Технология Cisco CleanAir: интеллектуальные средства в действии

В этом документе рассматриваются вопросы борьбы с радиочастотными помехами, возникающими в результате совместного интенсивного использования полосы частот. В нем описаны ограничения, присущие типовым микросхемам WiFi, и то, как эти ограничения влияют на возможности ИТ-подразделений по сбору данных о состоянии радиосреды, имеющих значение при принятии решений по эффективному устранению возникающих проблем. Кроме того, в нем представлены сведения о технологии Cisco® CleanAir и рассказано о том, как интеграция интеллектуальных средств контроля состояния радиосреды в сеть позволяет пользователям получать полное представление о действительном использовании полосы частот, выделенной для функционирования WLAN. Именно такое представление требуется для упреждающего управления сетями WiFi с целью обеспечения поддержки критически важных и чувствительных к временным задержкам приложений, используемых в современных больницах, территориально распределенных корпорациях, магазинах розничной торговли, офисах и на производственных участках.

Рост значения сетей WiFi

Первые корпоративные сети WiFi были всего лишь дополнительным удобством и использовались для доступа к Интернету в холлах или конференц-залах. Для такого применения уровень производительности, при котором характеристики передачи трафика не гарантируются, был вполне приемлем.

Сегодня технология WiFi развилась настолько, что беспроводные сети используются в качестве коммуникационной платформы многих критически важных приложений. В больницах сети WiFi используются для удаленного доступа к данным о пациентах и удаленного мониторинга второстепенных систем отслеживания состояния больных. В розничной торговле и на производстве сети WiFi используются для осуществления логистики и торговых операций. В офисах небольших филиалов начинают использовать сети WiFi в качестве единственного способа доступа к сети, постепенно отказываясь от проводных подключений. И все чаще сети WiFi используются для передачи голосовой и видеоинформации, которая очень чувствительна к воздействию помех.

Во всех приведенных выше примерах сети WiFi должны обеспечивать очень высокий уровень надежности. Неожиданные простои, возникающие в сетях WiFi из-за помех, на сегодняшний день недопустимы.

Определение решения

Средства анализа спектра (SI) поддерживают сбор данных об активности радиочастотного спектра, полученные от усовершенствованных алгоритмов обнаружения помех, аналогичных используемым в вооруженных силах. Средства SI позволяют обнаруживать все устройства, совместно использующие полосу частот: как устройства WiFi, так и источники помех, отличные от WiFi-устройств. Для каждого устройства, работающего в нелицензируемой полосе частот, средства SI могут определить тип устройства, его местоположение, а также определить, как это устройство влияет на сеть WiFi.

Управление радиосредой основано на интенсивном использовании данных, предоставляемых средствами анализа спектра, и изменении параметров сети с целью повышения производительности и снижения текущих расходов при эксплуатации сетей WiFi. Информация о серьезности и длительности помех может использоваться для определения степени их воздействия на сеть и устранения возникающих проблем. Кроме того, эту информацию можно сохранять для последующего выполнения анализа исторических данных и выявления тенденций. Контекстные данные, например, сведения о местоположении, и механизмы общесистемной корреляции превращают управление состоянием радиосреды в многосторонний упреждающий механизм, позволяющий повысить надежность, производительность и безопасность WLAN.

Хотя автономные средства SI сторонних производителей уже существуют на рынке некоторое время, реализовав средства SI непосредственно в схемотехнической базе новых точек доступа, корпорация Cisco сделала серьезный шаг вперед. Cisco CleanAir — это революционная и первая в отрасли технология, открывающая руководителям ИТ-подразделений доступ к многообразной информации о спектре, которая автоматически собирается о каждом источнике помех, не работающем по стандарту 802.11. Предоставляемые технологией CleanAir средства анализа спектра позволяют выйти на новый уровень управления радиосредой. В отличие от предыдущих средств управления радиосредой, которые могли применяться только к другим устройствам WiFi и, как правило, были отделены от беспроводной сети, новые встроенные средства управления радиосредой являются неотъемлемой частью беспроводной сети. Средства управления радиосредой второго поколения обладают полной информацией обо всех устройствах, использующих полосу частот, и способны предпринимать действия по оптимизации производительности сети путем подавления или обхода помех.

Производительность и надежность

Помимо понимания причин возникновения помех, сотрудникам ИТ-подразделений необходимо, чтобы сеть по возможности автоматически разрешала возникающие проблемы, что позволит снизить текущие расходы (OpEx) и свести к минимуму простои сети. Такой тип автоматизированной настройки относится к области управления радиоресурсами (RRM), являющейся слоем программного обеспечения в инфраструктуре, который автоматически настраивает параметры сети для поддержания должного уровня производительности. Более ранние поколения средств RRM не уделяли должного внимания вопросам борьбы с помехами, за исключением некоторых сведений об имеющемся "шуме". Новое поколение средств RRM совместно со встроенными средствами SI обладает полной информацией об источниках помех, что позволяет принимать действительно продуманные решения и достигать новых высот надежности.

Встроенные средства анализа спектра можно использовать не только для автоматизированного управления радиоресурсами, но и для решения более широкого круга задач по управлению радиосредой в масштабах системы. Руководителям, ответственным за функционирование сетей WiFi, эти задачи могут показаться новыми, но руководителям, ответственным за функционирование проводных сетей, они давно знакомы:

- разрешение проблем производительности в режиме реального времени;
- проведение технической экспертизы периодически возникающих проблем или проблем, имевших место в прошлом;
- создание отчетов по использованию спектра и тенденциям к возникновению помех;
- сопоставление проблем, вызванных помехами между несколькими точками доступа, как для определения степени воздействия на работу сети, так и для снижения количества лишних сигналов о потенциальной опасности.

Безопасность беспроводных сетей

Задачей сети WiFi прежде всего является не только предоставление должного уровня производительности, но и обеспечение соответствующей степени безопасности. Очень много внимания в отрасли уделяется тому, чтобы понять, как точки доступа злоумышленника могут послужить точками проникновения в корпоративную сеть. Для этих целей были созданы системы обнаружения и предотвращения вторжений в беспроводные сети (wIDS/wIPS). Однако существующие решения IDS и IPS обладают рядом существенных недостатков, которые нельзя устранить без использования дополнительных средств анализа спектра.

Существующие системы IDS/IPS не могут обнаруживать точки доступа, работающие с проприетарными расширениями наподобие Super G (от Atheros). В результате эти легкодоступные устройства остаются незамеченными. Кроме того, злоумышленник может взять стандартное оборудование WiFi (например, ПК под управлением Linux) и изменить его так, чтобы оно работало на нестандартных каналах или с другими нестандартными схемами модуляции. Обнаружение этих расширенных или модифицированных устройств возможно только при анализе физического уровня радиосреды.

Помимо устройств WiFi для нарушения безопасности сети можно использовать и многие другие типы оборудования, отличные от WiFi-устройств, включая точки доступа Bluetooth, точки доступа, работающие по старым стандартам, например, 802.11FH, и беспроводные мосты, функционирующие в соответствии с проприетарными протоколами. Например, мосты могут отправлять данные злоумышленнику, находящемуся в нескольких милях от вашего здания. И в этом случае обнаружение этих типов устройств возможно только при анализе излучения всех устройств, обнаруженного в эфире.

Помимо угрозы, исходящей от устройств злоумышленников, всегда существует опасность, что злоумышленник попытается остановить работу вашей сети WiFi с помощью радиочастотной атаки типа "отказ в обслуживании" (DoS). Хотя системы IDS/IPS отслеживают многие атаки DoS "протокольного уровня", они не обнаруживают атаки DoS радиочастотного уровня, которые можно осуществить с помощью устройств подавления беспроводной сети или устройств беспроводной сети, использующихся в диагностическом режиме подавления.

Помимо преднамеренных атак, некоторые простые устройства, например, беспроводные видеокамеры или аналоговые беспроводные телефоны могут случайно подавить беспроводную сеть. Встроенные средства анализа спектра и средства управления радиосредой очень эффективны в обнаружении угроз безопасности типа "отказ в обслуживании" на радиочастотном уровне.

Интеграция средств управления радиосредой

Ограничения стандартного оборудования WiFi

На базовом уровне стандартный набор микросхем WiFi имеет весьма ограниченные возможности для интеграции средств SI. Это объясняется тем, что наборы микросхем WiFi главным образом проектировались только для получения сигналов WiFi. Они не распознают другие типы сигналов (за исключением радара DFS). Стандартные наборы микросхем не могут даже передавать достаточно информации для средств SI, работающих на более высоких уровнях программного обеспечения.

Точнее говоря, когда набор микросхем WiFi замечает передаваемый кадр, который не может распознать, он, как правило, может сообщить только ограниченные данные: 1) получен непонятный кадр, 2) уровень мощности кадра и 3) время начала и окончания кадра. Обратите внимание, что этот кадр может исходить от устройства WiFi, работающего на другом канале или на том же самом канале, но расположенном слишком далеко, что мешает его надлежащему приему. Или же кадр может исходить от источника, отличного от WiFi-устройства. Как правило, более подробная информация о типе модуляции кадра, о его месте в рамках канала и другие данные недоступны. Кроме того, у программного обеспечения нет доступа к актуальным данным, полученным вместе с кадром, для проведения дальнейшего анализа.

Несмотря на все эти ограничения, микросхему WiFi можно использовать для подсчета количества неопознанных кадров и для вычисления общего объема помех, а также средней интенсивности помех. К сожалению, такой подход не предоставляет всей информации, необходимой для реального разрешения проблем. При таком подходе "совокупных помех" невозможно узнать конкретный тип помехи (например, является ли она соканальной помехой WiFi или другим типом помехи), а также определить, исходит ли помеха от одного источника или от нескольких, где расположен источник помехи и т.п. Отсюда следует, что объем данных SI, которые можно собрать с помощью стандартного набора микросхем WiFi, весьма ограничен.

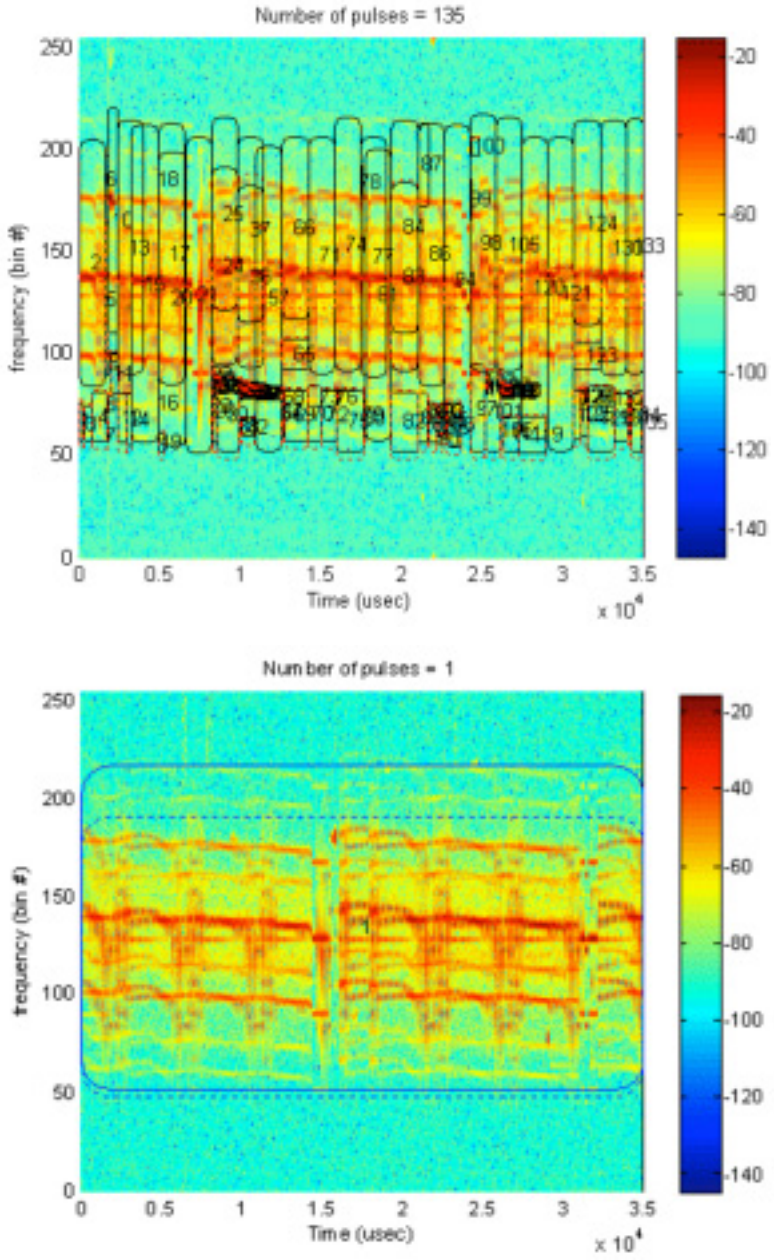
Технология Cisco CleanAir: специализированное аппаратно-программное решение

Чтобы обойти ограничения видимости, характерные для стандартных наборов микросхем WiFi, Cisco создала встроенное решение с запатентованными чипами и программным обеспечением, которые были специально спроектированы для анализа и классификации всего радиочастотного взаимодействия. (На сегодняшний день на данную технологию получено более 25 патентов.) По существу, Cisco взяла технологию, лежащую в основе средства анализа Cisco Spectrum Expert, и встроила ее непосредственно в инфраструктуру, включая глубокую интеграцию в рамках микросхемы WiFi. Это серьезная разработка. Она демонстрирует то, что беспроводные сети для корпораций уже давно перешли из разряда желательного дополнения в разряд насущной необходимости. Компаниям уже давно недостаточно возможностей, предоставляемых оборудованием WiFi потребительского уровня.

Собственное решение Cisco начинается с аппаратного ядра Cisco Spectrum Analysis Engine (SAgE), которое непосредственно встроено в микросхему WiFi новых точек доступа Cisco Aironet® серии 3500. Ядро SAgE выполняет операции, требующие большой вычислительной мощности, например, быстрое преобразования Фурье (FFT) с высокой точностью и операции по обнаружению импульсов. (Импульс — это выброс радиочастотной энергии по частоте и во времени.) По сути, ядро SAgE выполняет базовые операции по анализу спектра, требующие настолько интенсивных вычислений, что их выполнение может быть недопустимо в программном обеспечении реального времени.

На рисунке 1 графически показано определение импульсов энергии с помощью SAgE. На первом рисунке отображены данные, поступающие от аппаратного блока обнаружения импульсов. На втором рисунке — данные, полученные после того, как программное обеспечение объединило импульсы, совпадающие настолько, что их можно рассматривать как один импульс.

Рис. 1 Обнаруженные импульсы радиочастотной энергии до и после фильтрации



После завершения обработки SAgE образцы интересующих радиоимпульсов передаются на уровень программного обеспечения для дальнейшего детального анализа. Выполнение такой обработки на основном радиопроцессоре негативно повлияло бы на производительность сети WiFi. Чтобы исключить такое влияние, аппаратное решение Cisco содержит собственное ядро обработки под названием DSP Vector Accelerator (DAvE), непосредственно встроенное в микросхему WiFi точки доступа. Ядро DAvE может выполнять вычисления высокой интенсивности, связанные с обработкой сигналов, называемые "Davelets" (например такие, как фильтрация, прореживание, развертка, обнаружение синхропоследовательностей и обнаружение модуляции), не задействуя ЦП. DAvE производит интенсивные вычисления, связанные с обработкой сигналов, которые в противном случае выполнялись бы основным ЦП.

Конечная стадия обработки происходит в модуле программного обеспечения, который работает на ЦП и называется "Sensord". Учтите, что нагрузка на ЦП существенно снижена, поскольку самая тяжелая часть обработки выполняется аппаратными блоками SAgE и DAvE. Программное обеспечение Sensord учитывает время и частоту кадров помех, а также выявленные параметры кадров, например такие, как тип модуляции и обнаруженные синхропоследовательности. Затем эта высокоуровневая информация используется для проведения итоговой идентификации и отделения одного устройства от другого. На этой стадии заключительной классификации предоставляется вся многосторонняя функциональность средств SI: вы получаете информацию о конкретном источнике помех, его местонахождении и о том, как его можно обойти.

Вопросы производительности при внедрении средств SI

Количество классификаторов
Технология CleanAir поддерживает набор из 20 классификаторов источников помех, отличных от устройств WiFi. Поскольку анализ происходит на уровне программного обеспечения, то по мере появления на рынке новых источников помех список классификаторов можно свободно расширять. Другими словами, с помощью лежащего в основе аппаратного решения можно определить помеху любого типа, даже ту, которая, возможно, появится в будущем. Для этого всего лишь потребуется обновить программное обеспечение.

Одновременное определение
Система классификации технологии CleanAir позволяет различать несколько одновременно работающих источников помех как одного и того же типа, так и разных типов. Более того, с помощью технологии CleanAir один радиомодуль может обнаруживать до 10 одновременно работающих устройств, создающих помехи. Это имеет большое значение, поскольку в реальных условиях работы количество одновременно работающих радиочастотных устройств может быть достаточно велико. Любые конкурирующие решения не такого высокого уровня и не способные различать одновременно работающие устройства в реальных условиях эксплуатации быстро потеряют свою эффективность и будут годны только для демонстрационных целей и лабораторных испытаний.

Время на определение
Работа устройств, создающих помехи, может быть кратковременной и непостоянной. Это обуславливается либо тем, что их быстро включают и выключают, либо тем, что их пользователь перемещается. В связи с этим классификация этих источников должна происходить быстро, пока не потерян сигнал от источника. Технология CleanAir позволяет точкам доступа классифицировать устройства за 30 секунд, а чаще всего классификация выполняется менее чем за 5 секунд. (Обратите внимание, что информирование о помехах может происходить с небольшой задержкой, поскольку необходимо собрать данные от нескольких точек доступа.)

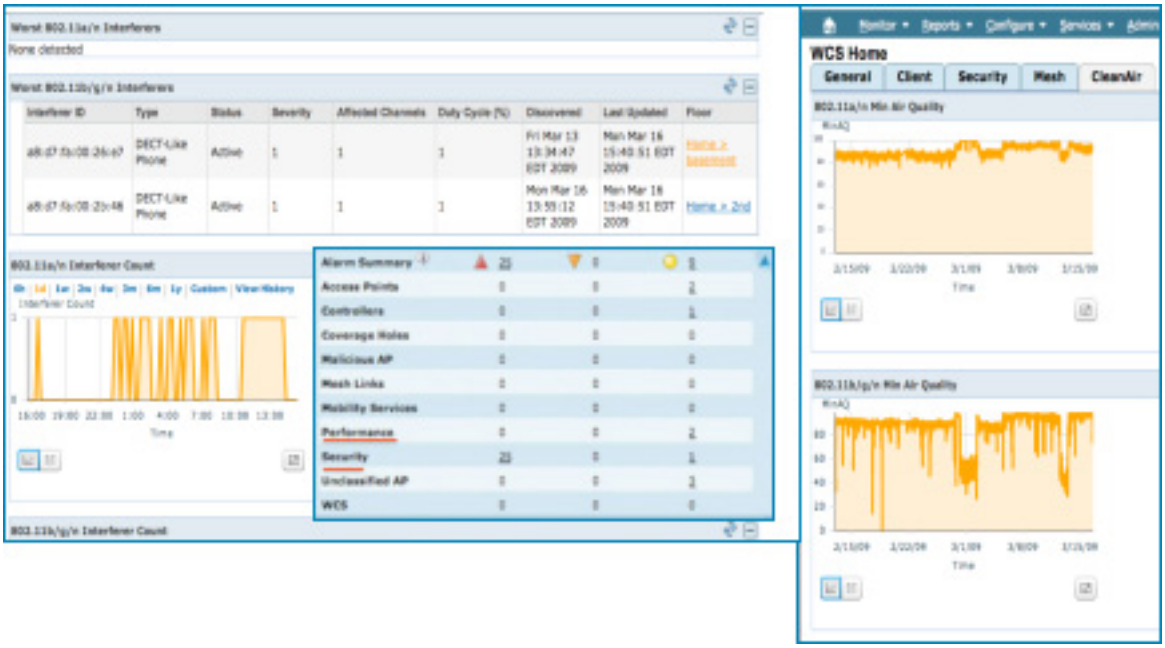
Вероятность ложных срабатываний
Очень важно определить источник помех, но не менее важно не сообщать о "мнимых", не существующих в действительности помехах или о неправильно идентифицированных помехах, что вынуждает сотрудников ИТ-подразделений тратить время на поиск устройств не того типа. Технология CleanAir обеспечивает низкий уровень ложных срабатываний даже в сильно загруженных радиочастотных средах, в которых одновременно работают сотни WiFi-устройств и устройств, отличных от WiFi. Снижая количество ложных срабатываний, технология CleanAir позволяет экономить время сотрудников ИТ-подразделений.

Технология CleanAir: значимость встроенных средств анализа спектра и управления радиосредой

В то время как продукт Spectrum Expert и решения на базе его инструментария играют важную роль в первую очередь при развертывании сети, интеграция технологии SI в инфраструктуру сети WiFi предоставляет гораздо более привлекательные преимущества. Во встроенном решении CleanAir ядро SI непосредственно встроено в точки доступа, а информация SI, в свою очередь, полностью интегрирована в сетевую архитектуру и системы управления, что позволяет осуществлять управление спектром на основе анализа.

Одно из преимуществ технологии CleanAir состоит в том, что она работает ежедневно и круглосуточно, постоянно отслеживая появление помех и проблем с качеством беспроводной связи (см. рис. 2). Это позволяет сотрудникам ИТ-подразделений применять профилактический подход к управлению спектром. Вместо того чтобы ждать получения информации о помехе от конечного пользователя (в виде заявки на устранение технической неисправности) и дальнейшего применения средства для анализа возникшей проблемы, сотрудники ИТ-подразделений могут находить помехи сразу же после их возникновения и незамедлительно предпринимать корректирующие действия. Кроме того, наличие хронологических данных, собираемых ежедневно и круглосуточно, позволяет проводить ретроспективный анализ. С помощью хронологических данных можно без особых проблем проводить анализ тенденций с течением времени.

Рис. 2 Наблюдение за устройствами, создающими помехи, тенденции качества беспроводной связи и уведомления в системе управления Cisco WCS



Возможность сопоставлять обнаруженные устройства по точкам доступа

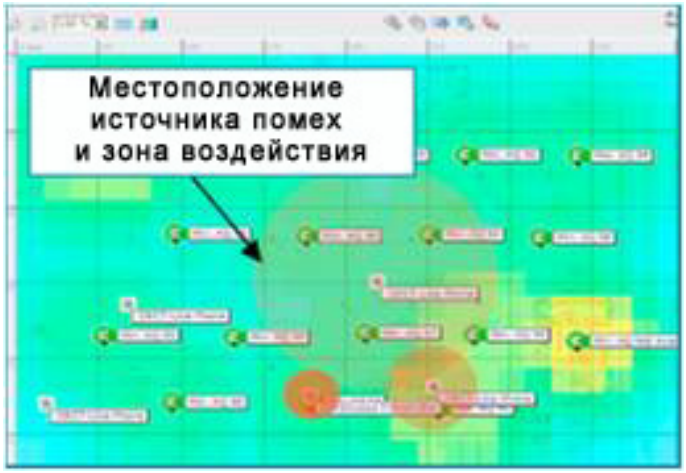
Во WLAN со встроенными средствами управления радиосредой существует вероятность обнаружения одного и того же создающего помехи устройства несколькими точками доступа. Если информация о каждом из этих устройств будет поступать отдельно, то администратор будет получать слишком много предупреждений. В рамках технологии CleanAir каждому обнаруживаемому точкой доступа устройству присваивается псевдо-MAC-адрес (PMAC), основанный на параметрах устройства. Затем эти адреса PMAC сравниваются с адресами PMAC, обнаруженными другими точками доступа. Если адреса PMAC двух устройств совпадают (и точки доступа находятся относительно недалеко друг от друга), то сведения, поступающие из этих двух точек доступа, группируются в один отчет. Потом этот сводный отчет отправляется администратору как информация об одном устройстве.

Кроме того, группировка играет существенную роль в определении местонахождения устройств. Пакет совпадающих адресов PMAC предоставляет системе несколько измерений мощности одного и того же устройства, что позволяет позднее произвести триангуляцию местонахождения данного устройства. Важными характеристиками группировки устройств являются возможность сети должным образом группировать устройства без избыточного объединения в группы (объединение устройств, которые не нужно объединять) или недостаточного объединения в группы (информирование о нескольких устройствах, являющихся на самом деле одним устройством).

Еще одно преимущество технологии CleanAir состоит в том, что она может работать удаленно. Во многих сетях WiFi сотрудники ИТ-подразделений, находящиеся в одном месте, управляют оборудованием, расположенным в нескольких зданиях одного комплекса или в различных географических точках. Поэтому физически перенести инструментарий в эти удаленные точки может быть не так просто. Особенно это касается сетей, развернутых для компаний с обширной сетью филиалов или же в случаях прерывистой работы источника помех. Благодаря встроенным в инфраструктуру средствам управления радиосредой сотрудники ИТ-подразделений могут удаленно получать информацию об условиях возникновения помех в любом месте сети.

Кроме того, технология Cisco CleanAir позволяет определять физическое местоположение устройств, являющихся источником помехи (рис. 3). В большинстве случаев одно и то же устройство, вызывающее помехи, будет обнаружено несколькими точками доступа. Корпорация Cisco разработала современную технологию для сравнения устройств, информация о которых получена из нескольких точек доступа, и определения тех данных, которые относятся к одному и тому же устройству. После сопоставления устройств можно определить точное местоположение устройства с помощью методов триангуляции, аналогичных методам, используемым инфраструктурными системами для обнаружения клиентов и меток WiFi.

Рис. 3 Определение местоположения создающих помехи устройств и зоны их воздействия



Возможно, самое большое преимущество, получаемое от интеграции технологии CleanAir в WLAN, состоит в том, что данные SI становятся доступными системе управления радиоресурсами точек доступа, где они могут использоваться для реализации автоматизированного подавления помех ежедневно и круглосуточно. Это совершенно новое поколение систем управления радиоресурсами, обеспечивающее гораздо большую степень надежности, нежели предыдущие версии, которые были неспособны обнаруживать помехи. Благодаря технологии CleanAir появилась возможность настраивать в сети автоматический обход помех многих типов.

Функциональные возможности унифицированной беспроводной сети Cisco с технологией CleanAir

Качество беспроводной связи и уведомления о производительности

Технология Cisco CleanAir предоставляет большой объем подробной информации о помехах. Для получения основных сведений о степени воздействия помех на сеть, технология Cisco CleanAir представляет всю подробную информацию как один обобщенный и простой для понимания показатель, называемый качеством беспроводной связи (AQ). AQ вычисляется для различных уровней: уровня канала, помещения и системы. Также поддерживаются уведомления AQ, благодаря которым происходит автоматическое информирование о падении AQ ниже требуемого порогового значения.

Визуализация с помощью карт

В сетях WLAN с технологией CleanAir анализируемые и обнаруживаемые устройства визуализируются на картах, предоставляемыми системой управления Cisco WCS и ядром сервисов мобильности Cisco. Помимо возможности видеть на карте точки доступа и клиентов, вы можете отслеживать, существуют ли на этой же карте создающие помехи устройства. В отношении производительности труда возможность видеть на карте создающие помехи устройства (а также зону их воздействия) позволяет вам определять, какие точки доступа, клиенты и зоны вашего помещения затронуты помехами.

С точки зрения обеспечения безопасности отслеживание устройств на карте позволяет незамедлительно информировать о том, в какую точку необходимо направить сотрудников отдела безопасности.

Уведомления безопасности

Помимо отображения на карте всех устройств, влияющих на безопасность сети, можно настроить выдачу уведомлений для определенного места, например, для конкретного этажа вашего здания. Это очень полезная функция, поскольку некоторые устройства могут представлять угрозу для сети в одних частях здания (например, в зоне проведения торгов) и не представлять ее в других (например, в вестибюле).

Возможности подавления помех

Кроме гибкого развертывания, технология CleanAir предоставляет улучшенную систему реагирования на помехи. В состав этой автоматизированной системы реагирования на помехи входят методы исключения постоянно присутствующих устройств и методы управления радиочастотным ресурсом в зависимости от состояния окружающей сигнально-помеховой обстановки.

Методы исключения постоянно присутствующих устройств определяют степень стабильности местоположения и частоты таких устройств (например, микроволновых печей и беспроводных видеокамер). В связи с этим, даже если такие устройства не обнаруживаются в данный момент на конкретном канале и в конкретном месте, известно, что, вероятнее всего, они снова появятся на том месте, где они были обнаружены ранее. Система отслеживает устройства этих типов и при осуществлении выбора каналов старается избегать каналов в тех местах, где были обнаружены постоянно присутствующие устройства.

Методы управления радиочастотным ресурсом в зависимости от состояния окружающей сигнально-помеховой обстановки опознают некоторые состояния как неблагоприятные и губительные по своей природе. Например, беспроводной телефон с непрерывным сигналом FM может привести к перебою в работе сети до нескольких минут (пока работает телефон). Поэтому существенное снижение качества беспроводной связи заставляет систему незамедлительно осуществлять смену канала для точки доступа, находящейся под воздействием помех. Обратите внимание, что смена канала происходит только для затронутой помехами точки доступа, при этом каскадных изменений в плане каналов соседних точек доступа не происходит.

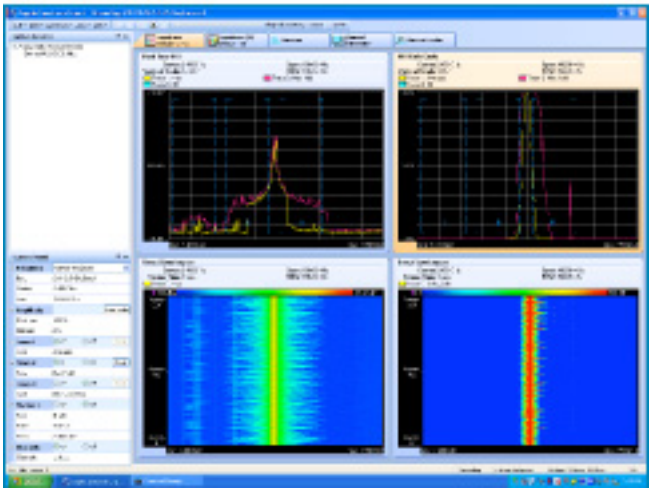
Несмотря на то, что во многих случаях самая лучшая реакция на возникшие помехи — это перемещение, удаление, замена или экранирование создающего помехи устройства вручную, тем не менее, весьма полезно иметь возможность автоматического подавления помех, чтобы временно, пока не будут предприняты другие действия, поддержать производительность сети на должном уровне. В некоторых случаях невозможно удалить источник помех, например, если он находится снаружи здания.

Точки доступа в качестве анализаторов

Наконец, технология CleanAir продолжает предоставлять экспертный взгляд на графики низкоуровневого спектра, сопоставляемые с графиками, предлагаемыми аналитическим средством Spectrum Expert. Любая точка доступа CleanAir может быть настроена как подключенный к сети сенсор, чтобы иметь возможность просмотра графиков спектра непосредственно по мере их получения радиомодулями точки доступа.

Хотя система действительно предоставляет массу высокоуровневых данных для анализа, включая сведения о классификации устройств и качестве беспроводной связи, всегда будут возникать случаи, когда потребуется взглянуть на сами низкоуровневые данные о спектре в режиме реального времени. Даже для тех предприятий, в штате которых нет соответствующего специалиста, функциональность Spectrum Expert Connect, показанная на рисунке 4, может быть использована внешним экспертом, помогающим в разрешении какой-либо труднодиагностируемой проблемы.

Рис. 4 Использование функциональности Spectrum Expert Connect для диагностики проблемы в точке доступа



Выводы

Поскольку сеть WiFi работает в совместно используемой нелицензируемой полосе частот, то встроенные средства анализа спектра и управления радиосредой представляют собой обязательный инструментарий, позволяющий обеспечить высокий уровень производительности, безопасности и надежности в сети WiFi. Управление радиосредой имеет критически высокое значения для предоставления конечным пользователям возможности мобильной работы с критически важными для деятельности компании приложениями по беспроводной сети.

Поскольку имеющихся у коммерческих микросхем WiFi ограниченных возможностей по отображению состояния радиоэфира недостаточно, то корпорация Cisco интегрировала запатентованное аппаратное и программное обеспечение для обработки спектра, специально разработанное для проведения анализа помех, и выпустила набор микросхем для создания беспроводных сетей корпоративного класса. Благодаря лежащим в основе возможностям аппаратного уровня технология Cisco CleanAir классифицирует и определяет местоположение отдельных источников помех и информирует о том, как они влияют на производительность и безопасность сети.

Хотя SI можно получить в виде такого набора средств, как Spectrum Expert, который оказывается весьма полезным на стадии предварительного развертывания, однако оптимальнее иметь технологию SI, встроенную непосредственно в инфраструктуру. Технология Cisco CleanAir предоставляет такую многостороннюю функциональность для управления радиосредой, как ежедневный круглосуточный профилактический мониторинг помех, уведомления о снижении качества радиосреды и снижении производительности, удаленное управление и обнаружение создающих помехи устройств. Но что наиболее важно, встроенная технология SI позволяет выйти на новый уровень автоматизированного управления спектром, который может распознавать и снижать влияние помех, основываясь на аналитической информации.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Отпечатано в США C11-599260-00 04/10