерференционное устройство для определенного радио. Это состоит из верхних 4 битов, генерируемых во время загрузки системы и более низких 12 битов рабочий номер.
Тип класса		тип класса устройств
Тип события		устройство вниз устройство обновляет
ID радиодиапазона		1 = 2.4 ГГц, 2 = 5 ГГц, 4 = 4.9 ГГц; зарезервированы 2 MSB. 4.9 ГГц не поддерживаются для начального релиза.
Timestamp		время обнаружения первоначального устройства
Интерференционный		1 – 100, 0x0 зарезервирован для неопределенных/скрытых

индекс степеней серьезности ошибки		степеней серьезности ошибки
Обнаруженный на каналах	битовый массив	поддержка обнаружения на составных каналах в том же радиодиапазоне
Интерференционный рабочий цикл	%	1 – 100%
ID антенны	битовый массив	Поддержка множественных отчетов об антенне зарезервирована для будущих версий.
Мощность передатчика (RSSI) на антенну	дБм	
Длина Подписи устройства		Длина поля "Device Signature". В настоящее время длина могла быть в диапазоне 0 - 16 байтов.
Подпись устройства		Параметр представляет или MAC-адрес уникального устройства или устройство подпись PMAC. См. определение PMAC ниже.

IDR произведен для каждого классифицированного устройства. Отдельное радио может отследить теоретическое бесконечное число устройств, подобных тому, что карта Эксперта по Спектру делает сегодня. Cisco протестировала сотни с успехом. Однако в развертывании в масштабе предприятия существуют сотни датчиков, и практический предел создания отчетов принужден для масштабирования целей. Для AP CleanAir сообщают о лучших десяти IDRs на основе степеней серьезности ошибки. Одно исключение из этого правила имеет место источника помех безопасности. Безопасности IDR всегда дают приоритеты независимо от степеней серьезности ошибки. Дорожки AP, которые IDRs были переданы контроллеру и добавляют или удаляют по мере необходимости.

Таблица 2: Пример таблицы отслеживания IDR на AP

Введите	SEV	WLC
Безопасность	1	X
Интерференция	20	X
Интерференция	9	X
Интерференция	2	X
Интерференция	2	X
Интерференция	1	X
Интерференция	1	X
Интерференция	1	X

Интерференция	1	X
Интерференция	1	X
Интерференция	1	
Интерференция	1	

Примечание: Источники помех, отмеченные как Источники помех Безопасности, являются назначенным пользователем и могут быть настроены через беспроводные сети > 802.11a/b/g/n> cleanair>, включают интерференцию для аварийного сигнала защиты. Любой источник помех, который классифицирован, может быть выбран для предупреждения trap-сообщения безопасности. Это передает trap-сообщение безопасности к WCS или другому настроенному приемнику прерываний на основе типа выбранного источника помех. Это trap-сообщение не содержит ту же информацию как IDR. Это - просто способ инициировать сигнал тревоги на присутствии источника помех. Когда источник помех определяется как проблема безопасности, он отмечен как таковой в AP и всегда включается в устройства TEN, о которых сообщают от AP независимо от степеней серьезности ошибки.

Сообщения IDR передаются в режиме реального времени. На обнаружении IDR отмечен как устройство. Если это останавливается, сообщение отключения устройства передается. Обновленное сообщение передается каждые 90 секунд от AP для всех устройств, в настоящее время отслеживаемых. Это обеспечивает обновления статуса отслеженных источников помех и контрольного журнала в конечном счете, или сообщение отключения было потеряно в пути.

[Air Quality](#)

Создание отчетов Air Quality (AQ) доступно от любого спектра способный AP. Air Quality является новой концепцией с CleanAir и представляет метрику “совершенства” доступного спектра и указывает на качество пропускной способности, доступной для канала Wi-Fi. Air Quality является прокручивающимся средним числом, которое оценивает влияние всех классифицированных интерференционных устройств против теоретического совершенного спектра. Масштаб составляет 0-100% с 100%, представляющими Хороший. Отчёты AQ передаются независимо за каждым радио. Последний отчёт AQ доступен для просмотра на GUI WLC и CLI. Отчёты AQ сохранены на WLC и опрошены регулярным интервалом WCS. По умолчанию составляет 15 минут (минимум) и может быть расширен на 60 минут на WCS.

[Почему AirQuality Уникален?](#)

В настоящее время самые стандартные микросхемы Wi-Fi оценивают спектр путем отслеживания всех пакетов/энергии, которые могут демодулироваться на, получают, и все пакеты/энергия, которые он передает. Любая энергия, которая остается в спектре, который не может демодулироваться или составляться действием RX/TX, смешана в категорию, названную шумом. В действительности много “шума” является фактически остатками от коллизий или пакетами Wi-Fi, которые падают ниже получить порога для надежной демодуляции.

С CleanAir проявлен другой подход. Вся энергия в спектре, который является определенно НЕ Wi-Fi, классифицируется и составляется. Мы можем также видеть и понять энергию, которая является модулируемым 802.11, и классифицируйте энергию, которая прибывает из источников канала Компании и Соседнего канала. Для каждого классифицированного устройства вычислен индекс степеней серьезности ошибки (см. раздел Степеней серьезности ошибки), положительное положительное между 0 и 100 – с 100 являющийся

самым серьезным. Интерференционные степени серьезности ошибки тогда вычтены из масштаба AQ (запускающийся в 100 – хороший) для генерации фактического AQ для канала/радио, AP, Пола, Создав или кампуса. AQ тогда является измерением влияния всех классифицированных устройств на среде.

Существует два определенных режима создания отчетов AQ: обычное и быстрое обновление. Обычный режим является режимом создания отчетов AQ по умолчанию. Или WCS или WLC получают, является в обычную частоту обновления (по умолчанию составляет 15 минут). WCS сообщает Контроллеру о периоде опроса по умолчанию, и WLC дает AP команду изменять усреднение AQ и отчетный период соответственно.

Когда пользователь выполняет развертку для Мониторинга> точки доступа> и выбирает радиointерфейс из WCS или WLC, выбранное радио размещено в быстрый режим создания отчетов обновления. Когда запрос получен, Контроллер дает AP команду изменять отчетный период AQ по умолчанию временно на неподвижную быструю частоту обновления (30 сек.), который позволяет видимость псевдореального времени в изменения AQ на радио-уровне.

Состояние создания отчетов по умолчанию “ON (включено)”.

Таблица 3: Отчёт о Air Quality

Имя параметра	Модули	Примечание
Номер канала		В автономном режиме – это было бы подаваемым каналом
Минимальный AQI		Самый низкий AQ обнаружен в течение отчетного периода.
Следующие параметры усреднены на AP за отчетный период:		
Индекс Air Quality (AQI)		
Питание всего канала (RSSI)	дБм	Эти параметры показывают суммарную мощность из всех источников включая оба источника помех и устройства WiFi.
Рабочий цикл всего канала	%	
Мощность помехи (RSSI)	дБм	
Интерференционный рабочий цикл	%	устройства non WiFi только

Несколько точек входа для каждого обнаруженного устройства присоединены к отчёту, упорядоченному степенями серьезности ошибки устройства. Формат для этих записей здесь:

Таблица 4: Данные устройства AQ

Имя параметра	МОДУЛИ	Примечания
Тип класса		тип класса устройств
Интерференционный индекс степеней серьезности ошибки		
Мощность помехи (RSSI)	дБм	
Рабочий цикл	%	
Количество устройства		
<i>общее количество</i>		

Примечание: В контексте создания отчетов спектра Air Quality представляет интерференцию из источников не-Wi-Fi и источников Wi-Fi, не обнаруживаемых AP Wi-Fi во время нормальной работы (например, старые устройства устройства скачкообразной перестройки частоты 802.11, измененные устройства 802.11, Смежные помехи в перекрываемых каналах, и т.д.). Информация о Wi-Fi базировалась, интерференцию собирает и сообщает относительно AP с помощью микросхемы Wi-Fi. Точка доступа в локальном режиме собирает информацию AQ для текущего канала (каналов) обслуживания. Точка доступа в режиме мониторинга собирает информацию для всех каналов, настроенных под опциями просмотра. Стандартные параметры настройки CUWN Страны, DCA и Всех каналов поддерживаются. Когда отчёт AQ получен, Контроллер выполняет требуемую обработку, и сохраните его в базе данных AQ.

[Понятия CleanAir](#)

Как ранее упомянуто, CleanAir является интеграцией технологии Cisco Spectrum Expert в AP Cisco. В то время как общие черты могли бы существовать, это - новое использование технологии, и много новых концепций представлены в этом разделе.

Cisco Spectrum Expert представил технологию, которая смогла положительно определить источники не-Wi-Fi энергии радиоизлучения. Это разрешило оператору фокусироваться на информации, такой как рабочий цикл и рабочие каналы, и делать обоснованное решение об устройстве и влиянии it на их сеть Wi-Fi. Эксперт по спектру позволил оператору тогда блокировать выбранный сигнал в приложение средства поиска устройства и физически определять местоположение устройства путем обхода вокруг с инструментом.

Цель проекта CleanAir должна пойти несколько шагов вперед путем важного удаления оператора далее из уравнения и автоматизации нескольких из задач в рамках управления системой. Поскольку можно знать то, что устройство и на что оно влияет, лучшие решения могут быть приняты в уровне системы на том, что сделать с информацией. Несколько новых алгоритмов были разработаны для добавления интеллекта к работе, которая была запущена с Cisco Spectrum Expert. Всегда существуют случаи, которые требуют физически отключения интерференционного устройства или принятия решения об устройстве и влиянии, которое вовлекает людей. Глобальная система должна излечить то, что может быть излечено и избежать того, чего можно избежать так, чтобы усилие исправить спектр, на который влияют, могло быть упреждающим осуществлением вместо реактивного.

[Режимы AP CleanAir операции](#)

Точка доступа в локальном режиме (рекомендовала) (LMAP) — AP Cisco CleanAir, работающий в режиме LMAP, служит клиентам на, он - назначенный канал. Это также контролирует Спектр на том канале и том канале ONLY. Трудная кремниевая интеграция с радио Wi-Fi позволяет аппаратным средствам CleanAir слушать между трафиком на канале, который в настоящее время не подается с абсолютно никаким штрафом пропускной способности подключенных клиентов. Это - обнаружение скорости линии, не прерывая трафик клиента.

Нет никаких CleanAir, живет обработанный во время обычного от просмотров канала. На нормальной работе Точка доступа в локальном режиме CUWN выполняет от канала пассивные просмотры альтернативных доступных каналов в 2.4 ГГц и 5 ГГц. Выключено просмотры канала используются для обслуживания системы, такого как метрики RRM и постороннее обнаружение. Частота этих просмотров не достаточна для сбора, вплотную живет требуемый для положительной классификации устройств, таким образом, информация, подбираемая во время этого просмотра, подавлена системой. Увеличение частоты от просмотров канала также не выбираемо, поскольку это отнимает у времени когда трафик радиосервисов.

Что это все означает? CleanAir AP в режиме LMAP только просматривает один канал каждой полосы постоянно. В обычной плотности предприятия должно быть много AP на том же канале, и по крайней мере один на каждом RRM принятия канала обрабатывает выбор канала. Источник помех, который использует узкополосную модуляцию (воздействует на или вокруг одиночной частоты) только обнаружен AP тот ресурс общего доступа тот разнос частот. Если интерференция является типом со скачкообразной перестройкой частоты (использует кратные частоты – обычно покрытие целой полосы), это обнаружено каждым AP, который может услышать его работающий в полосе.

Рис. 4: Пример обнаружения AP LMAP

В 2.4 ГГц LMAPs имеют достаточную плотность для общего обеспечения по крайней мере трех точек классификации. Минимум трех точек обнаружения требуется для разрешения местоположения. В 5 ГГц существует 22 канала, работающие в Соединенных Штатах, таким образом плотность обнаружения и достаточная плотность местоположения менее вероятны. Однако, если интерференция воздействует на канал, занятый CleanAir AP, она обнаруживает его и предупреждение, или предпримите шаги, чтобы смягчить, если активированы те опции. Большая часть замеченной интерференции ограничена частью на 5.8 ГГц полосы. Это - то, где пользовательские устройства живут и следовательно где с этим, скорее всего, встретятся. При необходимости можно ограничить план каналов для принуждения большего количества AP к тому пространству. Однако это действительно не гарантировано. Помните, интерференция является только проблемой, если это использует спектр, вам нужно. Если ваш AP не находится на том канале, вероятно, что вы все еще имеете много в запасе спектра для перемещения в. Что, если потребность контролировать все 5 ГГц ведет политика безопасности? См. определение Точки доступа в режиме мониторинга ниже.

Точка доступа в режиме мониторинга (дополнительная) (MMAP) — Точка доступа в режиме мониторинга CleanAir выделена и не служит трафику клиента. Это предоставляет полностью занятое сканирование всех каналов с помощью 40 МГц, живет. CleanAir поддерживается в режиме отслеживания наряду со всеми другими текущими приложениями режима отслеживания включая Адаптивный WIPS и усовершенствование местоположения. В двойной радио-конфигурации это гарантирует, что обычно просматриваются все каналы полос.

Включенный MMAPs CleanAir может быть развернут, поскольку часть распространяющихся

развертываний CleanAir позволила LMAPs предоставить дополнительную страховую защиту в 2.4 и 5 ГГц, или как автономное решение для наложения для функциональности CleanAir в существующих развертываниях non-CleanAir AP. В сценарии, как упомянуто выше, где безопасность является основным драйвером, вероятно, что Адаптивный WiPS также был бы требованием. Это поддерживается одновременно с CleanAir на том же MMAP.

Существуют некоторые явные различия в том, как некоторые функции поддерживаются при развертывании как решение для наложения. Thisis покрыт обсуждением моделей развертывания в этом документе.

Режим Подключения Эксперта по спектру – (дополнительное) Подключение SE — AP
Подключения SE настроен как специализированный Датчик Спектра, который позволяет соединению приложения Cisco Spectrum Expert, работающего на локальном хосте использовать CleanAir AP в качестве удаленного датчика спектра для локального приложения. Соединение между Экспертом по Спектру и удаленным AP обходит контроллер на плоскости данных. AP остается в контакте с контроллером на уровне управления. Этот режим позволяет просматривать необработанных данных спектра, таких как графики FFT и подробные измерения. Вся функциональность системы CleanAir приостановлена, в то время как AP находится в этом режиме, и никакие клиенты не обслуживаются. Этот режим предназначен для удаленного устранения проблем только. Приложение Эксперта по Спектру является приложением MS Windows, которое соединяется с AP через сеанс TCP. Это может поддерживаться в VMware.

[Индекс степеней серьезности ошибки и Air Quality](#)

В CleanAir было представлено понятие Air Quality. Air Quality является измерением процента времени, когда спектр в определенном наблюдаемом контейнере (радио, AP, Полоса, Пол, Создавая) доступен для трафика Wi-Fi. AQ является функцией индекса степеней серьезности ошибки, который вычислен для каждого классифицированного источника помех. Индекс Степеней серьезности ошибки оценивает каждого не - устройства Wi-Fi по воздушным характеристикам и вычисляет, какой процент времени спектр не доступен для Wi-Fi с этим подарком устройства.

Air Quality является продуктом индексов степеней серьезности ошибки всех классифицированных источников помех. Об этом тогда сообщают как полный Air Quality по радио/каналу, полосе или домену распространения RF (пол, создавая) и представляет общие затраты против доступного эфирного времени всех не - источники Wi-Fi. Что-либо, что оставляют, теоретически доступно сети Wi-Fi для трафика.

Это теоретически, потому что существует целая наука позади измерения эффективности трафика Wi-Fi, и это выходит за рамки этого документа. Однако знание, что интерференция или не влияет на ту науку, является основной целью, если ваш план является успехом в определении и смягчении точек боли.

Что делает источник помех серьезным? То, что определяет, /или ли это, не является проблемой? Как я использую эту информацию для управления моей сетью? Эти вопросы обсуждены в этом документе.

Простым языком не - использование Wi-Fi сводится, как часто другое радио использует мой спектр сетей (Рабочий цикл) и насколько громкий он относительно моих радио (RSSI/местоположение). Энергия в канале, который замечен интерфейсом 802.11, пытающимся обратиться к каналу, воспринята как рабочий канал, если это выше

определенного энергетического порога. Это определено оценкой очистки канала (CCA). Wi-Fi использует слушание перед методом доступа к каналу разговора для состязательного свободного доступа PHY. Это на CS A CA (-CA=collision предотвращение).

RSSI источника помех определяет, можно ли это услышать выше порога CCA. Рабочий цикл на времени передатчика. Это определяет, насколько персистентная энергия находится в канале. Выше рабочий цикл чаще канал заблокирован.

Простые степени серьезности ошибки могут быть продемонстрированы этот путь затем с помощью строго RSSI и Рабочий цикл. В целях рисунка принято устройство с 100%-м рабочим циклом.

Рис. 5: Поскольку сигнал помех уменьшается - увеличения AQI

В графике на этом рисунке вы видите, что как мощность сигнала интерференционных уменьшений, увеличивается получающийся AQI. Технически, как только сигнал падает ниже -65 дБм, AP больше не блокируется. Действительно необходимо думать, примыкают к влиянию, которое это оказывает на клиентов в ячейке. 100%-й рабочий цикл (DC) гарантирует постоянное разрушение клиентских сигналов с недостаточным SNR в присутствии шума. AQ быстро увеличивается, как только мощность сигнала падает ниже -78 дБм.

До сих пор существует два из трех значительных воздействий интерференции, определенной в основанной метрике Air Quality степеней серьезности ошибки:

- Блокирование CCA
- Разрушенный SNR

Интерференция является прямой при рассмотрении 100%-го DC. Это - тип сигнала, чаще всего используемого на демонстрациях влияния интерференции. Легко видеть в спектрограмме, и это имеет очень драматическое влияние на канале Wi-Fi. Это действительно происходит в реальных условиях также, например в камерах аналоговый видеосигнала, детекторах движения, телеметрическом оборудовании, сигналах TDM и более старых беспроводных телефонах.

Существует много сигналов, которые не являются 100%-м DC. Фактически, большая интерференция, с которой встречаются, является интерференцией этого типа: переменная к минимальному. Здесь становится немного более трудным вызвать степени серьезности ошибки. Примерами интерференции этого типа является Bluetooth, Беспроводные телефоны, беспроводные динамики, телеметрические устройства, более старые 802.11fh механизм и так далее. Например, одиночная гарнитура Bluetooth не наносит много ущерба в среде Wi-Fi. Однако три из них с перекрывающимся распространением могут разъединить телефон Wi-Fi, если обойдено через.

В дополнение к CCA существуют условия в спецификациях 802.11, таких как окно конфликта, которое необходимо для размещения эфирного времени других основных протоколов. Затем вы добавляете к этому различные механизмы QoS. Все это резервирование сред используется другими приложениями, чтобы увеличить эффективность эфирного времени и минимизировать коллизии. Это может сбить с толку. Однако, потому что все интерфейсы в эфире участвуют и договариваются о той же группе стандартов, она работает очень хорошо. Что происходит с этим упорядоченным хаосом, когда вы представляете очень удельную энергию, которая не понимает механизмы конфликта при попытке одновременной передачи данных или в этом отношении даже не участвует в CS A CA? Ну, погром фактически, к большему или меньшей степени. Это

зависит, насколько занятая среда - когда испытана интерференция.

Рис. 6: Подобные но другие рабочие циклы канала

Вы можете иметь два идентичных сигнала с точки зрения Рабочего цикла, как измерено в канале и амплитуде, но иметь два полностью разных уровня интерференции, испытанной на сети Wi-Fi. Быстрое повторение коротких импульсов может быть более разрушительным к Wi-Fi, чем относительно медленное повторение толстого. Посмотрите на передатчик помех RF, который эффективно завершает работу канала Wi-Fi и регистрирует очень мало рабочего цикла.

Чтобы сделать надлежащую оценку задания, вам нужно лучше понимание представленного интервала минимального вмешательства. Интервал минимального вмешательства составляет факт, что импульсы in-channel прерывают действие Wi-Fi в течение некоторого периода дольше, чем их фактическая продолжительность, из-за трех эффектов:

- Уже считая в обратном порядке, устройства Wi-Fi должны ждать дополнительный период DIFS после интерференционного импульса. Этот случай типичен для в большой степени загруженных сетей, где интерференция запускается, прежде чем счетчик отката Wi-Fi считал в обратном порядке для обнуления.
- Если новый пакет поступает, чтобы быть переданной серединой интерференции, устройство Wi-Fi должно дополнительно замедлить использование произвольного значения между нулем и CW_{min} . Этот случай типичен для слабо загруженных сетей, где интерференция запускается, прежде чем пакет Wi-Fi поступает в MAC для передачи.
- Если устройство Wi-Fi уже передает пакет, когда интерференционный пакет поступает, весь пакет должен ретранслироваться со следующим более высоким значением CW до CW_{max} . Если интерференция запускается второй, частично через существующий пакет Wi-Fi, этот случай типичен.

Если спина от времени истекает без успешной повторной передачи, то следующие отступают, удваивает предыдущее. Это продолжает неуспешную передачу до CW_{max} , достигнут, или TTL превышен для кадра.

Рисунок 7 - Для 802.11b/g $CW_{min} = 31$, для 802.11a CW_{min} равняется 15, у обоих есть $CW_{max} 1023$

В реальной сети Wi-Fi трудно оценить среднюю продолжительность этих трех эффектов, потому что они - функции количества устройств в BSS, накладываясь на BSSs, действие устройства, длины пакета, поддержало скорости / протоколы, QoS и существующее действие. Поэтому следующая лучшая вещь состоит в том, чтобы создать метрику, которая остается постоянной как контрольная точка. Это - то, что делают Степени серьезности ошибки. Это измеряет влияние одиночного источника помех против теоретической сети и поддерживает постоянный отчет степеней серьезности ошибки независимо от базового использования сети. Это дает нам относительную точку для взгляда на через инфраструктуру сети.

Ответ на вопрос, "насколько не - интерференция Wi-Fi плоха", субъективен. В слабо загруженных сетях довольно возможно иметь уровни не - интерференция Wi-Fi, которые остаются незамеченными пользователями и администраторами. Это - то, что ведет для беспокойства в конце. Природа беспроводных сетей должна стать более занятой в течение долгого времени. Успех приводит к более быстрому организационному принятию, и к передаваемым новым приложениям. Если существует интерференционный подарок со дня один, довольно вероятно, что сеть имеет проблему с этим, когда это становится достаточно занятым. Когда это происходит, для людей трудно полагать, что что-то, что было прекрасно

по-видимому все время, является преступником.

Как мы используем Air Quality CleanAir и метрики Степеней серьезности ошибки?

- AQ используется, чтобы разработать и контролировать базовое измерение спектра и предупреждение на изменениях, указывающих на влияние на производительность. Можно также использовать его для долгосрочной оценки тенденции посредством создания отчетов.
- Степени серьезности ошибки используются для оценки интерференции, влияют на потенциал и располагают по приоритетам отдельные устройства для смягчения.

PMAC

Передатчики Wi-Fi по-прежнему являются менее, чем дружественными когда дело доходит до уникальных характеристик, которые могут использоваться для определения их. Это по существу, что сделало решение для Cisco Spectrum Expert настолько революционным. Теперь с CleanAir существуют множественные AP, что потенциально все слышит ту же интерференцию в то же время. Корреляция этих отчетов изолировать уникальные экземпляры является проблемой, которая должна была быть решена для обеспечения дополнительных характеристик, таких как местоположение интерференционных устройств, а также точное количество.

Введите Псевдо MAC или PMAC. Поскольку устройство аналоговый видеосигнала не имеет MAC-адреса или в нескольких случаях, никакая другая определяющая цифровая метка, алгоритм должен был быть создан для определения уникальных устройств, сообщаемых от нескольких источников. PMAC вычислен как часть классификации устройств и включен в интерференционную запись устройства (IDR). Каждый AP генерирует PMAC независимо, и в то время как это не идентично для каждого отчета (как минимум, измеренный RSSI устройства является, вероятно, другим в каждом AP), это подобно. Функция сравнения и оценки PMACs вызвана, объединившись. PMAC не представлен на интерфейсах клиента. Только результаты слияния доступны в форме кластерного ID. Это слияние обсуждено затем.

Рис. 8: Необработанное обнаружение интерференции

В этом рисунке вы видите несколько AP все создание отчетов DECT, таких как Телефонная энергия. Однако AP в этом рисунке фактически сообщают относительно присутствия двух отдельных DECT, таких как Телефонные источники. Перед присвоением PMAC и последующего слияния, существует только классификация устройств, которая может вводить в заблуждение. PMAC дает нам способ определить отдельные источники помех, даже если у них нет логической информации, которая может использоваться, такие как адрес.

Слияние

Существует несколько AP все создание отчетов об аналогичном устройстве. Для каждого AP создания отчетов PMAC назначен на классифицированный сигнал. Следующий шаг должен объединить PMACs, которые вероятны то же исходное устройство одиночным отчетом для системы. Это - то, что слияние делает, консолидируя множественные отчеты одиночному событию.

Слияние использования пространственная близость AP создания отчетов. Если существует

шесть подобных IDRs с пятью от AP на том же полу и другом из здания на расстоянии в одну милю, маловероятно, что это - тот же источник помех. Как только близость установлена, вычисление вероятности выполнено для дальнейшего соответствия с отдельными IDRs, которые принадлежат, и результат назначен на кластер. Кластер представляет запись того интерференционного устройства и перехватывает отдельные AP, которые сообщают относительно него. Последующие отчеты IDR или обновления на том же устройстве придерживаются того же процесса, и вместо того, чтобы создать новый кластер, совпадают с существующим. В кластерном отчете один AP определяется как Кластерный Центр. Это - AP, который слышит интерференцию самое громкое.

Рис. 9: После Слияния РМАС - слушание AP то же физическое устройство определены

Объединяющийся алгоритм работает на включенном WLC каждого CleanAir. WLC выполняет функцию слияния для всего IDRs от AP, которые физически привязаны к нему. Весь IDRs и получающиеся объединенные кластеры переданы MSE, если он существует в системе. Системы с несколькими WLC требуют, чтобы MSE предоставил объединяющиеся сервисы. MSE выполняет более усовершенствованную функцию слияния, которая стремится объединиться, кластеры сообщили от других WLC и сведений о размещении извлечения, о которых сообщают WCS.

Почему нам нужен MSE для слияния IDRs через множественные WLC? Поскольку одиночный WLC только знает соседние узлы к AP, физически привязанным к нему. Близость RF не может быть определена для IDRs, прибывающего из AP, расположенных на других контроллерах, пока у вас нет представления всей системы. MSE имеет это представление.

То, как физическая близость определена, отличается, в зависимости от того, как вы внедряете CleanAir также.

- Для распространяющихся реализаций LMAP AP все участвуют в Обнаружении соседей, таким образом, это - легкий вопрос для консультации, соседний узел RF перечисляют и определяют пространственные отношения для IDRs.
- В модели наложения MMAP у вас нет этой информации. MMAPs являются пассивными устройствами и не передают соседние сообщения. Поэтому установление пространственных отношений одного MMAP к другому MMAP должно быть сделано с помощью координат X и y из системной карты. Чтобы сделать это, вам также нужен MSE, который знает о системной карте и может предоставить объединяющиеся функции.

Больше подробности о других режимах работы, а также практическом совете развертываний покрыто разделом моделей развертывания.

Развертывание AP в смешанном режиме – AP LMAP CleanAir с наложением AP MMAP CleanAir является лучшим подходом к высокой точности и общему покрытию. Можно использовать соседний список, созданный полученными соседними сообщениями для MMAP как часть объединяющейся информации. Другими словами, если у вас есть РМАС от AP LMAP и РМАС от MMAP, и MMAP показывает AP LMAP как соседний узел, тогда эти два могут быть объединены с высокой степенью уверенности. Это не возможно с CleanAir MMAPs, развернутым в устаревших стандартных AP, потому что те AP не производят IDRs для сравнения процессу слияния. MSE и ссылки X и y все еще необходимы.

[Точность размещения Wi-Fi non](#)

Определение местоположения радиопередатчика в теории является довольно прямым

процессом. Вы производите выборку полученного сигнала от нескольких размещений, и вы триангулируете на основе силы полученного сигнала. На сети Wi-Fi клиенты расположены и метки RFID Wi-Fi с хорошими результатами, пока существует достаточная плотность приемников и соответствующего Signal to Noise Ratio. Клиенты Wi-Fi и метки передают зонды на всех поддерживаемых каналах регулярно. Это гарантирует, что все AP в диапазоне слышат клиента или МЕТКУ независимо от канала, которому это служит. Это предоставляет большую информацию для работы с. Мы также знаем, что устройство (метка или клиент) подписывается на спецификацию, которая управляет, как это работает. Поэтому можно быть уверенными, что устройство использует всенаправленную антенну и имеет предсказуемую начальную мощность передачи. Устройства Wi-Fi также содержат логическую информацию, которая определяет его как уникальный источник сигнала (MAC-адрес).

Примечание: Нет никакой гарантии точности для местоположения не - устройства Wi-Fi. Точность может быть довольно хорошей и полезной. Однако существует много переменных в мире бытовой электроники и неумышленной электрической помехи. Любое ожидание точности, которая получена от текущего клиента или моделей точности размещения Метки, не применяется к не - местоположение Wi-Fi и функции CleanAir.

Источники помех Wi-Fi по-прежнему излагают специальную возможность стать творческими. Например, что такое, если сигнал вы пытаетесь расположить, узкий видеосигнал (1 МГц), который только влияет на один канал? В 2.4 ГГц это, вероятно, хорошо работает, потому что большинство организаций имеет достаточную плотность, чтобы гарантировать, что по крайней мере три AP на том же канале услышат его. Однако в 5 ГГц это более трудно, так как большинство устройств не-Wi-Fi только работает в полосе на 5.8 ГГц. Если RRM включили DCA с каналами страны, количеством AP, фактически назначенных в снижениях на 5.8 ГГц, потому что его цель состоит в том, чтобы распространить повторное использование канала и использовать открытый спектр. Это звучит плохо, но помните, не обнаруживаете ли вы его, тогда это - "not interfering" с чем-либо. Поэтому действительно не проблема с точки зрения интерференции.

Если ваши проблемы развертывания расширяются на безопасность, это - однако, проблема. Для получения надлежащего покрытия, вы требуете, чтобы некоторые AP MMAP в дополнение к AP LMAP гарантировали полное спектральное покрытие в полосе. Если ваше единственное беспокойство защищает операционное пространство, вы используете, то можно также ограничить каналы, доступные в DCA, и вызвать увеличенную плотность в диапазонах канала, которые вы хотите покрыть.

Параметры RF не - устройства Wi-Fi могут и действительно значительно различаться. Оценка должна быть сделана на основе типа устройства, которое обнаруживается. Стартовый RSSI источника сигнала должен быть известен хорошей точностью. Можно оценить это на основе опыта, но если устройство будет иметь направленную антенну, то вычисления будут выключены. Если устройство будет работать на заряде батареи и будет испытывать перекосы напряжения или пики, как это работает, то это изменится, как система видит его. Реализация другим изготовителем известного продукта не могла бы оправдать надежды системы. Это будет влиять на вычисления.

К счастью, Cisco имеет некоторый опыт в этой области, и размещение устройства не-Wi-Fi фактически работает вполне хорошо. Мнение, которое должно быть высказано, - то, что точность не - размещение устройства Wi-Fi имеет много переменных для рассмотрения, увеличения точности с питанием, рабочим циклом и количеством каналов, слыша устройство. Это - хорошие новости, потому что более высокое питание, более высокий рабочий цикл, устройства, которые влияют на составные каналы, обычно, что, как полагают,

серьезно, насколько идет интерференция к сети.

Модели развертывания CleanAir и Рекомендации

AP Cisco CleanAir, прежде всего, являются точками доступа. То, что это означает, - то, что нет ничего по сути другого о развертывании этих AP по развертыванию никакого другого в настоящее время поставляющего AP. То, что изменилось, является введением CleanAir. Это - пассивная технология, которая не влияет на использование сети Wi-Fi ни в каком случае кроме стратегий смягчения, на которые обращают внимание, RRM ED и PDA. Они только доступны в установке Гринфилда и настроены прочь по умолчанию. Этот раздел будет иметь дело с чувствительностью, плотностью и требованиями покрытия для хорошей функциональности CleanAir. Они не все это отличающееся от других установленных моделей технологии, таких как Голос, Видео или развертывания Местоположения.

Допустимые модели развертывания для продуктов CleanAir и работоспособности функции.

Таблица 5: модели развертывания CleanAir по сравнению с функциями

	Функция	Нало жени е ММА Р	Встро енный LMAP
Сервис AP	CleanAir	X	X
	Контролируя (RRM, Жулик, WIPS, Местоположение, и т.д.)	X	X
	Трафик клиента		X
Обнаружить	Обнаружьте и Проанализируйте радиочастотные сигналы	X	X
Классифициро вать	Классифицируйте Отдельные Источники помех со степенями серьезности ошибки влияния	X	X
Смягчить	Управляемые событиями изменения канала		X
	Избежание настойчивых устройств		X
Расположиться	Найдите на карте с зоной влияния		X
Устранение неполадок управляет, визуализируют	Подключение Cisco Spectrum Expert	X	X
	Интеграция WCS	X	X

CleanAir является пассивной технологией. Все, что это делает, слышат вещи. Поскольку AP слышит намного дальше, чем он может эффективно говорить, это делает его простой задачей, чтобы сделать корректный дизайн в среде Гринфилда. Понимание, как хорошо CleanAir слышит, и как классификация и обнаружение работают, даст вам ответы, в которых вы нуждаетесь для любой конфигурации CleanAir.

Чувствительность обнаружения CleanAir

CleanAir зависит от обнаружения. Чувствительность обнаружения более щедра, чем требования пропускной способности Wi-Fi с требованием SNR на 10 дБ для всех классификаторов и многих действующих вниз к 5 дБ. В большинстве мыслимых развертываний, где покрытие является распространяющимся, не должно быть никаких проблем на слушании и обнаружении интерференции в инфраструктуре сети.

То, как это ломается, просто. В сети, где среднее питание AP в или между 5-11 дБм (уровни мощности 3-5) тогда класс 3 (1 мВт / 0 дБм) устройство Bluetooth должно быть обнаружено вниз к -85 дБм. Повышение минимального уровня шума выше этого уровня создает небольшое ухудшение в дБ обнаружения для дБ. В целях дизайна стоит добавить буферную зону, заставляя минимальную цель проекта сказать -80. Это предоставит достаточное наложение в большинстве мыслимых ситуаций.

Примечание: Bluetooth является хорошим классификатором для разработки для того, потому что он представляет питание заднего конца, мудрое в устройствах, которые вы искали бы. Что-либо понижается, обычно даже не регистрируется на сети Wi-Fi. Это также удобно (и легко доступно) протестировать с тем, потому что это - устройство скачкообразной перестройки частоты и будет замечено каждым AP, независимо от режима или канала в 2.4 ГГц.

Важно понять ваш источник помех. Например, Bluetooth. Вот множественные разновидности этого на рынке в настоящее время, и радио и спецификация продолжили развиваться, как большинство технологий делает в течение долгого времени. Гарнитура Bluetooth, которую вы использовали бы для своего сотового телефона, наиболее вероятно class3 или class2 устройство. Это воздействует на малую мощность и делает вполне достаточное использование адаптивных профилей питания, которое расширяет срок службы аккумулятора и уменьшает интерференцию.

Гарнитура Bluetooth будет часто передавать на разбивке на страницы (Режим обнаружения), пока не привязано. Затем это пойдет бездействующее, пока не необходимый для сохранения питания. CleanAir только обнаружит активную передачу BT. Никакой RF, тогда ничто для обнаружения. Поэтому, если вы переходите к тесту с чем-то, удостоверьтесь, что он передает. Играйте немного музыки через него, но вынудите его передать. Подключение Эксперта по спектру является удобным способом проверить, ли что-то, или является "not transmitting" и закончит большой потенциальный беспорядок.

Развертывание с нуля

CleanAir был разработан к комплименту, что в основном считают обычной реализацией плотности. Это определение Обычных продолжает развиваться. Например, всего пять лет назад 300 AP в той же системе считали большой реализацией. В большом мире – это все еще. Количество 3 000-5 000 AP со многими сотнями из них делящийся знаниями из первоисточника посредством распространения RF обычно замечается.

То, что важно для понимания:

- CleanAir LMAP поддерживает назначенный канал **только**.
- Покрытие полосы внедрено путем обеспечения, что покрыты каналы.
- CleanAir AP может услышать очень хорошо, и граница активной ячейки не является пределом.
- Для решений для Местоположения значение сокращения RSSI составляет -75 дБм.
- Минимум трех качественных измерений требуется для Разрешения Местоположения.

В большинстве развертываний трудно отобразить зону уверенного приема, которая не будет иметь по крайней мере трех AP в выстреле уха на том же канале в 2.4 ГГц. Если нет, то разрешение местоположения страдает. Добавьте Точку доступа в режиме мониторинга и используйте рекомендации. Помните, что сокращение местоположения составляет -75 дБм, исправляет это, потому что MMAP слушает все каналы.

В местоположениях, где существует минимальное разрешение местоположения плотности, вероятно, не поддерживается. Но, вы защищаете канал активного пользователя чрезвычайно хорошо. Также в такой области, вы обычно не говорите о большом количестве пространства, настолько располагающийся источник помех не излагает ту же проблему как жильё мультипола.

Вопросы развертывания сводятся к планированию сети для желаемой емкости, и гарантируя наличие в распоряжении корректных компонентов и сетевых путей для поддержки функций CleanAir. Близость RF и важность Отношений Соседнего узла RF не могут быть преуменьшены. Удостоверьтесь, что поняли PMAC и процесс слияния хорошо. Если сеть не имеет хорошего дизайна RF, соседние отношения обычно влияют. Это влияет на производительность CleanAir.

Развертывания наложения MMAP

Если вы планируете установить CleanAir MMAPs как наложение к существующей сети существуют некоторые ограничения, которые необходимо иметь в виду. Программное обеспечение CleanAir 7.0 поддерживается на всех контроллерах поставки Cisco. Каждый контроллер модели поддерживает максимальную номинальную емкость AP с CleanAir LMAPs. Существуют пределы в количестве MMAPs, который может поддерживаться. Максимальное число MMAPs является функцией памяти. Контроллер должен сохранить подробные данные AQ для каждого отслеживаемого канала. LMAP требует двух хранилищ каналов информации о AQ. Однако MMAP пассивно просматривает, и данные канала могут быть 25 каналами на AP. Используйте таблицу ниже для руководства по проектированию. Всегда обращайтесь к документации текущего релиза для текущей информации выпуском.

Таблица 6: MMAP ограничивает на WLC

Controller	Max # AP	Кластеры	Записи устройств	Поддерживаемый CleanAir MMAPs
2100	25	75	300	6
2504	50	150	600	50
WLCM	25	75	300	6
4400	150	75	300	25
WISM 1	300	1500	7000	50
WISM2	100	5000	20000	1000

	0			
5508	500	2500	10000	500

Примечание: Номера, указанные на кластеры (объединенные интерференционные отчёты) и записи устройства (отдельные Отчёты IDR прежде, чем объединиться), щедры и очень маловероятны быть превышенными в даже худших средах.

Предположим, что вы просто хотите развернуть CleanAir как сенсорную сеть, чтобы контролировать и быть предупрежденными о не - интерференция Wi-Fi. В каком количестве AP Режим отслеживания (MMAPs) вы нуждаетесь? Ответ обычно является 1-5 MMAP к радио LMAP. Это, конечно, зависит от вашей модели покрытия. Сколько покрытия вы добиваетесь с AP MMAP? Вполне немного фактически, так как вы строго слушаете. Чем если бы также необходимо было связаться и передача, зона уверенного приема намного больше.

Как насчет вас визуализируют это на карте (можно ли использовать какое-либо программное средство планирования доступное выполнение подобной процедуры, как описано ниже)? Если вы имеете WCS и уже создали системные карты, то это - легкое осуществление. Используйте режим планирования в картах theWCS.

1. Выберите Monitor> Maps.
2. Выберите карту, с которой вы хотите работать.
3. В углу справа использования экрана WCS кнопка с зависимой фиксацией, чтобы выбрать Planning Mode, затем нажать идут.**Рис. 10: Режим Планирования WCS**
4. Выберите ADD APs.
5. Выберите руководство.
6. Выберите тип AP. Используйте антенну по умолчанию для внутреннего или измените для соответствия с развертываниями: 1 Мощность передатчика AP и для 5 ГГц и для 2.4 ГГц является –Class3 ВТ на 1 дБм = 1 мВт
7. Выберите ADD AP в нижней части.**Рис. 1-1: Добавьте AP в планировщике WCS**
8. Переместите AP, чтобы разместить в вашу карту и выбрать применяются.
9. Карта тепла заполняет. Выберите -80 дБм для сокращения RSSI наверху карты, перерисовки карты, если это - изменение.

Вот то, что ваш CleanAir MMAP покрывает для 1 дБм к-80 дБм. Эти результаты показывают ячейку с радиусом 70 футов или 15,000 футов / 2 из покрытия.

Рисунок 12: Покрытие в качестве примера CleanAir MMAP с помощью питания на 1 дБм и сокращения на-80 дБм для покрытия

Примечание: Следует иметь в виду, что это - прогнозирующий анализ. Точность этого анализа зависит непосредственно от точности карт, используемых для создания его. Это выходит за рамки этого документа для обеспечения пошаговой инструкции по тому, как отредактировать карты в WCS.

Хорошим вопросом, который вы хотите задать, являются “эти MMApS, переходят быть развернутым строго для CleanAir?” Или, вы - переходить, используют преимущества многих преимуществ, которые могут быть получены из включения контролируемых AP в вашей сети?

- Адаптивный WIPS
- Постороннее обнаружение

- Усовершенствование местоположения

Все они работа приложений с CleanAir включили AP. Для Адаптивного wIPS обратитесь к [Cisco Адаптивное wIPS Руководство по развертыванию](#), поскольку рекомендация покрытия Адаптивного wIPS подобна, но зависит от ваших целей и потребностей клиентов. Поскольку службы определения местоположения гарантируют, что вы рассматриваете и понимаете требования развертываний для своей технологии. Все эти решения являются дополнительными с целями проекта CleanAir.

[Смешивание CleanAir LMAP и устаревших AP non CleanAir в той же установке](#)

Почему я не должен смешивать CleanAir LMAP и Устаревшие AP LMAP в той же физической области? Этот вопрос принадлежит этому варианту использования:

“У меня в настоящее время есть развернутые AP non CleanAir (1130,1240, 1250, 1140) в автономном режиме. Я хочу добавить всего несколько AP CleanAir для увеличения моего покрытия/плотности. Почему я не могу только добавить некоторые AP и получить все функции CleanAir?”

Это не рекомендуется, потому что CleanAir LMAPs только контролирует служащий канал, и все функции CleanAir полагаются на измерительную плотность по качеству. Эта установка привела бы к неразборчивому покрытию полосы. Вы могли закончить с каналом (или несколькими), который не имеет никакого покрытия CleanAir вообще. Однако, с основной установкой, вы использовали бы все доступные каналы. Принятие RRM сознает ситуацию (рекомендовал), чтобы было совершенно возможно, что все AP CleanAir могли быть назначены на тот же канал в стандартном процессе установки. Вы распространяете их, чтобы попытаться получить лучшее пространственное возможное покрытие, и это фактически увеличивает разногласия этого.

Конечно, можно развернуть несколько AP CleanAir в с существующей установкой. Это - AP и функционировало бы прекрасное с точки зрения покрытия и клиента. Функциональность CleanAir поставилась бы под угрозу и нет никакого способа действительно гарантировать то, что система была бы или не говорить вам относительно вашего спектра. Существует слишком много опций в плотности и покрытии, которое может быть представлено для предсказания. Что работало бы?

- AQ был бы допустим для радио создания отчетов только. Это означает, что для канала только важно, что это служит, и это могло измениться в любое время.
- Интерференционные предупреждения и зона влияния были бы допустимы. Однако любое полученное местоположение было бы подозреваемым. Лучше всего оставить это всеми вместе и принять самое близкое разрешение AP.
- Стратегиям смягчения не рекомендовалось бы работать, потому что большинство AP в развертываниях не будет управлять тем же путем.
- Вы были бы в состоянии использовать AP для рассмотрения спектра от Подключения Спектра.
- У вас также была бы опция для временной коммутации к режиму отслеживания в любое время для выполнения полного просмотра среды.

В то время как существуют некоторые преимущества, важно понять ловушки и отрегулировать ожидания соответственно. Это не рекомендуется, и проблемы, являющиеся результатом этого типа развертываний, не приемлемы на основе этой модели развертывания.

Лучшая опция, если ваш бюджет не поддерживает добавляющие AP, которые не служат трафику клиента (MMAP), должна собрать достаточно AP CleanAir для развертывания вместе в одиночной области. Любая область, которая может быть включена на области карты, может содержать Гринфилда развертывания CleanAir с полнофункциональной поддержкой. Единственное предупреждение на этом было бы местоположением. Вам все еще нужно достаточно плотности для местоположения.

[Работа AP CleanAir и устаревшими AP на том же контроллере](#)

В то время как не желательно смешать устаревшие AP и AP CleanAir, работающие в автономном режиме в той же области развертываний, что относительно того, чтобы выполнить обоих на том же WLC? Это прекрасно подходит. Конфигурации для CleanAir только применимы к AP та поддержка CleanAir.

Например, в параметрах конфигурации RRM и для 802.11a/n и для 802.11b/g/n вы видите и RRM ED и конфигурации PDA для RRM. Можно было бы полагать, что они будут плохи, если применено к AP, который не был CleanAir способный AP. Однако даже при том, что эти функции действительно взаимодействуют с RRM, они могут только быть инициированы событием CleanAir и отслежены к AP, который иницирует их. Нет никакого шанса, что не - CleanAir AP применились к этим конфигурациям их, даже при том, что конфигурация применяется к целой группе RF.

Это поднимает другой важный вопрос. В то время как конфигурации CleanAir на 7.0 или более позднем контроллере являются эффективными для любого CleanAir AP, который подключает к тому контроллеру, RRM ED и PDA являются все еще конфигурациями RRM.

[Функции CleanAir](#)

Реализация CleanAir привлекает многие из подарка элементов архитектуры в CUWN. Это было разработано, чтобы укрепить и добавить функциональность к каждому компоненту системы, и привлекает информацию, которая уже присутствует, вершина улучшает удобство пользования и тесно интегрирует функции.

Это - полный отказ, классифицированный в уровни лицензии. Заметьте что необязательно иметь WCS и или MSE в системе для получения хорошей функциональности от системы. MIB доступны на контроллере и открыты для тех, кто хочет интегрировать эти функции в существующую систему управления.

[Требования к лицензии](#)

[Система базовой](#)

Для основной системы CleanAir требования являются CleanAir AP и WLC, который выполняет версию 7.0 или код следующих версий. Это предоставляет и CLI и GUI WLC для интерфейса клиента, и все ТЕКУЩИЕ ДАННЫЕ отображены, включая источники помех, о которых сообщает полоса и функция подключения SE. Сигналы о нарушении безопасности (Источники помех, определяемые как проблема безопасности), объединены прежде, чем инициировать trap-сообщение SNMP. Как ранее сообщили, хотя, слияние WLC ограничено представлением просто AP, привязанных к тому контроллеру. Нет никакой исторической поддержки анализа тенденции изменения, поддерживаемого непосредственно от

интерфейсов WLC.

WCS

Добавление WCS BASIC и управление контроллером добавляют отклоняющуюся поддержку AQ и сигналов тревоги. Вы получаете историческое создание отчетов AQ, пороговые предупреждения через SNMP, поддержку Информационной панели RRM, поддержку Сигнала о нарушении безопасности и много других преимуществ включая инструмент диагностики клиентов. То, что вы не получаете, является Интерференционной историей и местоположением. Это сохранено в MSE.

Примечание: Добавление MSE к WCS для местоположения требует и WCS плюс лицензия и характеристик лицензирования с учетом контекста для MSE.

MSE

Добавление MSE и решения для местоположения сети поддерживает историческое создание отчетов IDR, а также основанные на местоположении функции. Для добавления этого к существующему решению CUWN вы требуете плюс лицензия на WCS, и CAS или лицензии с учетом контекста на цели местоположения.

1 Источник помех = 1 лицензия CAS

Источниками помех управляют через с учетом контекста и интерференцию, которая отслежена в системе, совпадает с клиентом в целях лицензировать. Существует много опций о том, как управлять этими лицензиями и для чего они используются.

На конфигурации WLC можно ограничить, какие источники помех отслежены для местоположения и сообщаемый в картах путем выбора их от **контроллера> беспроводные сети> 802.11b/a>** меню **CleanAir**.

Там сообщают об интерференционных устройствах, выбранных, и принимающий решение проигнорировать их не допускает их в систему местоположения и MSE. Это является абсолютно отдельным от того, что фактически происходит в AP. Все классификаторы всегда обнаруживаются на уровне AP. Это определяет то, о чем сообщают isdone с IDR. При использовании это для ограничения создания отчетов, то это довольно безопасно, потому что вся энергия все еще замечена в AP и перехвачена в отчётах AQ. Отчёты AQ вспыхивают способствующие источники помех по категориям. При устранении категории здесь для сохранения лицензирования, об этом все еще сообщают как влияющий фактор в AQ, и вы предупреждены при превышении порога.

Конфигурация **Рисунок 13: WLC CleanAir - создание отчетов**

Например, предположите сеть, которую вы устанавливаете, находится в розничной среде, и карта нарушена целями Bluetooth, прибывающими из гарнитур. Вы могли устранить это путем отмены выбора Ссылки Bluetooth. Если бы в некоторое время спустя Bluetooth стал проблемой, то вы видели бы, что эта категория повышается в вашем создании отчетов AQ, и могли бы реактивировать по желанию. Нет никакого интерфейсного требуемого сброса.

У вас также есть Element Manager под конфигурациями MSE: **WCS> Сервисы мобильности> Ваш MSE> Контекстно-зависимая служба> администрирование> отслеживание Параметров.**

Рисунок 14: MSE Element Manager с учетом контекста

Это дает пользовательский полный контроль, чтобы оценить и управлять тем, для чего используются лицензии и как они разделены между целевыми категориями.

[Матрица функций CleanAir](#)

Таблица 7: матрица Функций CleanAir Компонентом CUWN

Функции Cisco CleanAir устройством	350 0 WL C	W CS	MS E
Радио-устранение проблем			
Air Quality и Интерференция AP/радио на GUI WLC и CLI - интерфейсах	X		
Пороговое trap-сообщение AQ (на радио) от WLC	X		
Интерференционное trap-сообщение Устройства (на Радио) от WLC	X		
Быстрый режим Обновления с текущими диаграммами AQ и источниками помех для радио	X		
CleanAir-поддерживающий RRM	X		
Режим Подключения Эксперта по спектру	X		
MIB спектра на WLC, откройтесь к третьим сторонам	X		
Сетевой Air Quality			
Панель мониторинга WCS CleanAir показывая Графическую историю AQ для всех полос		X	
Отслеживание истории AQ и отчёты		X	
AQ Heatmap и объединенный AQ (на пол) на карте этажа WCS		X	
Возглавьте устройства N для AP, показанного как опция парения на карте этажа WCS		X	
CleanAir-поддерживающая информационная панель RRM WCS		X	
CleanAir-поддерживающая Информационная панель Безопасности WCS и отчёты		X	
CleanAir-поддерживающий инструмент диагностики клиентов WCS		X	
Местоположение			
Панель мониторинга WCS CleanAir с Вершиной N устройства со степенями серьезности ошибки			X
Слияние интерференционных			X

устройств через AP			
Интерференционное отслеживание истории устройства с отчётами			X
Местоположение источников помех – Зона Влияния			X

Функции, поддерживаемые на WLC

Минимальная требуемая конфигурация для Cisco CleanAir является AP Cisco CleanAir и WLC, который выполняет версию 7.0. С этими двумя компонентами можно просмотреть всю информацию, предоставленную AP CleanAir. Вы также получаете функции смягчения, доступные с добавлением AP CleanAir и расширений, предоставленных через RRM. Эта информация доступна для просмотра через CLI или GUI. Фокус находится на GUI в этом разделе для краткости.

Air Quality WLC и интерференционные отчёты

На WLC можно просмотреть текущий AQ и Интерференционные отчёты из меню графического интерфейса пользователя. Для просматривания интерференционных отчетов должна быть интерференция, активная, как отчёт для существующих условий только

Отчет об устройствах, создающих помехи

Выберите Monitor> Cisco CleanAir> 802.11a/802.11b> Интерференционные Устройства.

Все активные интерференционные устройства, сообщаемые Радио CleanAir, перечислены созданием отчетов Радио/AP. Подробные данные включают Название AP, ID Слота радиоблока, Интерференционный Тип, Неисправные каналы, Обнаруженное Время, Степени серьезности ошибки, Рабочий цикл, RSSI, Идентификатор устройства и Кластерный ID.

Рисунок 15: Доступ к отчету об устройствах, создающих помехи WLC

Отчёт о Air Quality

О Air Quality сообщают по Радио/каналу. В примере ниже, AP0022.bd18.87c0 находится в режиме отслеживания и отображает AQ для каналов 1-11.

Установка переключателя в конце любой линии позволяет опцию показа этой информации на радио-подробном экране, который включает всю информацию, собранную интерфейсом CleanAir.

Рисунок 16: Отчет об устройствах, создающих помехи WLC

Конфигурация CleanAir – AQ и контроль за Trap-сообщениями Устройства

CleanAir позволяет вам определять и порог и типы trap-сообщений, которые вы получаете. Конфигурация полосой: Беспроводные сети> 802.11b/a> CleanAir.

Конфигурация Рисунок 17: WLC CleanAir

Параметры CleanAir

Можно включить и отключить CleanAir для всего контроллера, подавить создание отчетов

всех источников помех и определить который источники помех сообщить или проигнорировать. Выбор определенных интерференционных устройств для игнорирования является полезной возможностью. Например, вы не могли бы хотеть отслеживать все гарнитуры Bluetooth, потому что они - относительно низкое влияние, и у вас есть многие из них. Выбор проигнорировать эти устройства просто препятствует тому, чтобы он был сообщен. RF, который прибывает из устройств, все еще вычислен в общий AQ для спектра.

Конфигурации trap-сообщения

Позволить/запретить (на по умолчанию) trap-сообщение AirQuality.

Порог аварийной сигнализации AQI (1 - 100). Когда вы устанавливаете порог AirQuality для trap-сообщений, это говорит WLC в том, какой уровень вы хотите видеть trap-сообщение для AirQuality. Порог по умолчанию равняется 35, который является чрезвычайно высоким. Для тестирования установка этого значения к 85 или 90 оказывается более практичной. На практике порог является переменным, таким образом, можно настроить его для определенной среды.

Включите Интерференцию для Аварийного сигнала защиты. Когда вы добавляете WLC к системе WCS, можно установить этот флажок для обработки интерференционных trap-сообщений устройства, поскольку аварийный сигнал защиты поймал в ловушку. Это позволяет вам выбирать типы устройств, которые появляются в панели сводки аварийных сигналов WCS как trap-сообщение безопасности.

Не поймайте в ловушку выбор устройства позволяет контроль над типами устройств, который генерирует сообщения прерывания интерференции/безопасности.

Наконец, статус RRM ED (Методы управления радиочастотным ресурсом в зависимости от состояния окружающей сигнально-помеховой обстановки) отображен. Конфигурация для этой функции покрыта под Методами управления радиочастотным ресурсом в зависимости от состояния окружающей сигнально-помеховой обстановки - EDRRM разделяют позже в этом документе.

Быстрый режим обновления* - подробность CleanAir

При выборе беспроводных сетей>> Radio точек доступа> 802.11a/b показывает весь из 802.11b или 802.11a радио, подключенные к WLC.

Установка переключателя в конце линии позволяет вам видеть любого радио-подробность (традиционные метрики по CleanAir использования, шум и т.п.) или подробность CleanAir.

Рисунок 18: Доступ к подробности CleanAir

Выбор CleanAir производит графический показ (по умолчанию) всей информации о CleanAir, имеющей отношение к тому радио. Отображенная информация находится теперь в Быстром Режиме Обновления по умолчанию. Это означает, что обновляется каждые 30 секунд от AP вместо 15-минутного периода усреднения, отображенного в обмене сообщениями уровня системы. Сверху донизу, все источники помех, обнаруживаемые тем радио наряду с интерференционными параметрами Типа, Неисправных каналов, Время обнаружения, Степени серьезности ошибки, Рабочий цикл, RSSI, Идентификатор устройства и Кластерный ID.

Радио Рисунок 19: CleanAir детализирует страницу

От этого рисунка отображенные диаграммы включают:

- Air Quality каналом
- Не - использование канала Wi-Fi
- Мощность помехи

Air Quality Каналом отображает Air Quality для канала, который проверяется.

Использование канала Wi-Fi по показываает использование, которое непосредственно относится к интерференционному отображаемому устройству. Другими словами, если вы избавляетесь от того устройства, вы возвращаете так много спектра для приложений Wi-Fi для использования.

Существует две категории, которые представлены здесь под подробными данными Air Quality:

- Смежная Выключено интерференция канала (AOI) — Это - интерференция от устройства Wi-Fi, которое не находится на рабочем канале создания отчетов, но накладывается на пространство канала. Для канала 6, отчет определил бы интерференцию, относящуюся к AP на каналах 4, 5, 7, и 8.
- Несекретный — Это - энергия, которая не относится окончательно к Wi-Fi или не - источники Wi-Fi. Фрагменты, коллизии, вещи этой природы; кадры, которые искажены до неузнаваемости. В CleanAir не должны быть высказаны предположения.

Мощность помехи отображает получить питание источника помех в том AP. Подробная информация об отображениях страницы CleanAir для всех отслеживаемых каналов. Приведенные выше примеры являются от Режим отслеживания (MMAP) AP. Точка доступа в локальном режиме показала бы ту же подробность, но только для текущего подаваемого канала.

CleanAir включил RRM

Существует две ключевых Функции Смягчения, которые присутствуют с CleanAir. Оба полагаются непосредственно на информацию, которая может только быть собрана CleanAir.

Методы управления радиочастотным ресурсом в зависимости от состояния окружающей сигнально-помеховой обстановки

Методы управления радиочастотным ресурсом в зависимости от состояния окружающей сигнально-помеховой обстановки (RRM ED) являются функцией, которая позволяет AP в бедствии обходить обычные интервалы RRM и сразу переключать каналы. CleanAir AP всегда контролирует AQ и сообщает относительно этого в 15-секундных интервалах. AirQuality является лучшей метрикой, чем доверие обычным измерениям шума микросхемы Wi-Fi, потому что AirQuality только сообщает относительно Классифицированных Интерференционных устройств. Это делает AirQuality надежной метрикой, потому что известно, о чем сообщают, не из-за энергии Wi-Fi (и следовательно не переходный обычный скачок).

Если на Air Quality достаточно влияют, для RRM ED только происходит изменение канала. Поскольку на Air Quality можно только влиять классифицированным, известным CleanAir не - источник помех Wi-Fi (или смежный перекрывающийся канал Wi-Fi), влияние понятно:

- Не аномалия Wi-Fi
- Кризисное условие в этом AP

Кризис означает, что заблокирован CCA. Никакие клиенты или AP не могут использовать

текущий канал.

При этих условиях RRM переключил бы канал на следующем проходе DCA. Однако это могло быть на расстоянии в несколько минут (до десяти минут в зависимости от того, когда последнее выполнение было выполнено), или пользователь, возможно, изменил интервал по умолчанию, и это могло быть более длинно (выбрал время привязки и интервал для более длинной операции DCA). RRM ED реагирует очень быстро (30 секунд) так пользователи, которые изменяются с AP, вероятно, не знают о кризисе, который был близок. 30 - 50 секунд не достаточно длинно для вызова справочного стола. Пользователи, которые не делают, не находятся ни в какой худшей форме, чем они были бы во-первых. Во всех случаях был определен источник помех, и причина изменения точки доступа регистрирует тот источник, и пользователи, которые имеют плохой роуминг, получают ответ относительно того, почему было внесено это изменение.

Изменение канала не случайно. Это выбрано на основе разделения устройств, таким образом это - интеллектуальный альтернативный выбор. Как только канал переключен существует защита от инициирования RRM ED снова в удерживать в нажатом состоянии таймере (60 секунд). Канал события также отмечен в DCA RRM для AP, на который влияют, для предотвращения return к каналу события (3 часа) в конечном счете, источник помех является неустойчивым событием, и DCA сразу не видит его. Во всех случаях влияние изменения канала изолировано к AP, на который влияют.

Предположим хакер, или кто-то плохого намерения разжигает передатчик помех на 2.4 ГГц, и все каналы заблокированы. Прежде всего все пользователи в радиусе банкротом так или иначе. Однако предположите, что RRM ED включает все AP, которые видят его. Все AP переключают каналы однажды, затем держатся в течение 60 секунд. Условие соблюдали бы снова, таким образом, другое изменение сработает с условием, все еще встречаемым после 60 секунд. Не было бы никаких каналов, оставленных измениться на, и действие RRM ED остановится.

Сигнал о нарушении безопасности исчерпал бы на передатчике помех (действие по умолчанию), и необходимо будет предоставить местоположение (если с MSE) или самый близкий AP обнаружения. RRM ED регистрировал бы главное событие AQ для всех неисправных каналов. Причина была бы передатчиком помех RF. Событие содержалось бы в произведенном домене RF и хорошо предупреждалось бы.

Теперь следующий вопрос, который обычно спрашивают, "что, если хакер идет вокруг с передатчиком помех, был бы тот не, которые заставляют все AP инициировать RRM ED?".

Уверенный вы переходите к триггерным изменениям канала RRM ED на всех AP, которым включили RRM ED. Однако, в то время как передатчик помех перемещается также - его эффект, и удобство пользования восстановлено, как только это перемещается. Это действительно не имеет значения, потому что у вас есть хакер, идущий вокруг с передатчиком помех в их разъединяющих пользователях руки везде, они идут. Это - проблема сам по себе. RRM ED не соединяет ту проблему. CleanAir, с другой стороны, также занят, предупреждая, располагаясь, и предоставляя историю местоположения того, куда они пошли и где они. Это хорошие вещи знать в таком случае.

К конфигурации обращаются под **беспроводными сетями > 802.11a/802.11b > RRM > DCA > Методы управления радиочастотным ресурсом в зависимости от состояния окружающей сигнально-помеховой обстановки.**

Рис. 20: Конфигурация методов управления радиочастотным ресурсом в зависимости от

состояния окружающей сигнально-помеховой обстановки

Примечание: Как только RRM ED иницирован на AP/Канале, который AP препятствуют возвратить к тому каналу в течение трех часов. Если источник сигнала неустойчив по своей природе, это должно предотвратить перегрузку.

Избежание настойчивых устройств

Избежание настойчивых устройств является другой функцией смягчения, которая только возможна с AP CleanAir. Устройство, которое периодически работает, такие как микроволновая печь, может представить разрушительные уровни интерференции, в то время как это работает. Однако, как только это больше не используется, воздух успокаивается снова. Устройства, такие как видеоканалы, наружное мостовое оборудование и микроволновые печи являются всеми примерами типа устройства, названного персистентным. Эти устройства могут работать постоянно или периодически, но что они все имеют, вместе с тем, что они часто не перемещаются.

RRM, конечно, видит уровни шума RF на данном канале. Если устройство работает достаточно долго, RRM даже перемещает активный AP от канала, который имеет интерференцию. Однако, как только устройство успокаивается, вероятно, что исходный канал представляет как лучший выбор еще раз. Поскольку каждый CleanAir AP является датчиком спектра, центр источника помех может быть оценен и расположен. Кроме того, можно понять, на какие AP влияет устройство, которое вы знаете, там, и потенциально управляет и разрушает сеть, когда она делает. Избежание настойчивых устройств позволяет нам регистрировать существование такой интерференции и помнить, что это там, таким образом, вы не размещаете AP назад в тот же канал. Как только Персистентное Устройство было определено, его "помнят" в течение семи дней. Если это не замечено снова тогда, что это очищено от системы. Каждый раз, когда вы видите его, часы запускаются.

Примечание: Информацию об Избежании настойчивых устройств помнят в AP и Контроллере. Перегрузка любого сброс значение.

Конфигурация для Избежания настойчивых устройств расположена в **беспроводных сетях> 802.11a/802.11b> RRM>, DCA> Избегаем Устройств.**

Чтобы видеть, регистрировало ли радио Персистентное Устройство, можно посмотреть статус в **беспроводных сетях>> Radio точек доступа> 802.11a/b>.**

Выберите радио. В конце линии нажимают кнопку с зависимой фиксацией и выбирают CleanAir RRM.

Статус Figure 21: CleanAir Избежания настойчивых устройств

Подключение эксперта по спектру

AP CleanAir могут все поддерживать режим подключения Эксперта по Спектру. Этот режим размещает радио AP в специализированный режим сканирования, который может вести приложение Cisco Spectrum Expert через сеть. Функции консоли Эксперта по Спектру, как будто это имело локальную установленную карту Эксперта по Спектру.

Примечание: Путь маршрутизируемой сети должен существовать между хостом Эксперта по Спектру и целевым AP. Порты 37540 и 37550 должны быть открыты для подключения. Протокол является TCP, и AP слушает.

Режим подключения Эксперта по спектру является расширенным режимом отслеживания, и как таковой, AP не служит клиентам, в то время как включен этот режим. Когда вы иницилируете режим перезагрузки точки доступа. Когда это воссоединяется с контроллером, это находится в режиме Подключения Спектра и генерировало ключ сеанса для использования для соединения приложения. Все, что требуется, является Cisco Spectrum Expert 4.0 или позже, и путь маршрутизируемой сети между хостом приложения и целевым AP.

Для инициирования соединения запустите путем изменения режима на от **беспроводных сетей> точки доступа> Все AP**.

Рисунок 22: Конфигурация режима AP

Перейдите к Режиму AP и выберите SE-Connect. Сохраните конфигурацию. Вы получаете два экрана предупреждения: одно уведомление, что режим подключения SE не является служащим клиенту режимом, второе предупреждение, что перезагружен AP. Как только вы изменили режим и сохранили конфигурацию, перешли к **Монитору>** экран **точек доступа**. Контролируйте статус AP и повторную загрузку.

Как только AP возражает, и повторные загрузки перешли назад на экран конфигурации точки доступа, вам нужен Ключ NSI для сеанса, который отображен там. Можно скопировать и вставить ключ NSI для включения в запуск Эксперта по Спектру.

Рисунок 23: Ключ NSI генерируется

Вам нужен Cisco Spectrum Expert 4.0. После того, как установленный, Эксперт по Спектру запуска. На начальном экране заставки вы видите новую опцию, Удаленный Датчик. Выберите Remote Sensor и вставку в Ключе NSI, и скажите Эксперту по Спектру IP-адрес AP. Выберите, с каким радио вы хотите соединиться и нажать ОК.

Рисунок 24: Экран connect Датчика Cisco Spectrum Expert

[WCS активировал опции CleanAir](#)

Когда вы добавляете WCS к соединению функции, вы получаете больше параметров экрана для получения информации о CleanAir. WLC может отобразить текущую информацию, но с WCS добавлена способность отследить, контролировать, предупредить, и сообщить об исторических уровнях AirQuality для всех AP CleanAir. Кроме того, способность коррелировать информацию о CleanAir к другим отмеченным наградой информационным панелям в WCS позволяет пользователю полностью понимать их спектр как никогда прежде.

Панель мониторинга WCS CleanAir

Домашняя страница имеет несколько добавленных элементов и настраиваема пользователем. Любой из элементов, отображенных на домашней странице, может быть перестроен к предпочтениям пользователя. Это выходит за рамки этого обсуждения, но помните его, поскольку вы используете систему. Что представляется, вот просто стандартный экран. Выбор вкладки CleanAir берет вас к доступной информации CleanAir в системе.

Рисунок 25: Домашняя страница WCS

Примечание: Настройки по умолчанию для страницы включают лучшие 10 отчётов об источниках помех полосой в углу справа. Если у вас нет MSE, этот отчёт не заполняет. Можно отредактировать эту страницу и добавить или удалить компоненты для настройки ее

к симпатии.

Рисунок 26: Панель мониторинга WCS CleanAir

Диаграммы отображены на этом изображении страницы рабочие исторические средние числа и минимумы для событий спектра CleanAir. Средний номер AQ для всей системы, как отображено здесь. Минимальная диаграмма AQ, например, отслеживает, полосой, минимальный AQ, о котором сообщают, полученный от любого определенного радио в системе в любой 15-минутный отчетный период. Можно использовать диаграммы для быстрого определения исторических минимумов.

Рисунок 27: Минимальная диаграмма истории Air Quality

Нажатие кнопки Enlarge Chart в нижнем правом углу в любом объекте диаграммы производит всплывающее окно с увеличенным представлением рассматриваемой диаграммы. Парение мыши в любой диаграмме производит штамп даты и времени и уровень AQ, замеченный в течение отчетного периода.

Схема 28: Увеличенная минимальная диаграмма Air Quality

Знание даты и времени дает вам информацию, что необходимо искать определенное событие и собрать дополнительные сведения, такие как AP, которые зарегистрировали событие и типы устройства, работающие в то время.

О сигналах порога AQ сообщают WCS как аварийные сигналы контроля функционирования. Можно также просмотреть их через панель Сводки аварийных сигналов наверху домашней страницы.

Рис. 29: Панель Сводки аварийных сигналов

Или Расширенный поиск или просто выбор категории производительности от панели сводки аварийных сигналов (если у вас есть аварийный сигнал контроля функционирования) приводят к списку аварийных сигналов контроля функционирования, которые содержат подробные данные об определенном событии AQ, которое является ниже настроенного порога.

Рисунок 30: Сигналы порога Air Quality

Выбор определенного события отображает подробность, отнесенную к тому событию включая дату, время, и самое главное AP создания отчетов.

Рисунок 31: подробность аварийного сигнала контроля функционирования

Конфигурации для Порогов Air Quality расположены под, Настроить > Контроллер, или от GUI WCS или от Графического интерфейса контроллера. Это может использоваться для всех Конфигураций CleanAir. Оптимальный метод должен использовать WCS, как только вы назначили контроллер на него.

Для генерации аварийных сигналов контроля функционирования можно установить порог AQ для нижнего предела такой как 90, или даже 95 (помните, что AQ способен 100 и плохо в 0). Вам нужна некоторая интерференция для инициирования его, такие как микроволновая печь. Не забудьте помещать чашку воды в нем сначала и выполнять его в течение 3-5 минут.

Отчёты об отслеживании истории Air Quality

AirQuality отслежен на каждом CleanAir AP на радио-уровне. WCS включает отчеты предыстории для того, чтобы контролировать и отклониться AQ в вашей инфраструктуре. К

отчётам можно обратиться путем навигации к панели запуска отчёта. Выберите Reports> Report Launchpad.

Отчёты CleanAir наверху списка. Можно принять решение посмотреть на Air Quality по сравнению со временем или худшими AP Air Quality. Оба отчёта должны быть полезными в отслеживании, как Air Quality изменяется в течение долгого времени и области определения, которые требуют некоторого внимания.

Рис. 32: Сообщите о панели запуска Карты CleanAir – Монитор> Карты

Выбор **Монитор> Карты** отображает карты, настроенные для системы. Средние и минимальные номера AQ представлены в иерархической форме соответствовать контейнерным уровням кампуса, здания и пола. Например, в здании выравнивают Среднее число/Минимум, AQ является средним числом всех AP CleanAir, содержащихся в здании. Минимумом является самый низкий AQ, о котором сообщает любой одиночный CleanAir AP. Смотря на уровень пола, средний AQ представляет среднее число всех AP, расположенных на том полу, и минимальный AQ является тем из одиночного худшего AQ от AP на том полу.

Рис. 33: Главная страница карт - показ Иерархии Air Quality

Выбор карты для данного пола предоставляет подробность, относящуюся к выбранному полу. Существует много способов, которыми можно просмотреть информацию о карте. Например, можно изменить метки AP для отображения, информация о CleanAir, такая как Статус CleanAir (показывает, какие AP способны), минимальные или средние значения AQ или Приблизительные и Минимальные значения. Значения относятся к выбранной полосе.

Рисунок 34: Метки AP показывают большую информацию о CleanAir

Вы видите источники помех, о которых сообщает каждый AP несколькими способами. Нависните над AP, выберите радио и выберите горячую ссылку источника помех показа. Это производит список всей Интерференции, обнаруженной на том интерфейсе.

Рисунок 35: Просмотр Интерференционных Устройств обнаружен на AP

Другой содержательный способ визуализировать влияние интерференции на карте состоит в том, чтобы выбрать интерференционную метку. Без MSE вы не можете определить местоположение интерференции на карте. Однако можно выбрать, показывают интерференционные метки, которые являются метками с источниками помех, в настоящее время обнаруживаемыми, применен ко всем радио CleanAir. Можно настроить это для ограничения количества отображенных источников помех. Выбор горячей ссылки во вкладке позволяет вам увеличивать масштаб к отдельным подробным данным источника помех, и все источники помех отображены.

AP Примечание: CleanAir могут отследить неограниченные количества источников помех. Они только сообщают относительно лучших 10, упорядоченных степенями серьезности ошибки с предпочтением, даваемым угрозе безопасности.

Рисунок 36: Интерференционная Метка, отображаемая на всех AP CleanAir

Полезный способ для визуализации не - интерференция Wi-Fi и это являются эффектом, должен просмотреть AQ как heatmap на показе карты. Сделайте это путем выбора heatmap и выбора Air Quality. Можно отобразить среднее число или минимальный AQ. Карта представлена с помощью образцов покрытия для каждого AP. Заметьте, что верхний правый угол карты является белым. Никакой AQ не представлен там, потому что AP находится в режиме отслеживания и пассивен.

Рисунок 37: карта тепла Air Quality CleanAir включил информационную панель RRM

CleanAir позволяет вам видеть то, что находится в нашем спектре, который является не - Wi-Fi. Другими словами, все те вещи, которые считали просто шумом, могут теперь быть сломаны, чтобы понять, если и как он влияет на вашу сеть передачи данных. RRM может и действительно смягчать шум путем выбора лучшего канала. Когда это происходит, решение обычно лучше, чем это было, но вы все еще позволяете чему-то, что не является вашей сетью передачи данных, занимать ваш спектр. Это уменьшает полный спектр, доступный вашим данным и голосовым приложениям.

Соединенный проводом и Беспроводные сети отличаются по этому на проводной сети, если вам нужно больше пропускной способности, можно установить больше коммутаторов, или портов или Интернет-соединений. Сигналы все содержатся в проводе и не вмешиваются друг с другом. В беспроводной сети, однако, существует ограниченная сумма доступного спектра. После того, как используемый, вы не можете просто добавить больше.

Информационная панель CleanAir RRM на WCS позволяет вам понимать то, что продолжается в вашем спектре путем отслеживания не - интерференция Wi-Fi, а также Сигнал от нашей сети, Интерференция от внешних сетей и балансировки всех в спектре, который доступен. Решения, которые предоставляет RRM, не всегда кажутся оптимальными. Однако часто существует что-то, что вы не видите который причины два AP для работы на тот же канал.

Информационная панель RRM - то, что мы используем для беговых соревнований, которые влияют на баланс спектра и предоставляют ответы относительно того, почему что-то - способ, которым это. Информацией о CleanAir, интегрируемой к этой информационной панели, является большой шаг вперед к полному управлению спектра.

Рисунок 38: Изменение канала CleanAir RRM обосновывает от Информационной панели RRM

Причины Изменения канала теперь включают несколько новых категорий, которые совершенствовали старую Шумовую категорию (что-либо, что не является Wi-Fi, распознан как шум Cisco и всеми другими конкурентами):

- Шум (CleanAir) представляет не - энергия Wi-Fi в спектре, как являющемся причиной или основной причиной к изменению канала.
- Персистентная интерференция Не-Wi-Fi указывает, что персистентный источник помех был обнаружен и вошелся в систему AP, и AP переключил каналы для предотвращения этой интерференции.
- Главное Событие Air Quality является причиной для изменения канала, вызванного функцией Методов управления радиочастотным ресурсом в зависимости от состояния окружающей сигнально-помеховой обстановки.
- Другой – всегда существует энергетический подарок в спектре, который не демодулируется как Wi-Fi и не может быть классифицирован как известный источник помех. Причины для этого - многие: сигналы слишком повреждены для разделения, перенесенные остатки от коллизий одна возможность.

Знание, что интерференция не-Wi-Fi влияет на вашу сеть, является большим преимуществом. Наличие вашей сети знает и действует на эту информацию, большое плюс. Некоторая интерференция, которую вы в состоянии смягчить и удалить, некоторые, которые вы не делаете (в случае излучения соседнего узла). Как правило, большинство организаций

имеет интерференцию на одном уровне или другом, и большая эта интерференция является нижним уровнем достаточно для не изложения любых реальных проблем. Однако более занятое, которое ваша сеть получает больше ей нужен незатронутый спектр.

CleanAir включил информационную панель безопасности

Устройства не-Wi-Fi могут предложить настоящий вызов безопасности беспроводной связи. Наличие способности исследовать сигналы на физическом уровне обеспечивает намного больше гранулированной безопасности. Обычный каждый день потребительские беспроводные устройства могут и действительно обходить обычную безопасность Wi-Fi. Поскольку все существующие приложения WIDs/WIPs полагаются на комплекты микросхем Wi-Fi для обнаружения, не было никакого способа точно определить эти угрозы до сих пор.

Например, возможно инвертировать данные в радиосигнале так, чтобы это были 180 градусов, несовпадающих по фазе от обычного сигнала Wi-Fi. Или, вы могли изменить среднюю частоту канала несколькими kHz и, пока у вас был клиентский набор к той же средней частоте, у вас будет частный канал, который не видела никакая другая микросхема Wi-Fi, или понять. Все, что требуется, является доступом к уровню HAL (многие доступны под GPL) для микросхемы и немного навыка. CleanAir в состоянии обнаружить и понять, каковы эти сигналы. Кроме того, CleanAir может обнаружить и определить местоположение атаки PhyDOS, такой как Затор RF.

Можно настроить CleanAir для создания отчетов о любом устройстве, которое классифицировано как угроза безопасности. Это позволяет пользователю определять то, что должно и не должно передавать в их средстве. Существует три способа просмотреть эти события. Самое удобное через панель Сводки аварийных сигналов, расположенную наверху домашней страницы WCS.

Более подробный анализ может быть получен при помощи вкладки Security Dashboard на главной странице. Это - то, где отображены все дополнительные сведения безопасности в системе. CleanAir теперь имеет свой собственный раздел в этой информационной панели, разрешающей вам получать полное понимание безопасности вашей сети из всех беспроводных источников.

Рисунок 39: Информационная панель Безопасности с интеграцией CleanAr

Независимо от того, где вы просматриваете эту информацию от, у вас есть AP обнаружения, время и дата события и текущий статус для работы с MSE, добавленным, можно выполнить периодические отчеты о просто событиях связанное с безопасностью CleanAir. Или, можно посмотреть на местоположение на карте и видеть историю события, даже если это перемещалось.

CleanAir включил Клиенту, Устраняющему неполадки Информационной панели

Клиентская информационная панель на домашней странице WCS является той, останавливаются для всех вещей для клиентов. Поскольку интерференция часто влияет на клиента, прежде чем она будет влиять на AP (более низкое питание, более плохие антенны) ключевая вещь знать, когда решение проблем производительности клиента состоит в том, если не - интерференция Wi-Fi является фактором. CleanAir был интегрирован к Инструменту диагностики клиентов на WCS по этой причине.

Обратитесь к сведениям о клиенте в любом случае, вы выбираете из информационной панели, или путем поиска на MAC-адресе или пользователе. Как только вам отобразили клиента, выберите Значок Инструмента диагностики клиентов для запуска Клиента,

Устраняющего неполадки Информационной панели.

Рисунок 40: клиент, устраняющий неполадки информационной панели - с CleanAir

Клиентские программные средства предоставляют полную информацию о статусе клиента в сети. Выберите вкладку CleanAir на Экране клиента Монитора. Если AP, к которому в настоящее время привязывается клиент, сообщает об интерференции, он отображен здесь.

Рисунок 41: вкладка CleanAir от Инструмента диагностики клиентов

В этом случае обнаруживаемая интерференция является DECT как телефон, и потому что степени серьезности ошибки - только 1 (очень низкий), это вряд ли доставило бы много неприятностей. Однако несколько Степеней серьезности ошибки 1 устройство могут вызвать проблемы для клиента. Клиентская Информационная панель позволяет вам быстро исключать, а также доказывать, проблемы логической формой.

MSE активировал опции CleanAir

MSE добавляет значительную часть информации к функциям CleanAir. MSE ответственен за все вычисления местоположения, которые намного более интенсивны для интерференции не-Wi-Fi, чем для цели Wi-Fi. Причина для этого является диапазоном условий, с которыми должно работать местоположение. Существует много источников помех не-Wi-Fi в мире, и они все работают по-другому. Даже среди аналогичных устройств могут быть большие различия в уровне сигнала или диаграммах направленности излучения.

MSE также, кто управляет слиянием устройств тот промежуток несколько контроллеров. Если вы вспоминаете, WLC может объединить устройства, что отчёты о AP, которыми он управляет. Но, интерференция может быть обнаружена, который присутствует на AP, которые не являются всеми на том же контроллере.

Все функции, которые улучшает MSE, расположены только в WCS. Как только вы определили местоположение интерференционного устройства на карте, существует несколько вещей, которые могут быть вычислены и представлены о том, как та интерференция взаимодействует с вашей сетью.

Панель мониторинга WCS CleanAir с MSE

Ранее в этом документе, Информационная панель CleanAir и как лучшие 10 источников помех на полосу не были бы отображены без MSE, была обсуждена. С MSE они теперь активны, потому что у вас есть интерференционное устройство и сведения о размещении от вклада MSE.

Рисунок 42: MSE включил информационную панель CleanAir

Верхние правые таблицы теперь заполнены с 10 самыми серьезными источниками помех, обнаруженными для каждой полосы: 802.11a/n и 802.11b/g/n.

Рисунок 43: худшая интерференция для 802.11a/n

Отображенная информация подобна тому из интерференционного отчёта из определенного AP.

- Интерференционный ID – это - запись базы данных для интерференции на MSE
- Введите – тип обнаруживаемого источника помех
- Статус – в настоящее время только отображает Активные источники помех

- Severity – степени серьезности ошибки вычислили для устройства
- Неисправные каналы – каналы, что устройство замечается влияющий Обнаруженный / последнее обновление штампы времени
- Пол – местоположение карты интерференции

При выборе местоположения пола это горячие ссылки вы к показу карты источника помех непосредственно, где много дополнительных сведений возможно.

Примечание: Существует еще одно различие вне наличия местоположения между информацией, отображенной об источниках помех по тому, что вы видите на уровне радио AP непосредственно. Вы, возможно, заметили, что нет никакого значения RSSI для интерференции. Это вызвано тем, что запись, как замечено здесь объединена. Это - результат множественных AP, сообщая об устройстве. Информация о RSSI больше не релевантна, и при этом это не было бы корректно для отображения его, потому что каждый AP видит устройство в другом уровне сигнала.

Карты WCS с размещением устройства CleanAir

Выберите ссылку в конце записи для навигации непосредственно к местоположению карты интерференционного устройства от информационной панели CleanAir.

Рисунок 44: Интерференция расположилась на карте

Теперь определение местоположения источника помех на карте позволяет нам понимать свое отношение ко всему остальному на карте. Чтобы к продукту определенная информация о самом устройстве (см. рисунок 36), передайте мышью по интерференционному значку. Заметьте AP обнаружения, это - список AP, который в настоящее время слышит это устройство. Кластерный Центр является AP, который является самым близким к устройству. Последняя линия показывает Зону Влияния. Это - радиус, что интерференционное устройство подозревалось бы в том, чтобы иметь отрицательные последствия.

Рисунок 45: интерференционная подробность от парения мыши

Зона Влияния является только половиной истории все же. Важно помнить, что устройство могло бы иметь длинную досягаемость или большую зону влияния. Однако, если степени серьезности ошибки низки, они могли бы или не могли бы иметь значения вообще. Зона влияния может быть просмотрена на карте путем выбора Interferers> Zone of Impact из меню отображения карты.

Теперь вы видите Зону влияния (ZOI) на карте. ZOI представлен как круг вокруг обнаруженного устройства, и его непрозрачность темнеет с более высоким уровнем важности. Это помогает визуализации влияния интерференционных устройств значительно. Маленький темный круг является намного больше беспокойства, чем большой полупрозрачный круг. Можно объединить эту информацию с любым другим показом карты или элементом, который вы выбираете.

Двойное нажатие (клавиши) на любом интерференционном значке берет вас к детальной регистрации для той интерференции.

Рисунок 46: запись интерференции MSE

Подробные данные источника помех включают большую информацию о типе источника помех, который обнаруживается. В верхнем правом угле поле справки, которое говорит о том, что это устройство и как этот определенный тип устройства влияет на вашу сеть.

Рисунок 47: подробная справка

Другие ссылки потока операций в детальной регистрации включают:

- Покажите Источники помех этого Типа – ссылки на фильтр для показа других экземпляров этого типа устройства
- Покажите Источники помех, влияющие на эту полосу – ссылки на фильтруемый показ всех тех же источников помех полосы
- Пол – связывается назад с местоположением карты для этого устройства
- MSE – связывает с созданием отчетов конфигурацию MSE
- Кластеризованный – связывается с контроллерами, которые выполнили начальное слияние
- Обнаружение AP – горячие ссылки на AP создания отчетов для использования в просмотре интерференции непосредственно от подробных данных AP

Интерференционная история местоположения

От окна командной строки в верхнем правом углу рекордного показа можно выбрать для просмотра истории местоположения этого интерференционного устройства.

История местоположения показывает позицию и все существенные данные, такие как время/дата и AP обнаружения интерференционного устройства. Это может быть чрезвычайно полезно в понимании, где интерференция была обнаружена и как это вело себя или повлияло на вашу сеть. Этой информацией является часть постоянной записи интерференции в базу данных MSE.

WCS – контролирует интерференцию

Содержание базы данных источника помех MSE может быть просмотрено непосредственно от WCS путем выбора Monitor> Interference.

Рисунок 48: показ Источников помех Монитора

Список сортирован статусом по умолчанию. Однако это может быть сортировано любым из содержащих столбцов. Вы могли бы заметить, что отсутствует информация о RSSI об источнике помех. Это вызвано тем, что они объединены записи. Множественные AP слышат определенный источник помех. Все они слышат его по-другому, таким образом, степени серьезности ошибки заменяют RSSI. Можно выбрать любые интерференционные ID в этом списке для отображения той же подробной записи, как был обсужден выше. Выбор типа устройства производит справочную информацию, которая содержится в записи. Выбор местоположения пола берет вас к местоположению карты интерференции.

Можно выбрать Advanced Search и сделать запрос базы данных Источников помех непосредственно, затем фильтровать результаты по множественным критериям.

Рисунок 49: усовершенствуйте интерференционный поиск

Можно выбрать все источники помех ID, Типом (включает все классификаторы), степени серьезности ошибки (диапазон), Рабочий цикл (диапазон) или местоположение (пол). Можно выбрать период времени, (Активный/Неактивный) статус, выбрать определенную полосу или даже канал. Сохраните поиск дальнейшего использования, если вам нравится.

Сводка

Существует два базовых типа информации, генерируемой компонентами CleanAir в системе: Отчеты об устройствах, создающих помехи и AirQuality. Контроллер поддерживает

базу данных AQ для всех подключенных радио и ответственен за генерацию пороговых trap-сообщений на основе настраиваемых пороговых значений пользователя. MSE управляет Отчетами об устройствах, создающих помехи и объединяет множественные отчёты, поступающие от контроллеров и AP, которые охватывают контроллеры в одиночное событие, и располагается в инфраструктуре. WCS отображает информацию собранной и обработанной другими компонентами в системе CUWN CleanAir. Отдельные информационные элементы могут быть просмотрены от отдельных компонентов как необработанные данные, и WCS используется, чтобы консолидировать и отобразить представление в масштабе всей системы и предоставить автоматизацию и рабочий поток.

Установка и проверка

Установка CleanAir является прямым процессом. Вот некоторые советы относительно того, как проверить функциональность для начальной установки. Если вы обновляете текущую систему или устанавливаете новую систему, лучший заказ операций придерживаться является кодом Контроллера, кодом WCS, то добавьте код MSE к соединению. Проверка на каждом этапе рекомендуется.

CleanAir включен на AP

Для добавления функциональности CleanAir в системе сначала необходимо включить это на контроллере через **беспроводные сети > 802.11a/b > CleanAir**.

Гарантируйте, что включают CleanAir. Это отключено по умолчанию.

После того, как включенный требуется 15 минут для распространения нормальной системы информации о Air Quality, потому что интервал создания отчетов по умолчанию составляет 15 минут. Однако вы видите результаты немедленно на уровне детализации CleanAir по радио.

Монитор > точки доступа > 802.11a/n или 802.11b/n

Это отображает все радио для данной полосы. Статус CleanAir отображен в **Административном статусе CleanAir** и **столбцах состояния CleanAir Oper**.

- Административный статус касается радио-статуса для CleanAir – должен быть включен по умолчанию
- Статус Oper касается состояния CleanAir для системы – это - то, что команда enable в меню controller упомянула выше средств управления

Если административный статус для радио отключен, рабочее состояние не может быть подключено. Предположение, что у вас есть Разрешение для Административного статуса, и для Рабочего состояния, можно выбрать, чтобы посмотреть детали CleanAir для данного радио с помощью кнопки с зависимой фиксацией, расположенной в конце строки. Выбор CleanAir для подробных данных размещает радио в Быстрый режим Обновления и предоставляет мгновенные (30-секундные) обновления Air Quality. Если вы получаете Air Quality тогда, CleanAir работает.

Вы могли бы или не могли бы видеть источники помех на этом этапе. Это зависит, если у вас есть кто-либо активный.

[CleanAir включен на WCS](#)

Как ранее упомянуто, у вас нет отчетов о Air Quality в течение максимум 15 минут, отображаясь во вкладке WCS> CleanAir после начального включения CleanAir. Однако создание отчетов Air Quality должно быть включено по умолчанию и может использоваться для проверки установки на этом этапе. Во вкладке CleanAir вам не сообщили об источниках помех в худших 802.11a/b категориях без MSE.

Можно протестировать индивидуально интерференционное trap-сообщение путем обозначения источника помех, который можно легко продемонстрировать как угроза безопасности в диалоге конфигурации CleanAir: Настройте> контроллеры> 802.11a/b> CleanAir.

Рисунок 50: конфигурация CleanAir - Аварийный сигнал защиты

Добавление источника помех для Аварийного сигнала защиты заставляет контроллер передавать сообщение прерывания на обнаружении. Это отражено во вкладке CleanAir под **Недавним** заголовком **Источников помех Угрозы безопасности**.

Без подарка MSE у вас нет функциональности для Монитора> Интерференция. Это ведет просто MSE.

[CleanAir включил установку MSE и проверку](#)

Нет ничего особенно специального о добавлении MSE к CUWN для поддержки CleanAir. После того, как добавленный, существуют некоторые определенные конфигурации, которые необходимо сделать. Гарантируйте синхронизацию и системных карт и контроллера перед включением CleanAir, отслеживающего параметры.

На консоли WCS выберите **Services>, Mobility Services> выбирает ваш MSE> Контекстно-зависимая служба> администрирование> Отслеживание Параметров**.

Выберите **Interferers** для включения интерференционного отслеживания MSE и создания отчетов. Не забудьте **сохранять**.

Рис. 5-1: MSE интерференционная конфигурация с учетом контекста

В то время как в Административном меню Контекстно-зависимых служб, также посетите Параметры Истории и включите Источники помех здесь также. Сохраните свой выбор.

Рис. 5-2: Параметры отслеживания истории с учетом контекста

Включение этих конфигураций сигнализирует синхронизируемый контроллер для начала потока информации CleanAir IDR к MSE и инициирует отслеживание MSE и процессы схождения. Возможно вытащить MSE и контроллер из синхронизации с точки зрения CleanAir. Это может произойти во время обновления кода контроллера, когда источники помех от нескольких контроллеров могли бы быть возвращены (деактивированный, и повторно активировал). Просто отключение этих конфигураций и реактивирование с сохранением вынуждают MSE повторно регистрировать со всеми синхронизируемыми WLC. Затем WLC передают новые данные к MSE, эффективно перезапуская процессы слияния и отслеживания источников помех.

Когда вы сначала добавляете MSE, необходимо синхронизировать MSE с организациями сети и WLC, для которых вы хотите для него предоставить сервисы. Синхронизация в большой степени зависит вовремя. Можно проверить синхронизацию и функции протокола

NMSP, перейдя к Сервисам> Сервисы синхронизации> Контроллеры.

Рис. 5-3: Контроллер - состояние синхронизации MSE

Вы видите синхронизирующий статус для каждого WLC, с которым вы синхронизируетесь. Особенно полезный инструмент расположен под Заголовком колонки MSE [Статус NMSP].

Выбор этого программного средства предоставляет полную информацию о состоянии протокола NMSP и может дать вам информацию о том, почему не происходит определенная синхронизация.

Рисунок 54: статус протокола NMSP

Одна из большого количества опытных общих проблем - то, что время на MSE и WLC не является тем же. Если это - условие, оно отображено на этом экране статуса. Существует два случая:

- Время WLC после времени MSE — Это синхронизируется. Но, существуют возможные ошибки при слиянии множественной информации о WLC.
- Время WLC перед временем MSE — Это не позволяет синхронизацию, потому что события еще не имели место согласно часам MSE.

Полезный прием должен использовать сервисы NTP для всех контроллеров и MSE.

Как только вам синхронизировали MSE, и CleanAir включил, должна существовать возможность для наблюдения Источников помех во вкладке CleanAir под Худшими 802.11a/b источниками помех. Можно также просмотреть их под Монитором> Интерференция, которая является прямым показом интерференционной базы данных MSE.

Один последний потенциальный глюк существует на показе Источников помех Монитора. Начальная страница фильтруется, чтобы только отобразить источники помех, которые имеют степени серьезности ошибки, больше, чем 5.

Рисунок 55: WCS - показ Источников помех Монитора

Это сообщается на начальном экране, но часто идет пропущенное при инициализации и проверке новой системы. Можно отредактировать это для отображения всех источников помех, просто заставив степени серьезности ошибки оценить 0.

Глоссарий

Существует много терминов, использованных в этом документе, которые не знакомы большому количеству пользователей. Несколько из этих сроков прибывают из Спектрального анализа, некоторые не.

- Ширина полосы разрешения (RBW), минимальный RBW — минимальная ширина полосы, которая может быть точно отображена. Карты SAgE2 (включая 3500) у всех есть минимальный RBW на 156 кГц на 20 МГц, живут, и 78 кГц на 40 МГц живут.
- Живите-А живут, период времени, получатель тратит слушание определенной частоты. Все облегченные точки доступа (LAP) делают от dwell's канала в поддержку постороннего обнаружения и метрик, собирающихся для RRM. Анализаторы спектра делают серия живет для покрытия целой полосы получателем, который только покрывает часть полосы.
- DSP — обработка цифровых сигналов

- SAgE — Механизм спектрального анализа
- Рабочий цикл — Рабочий цикл является активным на времени передатчика. Если передатчик активно использует определенную частоту, единственный способ, которым другой передатчик может использовать ту частоту, состоит в том, чтобы быть громче, чем первое, и значительно громче в этом. SNR margin необходим для понимания его.
- Быстрое преобразование Фурье (FFT) — Для заинтересованных математикой, погуглите это. По существу FFT используется, чтобы определить количество аналогового сигнала и преобразовать выходные данные от Промежутка времени до Частотной области.

Дополнительные сведения

- [Cisco Systems – техническая поддержка и документация](#)